N°64

Casser les codes et décrypter l'info

PIRATE INFORMATIQUE

Juin / Août 2025

GUIDE 2025

TOP 5 VPN GRATUITS

MOTS DE PASSE

QUANTIQUE + IA = CRAQUAGE INSTANTANÉ

PASSW***

Le GUIDE ULTIME du

HACKER

Les vraies SOLUTIONS GRATUITES

STREAMING

TOP 7 ALTERNATIVES gratuites à SPOTIFY

CRYPTOMATOR

PROTÉGEZ VOS DOSSIERS SENSIBLES SUR PC & DANS LE CLOUD

BLACK DOSSIER

I2P ACCÉDEZ AU RÉSEAU CACHÉ & ANONYME

SOMMAIRE

BLACK DOSSIER 11–21

I2P ACCÉDEZ AU RÉSEAU CACHÉ & ANONYME

HACKING

ANONYMAT

SOUTENEZ-NOUS !

Vous découvrez ce magazine en l'ayant téléchargé illégalement ? C'est de bonne guerre, nous sommes pour le partage ! Merci de l'intérêt que vous portez à nos articles, mais pour que nous puissions continuer l'aventure, pensez à acheter le magazine : offrez-le, parlez-en autour de vous ! *Pirate Informatique* existe depuis plus de 10 ans, sans publicité et sans hausse de prix !

PROTECTION

MULTIMÉDIA

PIRATE INFORMATIQUE
N°64

Juin - Août 2025

Une publication du groupe ID PRESSE
1104, Chemin de la Batterie
13500 Martigues

Directeur de la publication :
David Côme

Directeur artistique :
Sergei Afanasiuk

Service Abonnement :
Indiquez la référence *Pirate Informatique* dans vos échanges
Tél. : 03 44 51 97 21
Email : abonnement.bii@gmail.com

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

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : en cours

ISSN : 1969 - 8631

«Pirate Informatique» est édité par SARL ID Presse, RCS Aix-En-Provence 491 497 665

Parution : 4 numéros par an.

ÉDITO

IA & POST-QUANTIQUE : LE CRÉPUSCULE DE L'ANONYMAT ?

Nous assistons à un basculement aussi silencieux qu'irréversible : le possible effondrement numérique de l'anonymat. Les experts l'anticipent, les GAFAM l'espèrent. La combinaison des IA génératives et des futures machines quantiques dessine un monde où aucune donnée n'est réellement protégée, où chaque identité peut être reconstruite, déduite, désanonymisée.
Une rétro-ingénierie de la vie privée s'annonce.

Le moindre échange, la moindre habitude, le plus anodin des like devient une pièce de puzzle pour des IA entraînées à profiler à l'échelle planétaire. Et demain, les calculateurs post-quantiques viendront peut-être balayer d'un revers d'algorithme les forteresses cryptographiques qui abritent encore nos derniers jardins secrets.

Bonne lecture !
La rédaction

CONSOLES DE JEU

NINTENDO DURCIT LE TON FACE AUX SWITCH MODIFIÉES : VERS UN BLOCAGE TOTAL ?

Depuis 2017, la Nintendo Switch est devenue l'une des consoles les plus piratées de sa génération. La faute à une faille matérielle critique présente dans les premières versions de la console. Cette brèche permettait le lancement de payloads non signés, ouvrant la voie à des systèmes alternatifs comme Atmosphère ou Hekate. Grâce à eux, certains installaient des thèmes personnalisés, des émulateurs, ou des homebrews. D'autres en profitaient pour charger illégalement des jeux commerciaux.

Nintendo n'est pas resté les bras croisés. La firme avait déjà mis en place des mécanismes de bannissement en ligne : une Switch modifiée pouvait être exclue des services réseau, empêchant jeu en ligne, eShop ou sauvegarde cloud. Mais le 8 mai 2025, la firme est allée plus loin en modifiant ses conditions générales d'utilisation (CGU) américaines : elle se réserve désormais le droit de désactiver totalement une console, même hors ligne, en cas de modification non autorisée. En clair, si Nintendo estime que vous avez modifié un composant matériel ou logiciel de sa console, la société pourrait rendre votre Switch inutilisable sans préavis !

Une évolution majeure qui transforme l'appareil acheté en simple licence conditionnelle. En Europe, cette mesure pourrait heurter le droit des consommateurs. Mais Nintendo affiche clairement sa cible : prévenir toute vague de hacks sur la Switch 2, officiellement lancée depuis juin.

SURVEILLANCE DE MASSE

SOCIALNET AIDE L'ADMINISTRATION AMÉRICAINE À CIBLER « LES COMMUNAUTÉS MARGINALISÉES ET LES MILITANTS »

ShadowDragon, entreprise américaine fondée en 2016 par Daniel Clemens, est au cœur d'une controverse sur la surveillance numérique outre-Atlantique. Son outil phare, SocialNet, collecte des données publiques de plus de 200 sites majeurs, tels que Facebook, TikTok, Tinder ou Duolingo, pour établir des profils détaillés sans le consentement des utilisateurs. Selon la Fondation Mozilla, ces données seraient utilisées par des agences gouvernementales comme l'ICE (Immigration and Customs Enforcement), qui est l'agence américaine de l'immigration et des douanes. Mozilla explique que le croisement des données collectées permet de déterminer l'identité, la localisation et les déplacements, le statut, les croyances et les réseaux d'un utilisateur. Les critiques soulignent que, bien que les données collectées soient techniquement publiques, leur agrégation et analyse à grande échelle posent des problèmes éthiques et juridiques, notamment en matière de vie privée et de libertés individuelles. Des organisations telles que l'Electronic Frontier Foundation et l'American Civil Liberties Union mettent en garde contre les risques d'une telle surveillance, « *notamment pour les communautés marginalisées et les militants* ».

EUROPOL

DDOS À LA DEMANDE : 6 PLATEFORMES DÉMANTELÉES

Europol a annoncé en mai dernier le démantèlement de six services majeurs de DDoS-for-hire, ces plateformes clandestines qui vendent des attaques informatiques sur commande. L'opération, baptisée PowerOFF, a permis la saisie de serveurs, de domaines, et l'arrestation de plusieurs administrateurs à travers l'Europe et l'Amérique du Nord.

Ces services illégaux — parfois accessibles pour quelques euros — permettaient à n'importe quel internaute malintentionné de lancer des attaques de type déni de service distribué (DDoS) contre des sites web, des services en ligne ou des infrastructures critiques.

Ces attaques, qui saturent les serveurs ciblés de requêtes jusqu'à les rendre inaccessibles, sont devenues une arme numérique courante, aussi bien dans les guerres économiques que dans le cyberactivisme ou le simple vandalisme.

Selon Europol, certains de ces sites revendiquaient plus de 10 000 clients et des millions d'attaques orchestrées en quelques années. En collaboration avec le FBI, la NCA britannique et plusieurs fournisseurs d'hébergement, l'opération PowerOFF marque une étape stratégique : elle vise à éradiquer l'offre à la source, plutôt que de courir après les attaques une par une.

AUSTRALIE

Salariés sous contrôle : chaque clic est surveillé

Une enquête parlementaire explosive vient de dévoiler l'ampleur d'une pratique inquiétante en Australie : la surveillance généralisée des salariés par leur employeur. Détection des frappes clavier, captures d'écran automatiques, analyse de la voix, reconnaissance faciale, enregistrements sonores... Dans de nombreuses entreprises, ces technologies sont utilisées sans encadrement clair, parfois à l'insu des employés.

Les outils intrusifs se banalisent, souvent sous couvert de productivité ou de cybersécurité. Mais les syndicats et chercheurs en éthique numérique tirent la sonnette d'alarme : il devient urgent de réguler. Le rapport parlementaire préconise l'adoption d'une loi nationale sur la protection de la vie privée au travail, inspirée du RGPD européen, afin de rééquilibrer le rapport de force entre employeurs et salariés.

La sénatrice indépendante Barbara Pocock résume la situation : « *Quand un logiciel enregistre chaque clic, chaque mot, chaque minute d'inactivité, on ne parle plus de supervision mais de contrôle total* ». En Australie, où aucune loi fédérale ne limite formellement la surveillance des employés, cette initiative pourrait ouvrir un débat crucial sur les libertés numériques en milieu professionnel.

En Bref...

BLOCAGE MASSIF DE SITES PIRATES EN FRANCE

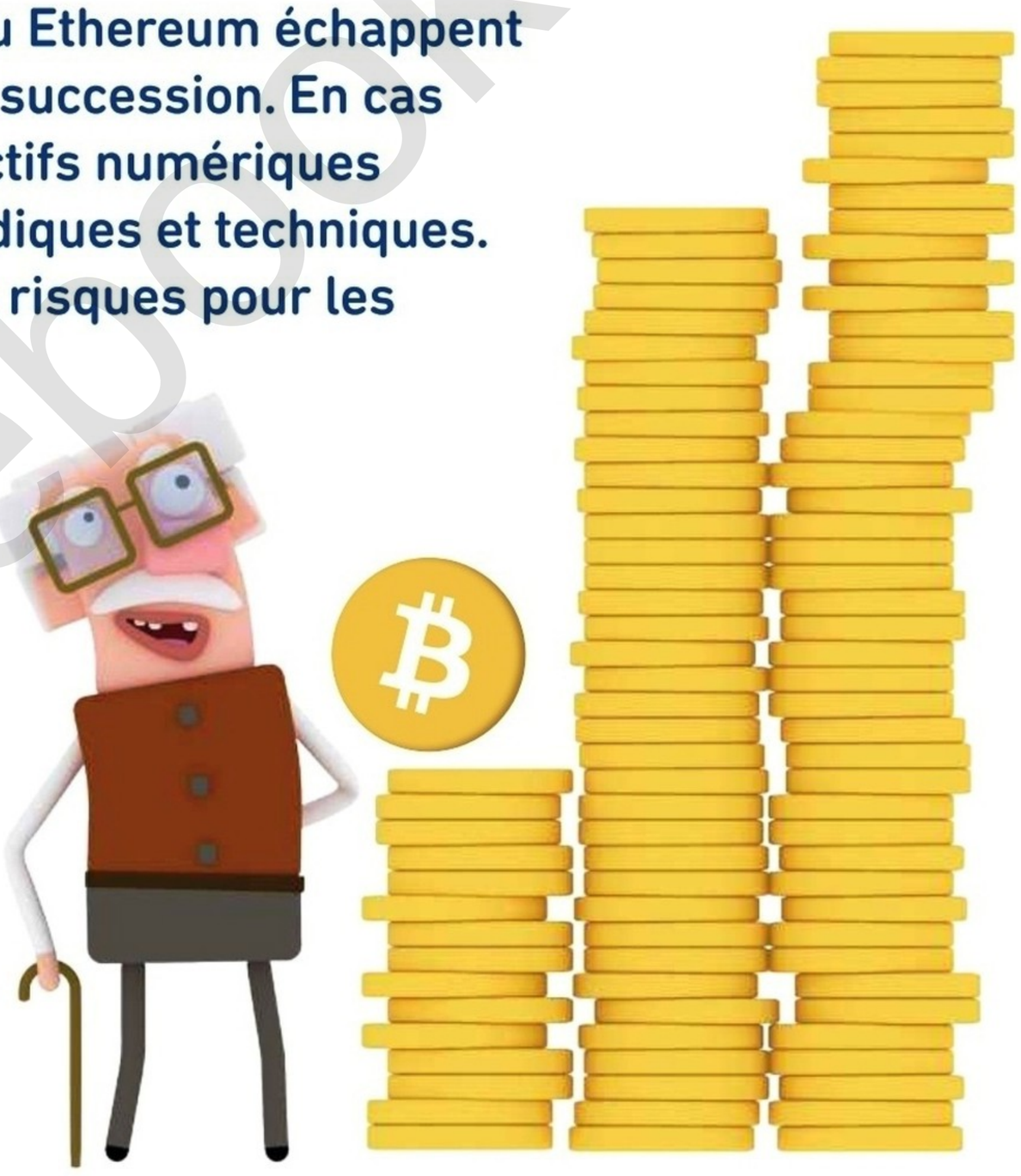
La guerre contre le streaming et le téléchargement illégal se poursuit en France. En avril dernier, à la demande d'ayants droit audiovisuels, le tribunal judiciaire de Paris a ordonné le blocage de 60 sites dont Monstream, Torrent9 et Cpasbien. Une course-poursuite sans fin dont l'efficacité à long terme n'a jamais été prouvée.

OPENDNS BLOQUÉ EN BELGIQUE : UN SCANDALE

La justice belge a ordonné le blocage d'OpenDNS, service DNS public utilisé notamment pour contourner les restrictions géographiques. Motif : la lutte contre le piratage de matchs sportifs. La Belgique franchit un cap inquiétant en matière de liberté d'accès au réseau, au risque de créer un dangereux précédent.

QUE DEVIENNENT LES CRYPTOACTIFS EN CAS DE DÉCÈS ?

Les cryptoactifs comme Bitcoin ou Ethereum échappent souvent aux règles classiques de succession. En cas de décès de leur détenteur, ces actifs numériques posent de sérieux problèmes juridiques et techniques. Comment les transmettre ? Quels risques pour les héritiers ? Et surtout, comment anticiper ?



Contrairement à un compte bancaire ou à un livret d'épargne, les cryptoactifs ne sont pas détenus dans une banque identifiable par un notaire ou par l'administration fiscale. Ils sont souvent stockés dans des portefeuilles numériques (wallets) protégés par des phrases de récupération (seed phrase) ou des clés privées, seuls moyens d'y accéder. En cas de décès, les plateformes d'échange – prestataire de services sur actifs numériques (PSAN) ou prestataire de services sur cryptoactifs (PSCA) – ne sont pas davantage informées ni tenues de rechercher les héritiers.

LE RÔLE DU NOTAIRE ET LE TESTAMENT MYSTIQUE

Le notaire joue un rôle crucial dans la transmission des actifs numériques, notamment à travers le testament mystique. Ce dernier est un document écrit par le testateur, signé, puis placé dans une enveloppe scellée. Il est remis en main propre à un notaire en présence de deux témoins. Ni le notaire ni les témoins ne connaissent le contenu du testament. Le contenu reste secret jusqu'à l'ouverture de la succession, une mesure de sécurité indispensable : n'oubliez jamais que le propriétaire de cryptos est celui qui possède les codes d'accès à leur stockage ! Un vol opportuniste est possible. Avec un testament mystique, les informations sensibles, telles que les clés privées ou les phrases de récupération, peuvent y être incluses sans risque de divulgation prématurée.

D'un point de vue légal, les cryptoactifs sont pourtant considérés en France comme des biens numériques, qui peuvent sans problème être intégrés à la succession au même titre qu'un compte-titres ou une œuvre d'art. Mais leur localisation décentralisée (sur une blockchain mondiale) et leur anonymat partiel compliquent le travail des notaires.

LES CRYPTOS, ANGLE MORT D'UNE SUCCESSION

Ces derniers n'ont actuellement aucun moyen de connaître l'existence de ces cryptoactifs… sauf si le défunt a pris ses dispositions en amont. Et même si des proches alertent le notaire, il ne suffit pas de savoir qu'un compte existe pour récupérer son contenu !
Sans clé privée, phrase de récupération, mot de passe de portefeuille ou identifiant d'une plateforme d'échange (comme Binance, Coinbase, Kraken…), les héritiers se heurtent à un mur infranchissable. Impossible d'accéder, de prouver la détention, ou de transférer les fonds.
Certaines plateformes centralisées peuvent cependant accepter des procédures de succession. C'est par exemple le cas de Coinbase, Binance ou Kraken : mais elles exigent notamment un certificat de décès, un acte notarié désignant les héritiers puis une vérification d'identité stricte. Les procédures peuvent être longues.

SI LA PERSONNE A PLACÉ SES ACTIFS DANS CE QUE L'ON APPELLE DES « WALLETS NON CUSTODIAL » (COMME METAMASK, LEDGER OU TRUST WALLET), LES PROCÉDURES DE RÉCUPÉRATION SONT TOUT SIMPLEMENT IMPOSSIBLES SANS LES IDENTIFIANTS ORIGINAUX. LES ACTIFS SERONT DÉFINITIVEMENT PERDUS SI LE DÉFUNT N'A PAS PRIS DE MESURE POUR ASSURER LA TRANSMISSION DE CES INFORMATIONS APRÈS SON DÉCÈS.

ANTICIPER SA SUCCESSION CRYPTO : LES SOLUTIONS CONCRÈTES

1. TENIR UN INVENTAIRE SÉCURISÉ DE SES ACTIFS

C'est l'étape la plus basique mais cruciale : rédiger un document listant tous les cryptoactifs détenus, leur localisation (wallet ou plateforme), et les informations nécessaires à l'accès. Ce document peut être manuscrit et conservé dans un lieu sûr, chiffré et stocké numériquement avec un mot de passe, confié à un notaire ou un avocat.

2. TRANSMETTRE LES ACCÈS DE FAÇON SÉCURISÉE

Plusieurs options s'offrent au détenteur pour prévoir simplement un accès post-mortem :
- Utiliser un coffre-fort numérique (comme Digiposte, KeePassXC, 1Password) pour stocker les accès, avec partage possible post-mortem.
- Opter pour un système de partage de clé chiffrée (ex : Shamir's Secret Sharing) permettant à plusieurs personnes de détenir des fragments d'une seed phrase.
- Inclure ces informations dans un testament (avec prudence, car le testament est un document accessible à d'autres et souvent non chiffré). Idéalement, optez pour un « testament mystique » (lire ci-contre).

3. UTILISER UN SERVICE DE SUCCESSION CRYPTO

Plusieurs services ont émergé pour faciliter la transmission des actifs numériques en cas de décès. Qu'il s'agisse d'un ou de plusieurs bénéficiaires, des procédures spécifiques existent et sont censées garantir et sécuriser l'accès puis le partage et transfert des cryptos selon les volontés du défunt. Nous vous présentons par exemple la solution française Ficonum page suivante.

4. INFORMER SES HÉRITIERS DE L'EXISTENCE DE CES ACTIFS

C'est l'un des points les plus souvent négligés : prévenir un proche de confiance (conjoint, enfant, notaire) que des cryptoactifs existent, et qu'ils nécessitent une procédure d'accès spécifique. Sans cette transmission, aucune recherche ne sera lancée.

FICONUM, LA SOLUTION FRANÇAISE POUR TRANSMETTRE SES CRYPTOS

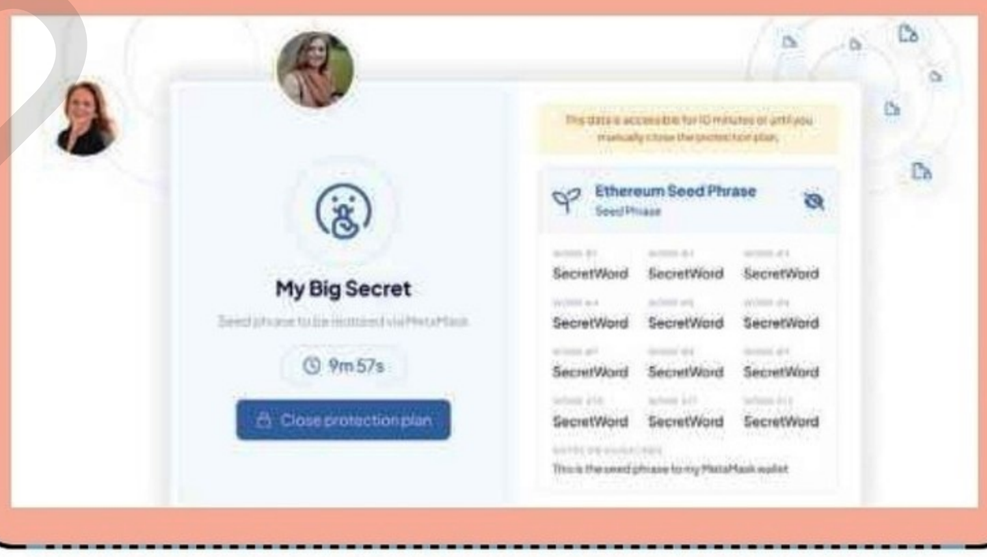
Ficonum est une plateforme française dédiée à la transmission sécurisée des actifs numériques, notamment des cryptomonnaies, en cas de décès ou d'incapacité. Elle permet aux détenteurs de cryptoactifs d'organiser leur succession de manière confidentielle et conforme au cadre juridique français.

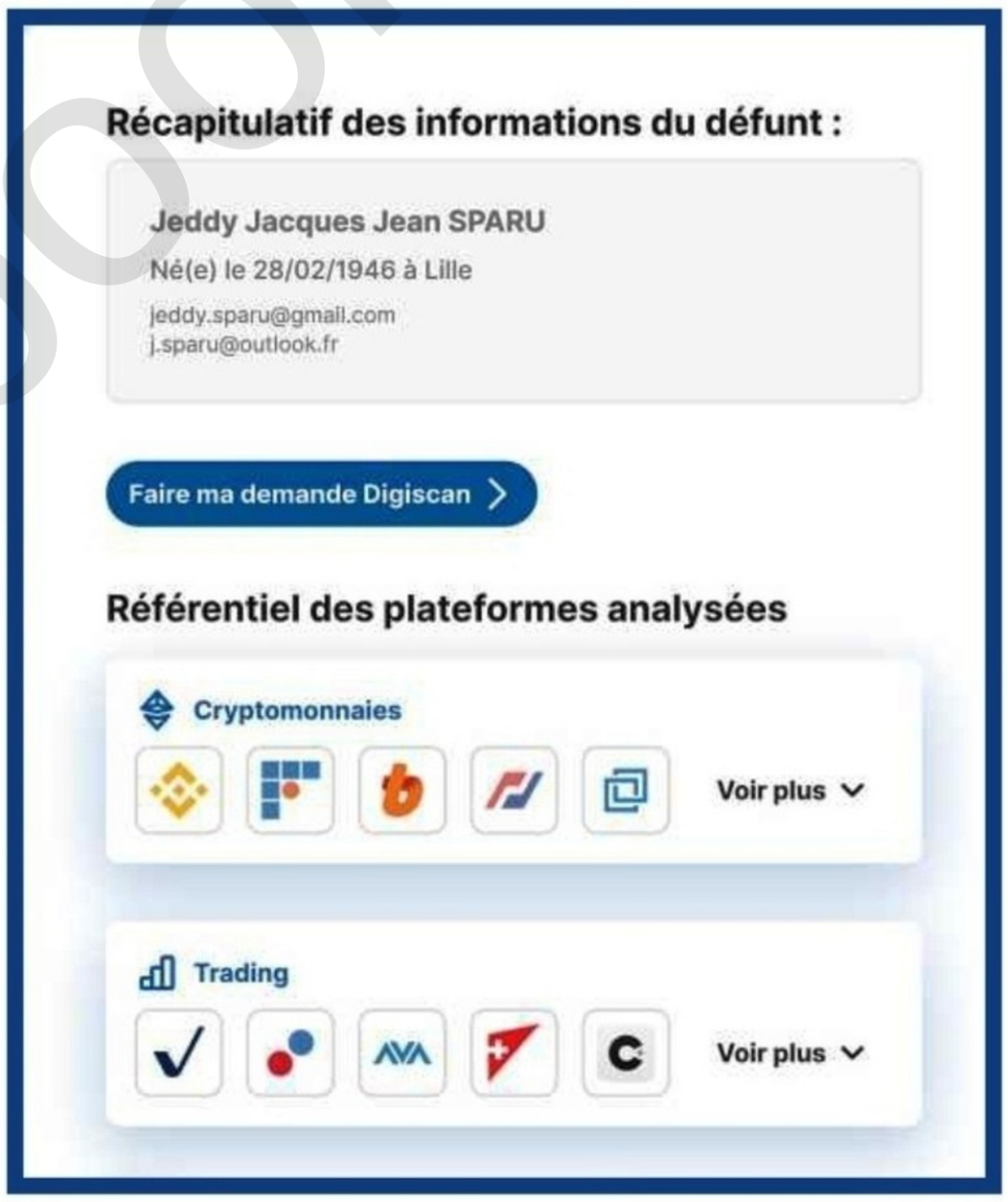
En matière de crytos, la confiance dans un service tiers n'a pas de prix. Protégé par le cadre juridique français et labellisé par le Conseil Supérieur du Notariat, Ficonum joue la carte de la sécurité à destination du public français. Les utilisateurs peuvent créer un espace sécurisé pour stocker les informations sur leurs portefeuilles (adresses, types de cryptoactifs) tout en listant les accès nécessaires (clés privées, seed phrases, identifiants) ainsi que les instructions spécifiques pour la transmission des actifs.

INHERITI : L'ALTERNATIVE BELGE EN MODE « SAFEKEYS »

Cette solution blockchain (développée par la société belge SafeTech Labs) permet, après un décès, la transmission sécurisée de données sensibles (clés privées, mots de passe, etc.) à des bénéficiaires désignés. L'originalité vient de la procédure mise en place : ces héritiers doivent rassembler leurs "SafeKeys" pour déclencher le déverrouillage des données du défunt. Les utilisateurs peuvent également configurer un "Dead Man's Switch" qui, en l'absence d'action de leur part dans un délai défini, déclenche la libération des clés aux bénéficiaires désignés. La version Community Edition est gratuite, tandis que des versions professionnelles sont payantes.

Lien : **inheriti.com**





EN CAS DE DISPARITION

Il est ensuite possible de désigner des bénéficiaires ou des personnes de confiance qui recevront les informations en cas de décès ou d'incapacité. La transmission des informations peut être déclenchée par un «Dead Man's Switch», c'est-à-dire en l'absence d'activité de l'utilisateur pendant une période définie ou par la notification d'un décès via un acte officiel transmis à Ficonum.
Ficonum propose aussi, dans sa formule sur-mesure, un accompagnement pour la rédaction de testaments, y compris le testament mystique **(Lire page 6)**,

qui permet de conserver la confidentialité des informations jusqu'à l'ouverture de la succession.
Toutes les informations sont chiffrées et stockées de manière sécurisée. L'accès au coffre-fort nécessite une authentification à deux facteurs ; les données ne sont accessibles qu'aux personnes autorisées, selon les conditions définies par l'utilisateur.
La Formule Essentielle donne accès au coffre-fort numérique et stockage des informations de base tandis que la formule Premium inclut des fonctionnalités avancées, telles que la désignation de bénéficiaires multiples et des options de déclenchement personnalisées.

À SAVOIR

DEAD MAN'S SWITCH (DMS)

L'objectif est d'assurer la transmission automatique et ultra simplifiée des informations que vous aurez définies et stockées. Le DMS est un mécanisme qui se déclenche si l'utilisateur ne réalise pas une action prédéfinie (comme se connecter ou répondre à un e-mail) dans un délai spécifié. Une fois déclenché, il libère les informations d'accès aux bénéficiaires désignés. De nombreuses plateformes et services en lignes proposent cette fonctionnalité. Le risque ? Si vous partez en voyage prolongé loin du monde connecté ou si perdez l'accès à votre email, la procédure pourrait s'enclencher sans que vous le vouliez !

SEED PHRASE : LA CLÉ DE VOÛTE DE VOTRE PORTEFEUILLE CRYPTO

Lorsqu'un utilisateur crée un nouveau portefeuille crypto – que ce soit avec MetaMask, Ledger, Trezor ou encore Trust Wallet – il se voit remettre une liste de 12, 18 ou 24 mots. Cette liste, appelée seed phrase ou phrase mnémonique, n'est pas choisie au hasard. Elle correspond à une clé maîtresse cryptographique qui permet de générer toutes les clés privées associées au portefeuille. Si vous possédez un wallet crypto, la seed phrase est bien l'élément central que vous devrez laisser à votre succession ! Mais c'est aussi le plus sensible.
Concrètement, votre seed phrase pourrait ressembler à une série anodine de mots comme «lion swim doctor essay fuel cancel easy display limb embark clump ecology». Pourtant, derrière cette simplicité apparente, se cache l'accès total à vos actifs numériques. Posséder la seed phrase revient à posséder le portefeuille lui-même : Celui qui détient cette liste de mots peut, en quelques clics, récupérer tous vos fonds et les transférer ailleurs, sans que vous puissiez intervenir. C'est pourquoi la sécurité de cette phrase est une priorité absolue. À l'inverse, perdre sa seed phrase signifie perdre l'accès définitif à ses cryptoactifs. Contrairement aux systèmes bancaires classiques, il n'existe ici aucune hotline, aucun mot de passe à réinitialiser. La responsabilité est totalement entre les mains de l'utilisateur.

SEED PHRASE ET MOT DE PASSE : ATTENTION À LA CONFUSION

Le mot de passe protège l'accès à l'application ou au périphérique (ex : déverrouiller l'application MetaMask sur votre smartphone). La seed phrase, elle, permet de restaurer intégralement votre portefeuille sur n'importe quel appareil, même si l'original est perdu ou détruit. Leur rôle n'est donc pas interchangeable, et la seed phrase doit bénéficier d'une protection encore plus renforcée.
Il ne faut jamais la stocker sur un service en ligne non chiffré ou trop facilement accessible (compte email, de messagerie ou cloud). Ne la prenez pas davantage en photo, un simple vol ou piratage de téléphone pourrait suffire à compromettre vos fonds. Privilégiez soit un stockage dans un coffre-fort numérique spécialisé, soit une copie physique à placer dans un coffre-fort bancaire ou notarié. Évitez enfin le papier pour éviter les dégâts du temps et les accidents (eau, feu, ...).

L'INFORMATIQUE FACILE

POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

LE **BLACK** DOSSIER

I2P :

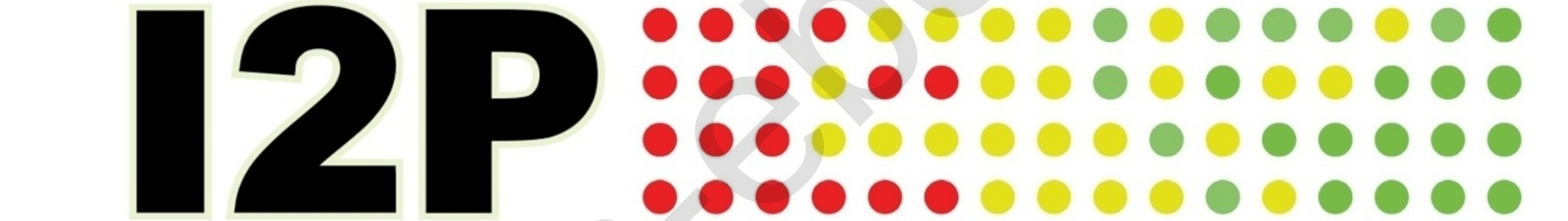
L'AUTRE RÉSEAU ANONYME

DONT (PRESQUE) PERSONNE NE PARLE

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

I2P, C'EST QUOI EXACTEMENT ? ET POURQUOI CE N'EST PAS "JUSTE UN AUTRE TOR"

Quand on parle de réseaux anonymes, c'est Tor qui vient immédiatement à l'esprit. Et pour cause : c'est le géant du secteur, avec son navigateur prêt à l'emploi, ses .onion, ses relais dans tous les coins du globe. Ce qu'on oublie souvent, c'est qu'il existe d'autres darknets, plus confidentiels et protégés. C'est là qu'entre en scène I2P, l'Invisible Internet Project.



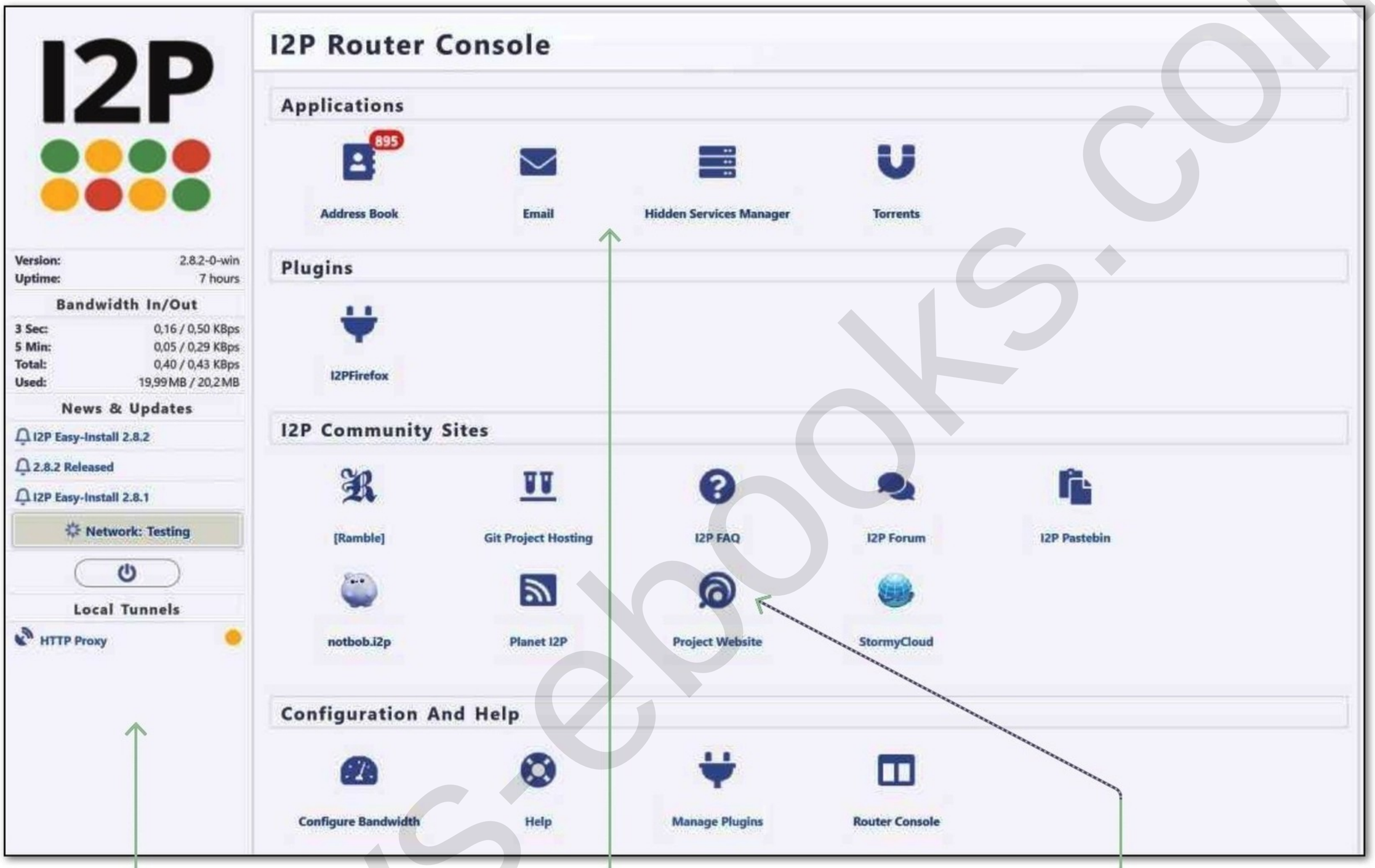
Contrairement à Tor, I2P n'est pas conçu pour accéder à l'Internet classique. C'est un réseau dans le réseau, une sorte d'Internet parallèle avec ses propres adresses (.i2p), ses propres services (torrents, mails, forums, blogs…) et ses propres règles.

TOR VS I2P

Bien sûr, Tor propose lui aussi un web caché — les fameux .onion. Ces adresses, comme protonirockerxow.onion, sont hébergées exclusivement sur le réseau Tor et ne sont pas accessibles depuis un navigateur standard. La différence, c'est qu'avec Tor, ce web caché

VOTRE CONSOLE I2P

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



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

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

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

est optionnel. Le navigateur Tor vous permet aussi de visiter Facebook, Wikipédia ou LeMonde.fr. Avec I2P, ce n'est pas le cas par défaut. I2P n'ouvre pas vers l'extérieur. Il crée un écosystème fermé, où tout – de la messagerie aux sites web – reste dans les murs du réseau. Et cela change à la fois la philosophie, la sécurisation (pas de nœud de sortie par exemple) et le public qui le fréquente. En fait, cela change tout. Est-ce que ça veut dire qu'I2P fonctionne sans Internet ? Pas vraiment. C'est un réseau superposé (overlay network) : il utilise lui aussi Internet comme tuyauterie, mais construit son propre langage, ses propres routes, ses propres espaces. Il ne fonctionne pas sans connexion Internet, mais il n'utilise pas le web

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

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

Pour dire la vérité, I2P, c'est moche. Beaucoup de sites sentent la naphtaline périmée (c'est pourtant scientifiquement improbable) tout en se moquant éperdument d'être ne serait-ce que compréhensibles. Mais va pour la beauté du geste… Il vous faudra de la patience et de l'apprentissage petit padawan.

COMMENT FONCTIONNE I2P ?

Bienvenue dans l'ingénierie de l'ombre ! Imaginez un Internet où personne ne sait d'où viennent les messages, où vont les données, ni qui héberge quoi. C'est exactement ce qu'I2P cherche à bâtir. Mais contrairement à Tor, ici, tout repose sur un mécanisme original : les tunnels unidirectionnels chiffrés.

Quand tu communiques sur I2P, tu ne crées pas une autoroute bidirectionnelle comme sur Tor. Tu construis deux tunnels distincts : un pour envoyer tes données, un autre, complètement différent, pour recevoir les réponses. Ainsi, pour une communication entre deux utilisateurs, quatre tunnels sont nécessaires : deux pour chaque sens de la communication.
Chaque tunnel traverse plusieurs relais (des nœuds du réseau) choisis aléatoirement. Le trajet est unique, temporaire, et reconstruit toutes les 10 minutes environ. Résultat ? Même si un maillon du tunnel est compromis, il n'a qu'une vision partielle du chemin. Aucun nœud ne connaît l'ensemble de la route.

LE GARLIC ROUTING

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

QUEL CHIFFREMENT ?

I2P emploie plusieurs couches de chiffrement pour assurer la confidentialité et l'intégrité des messages :
- Chiffrement asymétrique : utilise l'algorithme ElGamal pour établir des clés de session.
- Chiffrement symétrique : utilise AES-256 en mode CBC pour chiffrer les données.
- Hachage : utilise SHA-256 pour l'intégrité des messages.
Chaque message est chiffré en couches, chaque nœud du tunnel ne pouvant déchiffrer qu'une couche, ce qui empêche tout nœud individuel de connaître l'origine et la destination finales du message.

"Le Garlic routing est conçu pour mieux résister aux attaques par corrélation que le routage en oignon. Il est idéal pour les services internes où l'on souhaite conserver l'anonymat."

- Jason Mallory, chercheur en sécurité réseau, conférence DarknetTech 2021

traditionnel. Vous pouvez vous installer dans I2P pour lire, écrire, publier, partager, chatter, sans jamais remettre un pied sur la toile classique. Comme l'a écrit Masayuki Hatta, chercheur en économie numérique dans Medium : «*I2P n'a pas besoin d'Internet pour être utile. Il devient son propre réseau - pas seulement une route, mais une destination*». Raaaâh, c'est beau...

VOUS AVEZ DIT EEPSITES ?

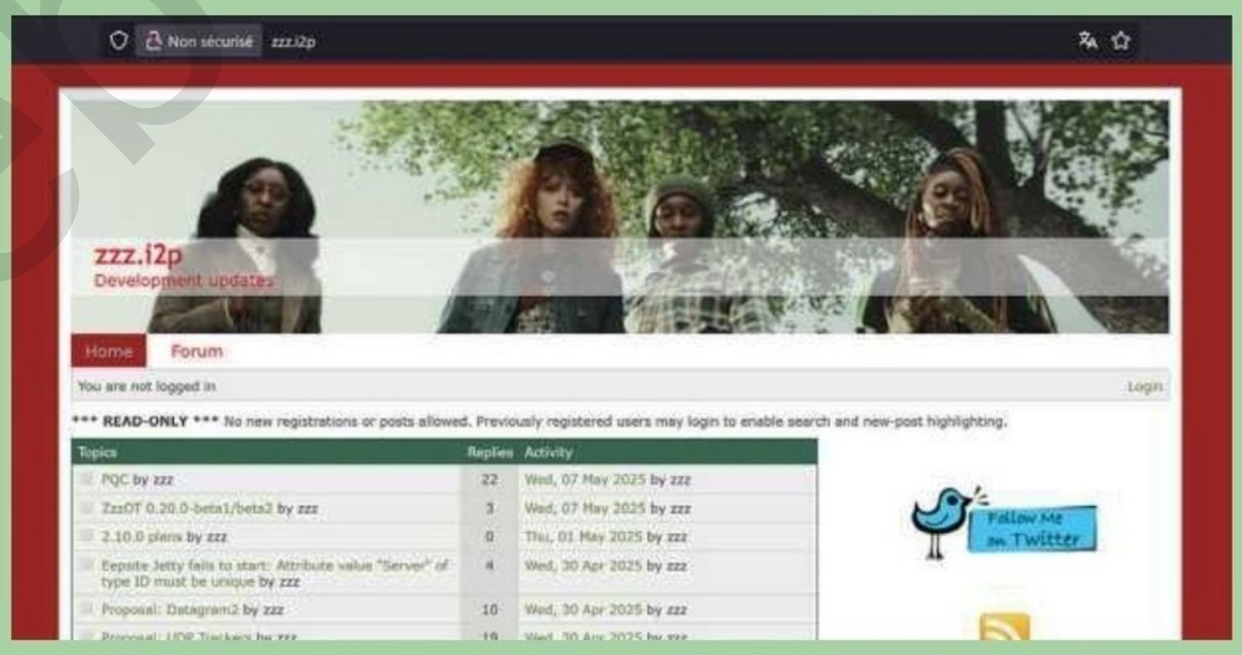
C'est un monde fermé, chiffré, et autosuffisant. Vous ne surferez pas sur YouTube ou Wikipédia avec I2P. Vous visiterez des eepsites – des sites uniquement accessibles à ceux connectés au réseau, comme tracker2post.i2p ou notbob.i2p. Autrement dit : pas de Google, pas de DNS publics, pas de surface. Juste les profondeurs.
Derrière, tout repose sur un principe fondamental : les tunnels unidirectionnels. I2P sépare totalement l'entrée et la sortie. Un tunnel pour envoyer, un autre pour recevoir, chacun passant par plusieurs relais différents. Résultat : si un tunnel est compromis, l'autre reste intact.
Autre particularité : pas de nœud central, pas de DNS, pas de hiérarchie. Le réseau se construit en peer-to-peer pur, avec une base de données décentralisée (la netDb) pour localiser les autres utilisateurs. Le tout, en Java, tournant en tâche de fond sur votre machine.
Pour vulgariser un peu : Tor, c'est comme utiliser un tunnel sous la ville pour accéder discrètement à un supermarché. I2P, c'est comme vivre dans une ville souterraine où tous les commerces, forums et messageries sont déjà là. Tu n'as plus besoin de remonter à la surface.

AUX ORIGINES DE L'INVISIBLE INTERNET PROJECT

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

DES CONTRIBUTEURS CLÉS

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



DEPUIS DE NOMBREUSES ANNÉES, ZZZ EST LE DÉVELOPPEUR LE PLUS INVESTI PUBLIQUEMENT DANS LE PROJET I2P. SON SITE ZZZ.I2P PERMET D'ÊTRE MAINTENU AU COURANT DE TOUTES LES NOUVEAUTÉS.

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

À SAVOIR

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

Comparatif : TOR et I2P, quelles différences ?

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

HÉBERGER UN SITE .I2P : COMMENT ÇA MARCHE?

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

VOTRE EEPSITE EST DISTRIBUÉ !

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

LE «MIRRORING» COMMUNAUTAIRE

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

QUI UTILISE I2P ?

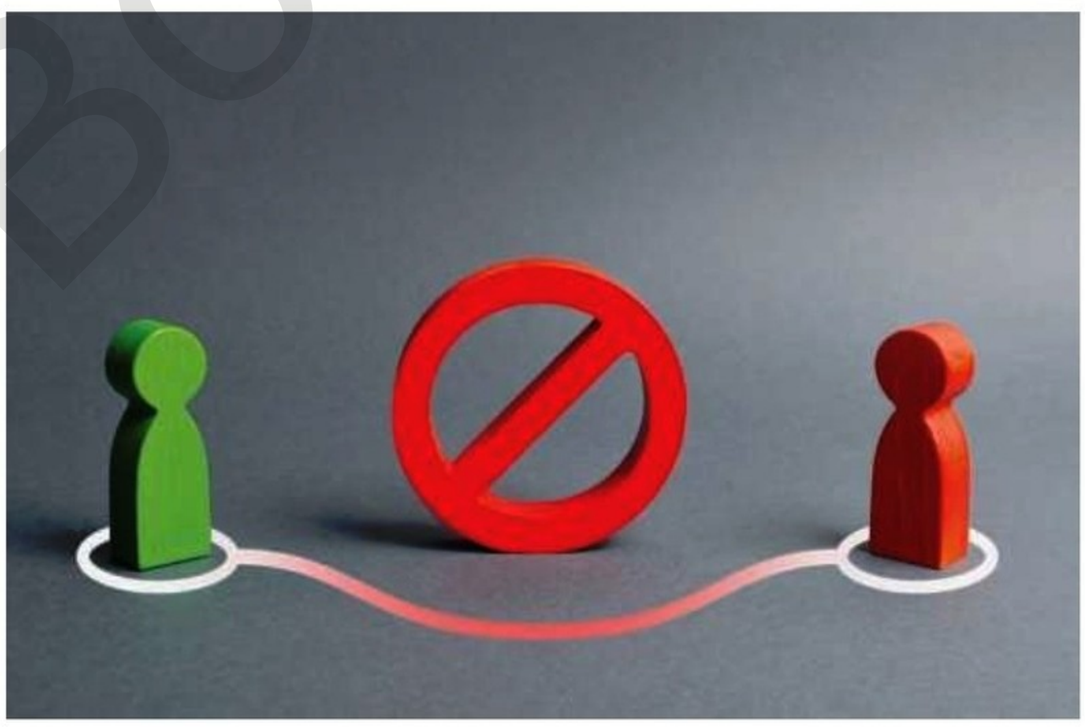
BIENVENUS DANS LE DARKNET CLAIR / OBSCUR

LA VERSION CLAIRE

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

1. LES MILITANTS SOUS PRESSION : Dans certains pays, publier un billet de blog critique peut suffire à finir en prison. I2P leur permet de créer des sites anonymes, hébergés dans le réseau. Pas d'IP à tracer, pas de DNS à bloquer. Eva Galperin, directrice de la cybersécurité chez

> Plus confidentiel et techno-geek, I2P échappe en partie à la « merdisation » de Tor. Mais la migration d'activités illégales semble s'accélérer.



EFF (Electronic Frontier Foundation), explique ainsi que « *Pour les journalistes en zones hostiles, I2P est un filet de sécurité. Il permet d'échanger, de publier, de chercher des informations… tout en gardant le silence numérique* ».

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

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

LA VERSION SOMBRE

I2P, en tant que réseau anonyme et décentralisé, attire des utilisateurs recherchant la confidentialité. Ok. Sous-entendu : c'est aussi l'endroit rêvé pour faire plein de trucs illégaux !
I2P avait jusqu'ici deux avantages : son audience plus geek et plus confidentielle que sur Tor ainsi qu'une absence de technologies e-commerce intégrables par défaut, ce qui en fait « une place de marché » a priori moins intéressante. Mais, face aux attaques par déni de service (DDoS) et à la surveillance accrue sur Tor, certains cybercriminels se tournent vers I2P.

TROIS EXEMPLES

En mars 2025, des chercheurs en cybersécurité ont par exemple identifié un cheval de Troie d'accès à distance (RAT) nommé «RATatouille» qui utilise le réseau I2P pour masquer ses communications avec les serveurs de commande et de contrôle (C2).
Le forum polémique Dread, connu pour héberger pléthore de discussions sur des activités illégales, est également passé chez I2P en avril 2022. À la suite de nombreuses attaques DDoS sur son site Tor, le forum a mis en place un miroir sur I2P, profitant de la résilience et de l'anonymat du réseau.
On évoquera enfin AlphaBay, l'un des plus grands marchés noirs du dark web. Il s'est relancé en 2021 avec des miroirs sur I2P en plus de Tor. Cette décision visait à diversifier les points d'accès et à renforcer la résilience face aux actions des forces de l'ordre.

DÉFENSES COMMUNAUTAIRES

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

COMBIEN D'UTILISATEURS SUR I2P ?

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

ET TOR, ALORS ?

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

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

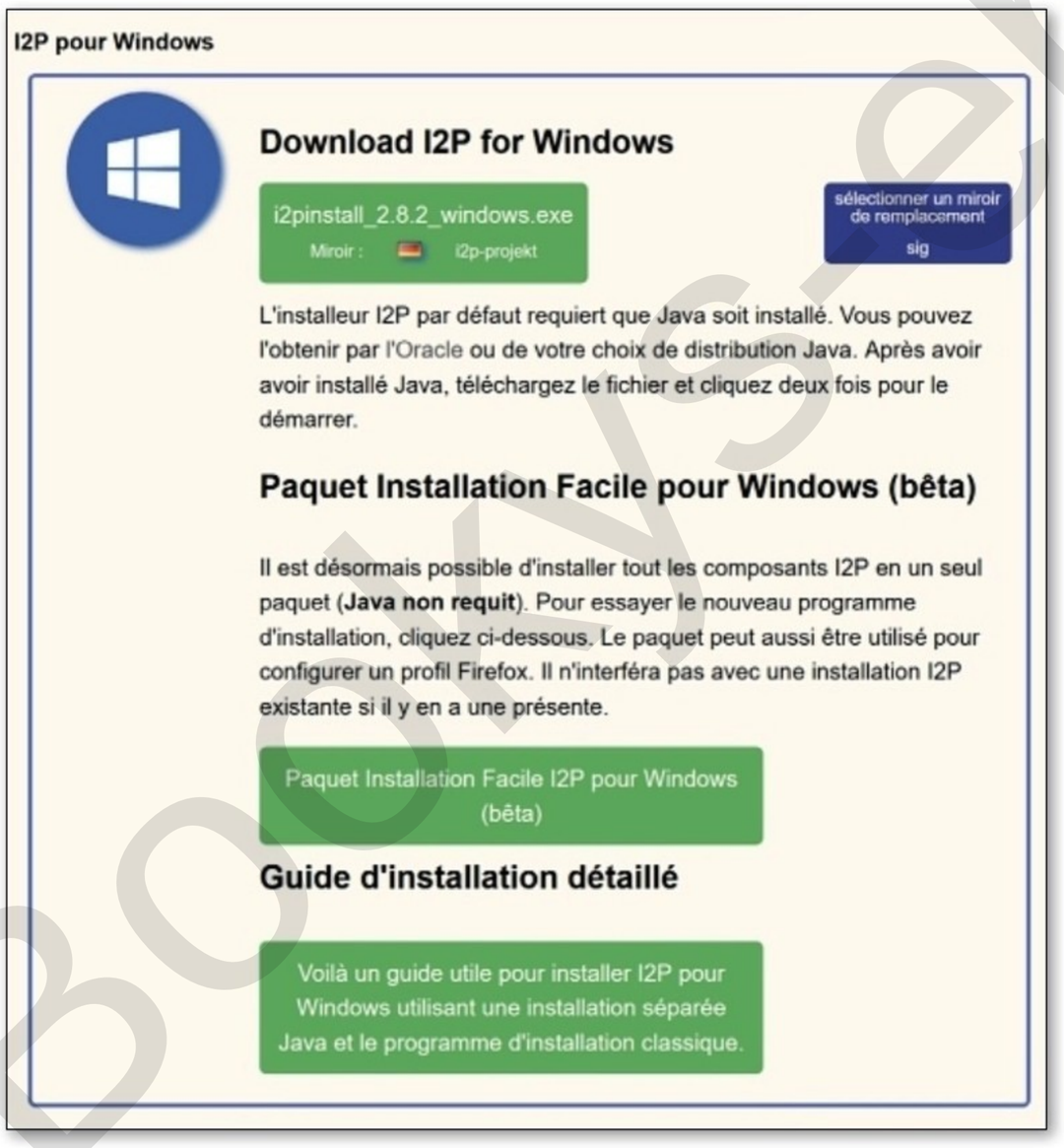
INSTALLEZ I2P ET PLONGEZ DANS SON DARKNET

I2P

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

01› TÉLÉCHARGER LE «PAQUET D'INSTALLATION FACILE »

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



À SAVOIR

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

INSTALLATION CLASSIQUE OU « PAQUET D'INSTALLATION FACILE » ?

Le "Paquet d'installation facile pour Windows (bêta)" d'I2P a été introduit en septembre 2022, comme indiqué lors de la réunion de développement du 6 septembre 2022. Il réduit drastiquement le nombre d'étapes nécessaires à l'installation de I2P.
Ce paquet a été conçu pour simplifier l'installation d'I2P sur Windows en incluant une machine virtuelle Java (JVM) embarquée, éliminant ainsi la nécessité d'installer Java séparément. Il configure enfin automatiquement un profil Firefox optimisé pour I2P, incluant des extensions telles que NoScript et HTTPS Everywhere.
Depuis sa sortie initiale, ce paquet a connu plusieurs mises à jour pour améliorer sa compatibilité et corriger des bugs, notamment sur Windows 11. Il est important de noter que, bien qu'il soit encore étiqueté comme "bêta", il est activement maintenu et recommandé pour les utilisateurs souhaitant une installation simplifiée d'I2P sur Windows.
Par contre, si après installation, vous rencontrez des problèmes de connexions, de configuration avec le firewall ou votre VPN, repassez par l'installation classique qui vous donnera la main sur beaucoup de réglages.

02› LANCEZ L'INSTALLATION.

Si Windows bloque le programme, cliquez sur **Informations complémentaires** puis **Exécutez quand même.** Sélectionnez la langue française et valider

l'emplacement d'installation sur votre PC puis **Fermer** à la fin de l'installation.

03› RÉGLAGES

Autorisez le parefeu Windows si demandé. Après quelques poignées de secondes, une fenêtre Firefox s'ouvrira, vous donnant accès à la configuration de la Console I2P. Cliquez sur **Next** pour valider la

langue puis le thème choisi (clair ou sombre).

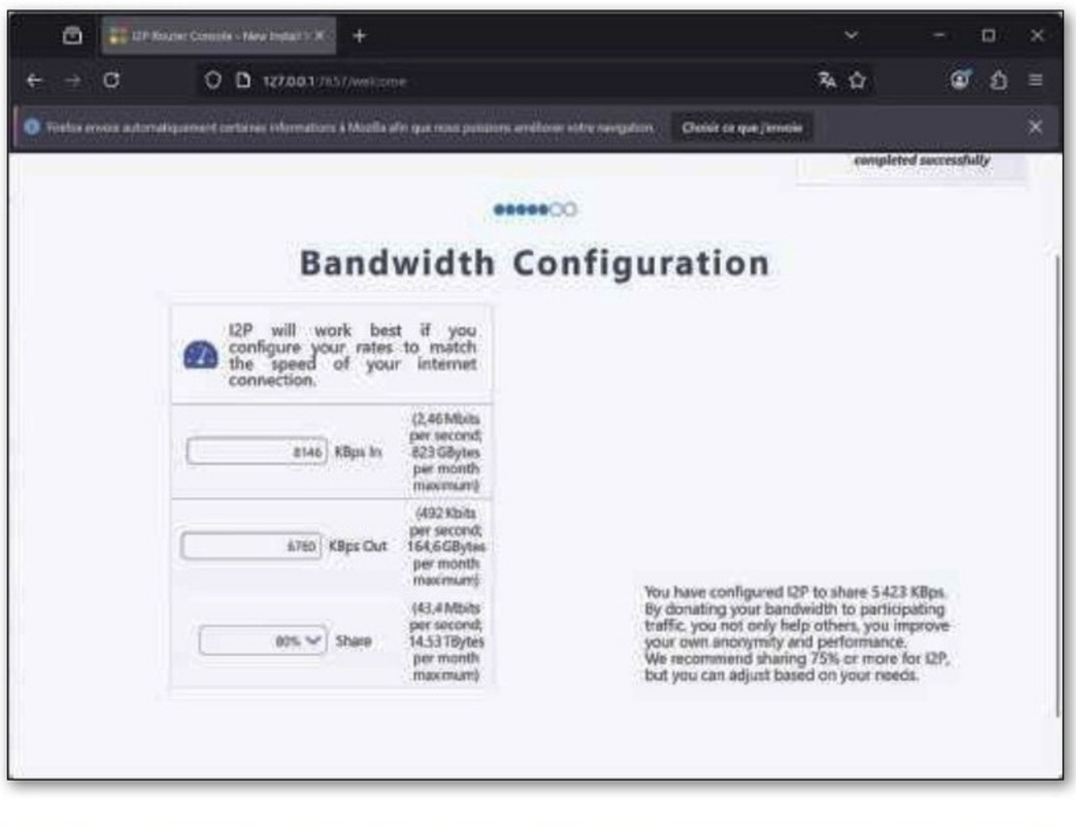
04› TEST DE VOTRE CONNEXION

Lancez le test de bande passante (**Next**). I2P utilise M-Lab, un service tiers, pour vous aider à tester votre connexion Internet et à trouver les

paramètres de vitesse optimaux. Pendant cette période, vous serez connecté directement au service de M-Lab avec votre véritable adresse IP. Une fois le test réussi, cliquez sur **Next**.

05› VOTRE ALLOCATION À I2P

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



06› ACCÉDEZ À I2P

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

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

À SAVOIR

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

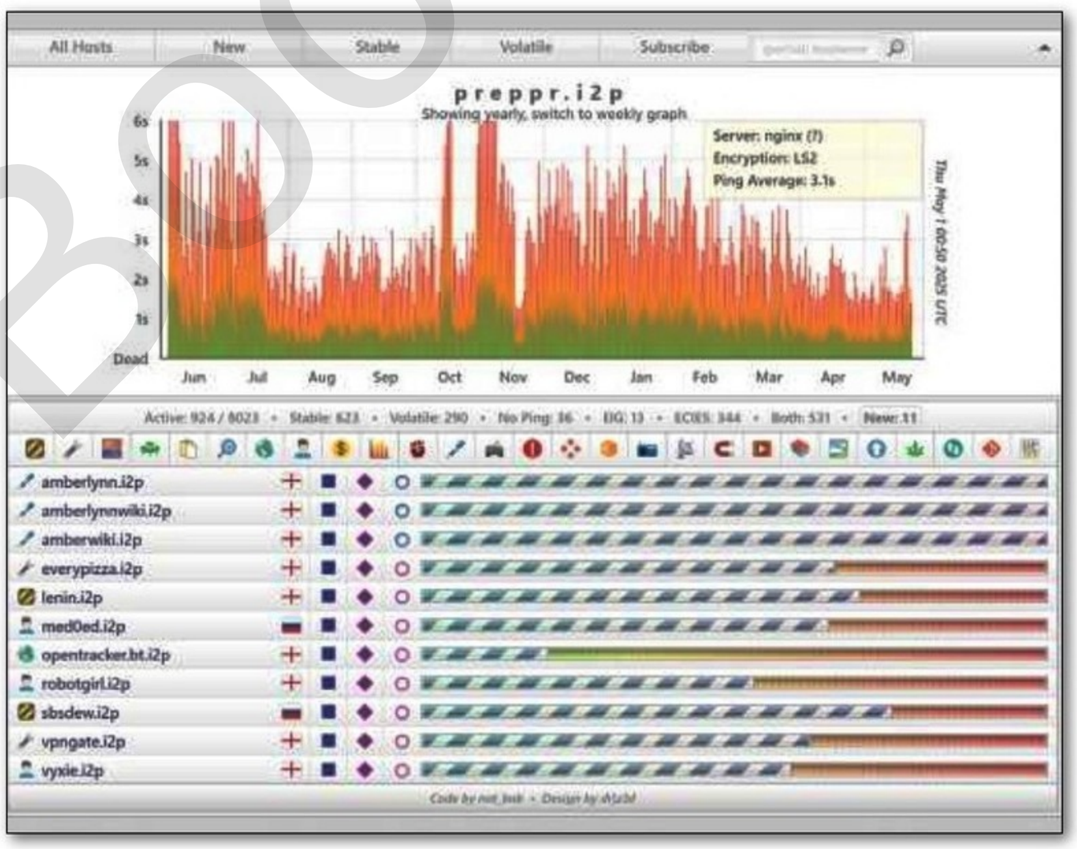
07› CONNEXION AU RÉSEAU

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

08› PREMIERS SITES .I2P

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

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



09› ÉTEINDRE ET REDÉMARRER I2P 1/2

Si vous fermez la fenêtre Firefox qui abrite votre session Console, vous quitter simplement le réseau, mais votre routeur reste actif. Pour ré ouvrir I2P,

ouvrez simplement une nouvelle fenêtre Firefox et rentrez l'adresse **http://127.0.0.1:7657/** pour redémarrer une session.

10› ÉTEINDRE ET REDÉMARRER I2P 2/2

Si vous avez cliqué sur **Shutdown**, vous arrêtez également le routeur qui fonctionne en tâche de fond. Vous serez peut-être obligé de le relancer si l'étape précédente ne fonctionne pas. Pour cela, selon votre version et méthode d'installation, via la recherche

Windows, trouvez et double-cliquez sur **Start I2P (GUI)** ou **I2P Router** ou **Browse I2P**. Attention, pas de panique, il se peut que vous attendiez une poignée de minutes avant que le routeur ne soit actif et que la console ne se relance.

PIRATE INFORMATIQUE

JE SOUTIENS
LE COMMERCE DE PROXIMITÉ,

JE VAIS CHEZ MON
MARCHAND DE JOURNAUX

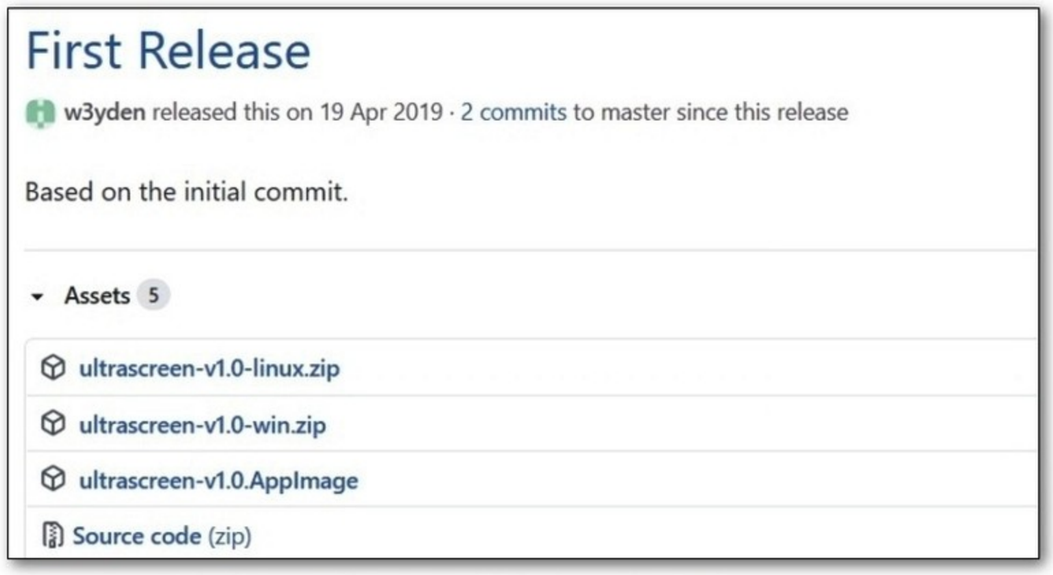
Direct éditeurs

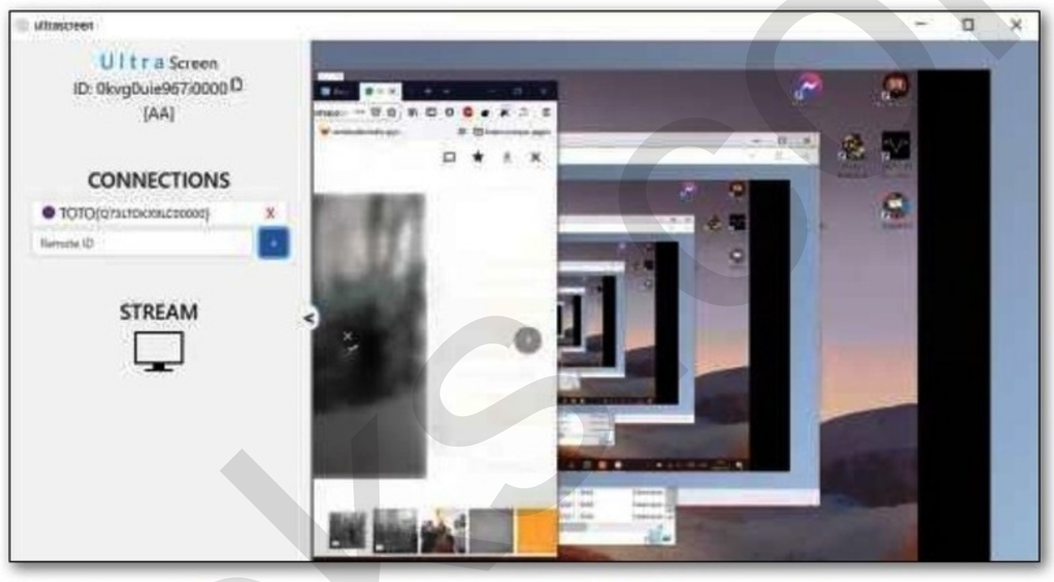
PARTAGEZ VOTRE ÉCRAN À DISTANCE

PRATIQUE

Vous voulez montrer à votre interlocuteur ce qui se passe sur votre écran, ou inversement ? Lancez UltraScreen sur les deux PC et suivez le guide.

INFOS [**Ultrascreen**]
Où le trouver ? [**https://tinyurl.com/ultrascreen**]
Difficulté : ☠☠☠





01› LANCER LE LOGICIEL

Téléchargez **ultrascreen-v1.0-win.zip**, puis faites un clic droit sur ce dossier compressé et sélectionnez **Extraire tout** puis **Extraire**. Ouvrez le dossier **ultrascreen-v1.0-win** et double-cliquez sur **ultrascreen.exe**. Si Windows essaie de vous empêcher de l'exécuter, cliquez sur **Informations complémentaires** puis sur **Exécuter**.

02› ÉTABLIR LA CONNEXION

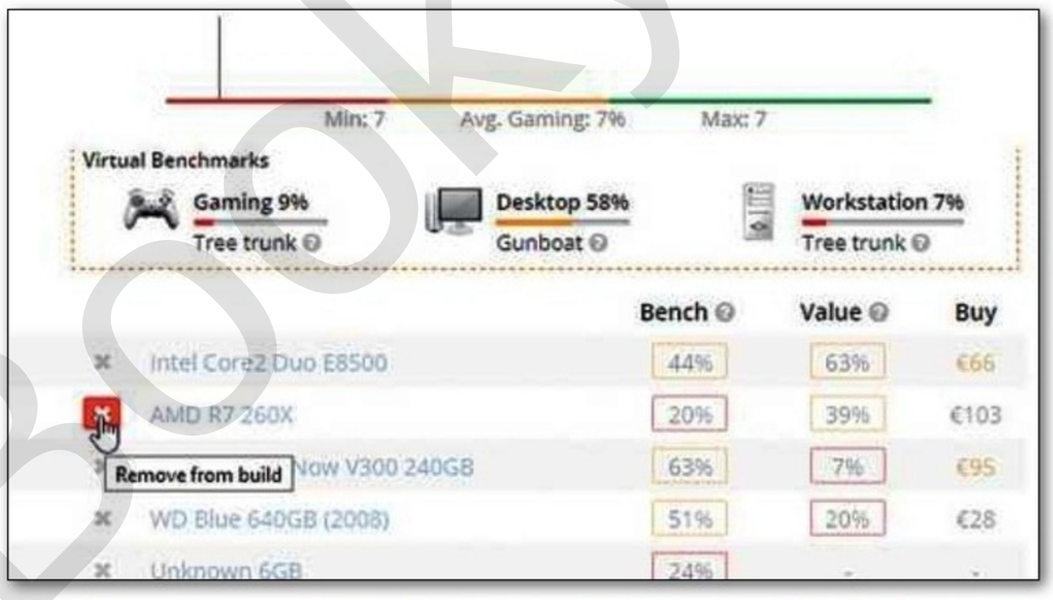
Tapez un nom d'utilisateur et cliquez sur **Login**. UltraScreen vous donne une clé d'identification (ID). Transmettez-la à votre interlocuteur. Celui-ci doit la saisir dans le cadre **Remote ID** et cliquer sur **+**. Cliquez sur **Stream** et choisissez ce que vous souhaitez partager. Par défaut cliquez sur **Entire screen**. Votre interlocuteur voit maintenant votre écran.

CHOISISSEZ DE NOUVEAUX COMPOSANTS

PRATIQUE

Après avoir testé votre ordinateur, UserBenchmark peut vous aider à choisir de nouveaux composants pour booster votre PC.

INFOS [**UserBenchmark**]
Où le trouver ? [**www.userbenchmark.com**]
Difficulté : ☠☠☠



01› ESSAYER LES PROPOSITIONS

Sur la page des résultats d'analyse, cliquez sur **Add to PC Build**. Ici, vous pouvez comparer les performances de votre PC avec celles que vous obtiendriez en changeant un composant. Dans la colonne de droite (**Alternative**), cliquez sur la croix à côté de l'élément à changer, puis en-dessous essayez les alternatives proposées en cliquant dessus.

02› ÉLARGIR LE CHOIX

A côté de chaque alternative, vous voyez une estimation des performances et du prix mais le choix est limité. Faites un clic droit en haut sur le composant à changer et **Ouvrir dans un nouvel onglet**. Une liste bien plus étoffée apparait alors. Pour intégrer un élément dans la simulation revenez sur l'onglet précédent, cliquez sur **Change Alternative...** et tapez la référence.

LOGICIEL LIBRE OU OPEN SOURCE :

Attention, ne pas confondre !

la frontière entre logiciel libre et Open Source tend à s'estomper sur le terrain, tant les projets collaboratifs abondent. Néanmoins, leur distinction reste essentielle : le libre rappelle que le numérique touche aux droits et libertés fondamentales, tandis que l'Open Source démontre l'efficacité de l'ouverture pour l'innovation.

Deux concepts nourrissent encore débats et confusions : le logiciel libre et l'Open Source. Si ces termes semblent interchangeables pour beaucoup, ils traduisent en réalité deux visions philosophiques et pratiques distinctes du logiciel. Pour comprendre cette nuance, il faut remonter aux origines du mouvement du logiciel libre dans les années 1980, et au tournant pragmatique qu'a proposé l'Open Source à la fin des années 1990.

LE LOGICIEL LIBRE : UNE QUESTION ÉTHIQUE AVANT TOUT

Le logiciel libre est né de l'initiative de Richard Stallman, informaticien du MIT, qui fonde en 1985 la Free Software Foundation (FSF). Selon lui, un logiciel est libre s'il respecte quatre libertés fondamentales :

1) Liberté d'utiliser le logiciel pour n'importe quel usage.

2) Liberté d'étudier le fonctionnement du programme et de l'adapter à ses besoins (accès au code source obligatoire).

3) Liberté de redistribuer des copies du logiciel.

4) Liberté d'améliorer le logiciel et de publier ses améliorations.

Le logiciel libre s'inscrit donc dans une démarche éthique et politique : il s'agit de garantir aux utilisateurs un contrôle total sur leur outil informatique, en s'opposant à la logique propriétaire et fermée des grandes entreprises technologiques.

Parmi les exemples historiques les plus connus et toujours parmi les plus utilisés de logiciels libres, nous pouvons citer GNU Emacs (éditeur de texte), LibreOffice (suite bureautique) ou encore GIMP (éditeur d'images).

RICHARD STALLMAN, À L'INITIATIVE DE LA TERMINOLOGIE, L'AFFIRME : « LE TERME "FREE" DANS "FREE SOFTWARE" EST UNE QUESTION DE LIBERTÉ, PAS DE PRIX. » (FREE SOFTWARE FOUNDATION, 1986).

TOP 30 LOGICIELS LIBRES ET OPEN SOURCE

Pour y voir plus clair et mesurer ce que ces programmes peuvent vous apporter au quotidien, voici notre sélection des 30 meilleurs logiciels libres, open source… ou les deux !

Nom	Catégorie	Description	Où le trouver ?
LibreOffice	Libre	Suite bureautique complète, alternative à Microsoft Office.	**www.libreoffice.org**
GIMP	Libre	Éditeur d'images avancé, alternative à Photoshop.	**www.gimp.org**
Scribus	Libre	Publication assistée par ordinateur (PAO).	**www.scribus.net**
Kdenlive	Libre	Éditeur vidéo non linéaire et libre.	**kdenlive.org**
Thunderbird	Libre	Client e-mail sécurisé développé par Mozilla.	**www.thunderbird.net**
Nextcloud	Libre	Solution de cloud personnel libre.	**nextcloud.com**
KeePassXC	Libre	Gestionnaire de mots de passe local sécurisé.	**keepassxc.org**
GCompris	Libre	Suite éducative pour les enfants.	**gcompris.net**
Jitsi Meet	Libre	Visioconférence libre et sécurisée.	**jitsi.org**
Tuleap	Libre	Gestion de projet agile et DevOps.	**www.tuleap.org**
Chromium	Open Source	Base open source du navigateur Google Chrome.	**www.chromium.org**
Vue.js	Open Source	Framework JavaScript pour interfaces dynamiques.	**vuejs.org**
FFmpeg	Open Source	Traitement audio et vidéo.	**ffmpeg.org**
Cassandra	Open Source	Base de données NoSQL distribuée.	**cassandra.apache.org**
Apache NiFi	Open Source	Automatisation de flux de données.	**nifi.apache.org**
Bitwarden	Open Source	Gestionnaire de mots de passe chiffré.	**bitwarden.com**
SumatraPDF	Open Source	Lecteur PDF rapide et léger pour Windows.	**www.sumatrapdfreader.org/free-pdf-reader.html**
ProjeQtOr	Open Source	Gestion de projet orientée qualité.	**www.projeqtor.org**
PDFsam	Open Source	Éditeur de PDF (fusion, séparation, rotation).	**pdfsam.org**
HedgeDoc	Open Source	Éditeur Markdown collaboratif.	**hedgedoc.org**
Mozilla Firefox	Libre et Open Source	Navigateur respectueux de la vie privée.	**www.mozilla.org/firefox**
VLC Media Player	Libre et Open Source	Lecteur multimédia universel.	**www.videolan.org/vlc/**
Blender	Libre et Open Source	Suite complète de création 3D.	**www.blender.org**
OBS Studio	Libre et Open Source	Enregistrement vidéo et streaming.	**obsproject.com**
Audacity	Libre et Open Source	Enregistrement et édition audio.	**www.audacityteam.org**
Inkscape	Libre et Open Source	Illustration vectorielle (SVG).	**inkscape.org**
Krita	Libre et Open Source	Peinture numérique professionnelle.	**krita.org**
Wireshark	Libre et Open Source	Analyseur de paquets réseau.	**www.wireshark.org**
Kali Linux	Libre et Open Source	Distribution Linux pour le pentesting.	**www.kali.org**
Metasploit Framework	Libre et Open Source	Plateforme d'exploitation et test d'intrusion.	**www.metasploit.com**

COMPARATIF : LOGICIEL LIBRE VS OPEN SOURCE

Critères	Logiciel libre	Open Source
Liberté d'utilisation	Oui	Oui
Accès au code source	Oui	Oui
Redistribution autorisée	Oui	Oui
Obligation de rester libre	Oui (copyleft)	Non (permissif possible)
Priorité	Liberté de l'utilisateur	Efficacité du développement
Finalité	Éthique, politique	Technique, économique
Origine	FSF (1985)	OSI (1998)
Position face aux solutions propriétaires	Forte opposition	Coopération possible

L'OPEN SOURCE : UN PRAGMATISME ÉCONOMIQUE

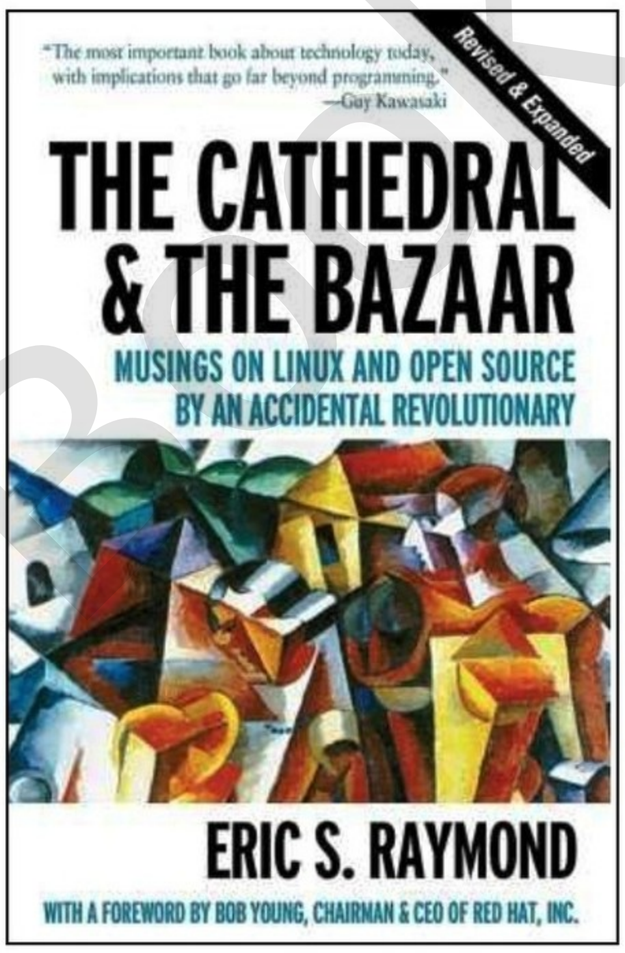
Face à l'image radicale et parfois politisée du logiciel libre, une partie de la communauté technologique initie en 1998 le mouvement Open Source, piloté notamment par Eric S. Raymond et Bruce Perens. Leur objectif est de rendre la collaboration sur le code plus attrayante pour le secteur privé, en se concentrant sur les avantages techniques et économiques, plutôt que sur les valeurs philosophiques.

L'Open Source Initiative (OSI) définit une dizaine de critères qu'un logiciel doit respecter pour être qualifié d'Open Source, dont :

1) La libre redistribution,

2) L'accès au code source,

3) La possibilité de modifier et de créer des travaux dérivés.



Eric S. Raymond l'explique dans son essai fondateur The Cathedral and the Bazaar (1999) : « *Le bon bazar est supérieur à la cathédrale : plus de regards signifient moins de bogues*. »

Autrement dit, plus un projet est ouvert à contributions, plus il sera robuste et innovant. Ici, l'enjeu est moins idéologique : l'Open Source met en avant l'efficacité du modèle de développement collaboratif.

On citera aussi en exemples quelques grands succès de l'open source comme Linux (noyau de système d'exploitation), Kubernetes (orchestration de conteneurs) ou Apache HTTP Server (serveur Web).

LES DEUX, MON CAPITAINE ?

D'un point de vue technique, un logiciel libre est (presque) toujours Open Source mais l'inverse n'est pas forcément vrai. Comme le souligne Stallman en 2009 : « *L'Open Source est une méthodologie de développement ; le logiciel libre est un mouvement social*. » (Free Software, Free Society). Un logiciel comme Mozilla Firefox est ainsi Open Source et libre, mais Mozilla préfère parler d'Open Source pour mieux dialoguer avec les entreprises et éviter l'étiquette politique que véhicule le terme « libre ».

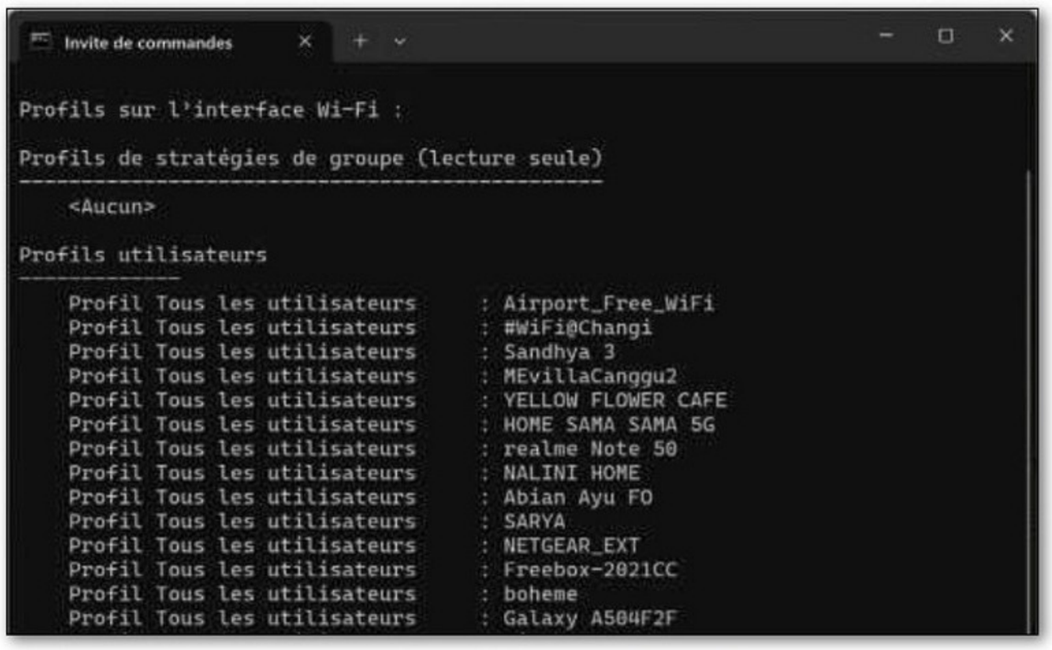
Cette différence a des impacts concrets : un développeur qui choisit la licence GNU GPL (libre) impose que toute modification reste également libre : on parle de copyleft. Avec une licence MIT ou Apache (Open Source permissives), un acteur peut intégrer le code dans un projet propriétaire sans avoir à publier ses modifications. C'est pourquoi, par exemple, Microsoft a massivement investi dans l'Open Source (rachetant GitHub, soutenant Linux), tout en conservant des pans entiers de son offre commerciale sous licences propriétaires.

RETROUVEZ LES MOTS DE PASSE WI-FI ENREGISTRÉS SUR SON PC

PRATIQUE

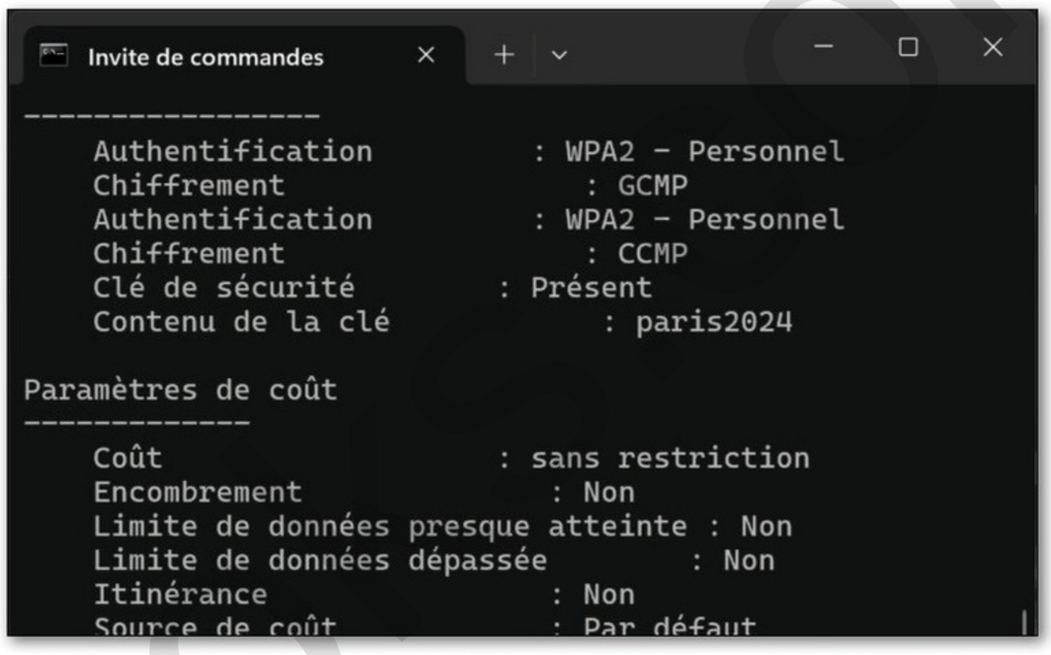
Vous voulez connecter un nouveau téléphone à votre Wi-Fi, mais vous avez oublié le mot de passe ? Ou vous voulez auditer ce que votre PC a stocké comme clés ? Accéder à toutes les clés Wi-Fi que votre PC a enregistrées dans sa mémoire. Voici la méthode « mode Terminal ».

INFOS
[Windows]
Difficulté : ☠☠☠



01› LISTER TOUS LES PROFILS WI-FI ENREGISTRÉS

Ouvrez l'invite de commandes (**cmd + Entrée**) en tant qu'administrateur. Tapez :
netsh wlan show profiles. Apparait la liste de tous les Wi-Fi enregistrés sur votre PC.



02› AFFICHER LE MOT DE PASSE D'UN PROFIL

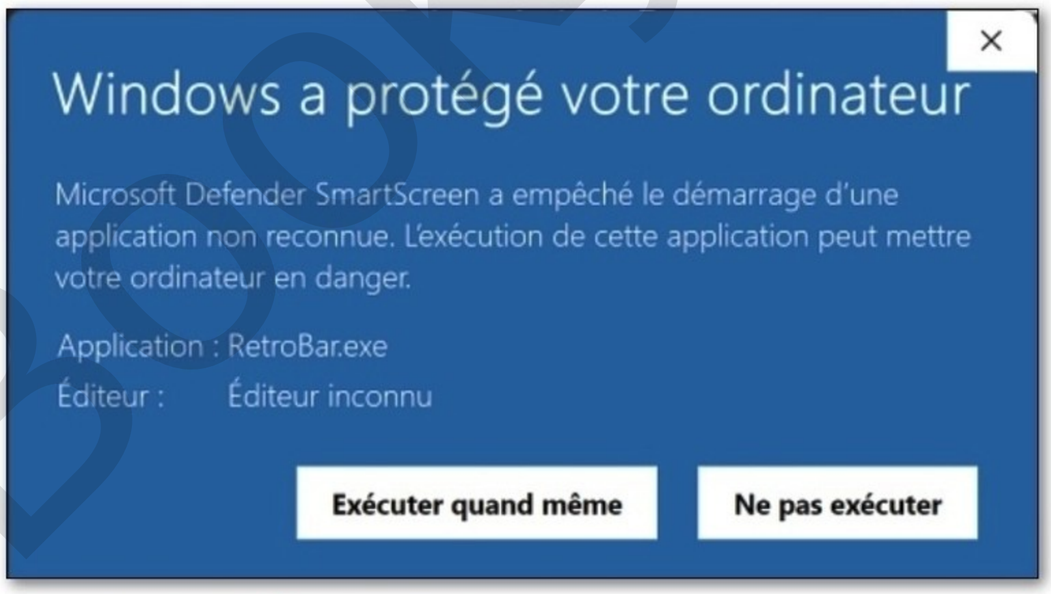
Remplacez le nom du réseau entre guillemets par le nom exact d'un des profils identifiés, comme ci-dessous :
netsh wlan show profile name=»Freebox-2021CC» key=clear
Cherchez ensuite la ligne : **Contenu de la clé : « motdepassewifi »**. Ce mot de passe est en clair, car Windows l'a enregistré pour pouvoir vous reconnecter automatiquement.

RETROUVEZ UNE BARRE DES TÂCHES ANNÉES 90 OU 2000 !

PRATIQUE

Avec RetroBar, pimpez votre PC moderne avec une barre des tâches vintage reprenant les graphismes et l'ergonomie des barres Windows des années 90 et 2000. RetroBar est un exécutable qui fait le boulot immédiatement !

INFOS [RetroBar]
Où le trouver ? [github.com/dremin/RetroBar]
Difficulté : ☠☠☠



01› EXÉCUTION

Téléchargez Retrobar et lancez l'exécution. Windows peut empêcher son démarrage, car l'application n'est pas reconnue. Cliquez sur **Informations complémentaires** puis sur **Exécuter quand même**. Votre nouvelle barre des tâches est remplacée instantanément !

02› PERSONNALISER OU RETIRER

En faisant un clic droit sur un espace vide de cette dernière, via **Propriétés**, vous pourrez choisir parmi près de 20 modèles (Windows 95-98, Vista, XP, etc.). Pour revenir à votre configuration initiale, il vous suffit de faire un clic droit sur votre barre des tâches puis **Quitter RetroBar**.

LA FIN DU MOT DE PASSE ?

QUANTIQUE + IA = CRAQUAGE INSTANTANÉ

Chaque année, Hive Systems publie un tableau estimant le temps nécessaire pour qu'un mot de passe soit craqué par force brute. L'édition 2025 met en lumière des tendances inquiétantes, notamment l'accélération du craquage grâce à la puissance des GPU modernes et l'utilisation détournée d'outils d'IA comme ChatGPT. Et, en sous-texte, c'est l'arrivée d'ordinateurs quantiques qui sonne l'alerte.

Les mots de passe que nous pensions sécurisés il y a peu seraient désormais vulnérables en un temps record selon certaines hypothèses. Face à une attaque de type force brute, le temps nécessaire à un hacker bien équipé pour cracker votre sésame résiste plutôt bien grâce aux stratégies de défense de nos comptes en ligne, qui ont également beaucoup évoluées ces dernières années. Mais, dans son rapport 2025, la société Hive Systems explique aussi que l'association de deux facteurs récents change les règles du jeu : l'arrivée sur le marché, début janvier, d'une nouvelle génération de cartes graphiques et l'utilisation de l'IA comme effet démultiplicateur, tant en termes de puissance que de méthodologie.

En 2025, plus de puissance côté hacker, mais des défenses plus solides également.

1# EN, VRAI, ÇA A L'AIR DE BIEN SE PASSER, NON ?

Depuis sa première édition en 2020, le célèbre tableau de Hive Systems repose sur une simulation réaliste d'une attaque par force brute. L'objectif est d'estimer le temps nécessaire à un attaquant pour deviner un mot de passe, en partant de zéro, sans connaissance préalable. Chaque année, les équipes de Hive utilisent les matériels les plus performants et créent une configuration type qui est censée être équivalente à celle d'un hacker ou d'un groupe de hackers professionnels solidement équipés. Il est intéressant de constater que certains types de mots de passe qui étaient censés être « inviolables » il y a encore 5 ans sont désormais considérés comme trop faibles pour résister à une attaque sérieuse aujourd'hui.
Pour son étude 2025, Hive Systems a utilisé un pool de douze GPU Nvidia RTX 5090, les fameuses cartes graphiques de Nvidia, présentées au CES 2025 de Las Vegas. Ce matériel haut de gamme est accessible aux attaquants disposant de ressources conséquentes (comptez 2350 euros par carte RTX 5090). La société a également choisi de mettre en face (côté défense) l'algorithme de hachage « bcrypt » avec un facteur de travail de 32, reflétant les pratiques courantes en matière de stockage sécurisé des mots de passe. Cette base de défense renforce globalement la sécurité de vos identifiants et parvient, en moyenne, a contrer l'augmentation des puissances de calcul des pirates. Enfin, les équipes de Hive sont parties du principe que l'attaquant ne disposait d'aucune information préalable et devait tester toutes les combinaisons possibles. Concrètement, sans faire durer le suspense, voici ci-dessous les résultats du stress test avec cette configuration de base.

LA CARTE GRAPHIQUE RTX 5090 EST LA DERNIÈRE NOUVEAUTÉ PRÉSENTÉE PAR NVIDIA DÉBUT 2025. C'EST SA PUISSANCE DE CALCUL QUI A SERVI DE RÉFÉRENTIEL AUX ÉQUIPES DE HIVE SYSTEMS.

Comme indiqué dans ce tableau, et nous ne vous apprenons rien, plus un mot de passe est long et varié, plus il devient difficile à craquer, même avec du matériel très puissant. Les combinaisons de lettres, chiffres et symboles offrent une résistance bien supérieure… et exponentielle dès lors que vous ajoutez un seul caractère supplémentaire.
Mais, ce qui est le plus intéressant, par rapport au même

TEMPS NÉCESSAIRE AU DÉCHIFFRAGE D'UN MOT DE PASSE EN FONCTION DE SA COMPLEXITÉ EN 2025

LONGUEUR DU MOT DE PASSE	CHIFFRES UNIQUEMENT	LETTRES MINUSCULES	LETTRES MAJUSCULES ET MINUSCULES	LETTRES MAJUSCULES ET MINUSCULES, CHIFFRES	LETTRES MAJUSCULES ET MINUSCULES, CHIFFRES, SYMBOLES
4 caractères	Instantané	Instantané	Instantané	Instantané	Instantané
6 caractères	Instantané	46 minutes	2 jours	6 jours	2 semaines
8 caractères	Instantané	3 semaines	15 ans	62 ans	164 ans
10 caractères	1 jour	40 ans	41000 ans	238 000 ans	803000 ans
12 caractères	3 mois	27000 ans	111 millions d'années	917 millions d'années	3 milliards d'années
16 caractères	2000 ans	12 milliards d'années	812 000 milliards d'années	13 quadrillions d'années	94 quadrillions d'années
18 caractères	284000 ans	8 trillions d'années	2 quintillions d'années	52 quintillions d'années	463 quintillions d'années

DEPUIS LES DÉBUTS DE LA CRYPTOGRAPHIE, NOUS OBSERVONS UN JEU DU CHAT ET DE LA SOURIS PERMANENT ENTRE CEUX QUI CHIFFRENT ET CEUX QUI VEULENT PERCER LE COFFRE-FORT ! ET, POUR L'INSTANT, À CONDITION QUE LES UTILISATEURS SUIVENT LES CONSEILS QUI LEUR SONT DONNÉS EN PERMANENCE (ARRÊTEZ AVEC 123456 !), LES SOURIS CRYPTOGRAPHES GARDENT L'AVANTAGE SUR LES CHATS HACKERS.

tableau fourni par Hive en 2020 **(https://tinyurl.com/HiveSistems)**, c'est que l'on observe toujours une plutôt bonne résistance de nos sésames malgré la nette montée en puissance des capacités de calcul. Notamment grâce à la défense bcrypt, considérée désormais comme un standard largement répandu, même si c'est loin d'être la plus puissante. En 2020, Hive prenait encore la fonction de hachage cryptographique MD5 comme référentiel, déjà dépassée à l'époque. On le voit, malgré un arsenal Nvidia flambant neuf, les systèmes de défense se sont mis à niveau ! Mais malheur aux services et sites qui n'auraient pas suivi le mouvement général.

2# AVEC L'IA, C'EST UN PEU PLUS COMPLIQUÉ. BEAUCOUP PLUS.

Mais c'est là où Hive douche notre optimisme béat. Nous serions en fait à un point de bascule potentiel. Et les chats pourraient rafler la mise sous peu.
Hive Systems rappelle que les résultats de son étude ne valent qu'à condition de respecter trois hypothèses centrales :

1) L'HYPOTHÈSE DU HACKER INVESTISSANT DANS SON PROPRE MATÉRIEL

Les pirates achètent et créent leur propre configuration d'attaque avec les meilleures cartes et processeurs du marché, en espérant un retour sur investissement.
Hive fait une contre-hypothèse audacieuse dans son rapport : et si les hackers avaient accès, gratuitement, aux puissances de calcul les plus incroyables, actuellement, pour mener leurs attaques ? Mais de quoi parle-t-on ? Toutes les grandes puissances du monde sont en train de développer sur leur sol des fermes à IA, encore plus gigantesques que les fermes à Bitcoins. Et que se passerait-il si un groupe de hackers - voire un État - se mettait à utiliser les ressources dédiées à l'IA pour mener leurs attaques de temps à autre ?
Hive prend l'exemple de ChatGPT. D'après OpenAI, le modèle ChatGPT-3 a été entraîné sur 10 000 GPU Nvidia A100 tandis que le modèle ChatGPT-4 a été entraîné sur 20 000 GPU Nvidia A100. Et le modèle exécutant ChatGPT-3 et ChatGPT-4 utilise une combinaison de GPU A100 et H100, sans chiffre exact communiqué — seulement « plusieurs milliers »
« *Nous n'avons pas pu mettre la main sur 20 000 GPU A100 (ni même 10 000 !) pour faire des tests nous-mêmes* », explique Hive. « *Mais nous pouvons faire des déductions grâce à la façon dont les FLOPS évoluent proportionnellement avec les hashes.* ». Si on met une partie de cette puissance de calcul en face du test initial de Hive, voilà ce qu'il se passe ci-dessous :

TEMPS NÉCESSAIRE AU DÉCHIFFRAGE D'UN MOT DE PASSE EN FONCTION DE SA COMPLEXITÉ AVEC 20000 X A100, SOIT LA PUISSANCE QUI A ENTRAINÉ CHATGPT-4

LONGUEUR DU MOT DE PASSE	CHIFFRES UNIQUEMENT	LETTRES MINUSCULES	LETTRES MAJUSCULES ET MINUSCULES	LETTRES MAJUSCULES ET MINUSCULES, CHIFFRES	LETTRES MAJUSCULES ET MINUSCULES, CHIFFRES, SYMBOLES
4 caractères	Instantané	Instantané	Instantané	Instantané	Instantané
6 caractères	Instantané	Instantané	Instantané	Instantané	24 minutes
8 caractères	Instantané	43 minutes	1 semaine	1 mois	3 mois
10 caractères	Instantané	3 semaines	112 ans	325 ans	1000 ans
12 caractères	3 heures	37 ans	151 000 ans	1 million d'années	5 millions d'années
16 caractères	4 ans	16 millions d'années	1 trillion d'années	18 trillions d'années	128 trillions d'années
18 caractères	388 ans	11 milliards d'années	2 quadrillions d'années	71 quadrillions d'années	631quadrillions d'années

Comme on le voit, dès aujourd'hui, les milliards dépensés dans des fermes à IA pourraient donner des idées à certains. Il s'agit plus d'une vue de l'esprit qu'autre chose, mais cela montre que l'évolution technologique actuelle, même avec des composants de silicium bien traditionnels, permet de franchir un cap en termes de déchiffrement. Et le quantique nous direz-vous ? Vous avez compris l'idée, ne vous inquiétez pas, cela arrive un peu plus loin.

2) L'HYPOTHÈSE D'UNE BONNE VIEILLE ATTAQUE DE FORCE BRUTE

Dans le test de Hive, les pirates utilisent une attaque dite de force brute : il s'agit d'une méthode de piratage informatique qui consiste à tester automatiquement toutes les combinaisons possibles pour deviner un mot de passe,

une clé de chiffrement ou un identifiant de connexion. Les pirates utilisent des logiciels spécialisés pour ce faire (comme Hydra, John the Ripper, ou Hashcat) et automatisent l'essai, un par un, de chaque mot de passe possible, jusqu'à trouver le bon. Par exemple : si le mot de passe est abc123, l'attaquant va tester aaa000, aaa001, etc., jusqu'à tomber sur abc123. Cela peut prendre du temps et c'est là que la notion de puissance de calcul intervient pour accélérer le processus en testant jusqu'à plusieurs millions de mots de passe par seconde. Sauf que les hackers ne se contentent pas de la force brute, mais mènent des attaques hybrides (dites par dictionnaire ou par variations typiques).

3) L'HYPOTHÈSE DE LA BOITE NOIRE

Les hackers sont censés tout ignorer du mot de passe à trouver ! Pas un indice, rien, ils doivent tout tester ! Et en partant de zéro, le nombre de combinaisons à tester est juste d'ordre cosmologique dès lors que l'on dépasse les 8 caractères avec mélanges de lettres, chiffres et symboles. Mais il suffirait de connaître deux ou trois caractères pour que tout change (vous vous rappelez de la complexité exponentielle de ce type de série). Ou de tester des bases de données avec des combinaisons probables (même un million, ce n'est rien !) en fonction du profil cible. Et c'est là que l'IA intervient.

COMMENT UN PIRATE PEUT-IL TESTER DES MILLIERS DE MOTS DE PASSE ?

Les attaques en ligne par brute force sont quasiment impossibles sur des sites bien protégés. En revanche, une grande majorité des attaques se fait hors ligne, à partir de bases de données volées (LinkedIn, Adobe, Dropbox...). Mais les pirates de disposent que du « Hash », chiffré et inutilisable en l'état. C'est là qu'ils vont utiliser un outil spécialisé (comme Hashcat) pour tester chez eux, tranquillement, des milliers ou des millions de mots de passe jusqu'à produire un hash qui matche avec l'un de ceux qu'ils auront trouvés dans leur base de données ! Si une correspondance est trouvée, le mot de passe est compromis et l'attaquant peut venir le vérifier tranquillement sur le site cible.

ET SI TOUS LES SERVEURS DÉDIÉS À L'IA SE METTAIENT À CASSER DU CHIFFREMENT ? C'EST LE JEU INTELLECTUEL AUQUEL S'EST AMUSÉ HIVE EN SE BASANT SUR LES PUISSANCES DE CALCUL DÉCLARÉES DE OPENAI.

TRAVAIL PRÉMÂCHÉ

Hive souligne que les LLMs (Large Language Models) comme ChatGPT peuvent aujourd'hui être détournés pour générer ce type de listes. Par exemple : un hacker demande à ChatGPT de générer 1 000 mots de passe probables pour une personne appelée « Julie Martin », fan de jeux vidéo et née en 1995. Résultat : des propositions du type Julie1995, JMartin_95, ZeldaFan95... qui seraient rapidement testées par une attaque dite «hybride». Cela tombera certainement à l'eau avec ces quelques essais... mais n'oubliez pas qu'un hacker actuel bien équipé ne teste pas 1000 mots de passe... mais plusieurs millions.

Nos cerveaux humains, même en imaginant produire un mot de passe original, ont toujours besoin d'une clé logique leur permettant de se rappeler de leurs sésames. Et, si vous croyez être original, et bien désolé de vous décevoir, vous êtes des milliers à avoir choisi des stratégies d'élaboration de mot de passe plus ou moins similaires !

> La logique humaine est prévisible, en tout cas prédictible. Pas un mot de passe créé au hasard

C'EST ENCORE LA FAUTE DE L'HUMAIN !

Et grâce à l'IA, au brassage des bases de données de millions d'identifiants et de mots de passe déjà révélées sur le Darnket, les pirates n'avancent plus en terrain inconnu. L'IA leur fournit des correspondances statistiques optimisées en fonction de la cible et des infos glanées sur cette dernière. Si vous avez intégré des facteurs humains dans votre mot de passe (mot du dictionnaire, nom du site à l'envers, date ou code postal, etc.) : le hacker ne teste plus des milliards et des milliards de combinaisons possibles, mais des millions voire que quelques centaines de milliers. Si votre mot de passe est 1H5 !$e8P/£, bravo : le pirate n'aura pas assez d'une vie pour le déchiffrer. En revanche, si c'est (avec le même nombre de caractères) MiMi93edf$, l'étau se resserre autour de votre compte EDF ! Car vous avez utilisé des référentiels humains. Et c'est là que l'IA arrive à trouver des correspondances et des schémas cognitifs dans l'élaboration de nos mots de passe qui étaient inaccessibles auparavant.

Même si OpenAI impose des garde-fous pour bloquer les usages malveillants, certains utilisateurs contournent ces restrictions via des prompts déguisés ou en utilisant des clones open source de modèles d'IA.

3# ÈRE POST QUANTIQUE EN APPROCHE : ON VA TOUS CREVER !

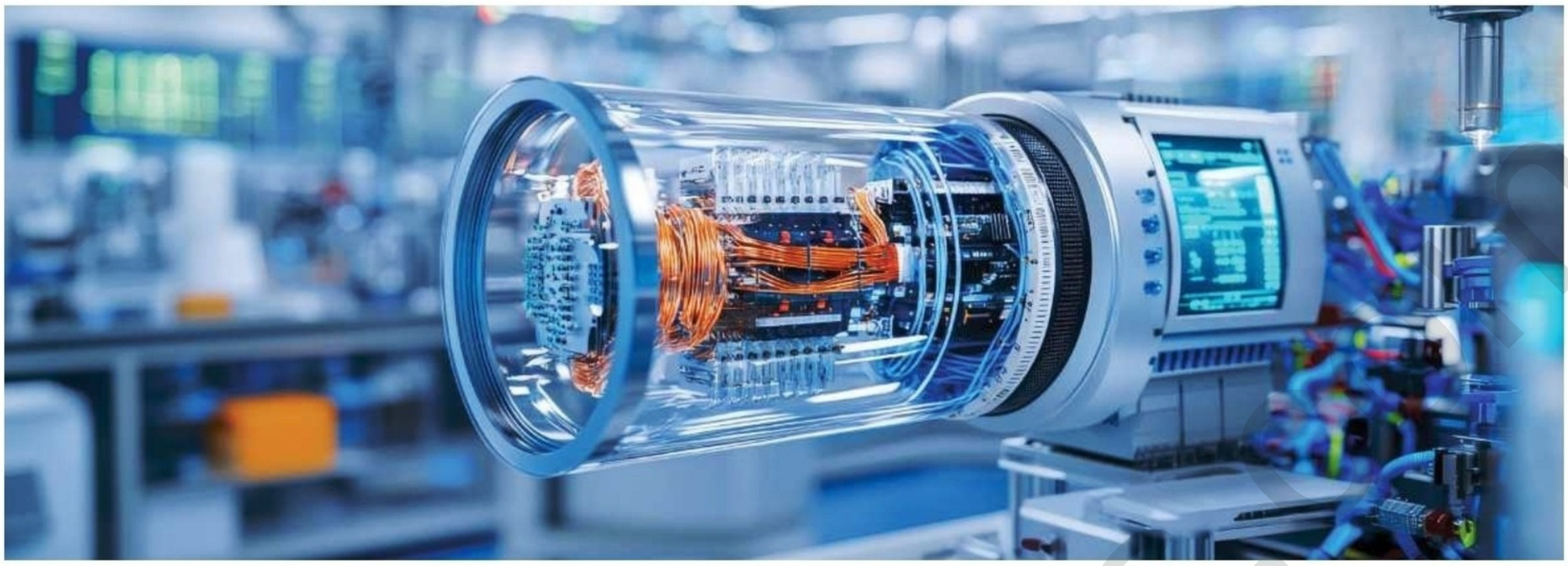
Savez-vous ce que font les Chinois (et certainement d'autres nations, ne soyons pas sectaires) en ce moment même, pendant que vous lisez cet article ? Ils aspirent des quantités phénoménales de données chiffrées, qu'ils ne savent pas décrypter pour l'instant, aux quatre coins du monde. Qu'elles viennent d'entreprises, d'États, de particuliers, de bases de données publiques ou privées : ils aspirent. Mais pourquoi nous direz-vous ? Parce que des chiffrements considérés comme inviolables aujourd'hui

seront brisés instantanément quand les ordinateurs quantiques seront déployés en dehors de leurs labos d'essais. Tout ce qui avait été tenu secret sera révélé si d'autres mesures de protection n'ont pas été prises. Oui, même le mail à votre tante Josiane envoyé le 8 mai 2022. L'ordinateur quantique – capable de résoudre en quelques secondes des problèmes que nos supercalculateurs actuels mettent des millénaires à traiter – pourrait rendre obsolètes nombre de technologies de chiffrement sur lesquelles repose toute notre sécurité numérique.

L'ÉPÉE DE DAMOCLÈS DE L'ALGORITHME DE SHOR

L'inquiétude repose principalement sur l'algorithme de Shor, un algorithme quantique développé en 1994, qui pourrait théoriquement briser le chiffrement RSA, encore largement

> Les premiers ordinateurs quantiques dignes de ce nom sont annoncés pour dans 10 ou 20 ans. Mais c'est maintenant qu'il faut se protéger d'eux !



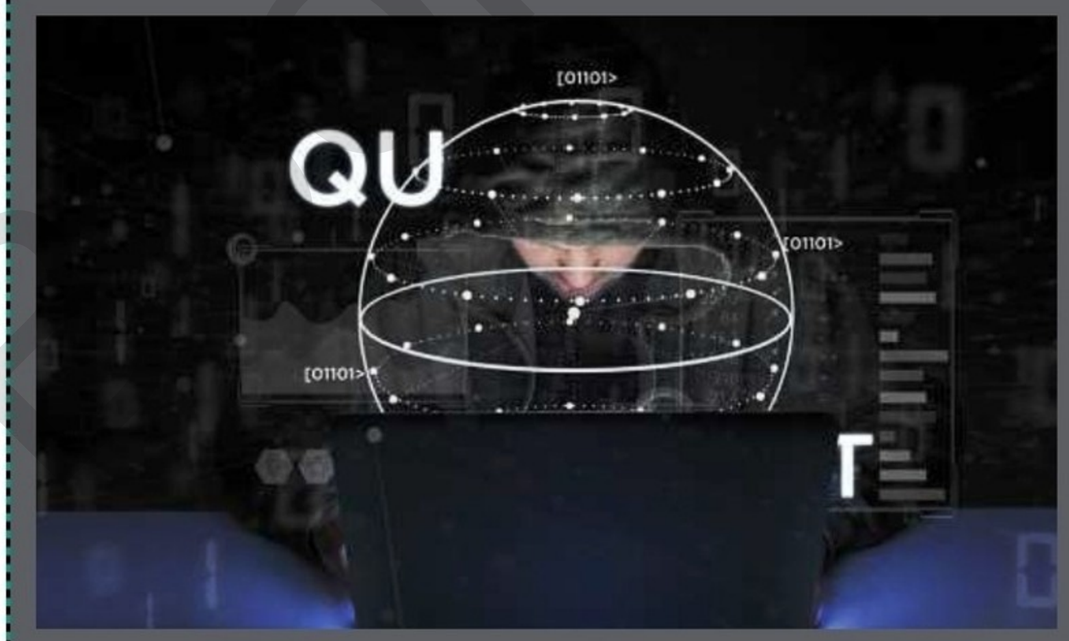
utilisé aujourd'hui pour sécuriser les communications, les signatures numériques ou les transactions bancaires. Le chiffrement RSA repose sur la difficulté, pour un ordinateur classique, de factoriser de très grands nombres premiers. Or, l'ordinateur quantique excelle justement dans ce genre de calcul parallèle.

Rassurons-nous : aucun ordinateur quantique n'est, à ce jour, capable de casser un chiffrement RSA 2048 bits. Il faudrait pour cela des millions de qubits logiques fiables, alors que les machines actuelles (comme celles d'IBM ou Google) en comptent quelques centaines au mieux, et avec une instabilité importante. On parle donc d'un horizon de 10 à 20 ans, selon la majorité des chercheurs.

Mais le risque, comme nous l'avons évoqué, est rétroactif. Comme le souligne Eva Maria Belser, chercheuse à l'Université de Fribourg, « *toutes les données interceptées aujourd'hui pourront être déchiffrées demain* » (Le Temps, 2023). Autrement dit, les espions numériques peuvent déjà stocker des communications chiffrées en attendant de les casser plus tard.

LA CRYPTOGRAPHIE POST-QUANTIQUE SE DÉPLOIE

Face à cette menace, une nouvelle discipline est en plein essor : la cryptographie post-quantique. Elle vise à développer des algorithmes résistants aux attaques d'ordinateurs quantiques… mais pouvant aussi être déployés sur les machines actuelles. En 2022, après un concours international lancé dès 2016, le NIST a annoncé la sélection de quatre premiers algorithmes post-quantiques, parmi lesquels : Kyber, pour le chiffrement général (remplaçant de RSA) ; Dilithium et



Falcon, pour les signatures numériques ; SPHINCS+, basé sur des arbres de hachage, également pour les signatures. "*Kyber et Dilithium devraient devenir les nouveaux piliers de la cybersécurité dans le monde post-quantique*", souligne Dustin Moody, cryptographe au NIST. Plus récemment, en mars 2024, le NIST a ajouté HQC (Hybrid Quasi-Cyclic), un algorithme français basé sur des codes correcteurs d'erreurs, fruit du travail de l'université de Limoges. « *On a "souffert" pour développer cet algorithme, alors l'attaquant lui aussi souffrira* », résume avec fierté Philippe Gaborit, coauteur de HQC.

Ces algorithmes reposent sur des problèmes mathématiques différents de ceux vulnérables à Shor, comme les réseaux euclidiens ou les arbres de hachage. Et bonne nouvelle : les premières implémentations sont déjà testées par des géants du numérique, à l'image de Cloudflare, IBM et Google, qui ont intégré Kyber dans des versions expérimentales de Chrome ou de leur infrastructure TLS. Cloudflare estime qu'en 2024, 40 % du trafic HTTPS est déjà sécurisé par ces nouveaux algorithmes, contre seulement 2 % l'année précédente.

L'EUROPE S'ORGANISE AUSSI

En parallèle du NIST, l'Europe s'active. L'ANSSI (France) et le BSI (Allemagne) mènent des travaux de standardisation, et le programme européen PQC-Europe vise à accompagner administrations et entreprises dans cette transition. Certaines banques testent déjà ces solutions pour leurs communications internes.

SÉLECTION

TOP 5 VPN GRATUITS

Cette année encore, Proton VPN conserve sa place de n°1. Windscribe, Hide Me et Tunnel Bear restent dans la sélection, mais vous observerez l'entrée d'un petit nouveau qui nous a enthousiasmés : PrivadoVPN qui fait la part belle au streaming et au P2P.

PROTON VPN – C'est qui l'patron ?!

C'est à Genève que nous retrouvons cette année encore notre chouchou : Proton VPN. Fruit du travail des ingénieurs du CERN et de ProtonMail, ce VPN suisse fait figure de rempart contre les regards indiscrets. Ici, pas de blabla marketing : tout est chiffré, audité, et transparent. En mai 2025, Proton VPN est le seul VPN gratuit du marché à offrir un trafic illimité, sans pub, sans collecte, sans compromis.

Illimité, mais seulement trois emplacements

Son interface, à la fois sobre et robuste, donne accès à trois emplacements (Japon, Pays-Bas, États-Unis) dans la version gratuite. C'est peu ? Oui. Mais ce que vous gagnez en sobriété, vous le conservez en anonymat total : politique «no-log» stricte, code open source, audit indépendant, et même un kill switch intégré pour les plus paranoïaques. En refusant toute concession avec des géants comme Google ou Amazon, Proton fait le pari rare de l'éthique sur le volume. Pas de P2P, pas de streaming dans la version gratuite — mais un tunnel sécurisé pour naviguer sans être pisté, ni vendu.

Lien : protonvpn.com/fr/free-vpn

WINDSCRIBE – 10 Go, 10 pays, 10 raisons de l'adopter

Il a l'accent de Toronto, l'âme d'un hacker indépendant, et un franc-parler qui en dit long sur son positionnement anti-GAFAM : Windscribe, c'est un VPN qui n'a pas peur de montrer les crocs. Dès son interface, simple et efficace, le ton est donné : «bloquez les pubs, chiffrez votre vie». Ici, les 10 Go de données mensuelles gratuites sont accompagnés de serveurs dans plus de 10 pays, du support P2P, et même d'un bloqueur de traqueurs intégré.

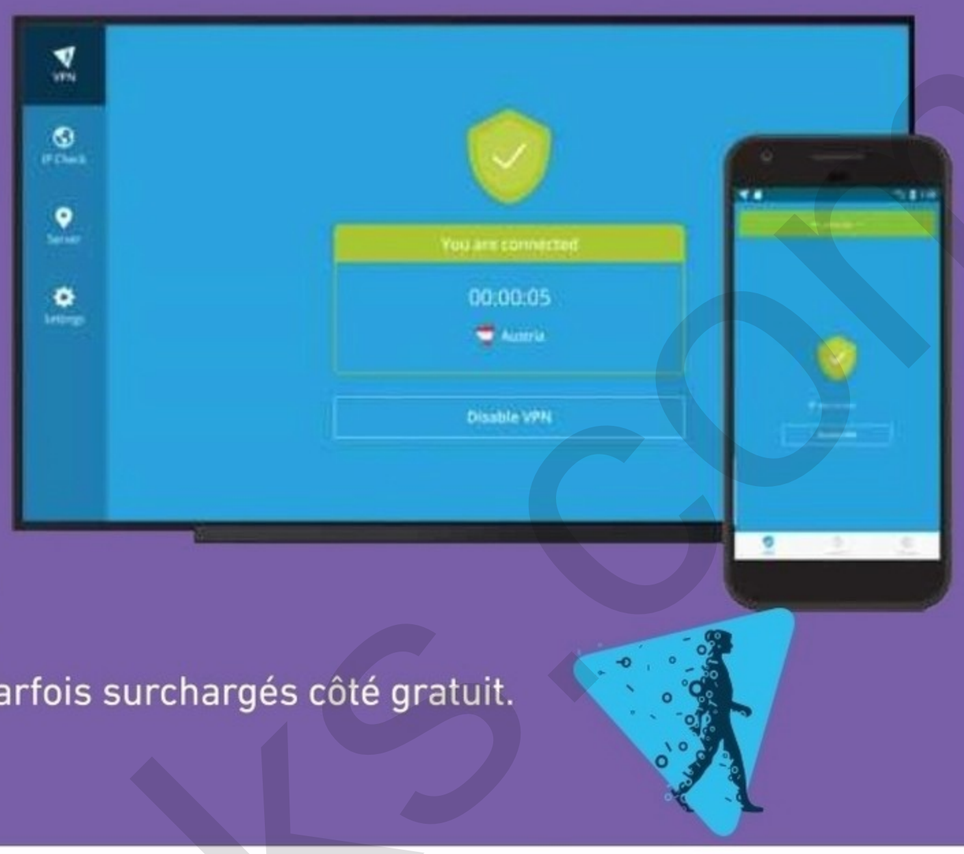
Les vrais savent

En mai 2025, il reste l'un des rares VPN à offrir une expérience de navigation riche sans inciter systématiquement à l'abonnement. Windscribe n'enregistre pas vos activités, et ses extensions (Firefox, Chrome) disposent de modules pour désactiver WebRTC (**lire page 36**) ou manipuler les headers. Certes, la version gratuite n'est pas illimitée, et certaines fonctions comme le double-hop ou le pare-feu restent réservées aux payants. Mais Windscribe est probablement le VPN gratuit le plus complet pour ceux qui veulent un service technique sans renier la confidentialité.

Lien : windscribe.com

HIDE.ME – Le méconnu qui coche (presque) toutes les cases

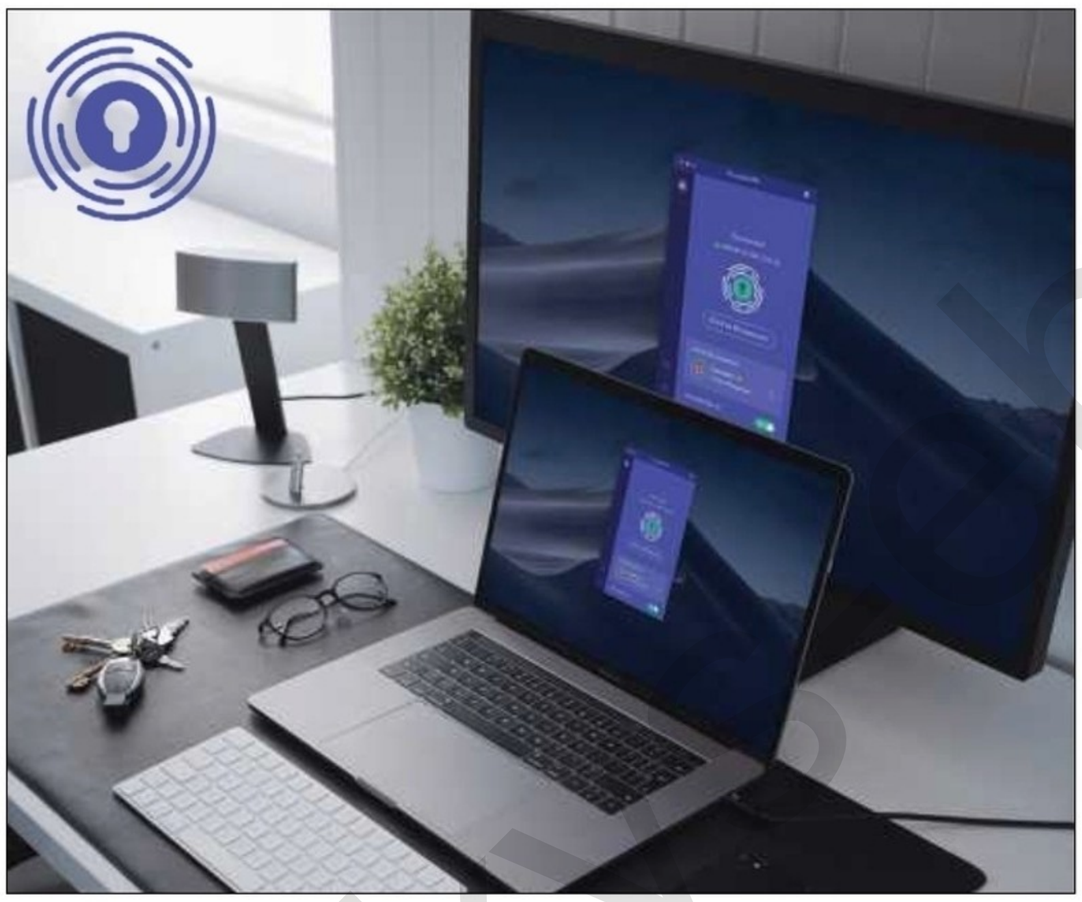
Il passe souvent sous le radar des comparatifs, et pourtant : hide.me coche en 2025 quasiment toutes les cases du VPN idéal… même dans sa version gratuite. Avec 10 Go de données mensuelles, 8 localisations de serveurs, une compatibilité P2P, un split tunneling finement paramétrable et un kill switch, hide.me offre une expérience qui flirte avec le premium.



Intuitif, simple, puissant

Basé en Malaisie, hors des alliances de surveillance type Five Eyes, hide.me affirme haut et fort sa politique "no logs" vérifiée par audit. Les applis sont bien conçues, notamment sur Windows et Android, avec des réglages détaillés pour les utilisateurs avancés. La navigation est fluide, les vitesses stables, et la protection DNS/IP est activée par défaut. Dommage toutefois que les performances en streaming soient encore aléatoires et que certains serveurs soient parfois surchargés côté gratuit.

Lien : hide.me/fr



PRIVADOVPN – Un petit Suisse caliente

Discret, mais ambitieux, PrivadoVPN incarne l'émergence d'un nouveau modèle hybride : celui du VPN gratuit pensé pour les streamers et les téléchargeurs occasionnels, sans vendre l'âme de ses utilisateurs. En mai 2025, la formule gratuite offre 10 Go/mois, un accès à 13 serveurs (y compris aux États-Unis et au Royaume-Uni), ainsi qu'une compatibilité Netflix et iPlayer déjà reconnue.

Il met le Kill switch dans le papier d'alu

Le fournisseur suisse mise sur une architecture sécurisée avec chiffrement AES-256, protocole WireGuard, et bien sûr une politique de confidentialité stricte. Sa neutralité helvétique garantit un certain équilibre entre ouverture fonctionnelle (streaming, P2P) et rigueur sécuritaire (pas de journaux, kill switch inclus).
Ce qu'on regrette : la nécessité de créer un compte, et l'absence de vérification indépendante à ce jour. Mais pour un usage mixte "anonymat + contenu", c'est un très bon compromis.

Lien : privadovpn.com

TUNNELBEAR – Pour les débutants… avec des oreilles d'ours

On le confondrait presque avec un gadget marketing. Et pourtant, TunnelBear est un vrai VPN, avec un vrai engagement pour la vie privée. Derrière son interface ludique à base de tunnels d'ours se cache une politique «no log» certifiée, un chiffrement robuste, et un logiciel open source audité chaque année. La version gratuite accorde seulement 2 Go de données par mois, ce qui le limite à des usages ponctuels.

Raaaâh, mais c'est facile !

Mais TunnelBear reste un formidable point d'entrée dans le monde des VPN pour les néophytes. L'expérience est fluide, les serveurs sont répartis dans plus de 20 pays, et l'installation ne prend que 30 secondes, montre en main. L'interface est si simple que même un enfant pourrait s'y connecter (mais ne lui dites pas !).
On regrette son rachat par McAfee (pas bien), qui suscite des interrogations sur son indépendance. Et ses fonctions avancées sont quasi inexistantes. Mais pour les novices, difficile de faire plus rassurant.

Lien : www.tunnelbear.com

DECRYPTAGE

FUITES WEBRTC : LA FAILLE INVISIBLE QUI SABOTE VOTRE ANONYMAT

Vous utilisez un VPN, pensez être invisible en ligne, naviguez sous les radars… et pourtant, un site peut toujours identifier votre véritable adresse IP. Cette fuite, aussi sournoise que courante, a un nom : WebRTC. Déployée massivement par les navigateurs modernes pour améliorer les communications en ligne, cette technologie pose aujourd'hui de graves questions de confidentialité, notamment pour les journalistes, les militants, les professionnels du renseignement… et tous les utilisateurs qui se croient à l'abri derrière un VPN.

WEBRTC, QU'EST-CE QUE C'EST EXACTEMENT ?

WebRTC (pour Web Real-Time Communication) est une technologie développée par Google en 2011, aujourd'hui intégrée nativement à la plupart des navigateurs (Chrome, Firefox, Edge, Brave, etc.).
Elle permet les communications audio, vidéo ou de partage de fichiers en temps réel, sans passer par un serveur central.

> Malgré l'usage d'un VPN, votre adresse IP et donc votre identité ne sont pas à l'abri d'une fuite. Comment vérifier et s'en protéger ?

En pratique, c'est ce qui permet à des services comme Google Meet, Discord, Jitsi ou même des services de transfert de fichiers peer-to-peer de fonctionner directement dans le navigateur, sans plugin externe.

LE PROBLÈME : WEBRTC PEUT EXPOSER VOTRE IP RÉELLE

Pour établir des connexions directes entre deux utilisateurs (connexion P2P), WebRTC utilise un mécanisme appelé STUN (Session Traversal Utilities for NAT). Ce processus oblige le navigateur à interroger les interfaces réseau de la machine, y compris votre adresse IP publique réelle… même si vous utilisez un VPN.
Résultat ? Un site malicieux peut insérer un simple script JavaScript dans sa page Web pour forcer votre navigateur à révéler :
- Votre adresse IP locale (LAN)
- Votre adresse IP publique réelle, non protégée par le VPN.
Cela se fait silencieusement, sans pop-up ni demande d'autorisation. Votre identité est donc traçable ainsi que le suivi marketing, la possibilité d'attaques ciblées, etc.

UNE TECHNOLOGIE À ENCADRER

WebRTC n'est pas une faille de sécurité à proprement parler : c'est une fonctionnalité, mais mal encadrée par les navigateurs. Avec l'essor de la vidéoconférence Web, des plateformes peer-to-peer, du télétravail, du métavers, WebRTC continuera de se généraliser. Et si les navigateurs ne mettent pas en place une gestion plus fine (autorisation site par site, alertes en cas d'exposition d'IP), cette technologie restera une porte dérobée au pistage.

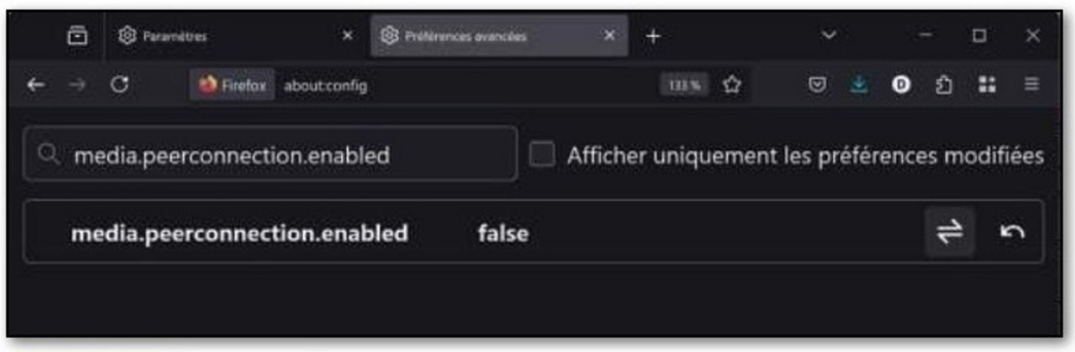
COMMENT SE PROTÉGER ?

PRATIQUE

Désactiver WebRTC peut limiter certains services spécifiques comme des messageries passant par le navigateur (Google Meet, Discord Web, Jitsi Meet, ztc.) ou certains services de transferts (Snapdrop, ShareDrop, ...) voire des services de surveillance à distance passant également par le navigateur. Mais, généralement, cela n'aura pas ou peu d'impact sur les usages Web habituels.

01› DÉSACTIVER WEBRTC DANS VOTRE NAVIGATEUR

> Firefox : Tapez **about:config** dans la barre d'adresse. Cherchez **media.peerconnection.enabled**. Passez-le **à False**.



> Brave : Paramètres > Boucliers > Protection contre WebRTC. Cochez **Empêcher WebRTC de révéler l'adresse IP locale**.

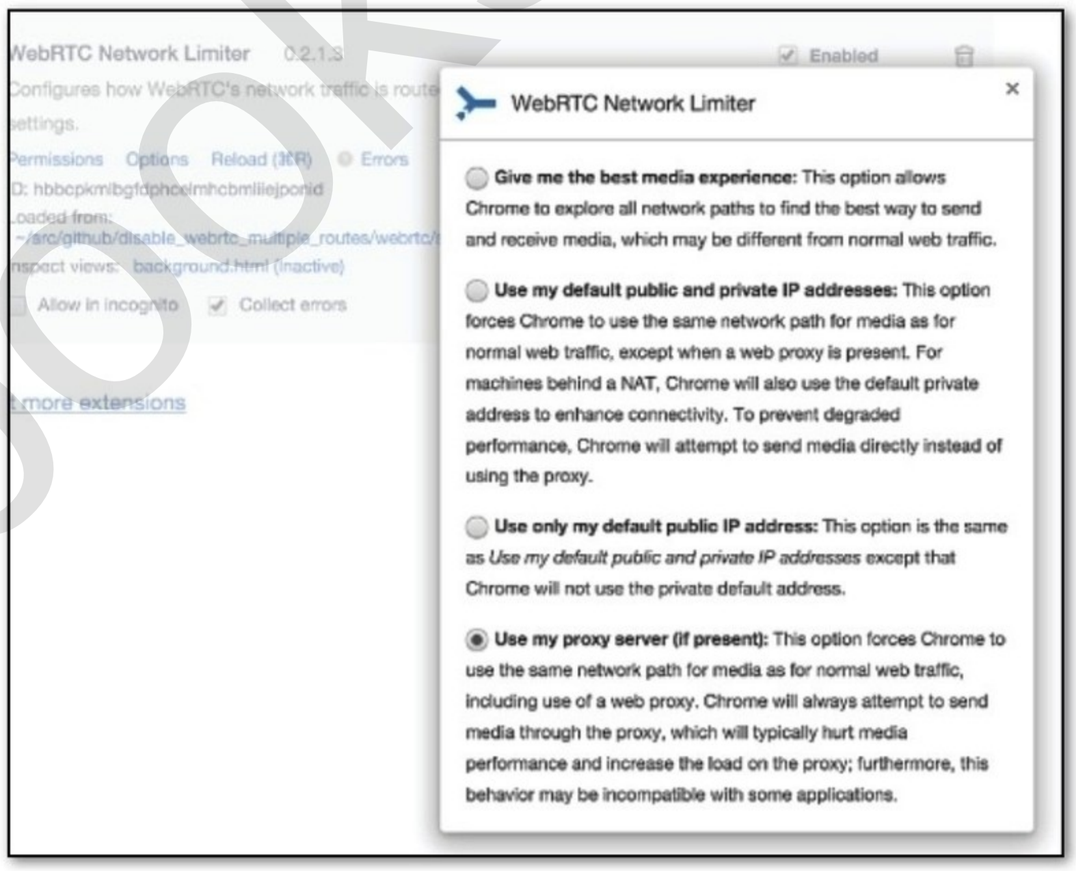
> Chrome/Edge : Pas de désactivation possible native via les paramètres. Utilisez l'extension WebRTC Control.

02› UTILISER UN NAVIGATEUR ORIENTÉ VIE PRIVÉE

Sur Tor et LibreWolf, par exemple, WebRTC est désactivé par défaut. Sans que vous ayez besoin d'intervenir dans about:config ni d'installer une extension.

03› EXTENSIONS SÉLECTIVES

Certaines extensions (comme **uBlock Origin** ou **WebRTC Network Limiter**) permettent de forcer WebRTC à n'utiliser que les IP relayées (et non votre IP locale ou réelle), ce qui réduit le risque sans casser complètement les appels audio/vidéo ou les services P2P que vous utilisez via le navigateur.



04› TESTER VOTRE EXPOSITION

Un service comme IP Leaks vous dira si votre IP réelle fuite, notamment suite à une compromission WebRTC. Nous vous présentons un tutoriel complet page suivante.

INFOS [IPLeaks] Où le trouver ? [https://ipleak.net.] Difficulté :

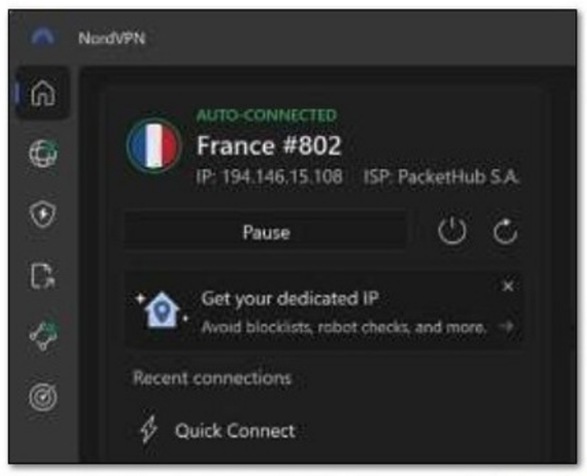
IPLEAKS : VÉRIFIEZ LES FUITES DE VOTRE IP MÊME AVEC UN VPN

PRATIQUE

Même avec un VPN actif, certaines technologies peuvent révéler votre véritable identité numérique. Des techniques comme WebRTC, le DNS non chiffré ou le fingerprinting peuvent exposer votre adresse IP réelle ou d'autres informations sensibles, compromettant ainsi votre anonymat.

01 › PRÉPARER VOTRE ENVIRONNEMENT

Avant de lancer le test, si vous utilisez un VPN, activez-le avant d'ouvrir ipleak.net. Fermez les autres onglets inutiles. Idéalement, utilisez un navigateur propre ou en navigation privée pour éviter les biais liés au cache.



02 › ACCÉDER AU SITE

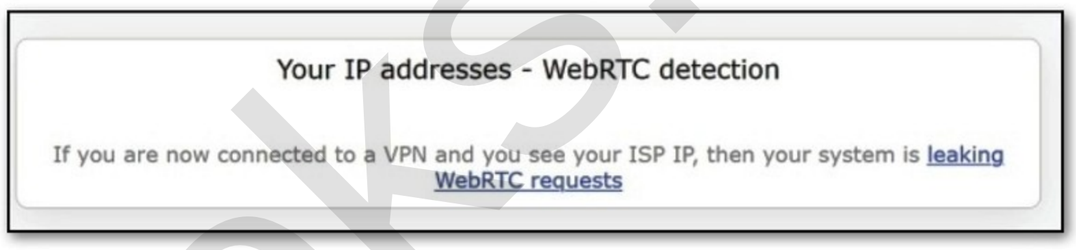
Rendez-vous sur **https://ipleak.net**. Le test se lance automatiquement. Vous verrez apparaître en quelques secondes plusieurs blocs d'informations.

03 › BLOC IP ADRESS

Il affiche l'adresse IP publique avec laquelle vous êtes vu sur Internet. Si vous n'utilisez pas de VPN, ce sera l'adresse fournie par votre FAI. Si vous utilisez un VPN, vous devriez voir l'adresse IP du serveur VPN ainsi que le nom d'hôte et la géolocalisation approximative (ville/pays). Si ces informations ne correspondent pas à votre VPN ou si deux IP s'affichent, dont l'une appartient à votre FAI, cela signifie que votre IP réelle fuite !

04 › BLOC WEBRTC DETECTION

Nous vous en parlions précédemment, le protocole WebRTC permet la communication directe entre navigateurs (vidéoconférence, P2P) mais peut exposer votre IP locale ou réelle, même avec un VPN. Si une IP publique (de votre FAI) apparaît : votre VPN est contourné par WebRTC.



05 › BLOC DNS ADRESSES

Ce bloc affiche les serveurs DNS utilisés pour résoudre les noms de domaine. Si vous voyez les DNS de votre FAI, votre anonymat est compromis : le VPN ne protège pas vos requêtes DNS. Vous devriez voir ici les DNS du VPN ou ceux que vous avez configurés (ex : Cloudflare, NextDNS). Ce test est l'un des plus importants : une fuite DNS est l'une des principales failles des VPN mal configurés.

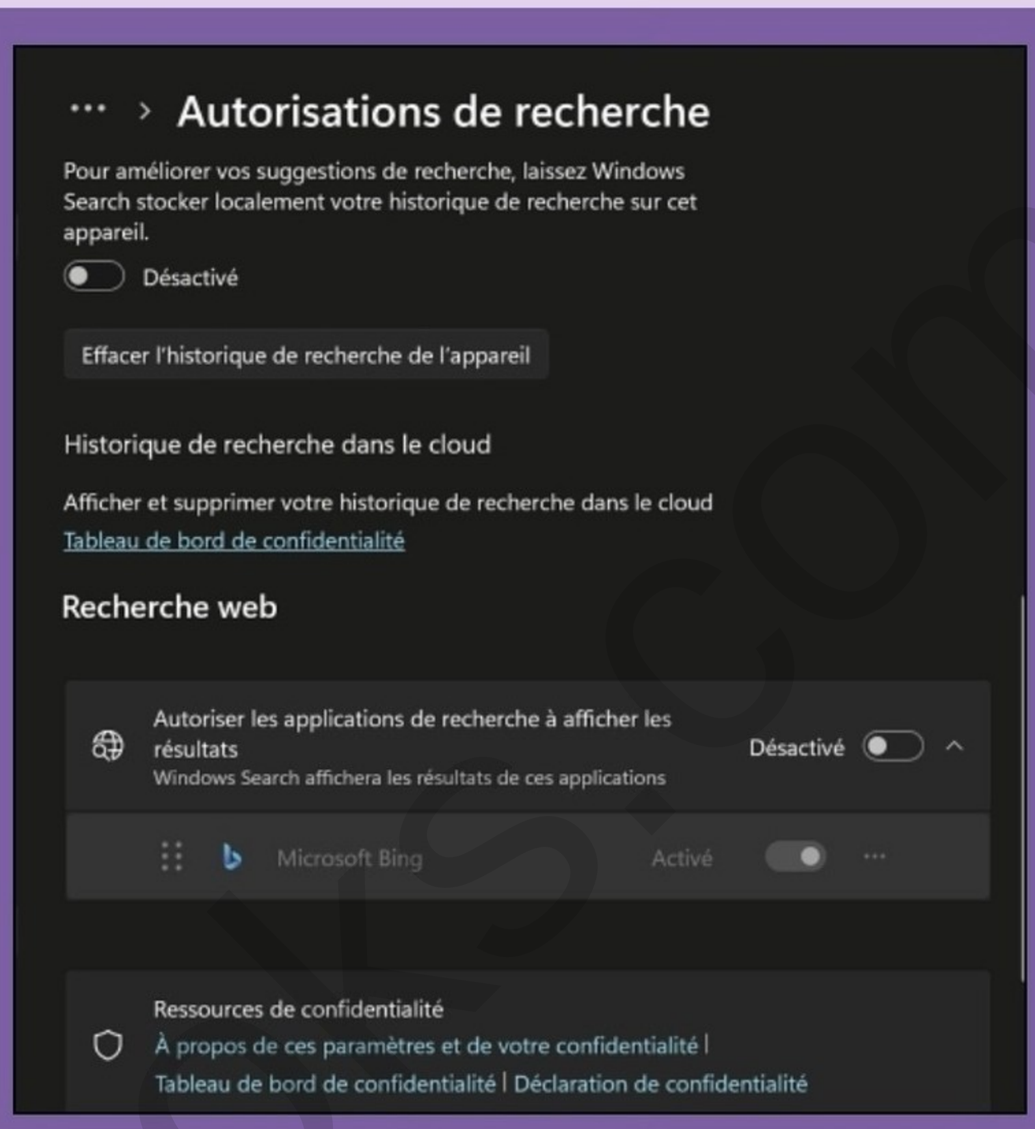
06 › VÉRIFIER UN SERVEUR SUSPICIEUX

Si vous avez un doute sur un serveur DNS, cliquez sur celui qui vous intéresse. Vous obtiendrez plus de détails. Après vérification, le serveur DNS montré en exemple et présent dans notre liste est bien utilisé par notre VPN même s'il est fourni par un prestataire partenaire. Pas de fuite donc.

Empêcher Microsoft d'envoyer vos recherches à Bing

> AVEC WINDOWS 11

Chaque fois que vous tapez quelque chose dans la barre de recherche du menu Démarrer, Windows ne se contente pas de fouiller votre disque dur : par défaut, votre requête est aussi transmise à Microsoft Bing, le moteur de recherche en ligne. Objectif ? Proposer des résultats web ou des recommandations… au prix de votre historique de recherche envoyé aux serveurs de Microsoft. Vous pouvez facilement désactiver cette fonctionnalité.
Pour Windows 11, ouvrez les **Paramètres** via **Windows + I**, allez sur **Confidentialité et sécurité > Recherche dans Windows** et descendez jusqu'à la section **Autorisations de recherche**. Vous pouvez désactiver toutes les autorisations de cette nouvelle fenêtre, notamment **Autoriser les applications de recherche à afficher les résultats** en bas de page.

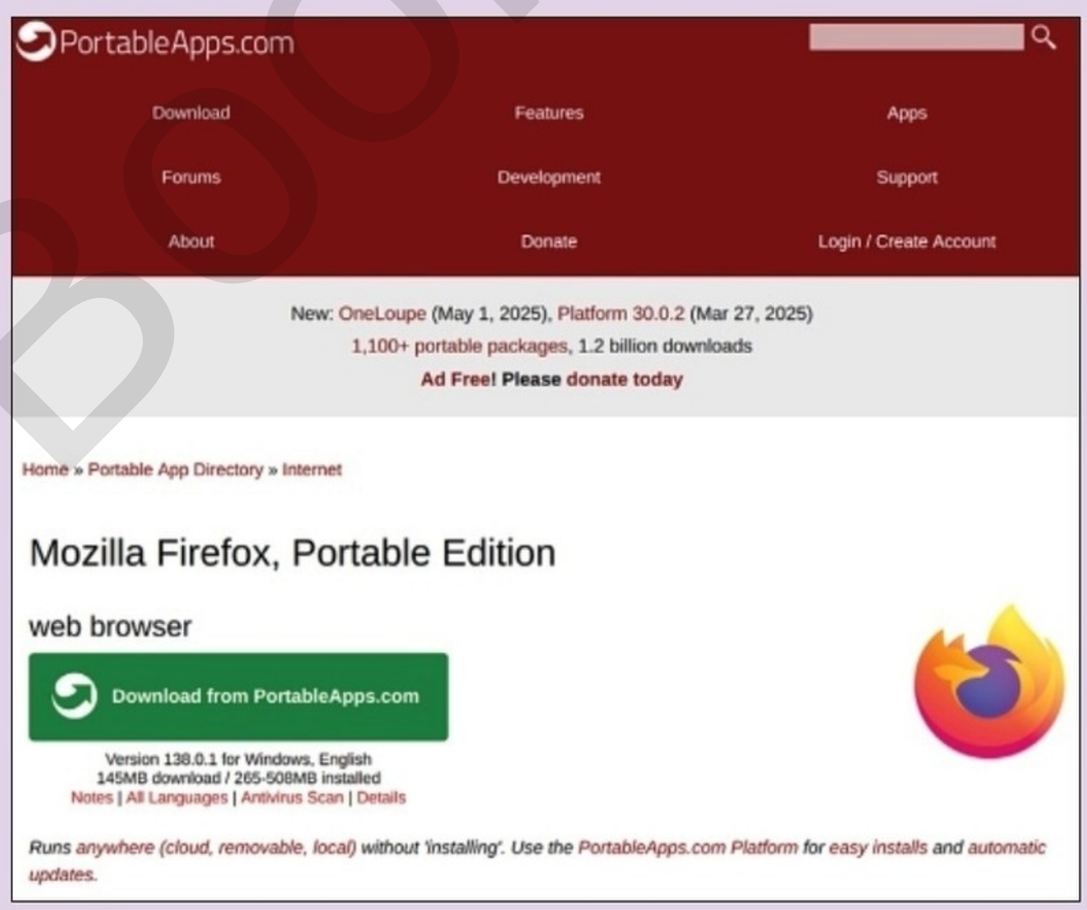


Utiliser un navigateur portable pour les navigations sensibles

> AVEC FIREFOX

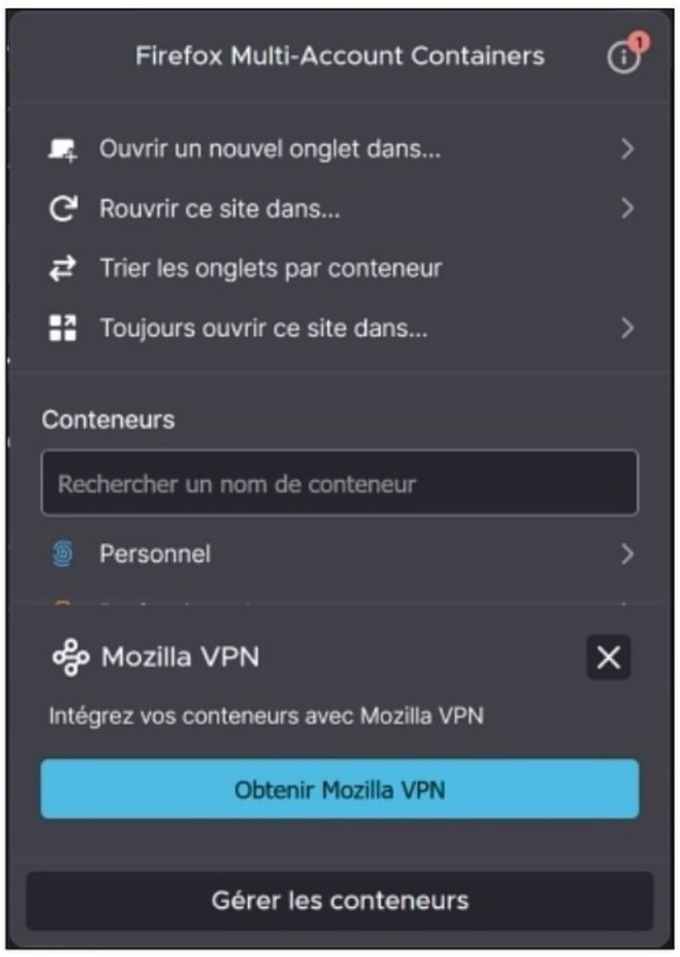
Un navigateur portable, tel que Firefox Portable, peut être exécuté depuis une clé USB sans laisser de traces sur l'ordinateur hôte. Téléchargez **Firefox Portable** depuis **PortableApps.com**.
Une fois l'exécutable **.paf.exe** téléchargé, double-cliquez pour lancer l'installation. Cette dernière ne modifie pas votre système. Le navigateur s'exécutera depuis le dossier où vous l'installez, comme sur une clé USB ! Allez ensuite dans l'emplacement choisi sur votre clé et double-cliquez sur **FirefoxPortable.exe**. Firefox démarre dans une version autonome, sans affecter votre Firefox habituel (s'il existe).

Lien : portableapps.com/apps/internet/firefox_portable



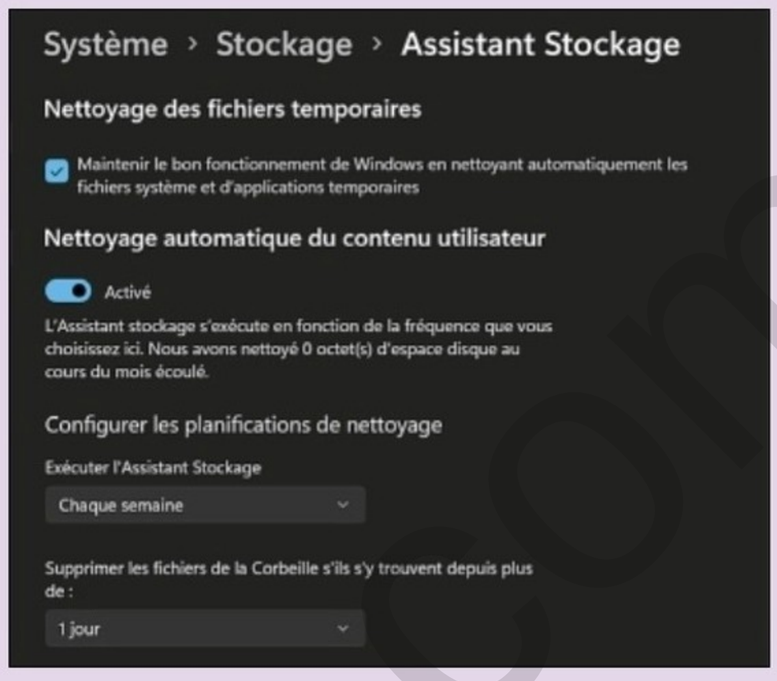
Containers : Cloisonner ses activités ! > AVEC FIREFOX

Firefox Multi-Account Containers est extension pour Firefox qui vous permet de séparer vos différentes identités en ligne (travail, personnel, shopping) dans des «conteneurs» isolés. Chaque conteneur fonctionne comme un profil distinct, avec ses propres cookies, sessions et stockage local. Cela empêche le suivi inter-sites et vous permet de rester connecté à plusieurs comptes simultanément sans interférence.



Ajoutez l'extension depuis le site officiel. Cliquez sur l'icône de l'extension dans la barre d'outils puis sélectionnez **Gérer les conteneurs** puis **Ajouter un conteneur**. Attribuez un nom, une couleur et une icône à chaque conteneur. Ouvrez un nouvel onglet dans le conteneur souhaité pour naviguer avec l'identité correspondante.

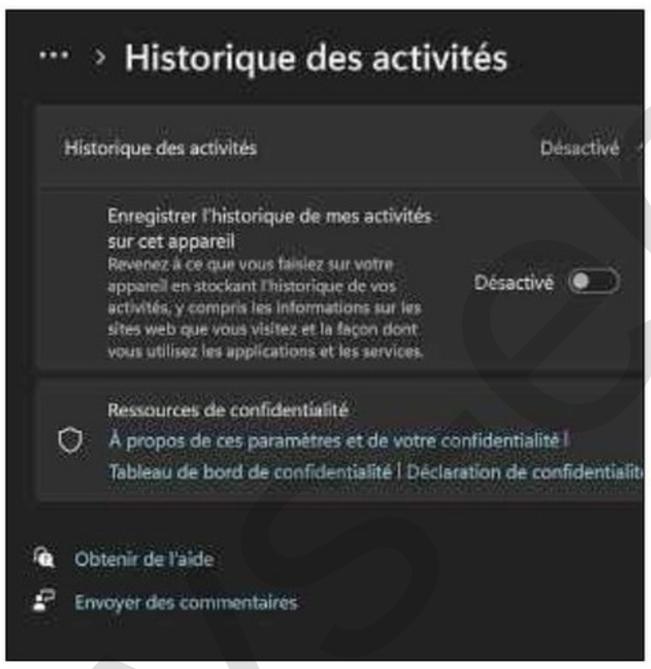
Supprimer automatiquement les fichiers temporaires et historiques > Avec Windows



L'Assistant de stockage de Windows 11 permet de libérer de l'espace disque en supprimant régulièrement les fichiers inutiles, tels que les fichiers temporaires et les éléments de la Corbeille. Et cela renforce aussi la confidentialité des données stockées sur votre PC !
Ouvrez les **Paramètres** (Windows + I) et allez dans **Système > Stockage**. Activez l'**Assistant de stockage**. Cliquez sur **Configurer l'Assistant de stockage ou l'exécuter maintenant**. Sous **Exécuter l'Assistant de stockage**, choisissez la fréquence souhaitée (par exemple, **Chaque semaine**).
Configurez les options de suppression :
- **Supprimer les fichiers de la Corbeille s'ils y sont depuis plus de :** sélectionnez une durée.
- **Supprimer les fichiers du dossier Téléchargements s'ils n'ont pas été ouverts depuis plus de :** sélectionnez une durée.

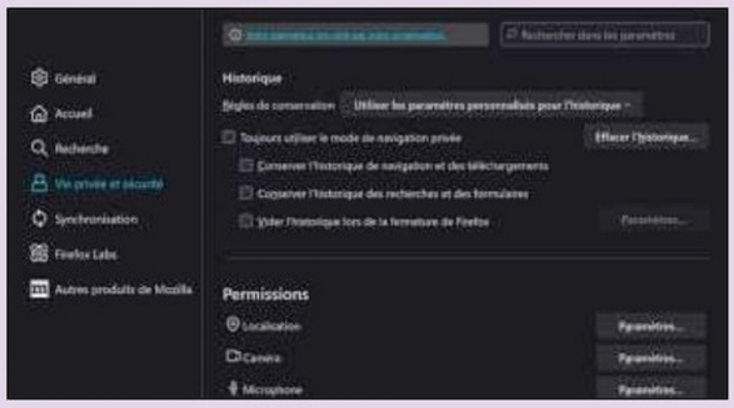
L'Assistant de stockage nettoiera désormais automatiquement votre système selon vos préférences.

Désactiver l'historique d'activité > Avec Windows 11



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

Activer la navigation privée permanente > Avec Firefox



La navigation privée empêche Firefox de sauvegarder votre historique, vos recherches, vos cookies et vos fichiers temporaires. Pourquoi ne pas activer le mode privé par défaut pour ce navigateur ?
Cliquez sur le menu (☰) puis sur **Paramètres**. Dans l'onglet **Vie privée et sécurité**, descendez jusqu'à la section **Historique**. Dans le menu déroulant, sélectionnez **Utiliser des paramètres personnalisés pour l'historique**. Cochez la case **Toujours utiliser le mode de navigation privée**. Redémarrez Firefox pour appliquer les modifications. Désormais, toutes vos sessions Firefox s'ouvriront en mode privé par défaut.

Vérifier les accès récents au microphone et à la webcam > Avec Windows

Surveiller l'utilisation de votre microphone et de votre webcam peut vous aider à détecter des activités suspectes ou non autorisées. Ouvrez les **Paramètres** (**Windows + I**). Allez dans **Confidentialité et sécurité > Microphone**. Faites défiler vers le bas pour voir la liste des applications ayant récemment accédé à votre microphone, avec les horodatages. Répétez l'opération pour la caméra en revenant à **Confidentialité et sécurité > Caméra**.

Comme dans une série américaine, le papier peut revenir pendant plusieurs saisons.

La force de tous les papiers, c'est de pouvoir être recyclés au moins cinq fois en papier. Cela dépend de chacun de nous.
www.recyclons-les-papiers.fr

Tous les papiers ont droit à plusieurs vies.
Trions mieux, pour recycler plus !

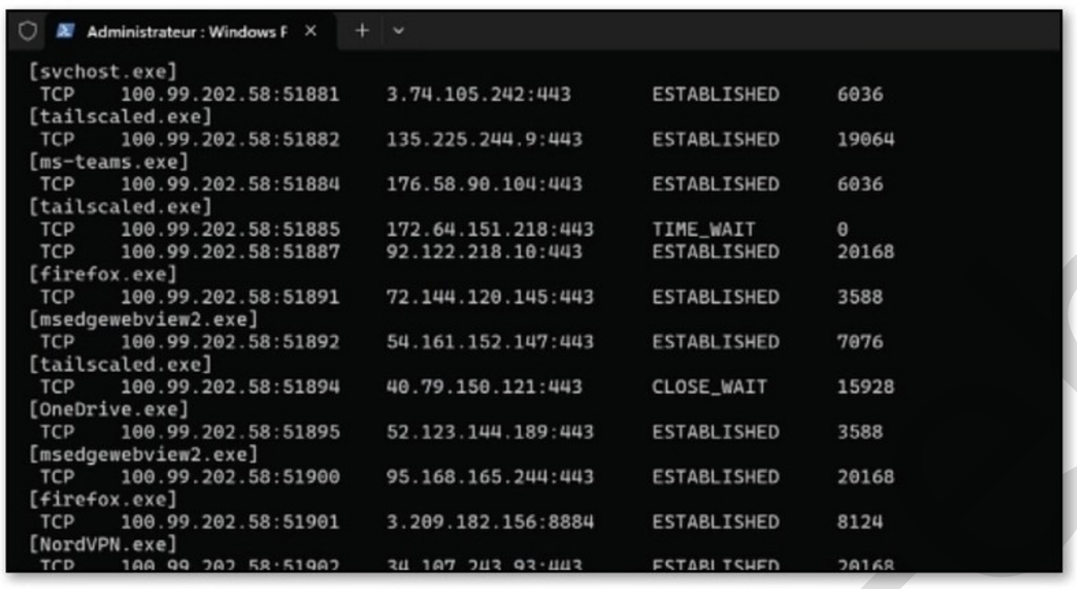
INFOS [Windows + AbuseIPdb + PQualityScore]
Où le trouver ? [abuseipdb.com ; tinyurl.com/ipquality]
Difficulté : ☠☠☠

VÉRIFIEZ SI VOTRE PC FAIT PARTIE D'UN BOTNET (ET COMMENT RÉAGIR)

Un botnet est un réseau de machines infectées et contrôlées à distance par des cybercriminels. Sans le savoir, votre PC peut être utilisé pour envoyer des spams, lancer des attaques DDoS, miner des cryptomonnaies, ... Parfois, aucun symptôme n'est visible à l'œil nu. D'où l'intérêt d'un diagnostic réseau discret.

01› NETSTAT + WHOIS 1/2

Ouvrez Invite de commandes en mode administrateur **(Windows + x > Terminal (admin))** et tapez **netstat -anob**. Recherchez les connexions étranges ou multiples vers des IP distantes.



02› NETSTAT + WHOIS 2/2

Copiez une IP suspicieuse et collez-la sur **whois.domaintools.com** ou **abuseipdb.com**. Des connexions actives vers des IP russes, chinoises ou hébergées sur des serveurs anonymes (sans raison connue) peuvent indiquer une compromission.

03› PQUALITYSCORE 1/2

Vous pouvez aussi utiliser des scanners spécialisés et gratuits. Nous vous conseillons PQualityScore. Cet outil en ligne analyse votre adresse IP pour détecter une activité suspecte, telle que l'utilisation de proxies, VPNs ou la participation à un botnet. Retrouvez-le ici : **https://tinyurl.com/ipquality**

04› PQUALITYSCORE 2/2

PQualit yaffiche directement votre IP. Confirmez en l'écrivant à nouveau dans le champ Check if this IP is a bot: et validez. L'outil en ligne vous indique alors si votre IP est susceptible d'être corrompue ou non. Attention, PQuality évalue l'adresse IP publique de votre connexion. Si vous utilisez un VPN ou un proxy, les résultats refléteront l'adresse IP de ces services.

SYMPTÔMES D'UNE POSSIBLE INFECTION PAR UN BOTNET

Soyez attentif aux signes suivants, qui peuvent indiquer que votre ordinateur est compromis :
- Ralentissement inhabituel du système ou de la connexion Internet,
- Activité réseau anormale, même lorsque vous n'utilisez pas activement Internet,
- Présence de processus inconnus dans le gestionnaire des tâches,
- Comportement étrange du système, comme des redémarrages inattendus ou des messages d'erreur inhabituels.

SÉLECTION

VOUS ÊTES INFECTÉ ?

TOP 3 MEILLEURS OUTILS ANTIBOT

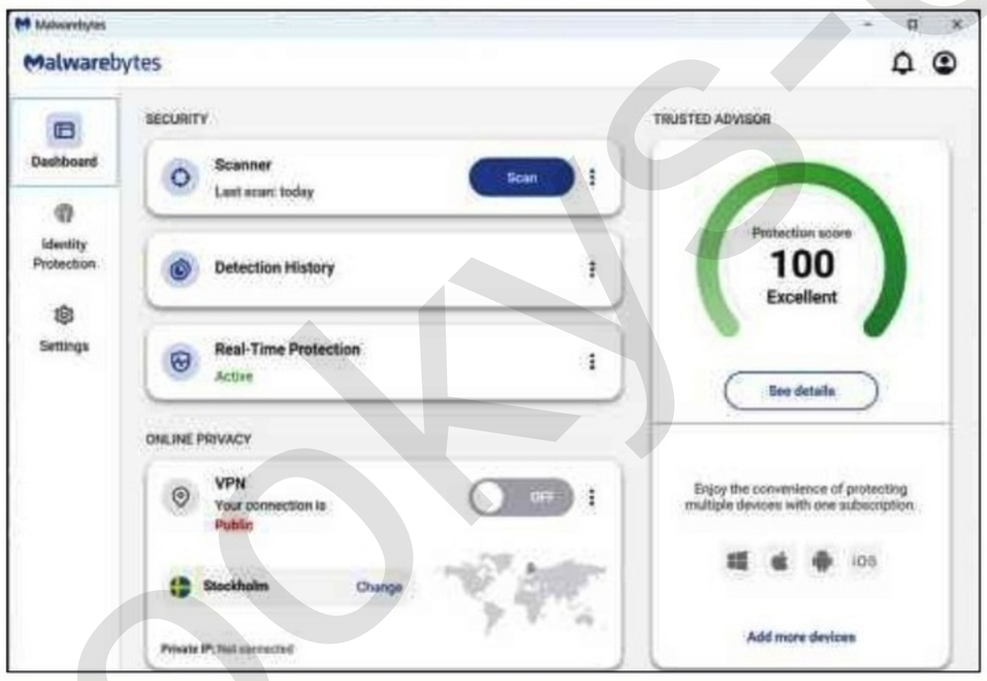
Si votre antivirus habituel a laissé passer un botnet, c'est qu'il n'est peut-être pas en mesure de le repérer et encore moins de l'éliminer. Il faut mobiliser des outils spécialisés, capables de détecter les connexions suspectes, les processus invisibles ou les modules installés en profondeur. Voici les 3 solutions les plus efficaces en 2025.

MALWAREBYTES

> LE NETTOYEUR DE CHOC

Depuis une décennie, Malwarebytes s'est taillé une réputation de bulldozer dans la lutte contre les malwares actifs. Sa version gratuite, bien qu'elle ne propose pas de protection en temps réel, reste l'une des plus redoutables pour éliminer une infection déjà présente. Là où d'autres se contentent d'identifier, Malwarebytes agit : il détecte et supprime les fichiers associés à des C&C (serveurs de commande et contrôle), nettoie les clés de registre modifiées, et désactive les tâches planifiées créées par les bots pour survivre aux redémarrages. L'interface est accessible, le moteur rapide et sa base est particulièrement efficace contre les familles de trojans spécialisés dans le botnet.

Lien : www.malwarebytes.com/fr



ESET ONLINE SCANNER

> LE SCANNER D'ÉLITE EUROPÉEN

L'éditeur slovaque ESET, reconnu pour la fiabilité de son antivirus NOD32, propose un outil redoutablement efficace pour les situations d'urgence : ESET Online Scanner. Ici, pas besoin d'abandonner votre antivirus habituel ou d'installer quoi que ce soit de permanent : un simple exécutable suffit à lancer une analyse complète, à la demande. Le programme scanne la mémoire vive, le registre système,

les programmes au démarrage, et surtout, il inspecte les fichiers dormants pouvant abriter un bot prêt à s'activer. L'interface est claire, les faux positifs rares, et l'utilisateur guidé à chaque étape.

Lien : www.eset.com/fr/online-scanner

NORTON POWER ERASER

> UN PEU D'AGRESSIVITÉ DANS CE MONDE DE BOTS

Développé par l'équipe de NortonLifeLock, Power Eraser est un outil radical. Il ne fait pas de cadeau aux logiciels suspects, quitte à s'exposer à des faux positifs. Ce scanner s'adresse aux utilisateurs avertis, qui veulent creuser plus loin lorsqu'un comportement douteux persiste malgré d'autres analyses. Particulièrement efficace contre les rootkits et les fichiers système détournés, Norton Power Eraser dispose d'un mode de scan agressif capable de redémarrer l'ordinateur pour inspecter le système avant même le démarrage de Windows. Il vérifie aussi les connexions réseau, les processus lancés et les fichiers exécutables contre une base cloud en temps réel. À manier avec prudence, donc, mais il peut faire la différence quand tous les autres outils ont échoué.

Lien : us.norton.com/support/tools/npe.html

TUTO

CRÉEZ UN ACCÈS WI-FI TEMPORAIRE POUR PARTAGER VOTRE CONNEXION

Transformer votre PC en hotspot Wi-Fi avec un SSID et un mot de passe temporaires est une astuce aussi pratique que méconnue. Un outil de partage ponctuel malin, idéal pour les geeks nomades ou précautionneux.

Partager sa connexion Internet, oui — mais pas n'importe comment et avec n'importe qui ! Plutôt que de communiquer le mot de passe principal de votre box Wi-Fi, pourquoi ne pas générer un accès temporaire, sécurisé et personnalisé via votre PC sous Windows ?
C'est possible, grâce à une fonction native, méconnue, mais puissante : le réseau hébergé («hosted network»), disponible depuis Windows 7 et encore fonctionnel sous certaines configurations de Windows 10 et 11.

COMMENT ÇA FONCTIONNE ?

La fonctionnalité repose sur la commande netsh wlan intégrée à Windows, qui transforme un PC doté d'un adaptateur Wi-Fi compatible en point d'accès logiciel (soft AP). Le système crée alors une nouvelle interface Wi-Fi virtuelle émettrice, avec un Nom du réseau (SSID) personnalisé et un Mot de passe (clé WPA2) temporaire (minimum 8 caractères). Le chiffrement est de type WPA2. Le routage du trafic Internet est assuré depuis la connexion principale vers les appareils connectés à ce réseau temporaire.

ATTENTION

Votre PC devra être équipé d'une carte Wi-Fi compatible avec le mode Hosted Network (la plupart des puces Intel le sont) et pouvoir exécuter les commandes avec un compte administrateur. N'oubliez pas enfin que ce réseau hébergé n'est pas permanent : il disparaîtra au redémarrage et nécessitera une reconfiguration partielle à chaque fois que vous en aurez besoin. C'est aussi une sécurité : si vous avez de bonnes raisons de donner un accès temporaire à un contact, vous n'aimeriez sans doute pas que cet accès devienne permanent.

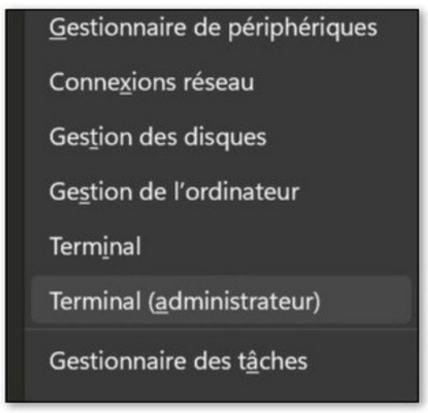
NOUVEAU HOTSPOT TEMPORAIRE AVEC WINDOWS

PRATIQUE

Nous travaillons ici sur un PC équipé de Windows 11, mais cette fonction existe depuis Windows 7. Les chemins d'accès sont différents d'un OS à l'autre, mais le principe reste le même.

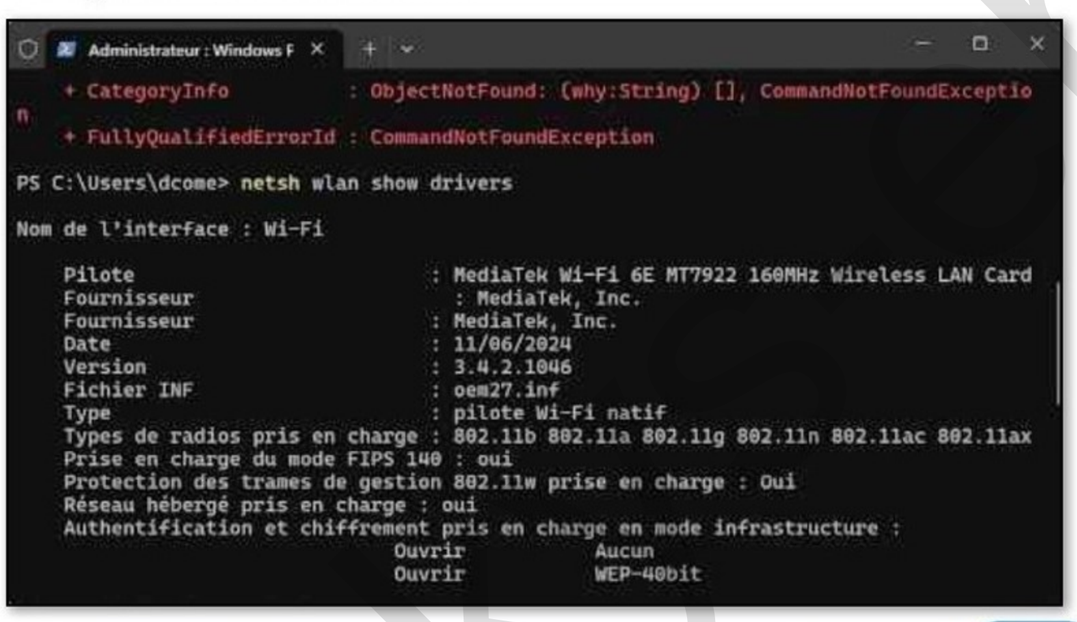
01› CARTE RÉSEAU COMPATIBLE 1/2

Prérequis : vous devez vérifier la compatibilité de votre carte Wi-Fi. Avant de commencer, assurez-vous que votre carte réseau prend en charge le mode Hosted Network : Ouvrez l'invite de commandes en tant qu'administrateur : appuyez simultanément sur **Windows + X** et sélectionnez **Invite de commandes (admin)** ou **Terminal Windows (admin).**



02› CARTE RÉSEAU COMPATIBLE 2/2

Tapez la commande suivante : **netsh wlan show drivers**
Recherchez la ligne : **Prise en charge du réseau hébergé : Oui**
Si la réponse est «Non», votre carte réseau ne prend pas en charge cette fonctionnalité.

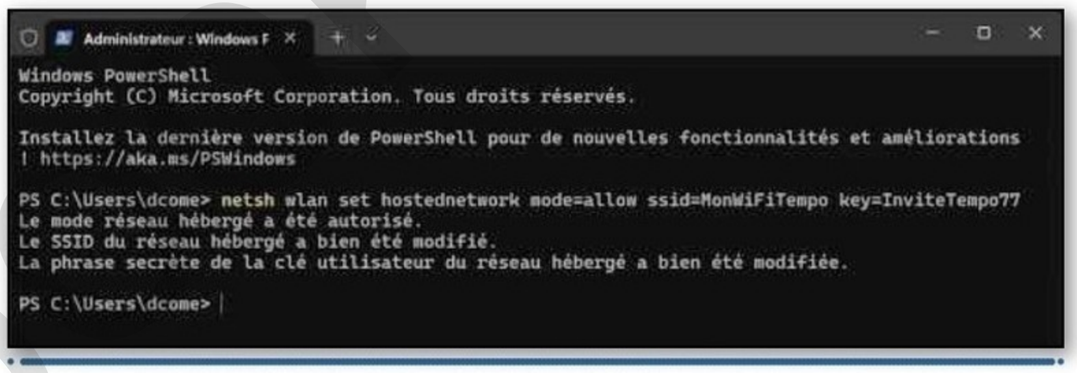


UN ACCÈS TEMPORAIRE PERMANENT ?

L'accès Wi-Fi temporaire créé avec la commande netsh wlan set hostednetwork n'est pas permanent. Le réseau hébergé est désactivé automatiquement à chaque redémarrage ou sortie de veille prolongée. La connexion partagée (dans l'onglet **Partage de votre carte réseau**) est également désactivée au redémarrage. Si vous utilisez un script manuel, vous devrez le relancer à chaque session pour réactiver le réseau. Mais, heureusement, les paramètres du réseau (ssid et key) restent mémorisés dans Windows tant que vous ne tapez pas la commande :
netsh wlan set hostednetwork mode=disallow
Vous n'aurez donc pas besoin de reconfigurer le nom du réseau et son mot de passe à chaque fois, seulement de relancer le réseau avec :
netsh wlan start hostednetwork

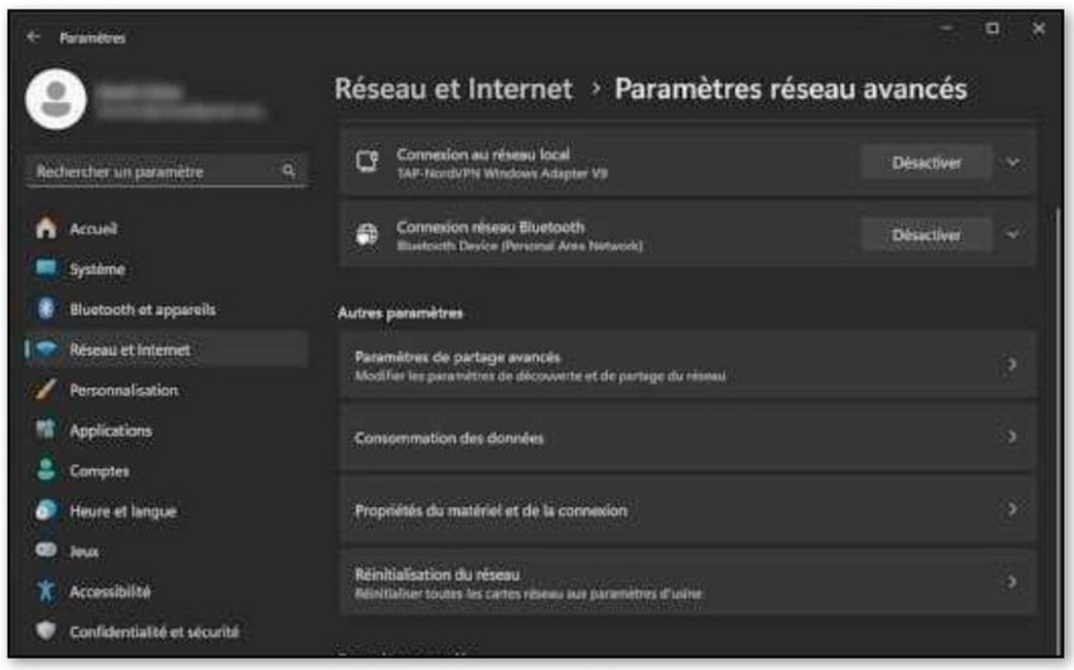
03› CRÉATION DE L'ACCÈS TEMPORAIRE

Toujours dans l'invite de commandes en tant qu'administrateur, tapez maintenant la commande suivante (en remplaçant « NomDuReseau » et « MotDePasse » par les nouveaux identifiants de votre choix) :
netsh wlan set hostednetwork mode=allow ssid=NomDuReseau key=MotDePasse
Démarrez ensuite le réseau avec la commande :
netsh wlan start hostednetwork
Votre PC émettra alors un réseau Wi-Fi avec le nom et le mot de passe spécifiés.



04› DONNER L'ACCÈS 1/2

Pour permettre aux appareils connectés d'accéder à votre Internet, ouvrez les paramètres de votre carte réseau. Allez dans **Paramètres > Réseau & Internet** puis faites défiler vers le bas et cliquez sur **Paramètres réseau avancés.** Sous la section **Paramètres associés**, cliquez sur **Plus d'options d'adaptateur.**



05› DONNER L'ACCÈS 2/2

Dans la nouvelle fenêtre, faites un clic droit sur l'adaptateur ayant accès à Internet (Wi-Fi ou Ethernet) et sélectionnez **Propriétés**. Allez dans l'onglet **Partage**. Cochez la case **Autoriser d'autres utilisateurs du réseau à se connecter via la connexion Internet de cet ordinateur**. Dans le menu déroulant, sélectionnez **Connexion réseau sans fil associée au réseau hébergé**. Cliquez sur **OK**.

SÉLECTION

TROUSSE DE SECOURS NUMÉRIQUE DU VOYAGEUR

Voyager, c'est s'ouvrir au monde, mais aussi exposer ses données personnelles à de nombreux risques : connexions Wi-Fi non sécurisées, vols de matériel, ou encore surveillance numérique. Voici une sélection d'outils incontournables pour voyager l'esprit tranquille.

PROTON VPN > Le meilleur VPN gratuit pour sécuriser votre WiFi

Vous êtes à l'aéroport d'Istanbul, et vous vous connectez au Wi-Fi gratuit pour consulter vos e-mails ou, inconscient que vous êtes !, faire un paiement en ligne. Sans VPN, votre trafic est lisible comme une carte postale. Avec Proton VPN, tout est chiffré de bout en bout. Votre adresse IP, même dans des pays à surveillance renforcée, et le VPN suisse ne garde aucun de vos logs. Dans sa version gratuite, ProtonVPN vous offre des serveurs dans 3 pays avec une bande passante illimitée, sans pub. Vitesse modérée, mais largement suffisante pour la navigation ou le streaming.

Lien : protonvpn.com

BITWARDEN > Ne perdez jamais un mot de passe, même à l'autre bout du monde

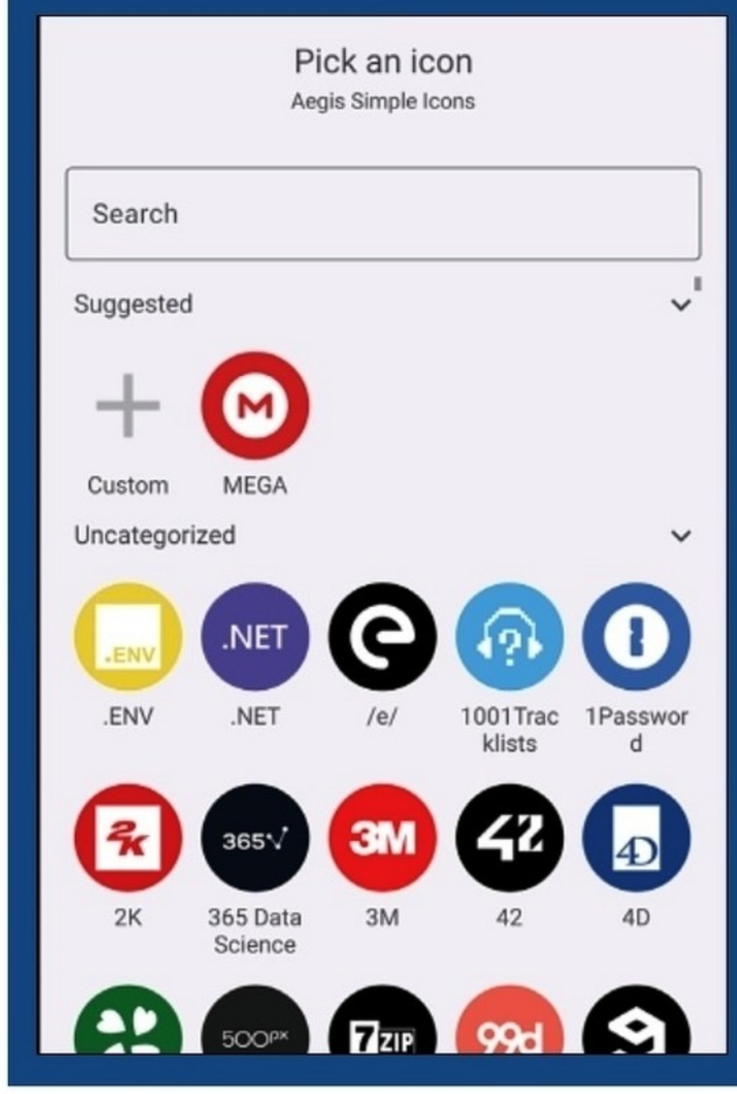
Vous avez besoin d'accéder à votre banque en ligne, mais vous ne vous souvenez plus du mot de passe (que vous avez bien fait de rendre complexe). Bitwarden vous le fournit instantanément. Ce coffre-fort chiffré centralise vos mots de passe, notes sécurisées, numéros de carte, etc. Il dispose même d'un mode offline, très pratique si vous êtes sans réseau.

Lien : bitwarden.com

AEGIS AUTHENTICATOR > Gardez vos codes 2FA hors des griffes de Google

Vous vous connectez à GitHub ou ProtonMail depuis un cybercafé à Bangkok. Le site vous demande un code 2FA. Aegis le génère localement, sans cloud, sans risque. Cette alternative libre à Google est garantie sans fuite de données. Aegis prend en charge les algorithmes HOTP et TOTP qui sont conformes aux normes de l'industrie et largement pris en charge, ce qui rend Aegis compatible avec des milliers de services en ligne.

Lien : github.com/beemdevelopment/Aegis



ARIANE

> Être alerté en cas de crise, partout dans le monde

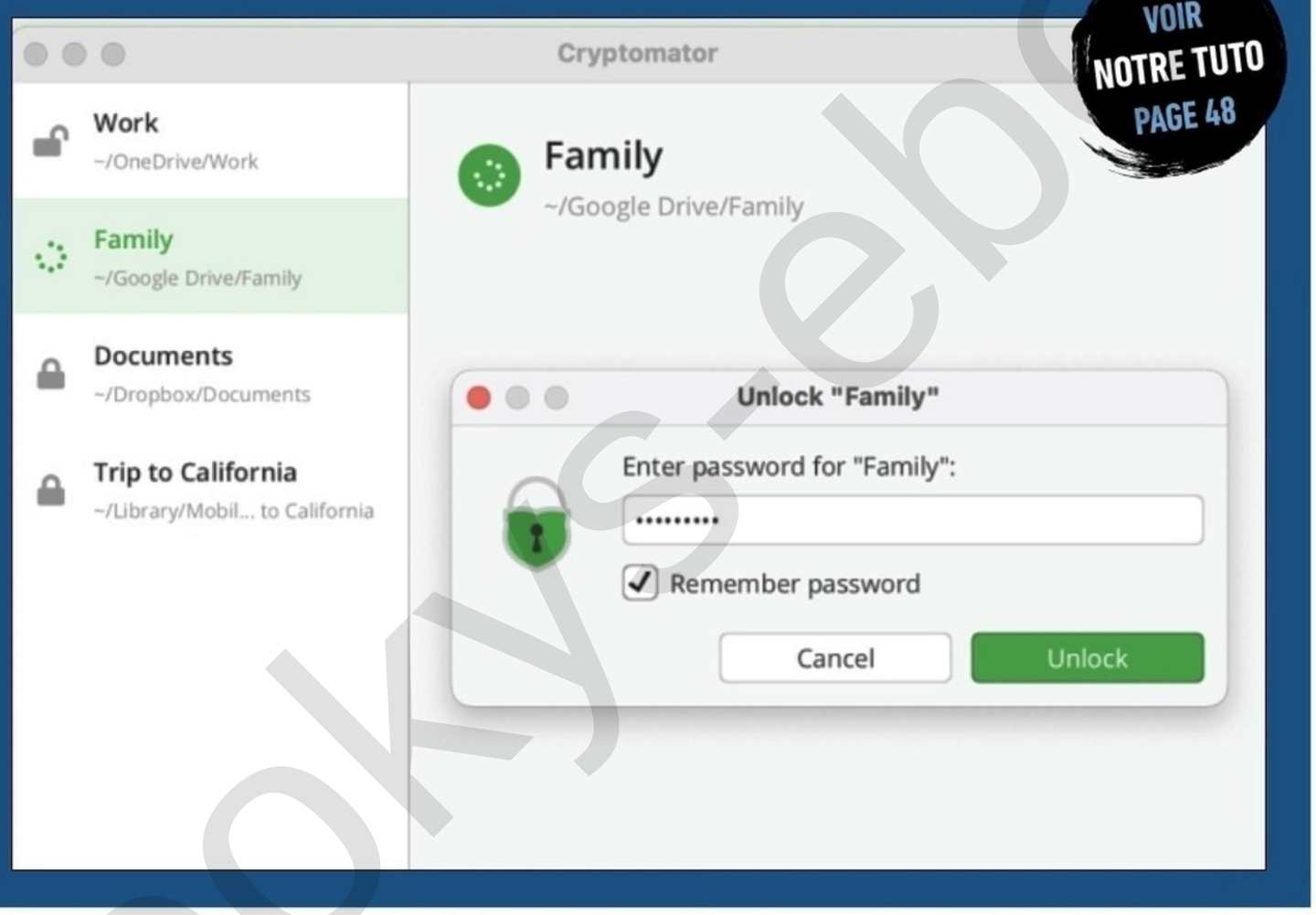
Vous êtes au Chili lors d'un tremblement de terre. Grâce au service Ariane, vous recevez immédiatement un SMS du consulat français avec les consignes. En vous inscrivant avant le départ, en cas de catastrophe ou de crise politique, vous êtes identifié et localisable. Ariane permet aux autorités de contacter également vos proches si vous le souhaitez.

Lien : pastel.diplomatie.gouv.fr/fildariane

CRYPTOMATOR > Chiffrez vos documents avant même de les envoyer dans le cloud

Vous sauvegardez vos papiers d'identité et billets d'avion dans Google Drive. Avec Cryptomator, vous les cryptez vous-même, sans confier les clés à Google. Idéal pour voyager avec des documents sensibles (CNI, passeport, contrats) et compatible avec les grands services de cloud gratuits.

Lien : cryptomator.org



SIGNAL > Discuter librement, même depuis une dictature

Vous êtes en Égypte ou à Dubaï, et vous devez envoyer un message à un proche. WhatsApp ou Messenger sont parfois filtrés ou peu sûrs. Signal vous garantit le chiffrement de bout en bout même en cas de censure. Aucune métadonnée collectée (pas même qui parle à qui, ni quand). Même les appels audio/vidéo sont sécurisés, fonctionnant même avec une mauvaise connexion. Signal est utilisée par les journalistes, les ONG et même Edward Snowden. Tout est dit.

Lien : signal.org

MAPS.ME > Ne jamais être perdu, même sans réseau

Vous partez en trek en Géorgie, sans connexion. L'application Maps.me vous permet de naviguer hors-ligne avec des cartes détaillées et gratuites. Elles sont téléchargeables en amont et offrent des infos pertinentes pour les itinéraires à pied, en voiture, à vélo (même les sentiers) avec intégration d'éléments locaux (distributeurs, restaurants, parkings...). Pratique en zones rurales, ou dans les pays où le roaming coûte un rein.

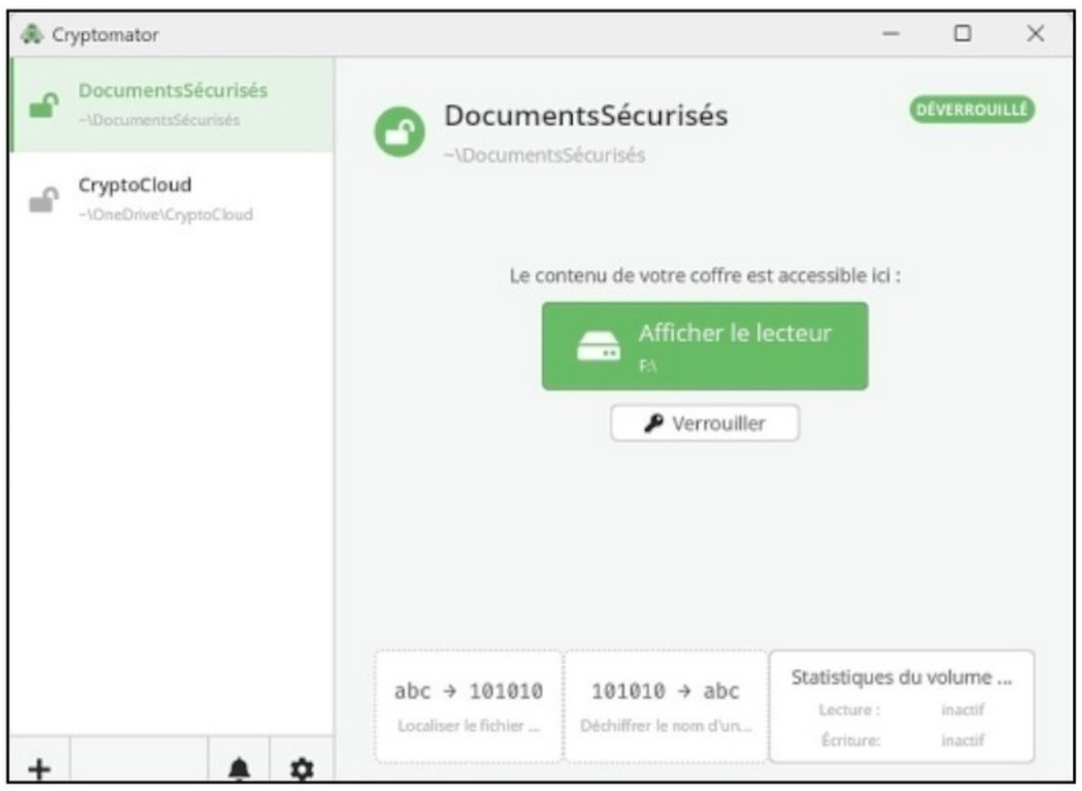
Lien : maps.me

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

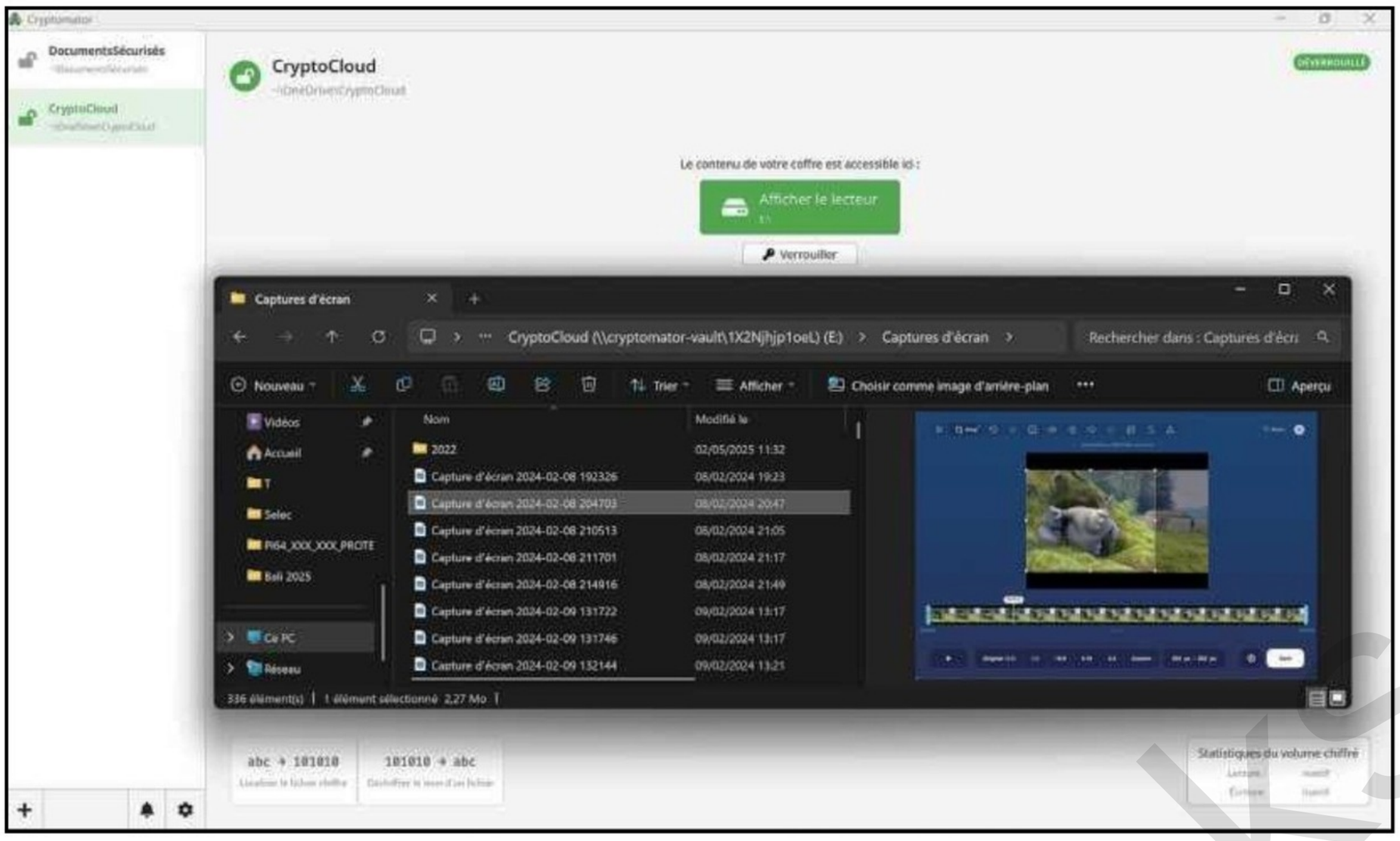
Cryptomator est un logiciel gratuit qui chiffre vos fichiers et dossiers en local, garantissant leur confidentialité avant toute synchronisation avec un service cloud. Compatible avec Dropbox, Google Drive, OneDrive et bien d'autres, il crée un coffre sécurisé accessible uniquement par mot de passe.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

À l'heure où le stockage dans le cloud est devenu un réflexe — notamment avec OneDrive intégré par défaut à Windows 11 — la question de la confidentialité de nos données n'a jamais été aussi cruciale. Les fichiers personnels, les documents de travail ou les archives sensibles que nous synchronisons dans le nuage peuvent être vulnérables s'ils ne sont pas protégés correctement. La gageure est de savoir chiffrer et sécuriser par mot de passe un dossier sur votre PC… tout en s'assurant que sa synchronisation sur le cloud bénéficiera de la même protection !

C'est ici que Cryptomator entre en scène. Ce logiciel libre, développé par l'équipe allemande de Skymatic, offre une solution élégante et robuste pour protéger en local vos dossiers avec un chiffrement de bout en bout, sans vous priver des avantages du cloud. Si vous utilisez un service de cloud (comme OneDrive, Dropbox, Google Drive…) qui synchronise et sauvegarde une partie du contenu de votre PC, Cryptomator s'occupe de tout de façon transparente



sans que vous ayez à vous en occuper. Il vous assurera que personne, pas même le fournisseur de cloud, ne puisse lire vos fichiers.



DANS UN DOSSIER PROTÉGÉ, CHAQUE FICHIER EST CHIFFRÉ INDIVIDUELLEMENT : QUAND VOUS MODIFIEZ UN ÉLÉMENT, LA SYNCHRONISATION NE CONCERNERA QUE CETTE MODIFICATION.

OPEN SOURCE, MAIS ULTRA INTUITIF

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

Dès son installation, Cryptomator vous permet de créer ce qu'il appelle un "coffre" (ou vault, en anglais). Il s'agit d'un répertoire spécial, protégé par mot de passe, qui se comporte comme un disque virtuel une fois ouvert. Ce coffre peut être situé n'importe où sur votre disque dur, y compris dans un dossier synchronisé avec OneDrive. Vous travaillez alors dans ce disque virtuel comme dans n'importe quel dossier Windows, en glissant vos fichiers ou en y enregistrant vos documents directement depuis vos applications.

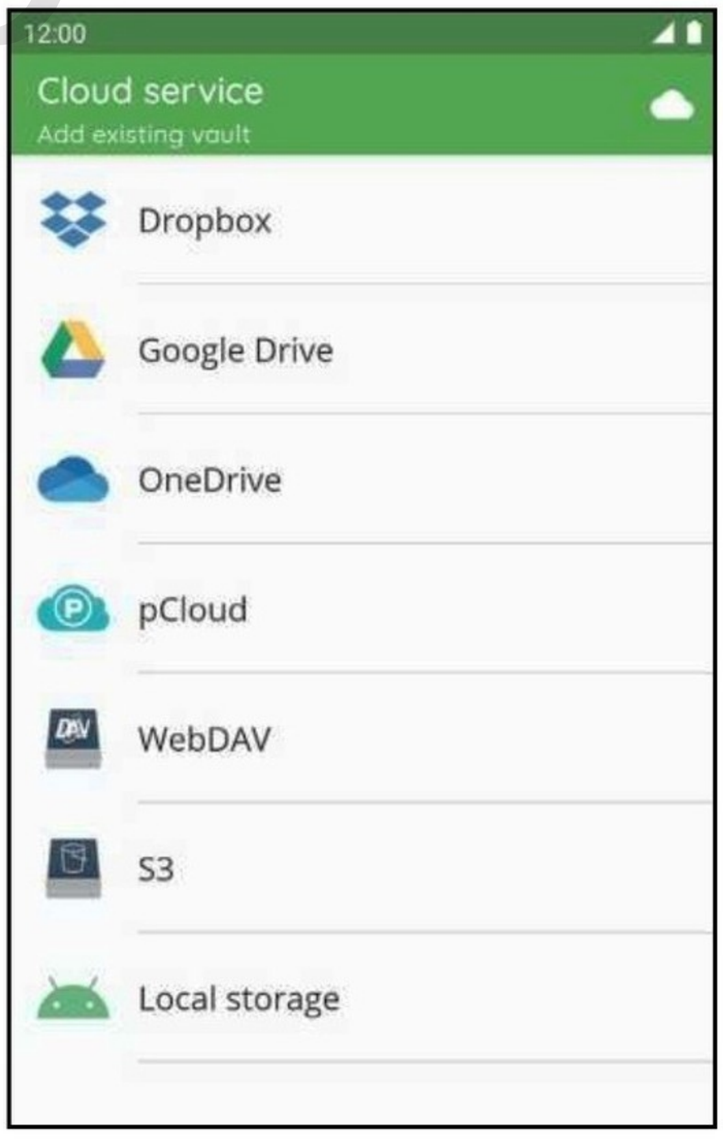
La magie opère en coulisses : chaque fichier que vous y déposez est chiffré individuellement en temps réel avec l'algorithme AES-256. Le contenu est illisible sans le mot de passe, mais également les noms des fichiers et la structure des dossiers. Mieux encore, contrairement aux conteneurs monolithiques (comme ceux générés par VeraCrypt), Cryptomator chiffre chaque fichier indépendamment, ce qui optimise la synchronisation dans le cloud : si vous modifiez un fichier, seul celui-ci est mis à jour sur OneDrive, pas l'ensemble du coffre.

PENSÉ POUR LE CLOUD, MAIS AUSSI POUR LE LOCAL

C'est ce qui fait toute la force de Cryptomator. Son architecture épouse les contraintes du stockage dans le cloud moderne : tout se passe en local sur votre machine, sans que les clés de chiffrement ne soient jamais envoyées vers Internet. Cela signifie que même si vos fichiers sont synchronisés automatiquement sur OneDrive, ils restent totalement illisibles sans passer par Cryptomator — y compris pour Microsoft.

À SAVOIR

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



SI CRYPTOMATOR EST GRATUIT SUR IOS, SA VERSION ANDROID EST ELLE PAYANTE, À 19,99 € POUR UN USAGE ILLIMITÉ ET AVEC LES FONCTIONS PREMIUM DÉVERROUILLÉES.

Vous pouvez tout à fait créer un coffre local, hors ligne, pour protéger vos dossiers sensibles sur votre disque dur ou sur une clé USB. C'est le premier tutoriel que nous vous présentons ci-après. Et pour ceux qui travaillent sur plusieurs appareils (PC portable, PC fixe, smartphone), Cryptomator existe également sur Android et iOS, avec la possibilité d'accéder à vos fichiers chiffrés sur OneDrive depuis votre mobile.

TUTO

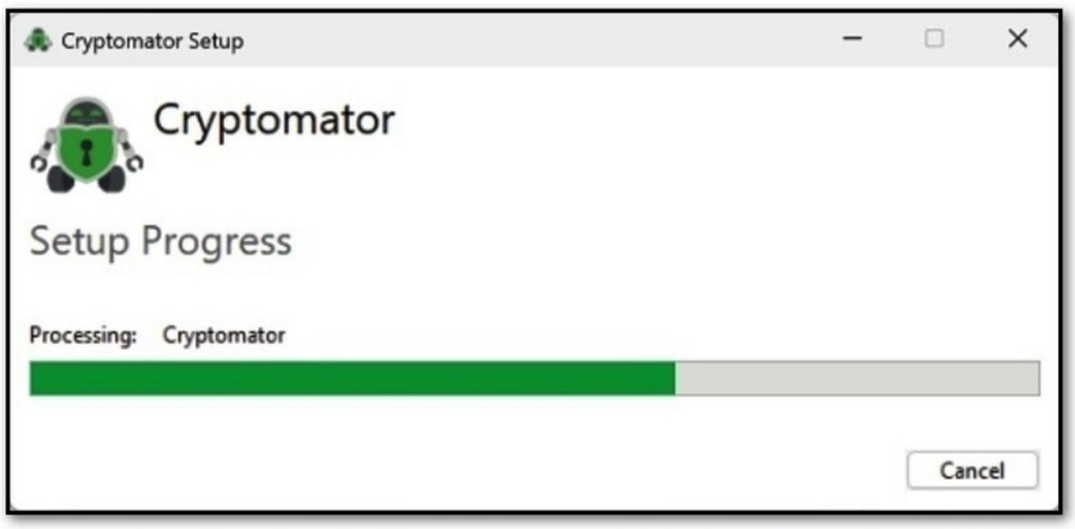
PRATIQUE

PROTÉGEZ VOS DOSSIERS EN LOCAL AVEC CRYPTOMATOR

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

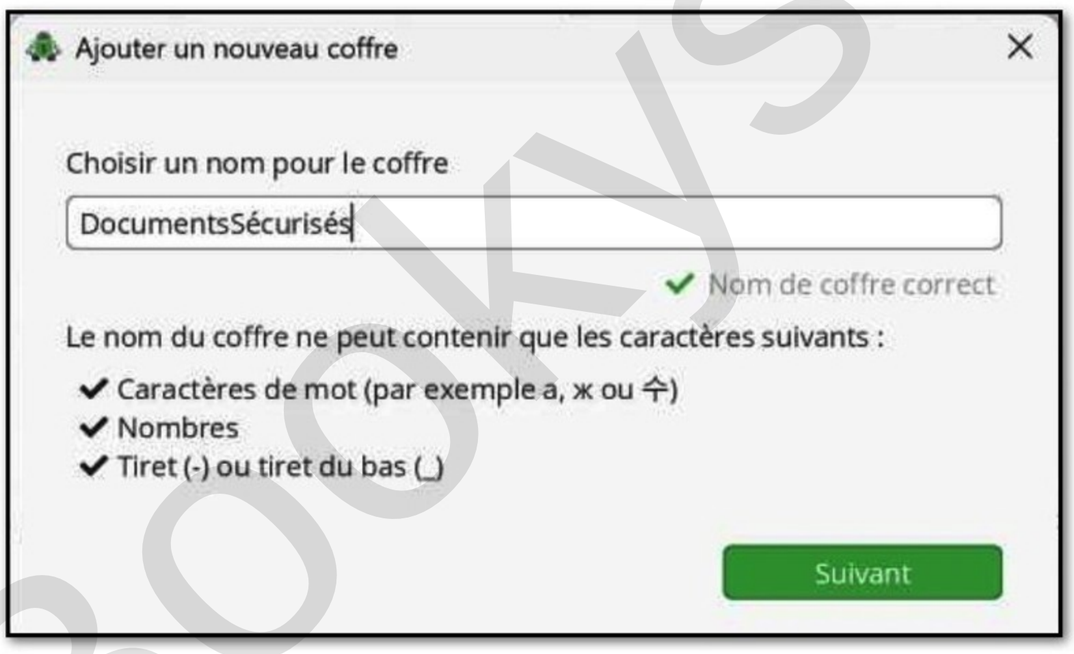
01› INSTALLATION DE CRYPTOMATOR

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



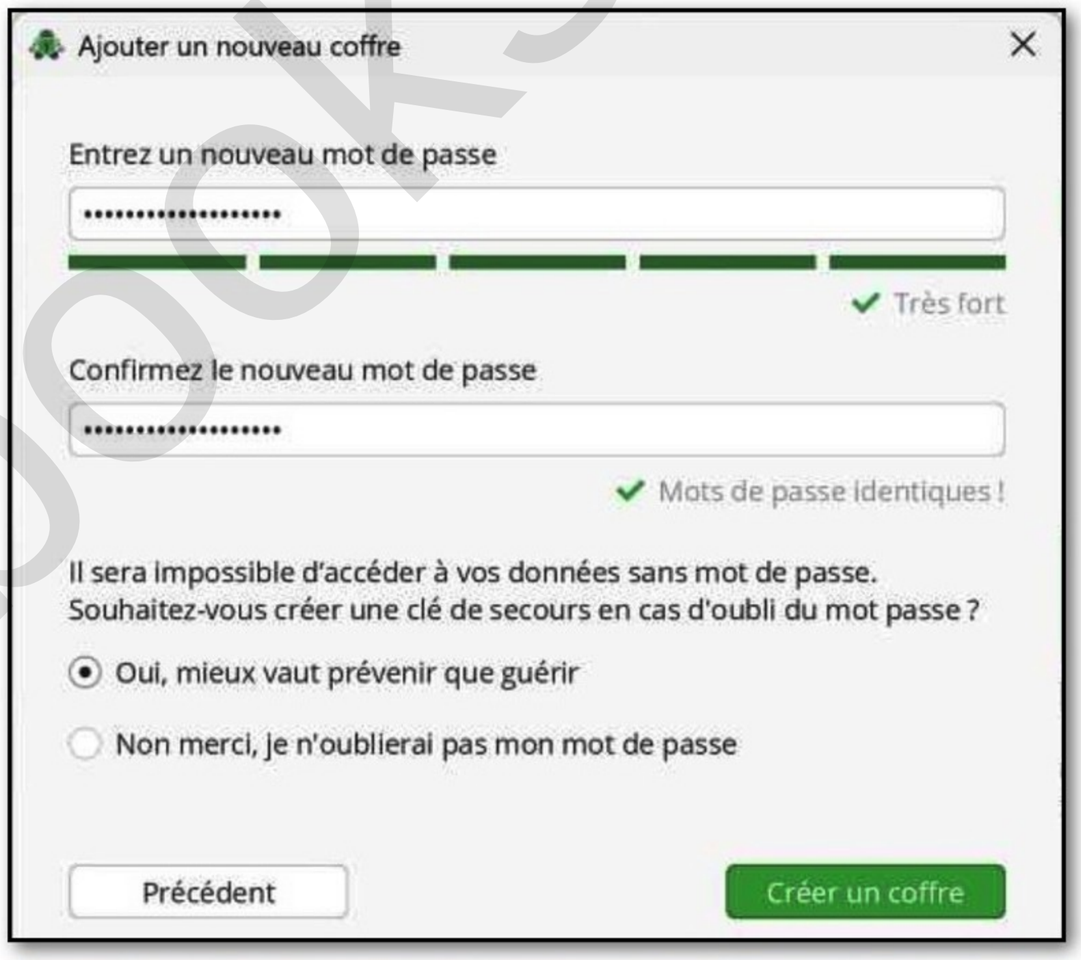
02› CRÉATION D'UN NOUVEAU COFFRE

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



03› VOTRE MOT DE PASSE

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



04› UTILISATION DU COFFRE

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

UTILISEZ CRYPTOMATOR SUR PC AVEC ONEDRIVE

PRATIQUE

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

Accès depuis un autre appareil

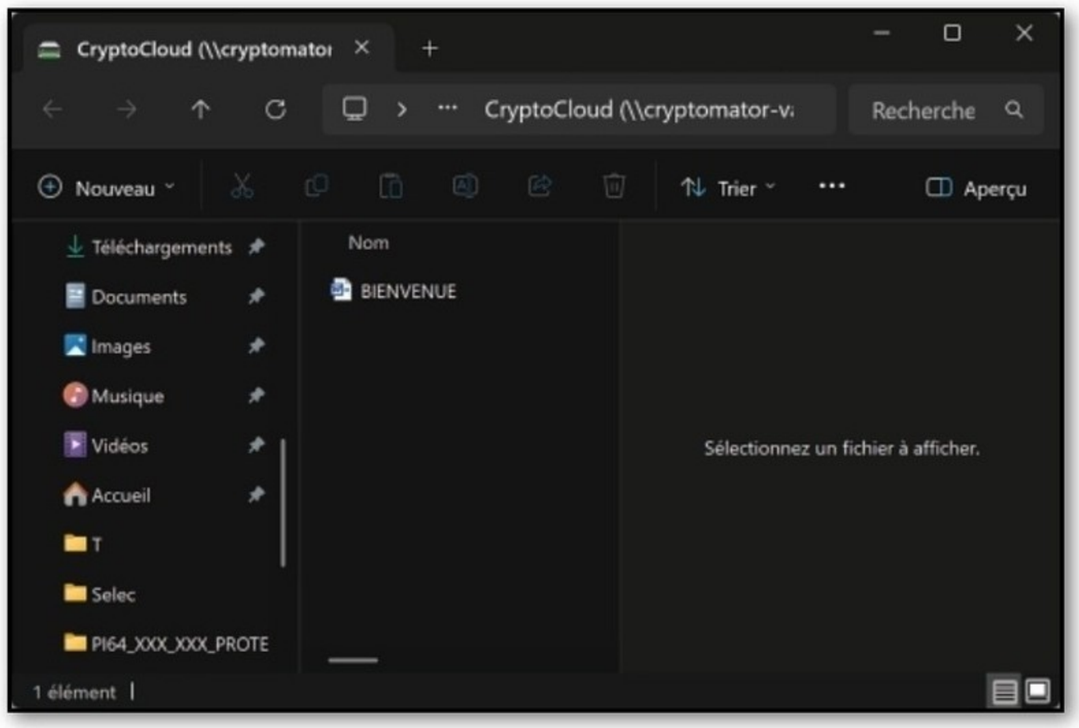
Sur un autre appareil synchronisé avec le même compte OneDrive, installez Cryptomator. Ajoutez le coffre existant en sélectionnant le fichier **masterkey.cryptomator** situé dans le dossier OneDrive correspondant. Déverrouillez le coffre avec le mot de passe défini précédemment pour accéder à vos fichiers.

01› CRÉATION D'UN NOUVEAU COFFRE-FORT

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

02› LECTEUR VIRTUEL

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



CONSEILS

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

DÉCRYPTAGE

RÉSEAUX SOCIAUX ET ESCROQUERIES : comment les repérer et s'en protéger

Les réseaux sociaux, conçus pour nous connecter, divertir ou faciliter nos achats, sont devenus le terrain de chasse privilégié des cybercriminels.

À travers de fausses boutiques sur Facebook, des publicités trompeuses sur YouTube ou du phishing sur Reddit, les escrocs exploitent chaque plateforme pour voler argent et données personnelles.

FACEBOOK, YOUTUBE ET TELEGRAM EN TÊTE DES MENACES

D'après le rapport de Gen sur les menaces du 4e trimestre 2024, Facebook concentre 56 % des escroqueries détectées sur les réseaux sociaux, suivi de YouTube (26 %) et de X/Twitter (7 %). Reddit (5 %) et Instagram (4 %) sont également visés. Telegram, bien que moins utilisé que WhatsApp, a détecté six fois plus de menaces, suggérant que ses fonctionnalités attirent davantage les cybercriminels.

RÉPARTITION DES MENACES

Facebook	56%
YouTube	26%
X (Twitter)	7%
Reddit	5%
Instagram	4%

LES ESCROQUERIES LES PLUS FRÉQUENTES

Les escrocs innovent constamment, mais certains types d'arnaques reviennent souvent :

- **Publicités malveillantes (27 %) :** Déguisées en offres légitimes, elles redirigent vers des sites ou programmes malveillants.

- **Faux sites marchands (23 %) :** Très présents sur Facebook et Instagram, ils vendent des produits contrefaits ou inexistants.

- **Phishing (18 %) :** Messages ou sites factices conçus pour soutirer identifiants ou coordonnées bancaires.

- **Arnaques financières (11 %) :** Fausses opportunités d'investissement ou de prêts.

- **Escroqueries générales (10 %) :** Tactiques variées pour soutirer argent ou données via la manipulation.

- **Faux supports techniques (5 %) :** Les cybercriminels se font passer pour un service client.

- **Arnaques sentimentales (3 %) :** Fausse relation en ligne destinée à extorquer de l'argent.

- **Autres escroqueries (2 %) :** Exploitent tendances ou niches spécifiques.

COMMENT LES ESCROCS EXPLOITENT CHAQUE RÉSEAU

Facebook	Fausse Marketplace et boutiques frauduleuses, souvent perçues comme vérifiées à tort.
YouTube	Publicités et liens trompeurs diffusant des malwares à une large audience.
X (Twitter)	Usurpations d'identité facilitées par l'achat de la vérification, souvent lors d'événements sensibles.
Reddit	Liens malveillants dissimulés dans des publications ou commentaires « utiles ».
Instagram	Fausses vitrines via Instagram Shopping, ciblant les acheteurs avec de belles présentations mensongères.

QUELQUES RÈGLES SIMPLES POUR LIMITER LES RISQUES

Si vous respectez les trois règles d'or suivantes, vous éviterez la plupart des arnaques possibles :

1# Vérifier qui se cache derrière un compte, une publicité
Vérifiez la traçabilité du communicant : le compte existe-t-il depuis longtemps ou vient-il d'être créé ? Des avis de sources différentes valident-ils son existence et son sérieux ? La société derrière une publicité est-elle identifiable, pouvez-vous déterminer sa localisation et son enregistrement juridique réel ? Fuyez si des zones d'ombres subsistent.

2# Ce qui est trop beau pour être vrai est trop beau pour être vrai
Qu'il s'agissent de cadeaux, d'opportunités financières ou sentimentales, méfiez-vous des propositions trop alléchantes. Au mieux vous perdrez du temps pour rien, au pire vous serez contraint de communiquer des données personnelles sensibles ou... de sortir votre porte-monnaie quand vous serez bien hameçonné et manipulé.

3# Ne cliquez pas sur des liens suspects !
Quel que soit le cas de figure, ne cliquez pas sur un lien non identifié à 100%. Que ce soit dans la description d'un contenu, les commentaires d'internautes ou lié à une publicité. Et n'oubliez pas que les escrocs sont passés maîtres dans l'art de dissimuler et maquiller la redirection réelle d'un lien : c'est la principale porte ouverte aux arnaques, vol de données ou activation d'un malware. Pour contrer ces tentatives, **lire notre tuto ci-dessous**.

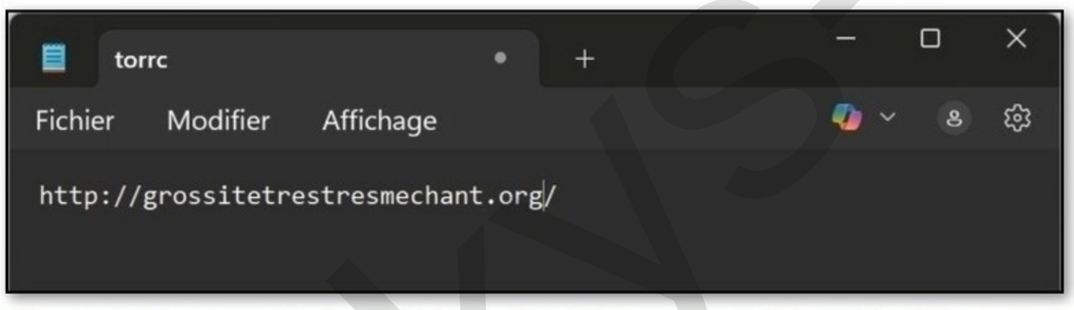
COMMENT VÉRIFIER SI UN LIEN EST OFFICIEL OU FRAUDULEUX ?

PRATIQUE

Les escrocs veulent vous faire passer des vessies pour des lanternes. La base consiste à trouver l'URL exacte vers lequel vous dirigera un lien ou une image. Puis de vérifier sa dangerosité.

01› ARNAQUE AU TEXTE D'ANCRAGE

Les cybercriminels dissimulent souvent des liens suspects en utilisant des textes d'ancrage trompeurs. Le plus simple pour débunker ce type de faux lien : faites un clic droit, copier l'URL puis collez-là dans un éditeur de texte de type Notepad. Vous découvrirez alors sa redirection réelle.



02› ARNAQUE AU LIEN INTÉGRÉ

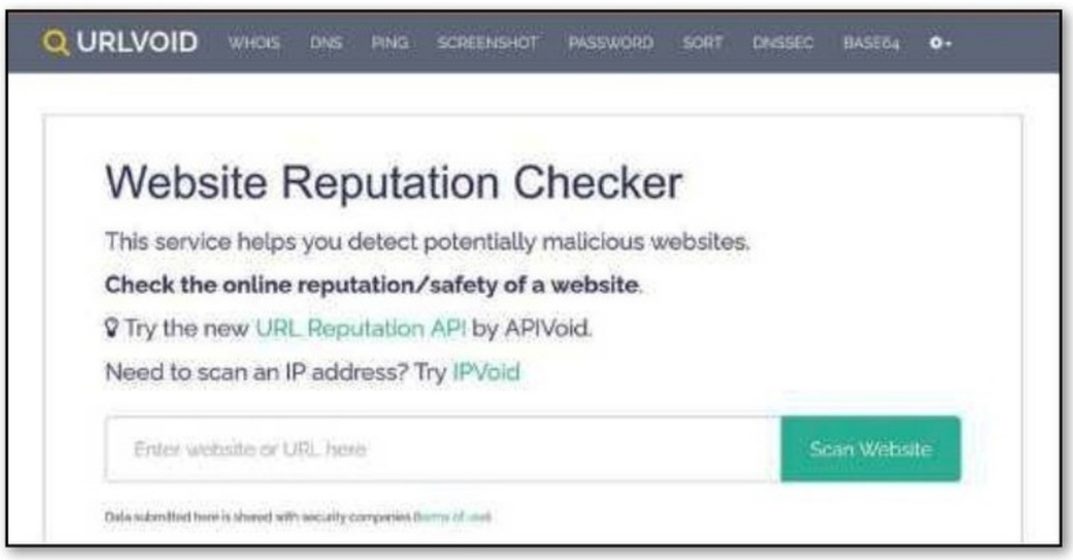
Si le pirate a camouflé le lien en l'intégrant dans un bouton ou une image, vous pouvez accéder au code public du message suspect, soit via votre navigateur soit via votre application (clic droit puis **Inspecter**). Généralement, recherchez **href=».** dans le code affiché.

03› ARNAQUE AU LIEN RACCOURCI

Le lien trouvé peut cependant avoir été raccourci grâce à un raccourcisseur d'URL (comme Bit.ly ou TinyurlL), ce qui vous empêche d'avoir accès immédiatement à son URL exacte. Dans ce cas, vous pouvez prévisualiser les URL raccourcis grâce à des services dédiés comme **checkshorturl.com** ou **www.getlinkinfo.com**.

04› VÉRIFIEZ LA RÉPUTATION D'UNE URL

De façon plus générale, passez par un site de vérification de lien. Nous vous conseillons **www.urlvoid.com** qui utilise plus de 30 moteurs de sécurité différents (BitDefender, Google Safe Browsing, Avira...) pour vérifier si une URL est potentiellement dangereuse, frauduleuse ou infectée (malwares, phishing, blacklists, ...).



Couper votre Internet en un clic

> Avec NetDisabler

Net Disabler est un outil pratique pour gérer l'accès à Internet sur un PC, que ce soit pour des raisons de sécurité, de concentration ou de contrôle parental.Développé par Sordum, Net Disabler permet de désactiver ou réactiver la connexion Internet en un clic, sans installation. Il offre quatre méthodes de blocage :

- Désactiver les adaptateurs réseau : coupe physiquement la connexion (LAN ou Wi-Fi).
- Bloquer via DNS : empêche la résolution des noms de domaine.
- Bloquer via un proxy : redirige le trafic vers un proxy inexistant.
- Bloquer via le pare-feu Windows : interdit les connexions sortantes.

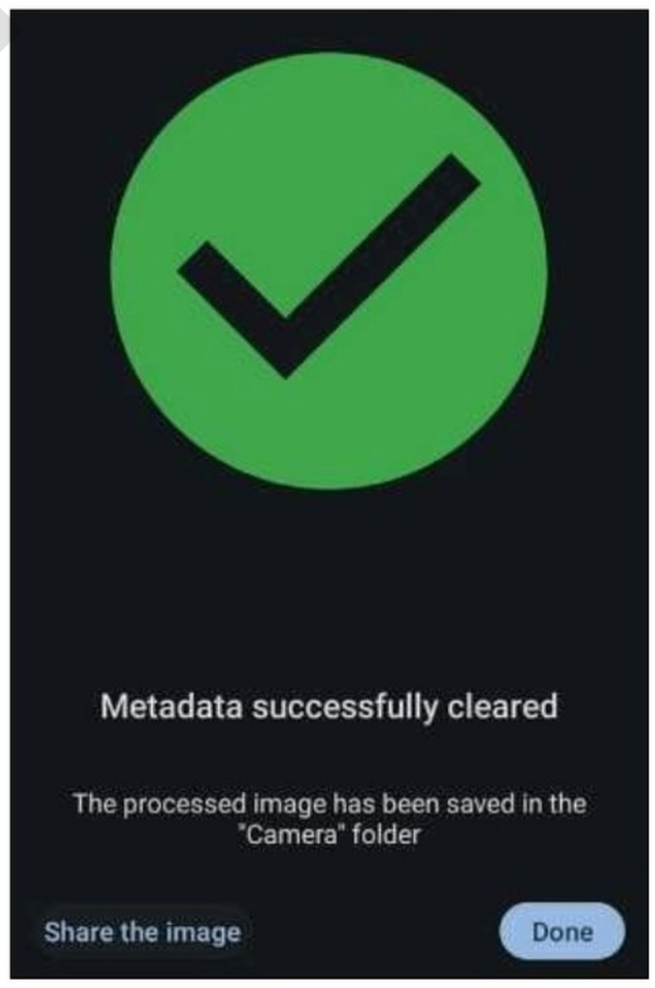
Ces méthodes peuvent être combinées pour renforcer l'efficacité du blocage. Téléchargez Net Disabler puis lancez l'exécutable (aucune installation requise). Sélectionnez une ou plusieurs méthodes de blocage (ex. : **Désactiver l'adaptateur réseau**). Cliquez enfin sur **Désactiver Internet** pour couper la connexion. Pour rétablir l'accès, cliquez sur **Activer Internet**. Une icône dans la barre des tâches vous donnera un accès rapide à ces fonctions.
Pour éviter l'accès à NetDisabler par un autre utilisateur, vous pouvez aussi configurer un mot de passe.

Lien : www.sordum.org/9660/net-disabler-v1-1/

Supprimer les métadonnées d'une photo

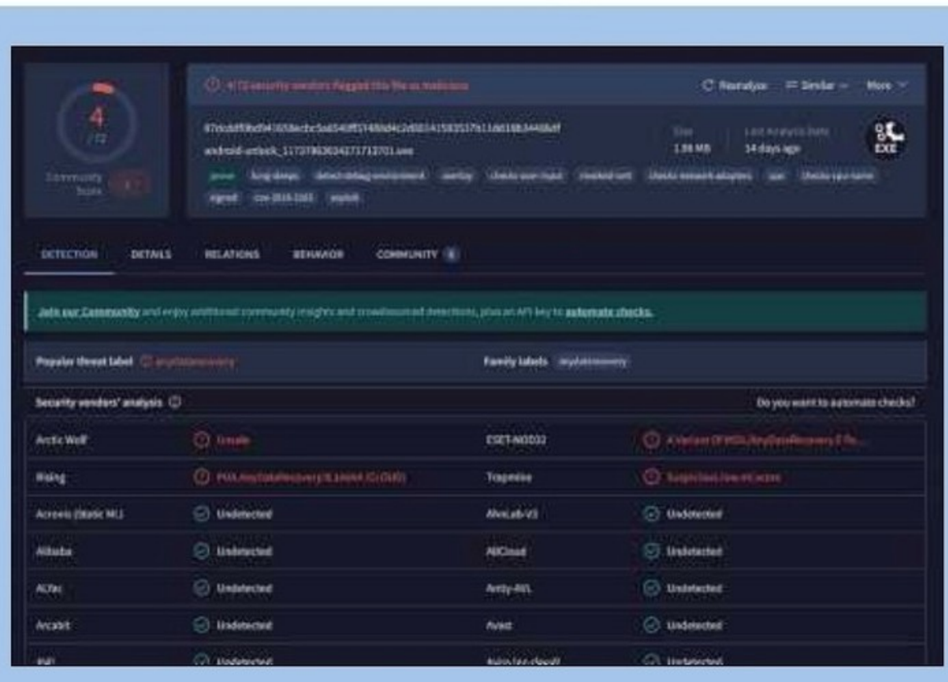
> Avec Android

Les métadonnées (EXIF) d'une photo peuvent contenir des informations sensibles comme la localisation GPS, la date, l'heure et le modèle de l'appareil. Les supprimer avant de partager une image permet de protéger votre vie privée. Utilisez l'application gratuite **Photo Metadata Remover**, disonible sur le Play Store. Ouvrez l'appli et sélectionnez la photo à nettoyer via **Choose Photos**. Appuyez sur **Remove Metadata** pour supprimer les données EXIF.



Scanner un fichier avec 70 antivirus

> Avec VirusTotal



Vous venez de télécharger un fichier depuis un forum, un lien WeTransfer ou un email ? Avant de l'ouvrir, il est toujours prudent de vérifier qu'il ne cache pas un malware. Plutôt que de compter uniquement sur votre antivirus local, vous pouvez le faire analyser gratuitement par plus de 70 moteurs antivirus simultanément, grâce au service VirusTotal (racheté par Google).
Pas besoin d'installation, tout se passe en ligne : une fois sur le site, cliquez sur **Choose File** et importer votre fichier à analyser (taille max : 650 Mo). Patientez quelques secondes : vous obtiendrez un score de détection, par exemple : 4 / 72 (4 antivirus sur 72 l'ont détecté comme suspect). Cliquez sur sur l'onglet **Behaviour** pour visualiser les actions potentielles du fichier (appel réseau, création de processus, etc.).

Lien : www.virustotal.com

Comment révoquer les applis qui ont accès à votre compte > Avec X (Twitter)

Quand vous vous connectez à des services tiers (jeux, apps mobiles, outils d'analyse, bots...), ceux-ci vous demandent parfois d'autoriser l'accès à votre compte X. Parfois, cela reste oublié, et ces services continuent d'avoir accès à vos informations... voire à vos DMs, vos likes, vos abonnements, etc. Bonne nouvelle : vous pouvez reprendre la main en quelques clics.

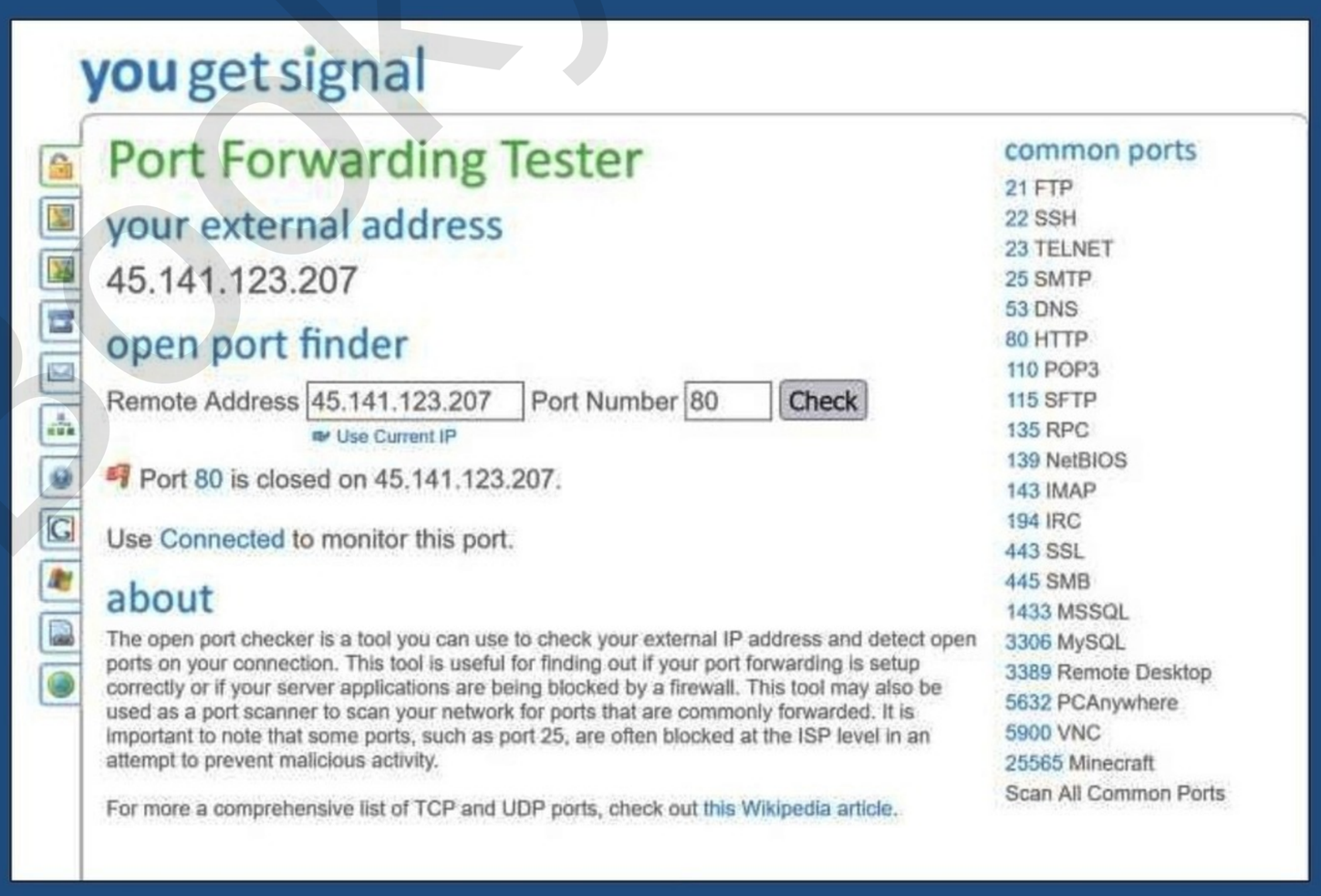
Dans le menu des paramètres, appuyez sur **Compte**, puis sur **Applications connectées**.
Vous verrez alors la liste de toutes les applications tierces qui ont actuellement un accès à votre compte. Pour chaque application, X affiche son nom, la date d'autorisation et le type d'accès accordé (lecture, écriture, etc.).
Cliquez sur l'application que vous ne reconnaissez pas ou n'utilisez plus puis sur **Révoquer l'accès**.
Attention : Si vous révoquez l'accès à une app que vous utilisez encore (ex. Buffer, IFTTT, TweetDeck), il faudra vous reconnecter et la réautoriser si besoin.
Même si vous n'êtes pas très actif, il est conseillé de faire cette vérification tous les 3 à 6 mois, surtout si : vous avez testé des bots, des jeux ou des extensions Chrome, etc.

Scanner des ports en ligne

> avec YouGetSignal

Vérifiez les ports ouverts sur votre réseau, sans installer nmap ou autre scanner grâce au service en ligne YouGetSignal. Connaître les ports ouverts... c'est aussi connaître les portes d'entrées non verrouillées sur votre PC.
Rendez-vous sur le site, puis dans **Remote Address**, laissez votre IP publique (détectée automatiquement). C'est dans **Port adress** que vous allez pouvoir tester le ou les ports de votre choix pour tester leur statut. Choisissez un port à tester, ex : 22 (SSH), 80 (HTTP), 3389 (RDP). Puis cliquez sur **Check**.
Si le résultat est **Open**, vous comprenez que le port est ouvert et il vous faudra vérifier si cet état est légitime ou dangereux. L'outil ne permet pas de scanner plusieurs ports d'un coup, mais il est très pratique pour vérifier rapidement si un service est exposé par erreur depuis l'extérieur.

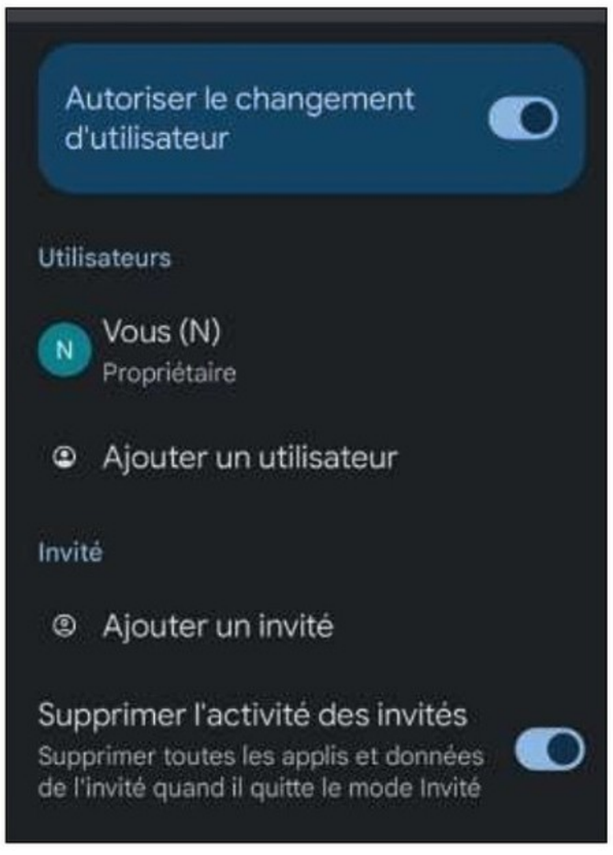
Lien : www.yougetsignal.com/tools/open-ports/



Activer le mode invité

> Avec Android

Le mode invité permet à une autre personne d'utiliser votre téléphone sans accéder à vos données personnelles.
Ouvrez les paramètres de votre appareil Android. Allez dans **Système > Utilisateurs**. Activez l'option **Utilisateurs multiples** ou **Autoriser le changement d'utilisateur** si ce n'est pas déjà fait. Appuyez sur **Ajouter un invité** pour créer un profil temporaire. Vous pourrez basculer immédiatement sur ce mode Invité puis le quitter quand votre proche vous rendra le téléphone.



SÉLECTION

TOP 3 ESSAYEZ LES MÉTA-MOTEURS DE RECHERCHE

1Fichier, Turbobit et autre MediaFire ont la cote pour héberger des contenus légaux… et illégaux, déposés par leurs utilisateurs. Néanmoins, pour y dénicher des fichiers, à moins d'y être invité, c'est un peu la croix et la bannière. Inutile de solliciter les moteurs de recherche standards tels que Google ou Bing de Microsoft. Ils ne vous seront d'aucune aide puisqu'ils passent leur temps à faire la chasse aux contenus douteux. Rabattez-vous sur des moteurs dédiés.

FILEPURSUIT

> DE LA RECHERCHE ET DU HASARD

Ce moteur offre une interface des plus claires. Il suffit d'entrer le nom du fichier recherché, de choisir une catégorie (vidéo, audio, ebook, appli ou archive) et de lancer la recherche. L'aide à la saisie est même disponible en français ! Les résultats s'affichent instantanément. Mais vous pouvez aussi y aller au petit bonheur la chance. FilePursuit propose un onglet Discover. En cliquant dessus, on tombe sur des serveurs de fichiers laissés en libre accès. Impossible de savoir à qui ils appartiennent (sauf à mener une recherche sur l'adresse IP indiquée en clair) ou ce qu'ils contiennent réellement. C'est à la fois amusant et déroutant.

Lien : filepursuit.com

AIO SEARCH > LE SPÉCIALISTE DU TORRENT

Ce métamoteur (moteur de recherche qui collecte les résultats de plusieurs autres moteurs de recherche) propose d'effectuer des requêtes pour dénicher des fichiers partout sur le Web auprès des plateformes de streaming et de partage de fichiers. Néanmoins, sa grande spécialité repose sur les fichiers Torrents. Il combine ainsi les résultats provenant de pas moins de 30 moteurs de recherche de liens torrents. Si avec ça vous ne trouvez pas ce que vous cherchez, c'est que ça n'existe pas. Son interface se montre plutôt sobre et agréable. On peut éliminer certaines plateformes des résultats et même ajouter d'autres moteurs de recherche. Il permet de trouver à peu près tout y compris les fichiers de sous-titres et même de simples images.

TURBOBIT.NET > QUE LA CHANCE SOIT AVEC VOUS

On ne peut pas dire que son interface ne soit très avenante ni très conviviale, mais elle fait le job. Et, que l'on ne s'y trompe pas : Turbobit.net ne se contente pas d'effectuer les recherches que vous souhaitez sur la plateforme de partage de fichiers Turbobit. Pour peu que vous cliquiez sur les bons liens placés sous le champ de recherche, vous pouvez également mener des requêtes sur Nitroflare, RapidGator ou encore Uploaded. Néanmoins, peu de résultats sont remontés sur les recherches que nous avons menées. Si vous cherchez un fichier bien précis, passez votre chemin.

Lien : turbobit.filesearch.io

TROUVER TOUS TYPES DE FICHIERS AVEC AIO SEARCH

PRATIQUE

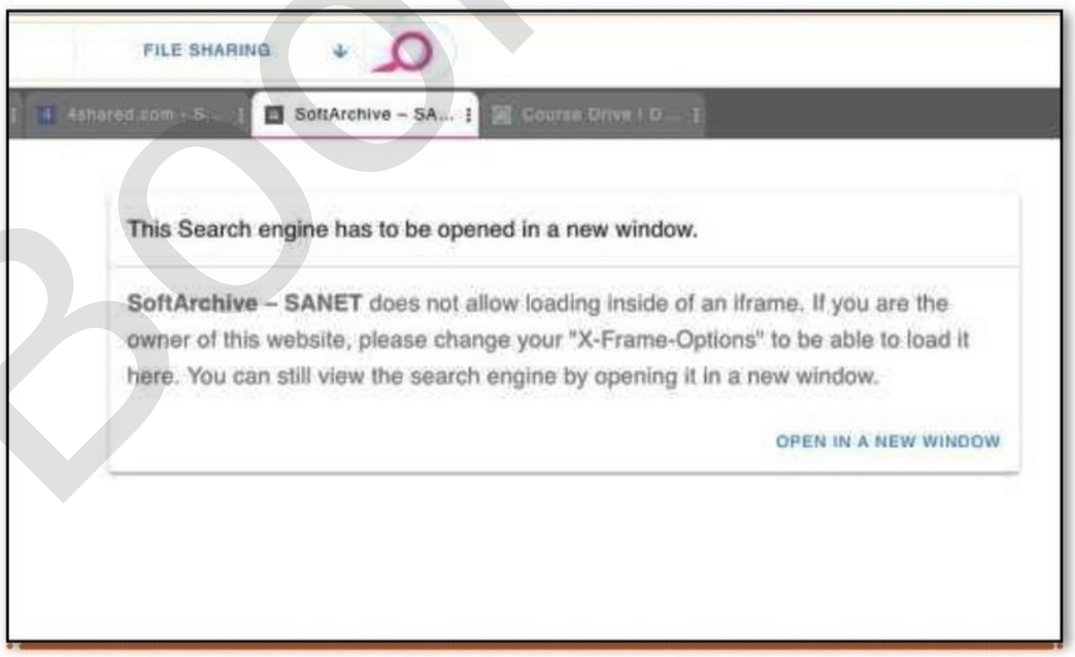
01› RECHERCHER SUR LES PLATEFORMES DE PARTAGE

Rendez-vous sur la page de AIO Search puis indiquez l'objet de votre requête dans le champ dédié. Cliquez sur la flèche

au bout de la ligne et, dans le menu déroulant qui s'affiche, optez pour **File sharing**. AIO va alors sonder les moteurs de recherche pour interroger diverses plateformes de partage comme Rapidgator, Depositfiles, Uploaded ou encore Nitroflare. Validez d'un clic sur **la loupe**.

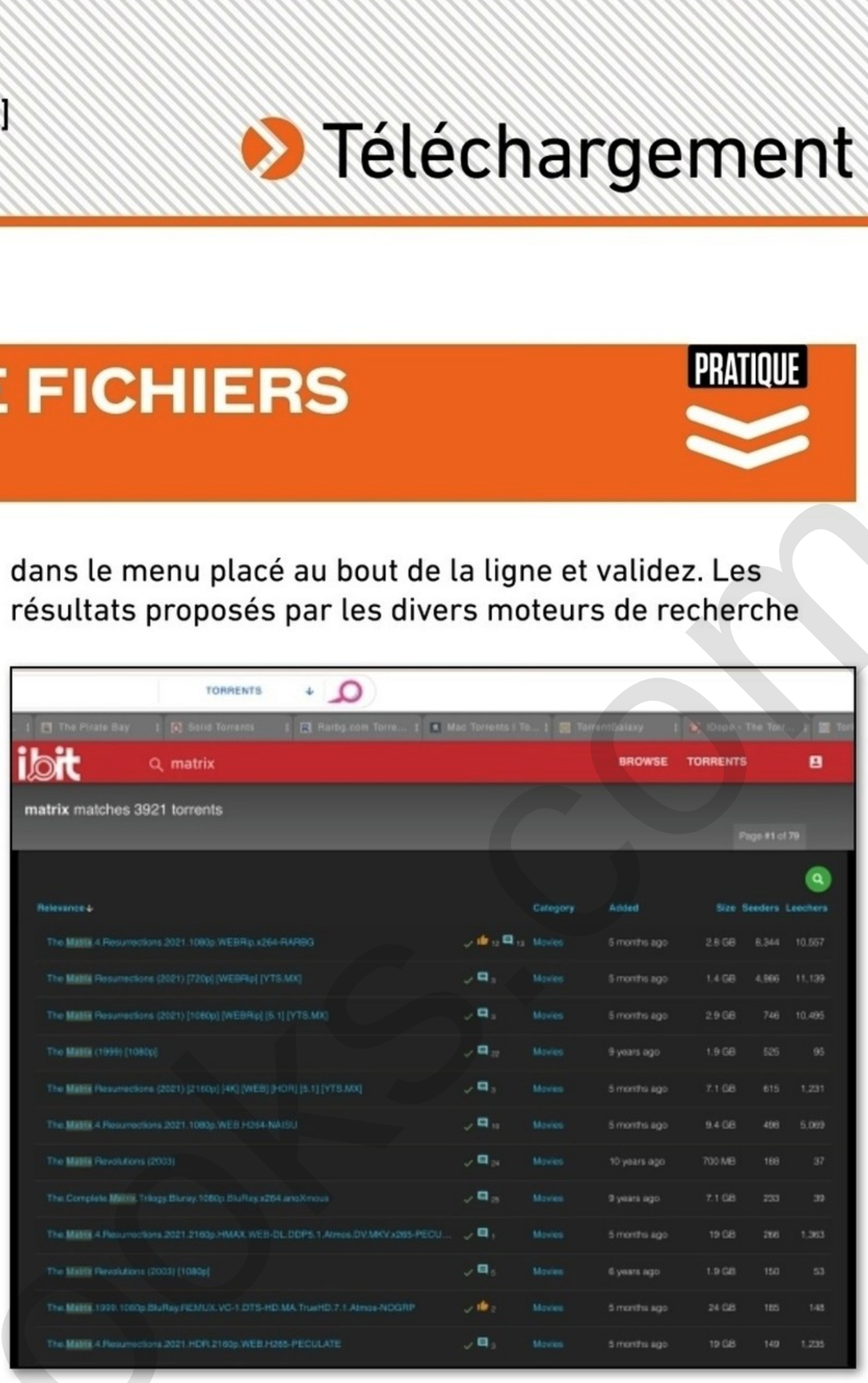
02› CHOISIR LA PLATEFORME DE PARTAGE

Une première liste de résultats s'affiche. Elle recense les contenus indexés par Google. Au sommet de la fenêtre figurent plusieurs onglets. Ils correspondent à d'autres plateformes interrogées. Cliquez sur l'un d'eux pour consulter les résultats trouvés. Parfois, les moteurs tombent à côté de la plaque et ne présentent que des réponses approximatives. Parfois vous devez aussi ouvrir la liste des éléments trouvés directement auprès d'un autre moteur de recherche dans un nouvel onglet.



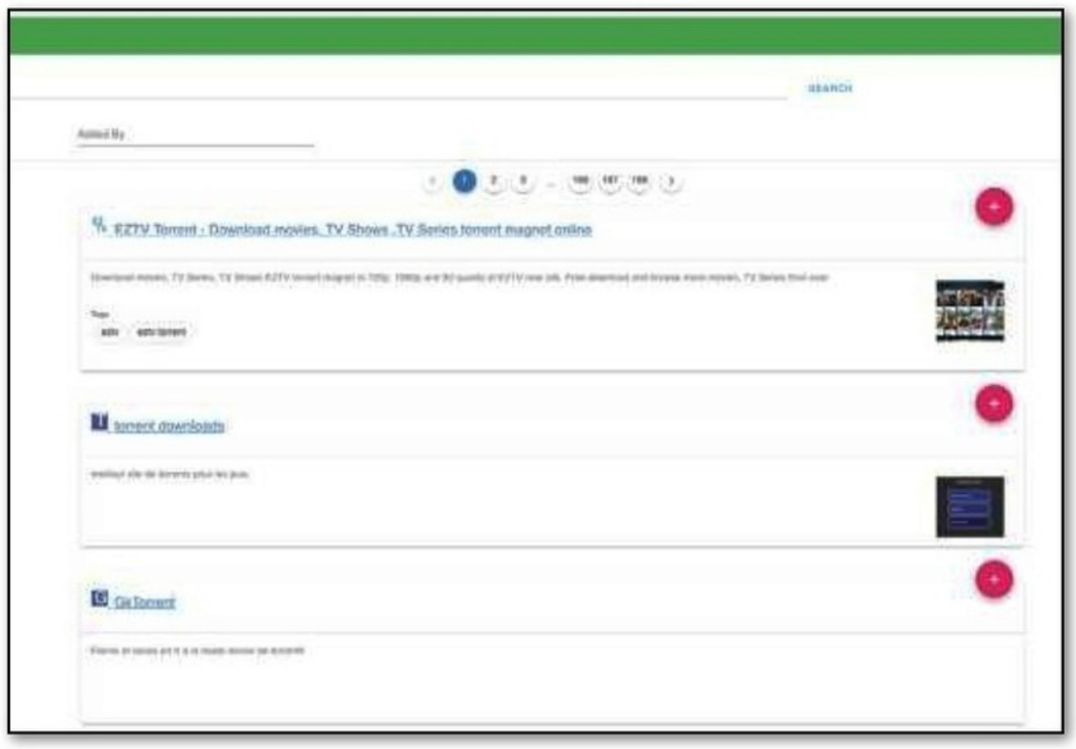
03› DÉNICHER DES LIENS TORRENT

AIO s'est fait une spécialité des liens Torrent. Le métamoteur peut ainsi interroger une trentaine de moteurs différents. Indiquez votre requête, optez pour **Torrents** dans le menu placé au bout de la ligne et validez. Les résultats proposés par les divers moteurs de recherche sont répartis dans des onglets séparés au sommet de la fenêtre. Il ne vous reste plus qu'à analyser les résultats et à faire votre choix.



04› ADAPTER AIO SEARCH À VOS BESOINS

AIO Search se montre modulaire. Vous pouvez à loisir modifier la liste des moteurs de recherche sur lesquels il s'appuie pour mener les requêtes. Il est possible d'ajouter de nouveaux moteurs, d'en retirer de la liste, etc. Cliquez sur l'icône en forme de **loupe** placée sous le champ de recherche. Une (très) longue liste de moteurs s'affiche. Cliquez sur le bouton **+** de celui que vous souhaitez ajouter. Si vous connaissez un moteur particulier, vous pouvez l'ajouter manuellement à la liste grâce au bouton **+** présent sous le champ de recherche et remplir sa fiche avec son adresse.



SÉLECTION

TOP 7 ALTERNATIVES À SPOTIFY GRATUITES & LÉGALES + qui respectent vos données

Vous cherchez des alternatives gratuites et légales à Spotify, Deezer ou Apple Music ? Et en plus, vous souhaitez confier vos oreilles à des services éthiques et respectueux de vos données personnelles ? Et bien, figurez-vous que vous êtes au bon endroit !

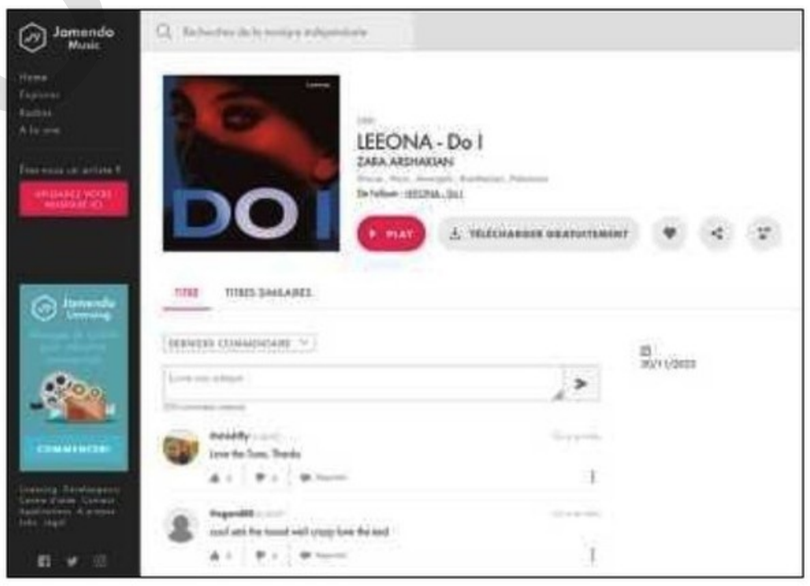
SOUNDCLOUD

> La scène indépendante à portée de clic

SoundCloud est une plateforme incontournable pour découvrir des artistes émergents et des morceaux inédits. Avec plus de 300 millions de titres disponibles, elle offre une richesse musicale impressionnante. La version gratuite permet d'écouter des morceaux en streaming, de créer des playlists et de suivre vos artistes préférés. Cependant, la qualité audio est limitée à 128 kbps et des publicités peuvent apparaître. Côté confidentialité, SoundCloud collecte certaines données, mais offre des paramètres pour gérer votre vie privée.

Lien : soundcloud.com

JAMENDO > La musique libre et légale



Jamendo est une plateforme dédiée à la musique libre de droits, idéale pour ceux qui cherchent à écouter ou utiliser de la musique en toute légalité. Elle propose un vaste catalogue d'artistes indépendants, avec la possibilité de télécharger des morceaux pour un usage personnel. Les utilisateurs peuvent créer des playlists et découvrir de nouveaux talents. Jamendo respecte la vie privée de ses utilisateurs et ne diffuse pas de publicités intrusives.

Lien : www.jamendo.com

FUNKWHALE

> Votre propre serveur de streaming

VOIR NOTRE TUTO PAGE 60

Funkwhale est une plateforme décentralisée qui permet d'héberger et de partager sa propre bibliothèque musicale. Elle fonctionne sur le principe du Fediverse, offrant une alternative aux services centralisés. Les utilisateurs peuvent créer des instances personnelles ou rejoindre des instances publiques (appelées Pods). Funkwhale respecte la vie privée et ne collecte pas de données personnelles.

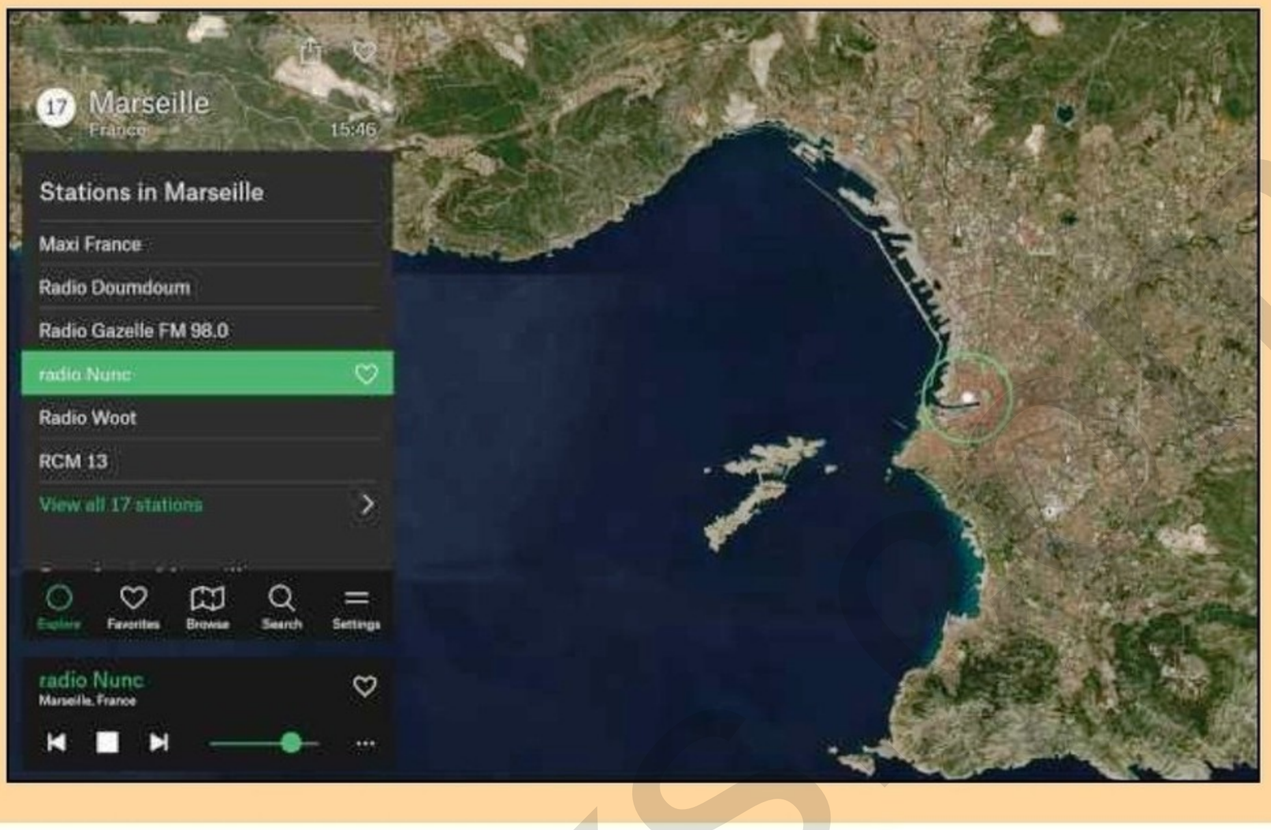
Lien : www.funkwhale.audio

RADIO GARDEN

> Voyage musical autour du monde

Radio Garden offre une expérience unique en permettant d'écouter des stations de radio du monde entier via une interface interactive en forme de globe terrestre. Il suffit de tourner le globe et de cliquer sur une ville pour écouter ses stations locales. L'application est gratuite, sans publicités intrusives, et ne nécessite pas de création de compte. Elle respecte la vie privée des utilisateurs en ne collectant pas de données personnelles.

Lien : radio.garden



THE GREAT 78 PROJECT

> Un trésor musical historique

The Great 78 Project est une initiative de l'Internet Archive visant à préserver et à rendre accessible une collection de disques 78 tours datant de la fin du XIXe au milieu du XXe siècle. Les enregistrements sont disponibles en streaming et en téléchargement gratuit. Le projet respecte la vie privée des utilisateurs et ne diffuse pas de publicités.

Lien : great78.archive.org

LIBRE.FM

> L'alternative éthique à Last.fm

Libre.fm est une plateforme communautaire qui permet de suivre vos habitudes d'écoute et de découvrir de nouveaux artistes. Elle fonctionne sans publicité et respecte la vie privée des utilisateurs en ne collectant pas d'informations personnelles. Libre.fm encourage l'utilisation de la musique sous licence libre et offre une expérience sans tracking ni collecte de données.

Lien : libre.fm

AUDIUS > Le streaming décentralisé

Audius est une plateforme de streaming musical basée sur la technologie blockchain. Elle permet aux artistes de partager leur musique directement avec leurs fans, sans intermédiaires. La version gratuite offre un accès illimité à la musique, sans publicités. Audius met l'accent sur la confidentialité et la transparence, en permettant aux utilisateurs de contrôler leurs données.

Lien : audius.co

TUTO

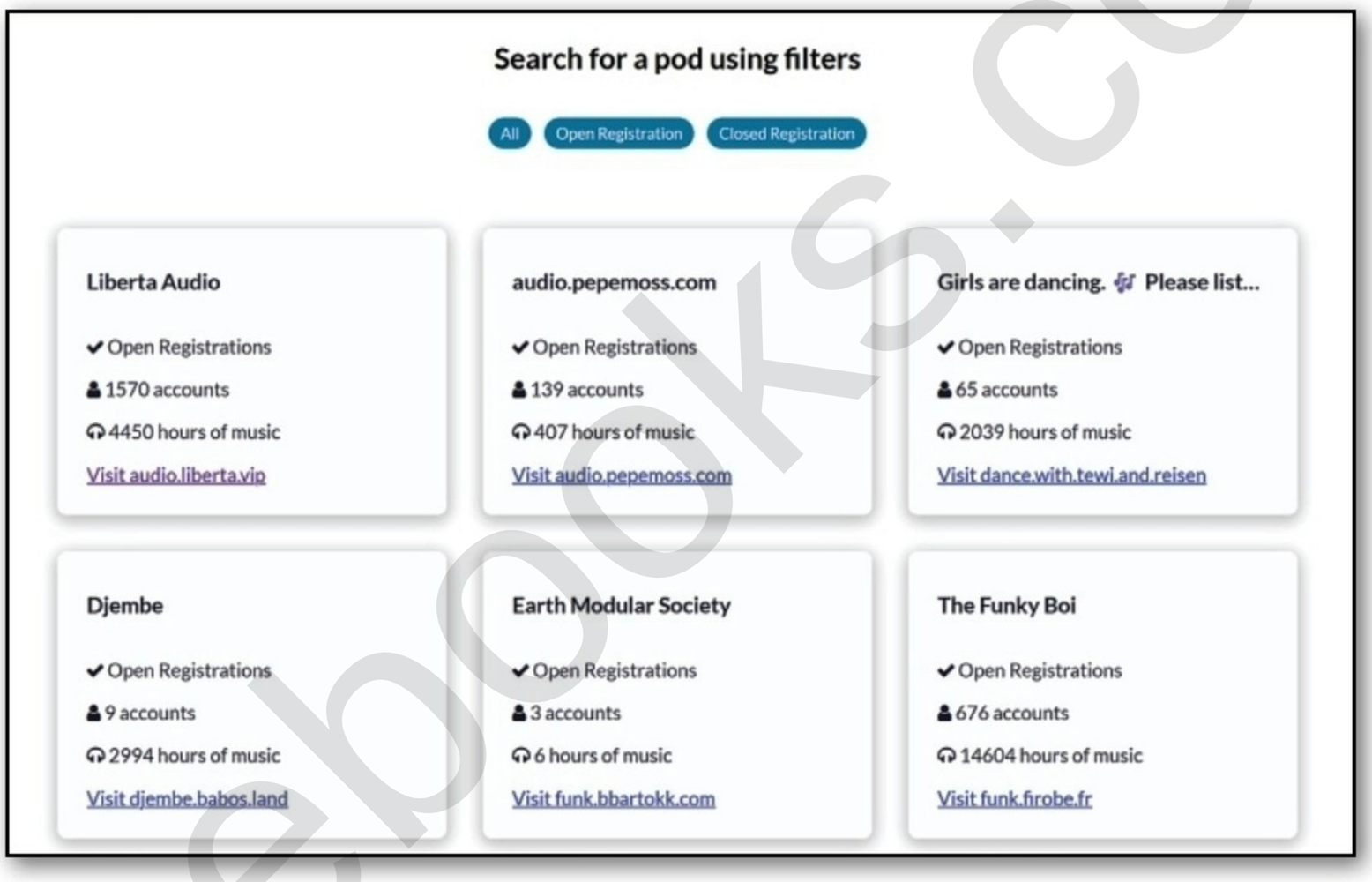
PRATIQUE

VOS PREMIERS PAS AVEC FUNKWHALE

Funkwhale est une plateforme de streaming audio libre, décentralisée et fédérée. Funkwhale est entièrement gratuit et open source. Les utilisateurs peuvent choisir de rejoindre des pods publics existants ou d'héberger leur propre instance.

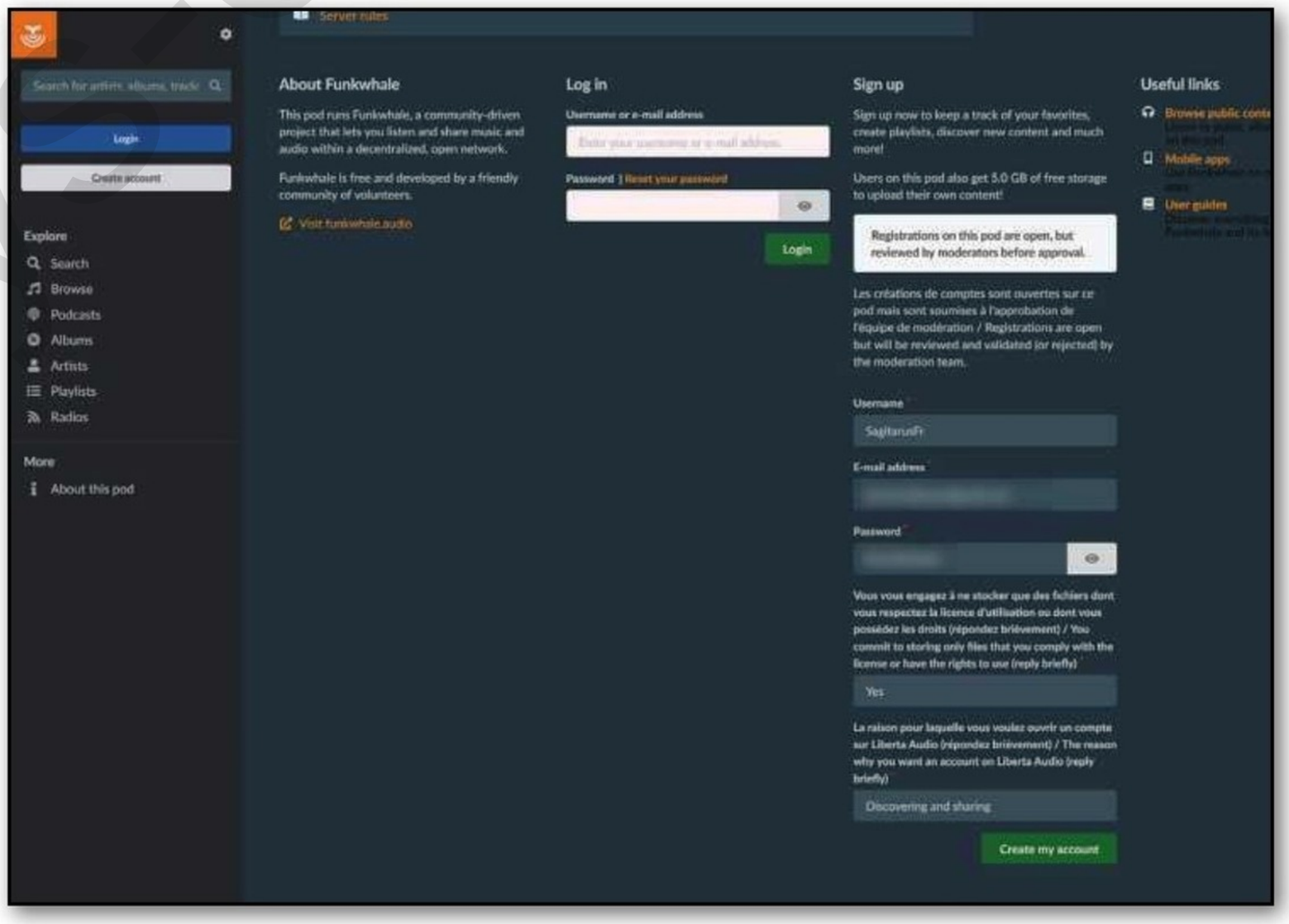
01› CHOISIR UN POD

Rendez-vous sur **funkwhale.audio** et cliquez sur **Get Started**. Commencez par sélectionner un pod public auquel vous inscrire via **Join an existing Pod > Find a Pod**. Via le filtre **Open registration**, choisissez (un peu au hasard) un pod avec une quantité appréciable de comptes liés et d'heures de musique disponibles.



02› CRÉER UN COMPTE

Inscrivez-vous via la colonne **Sign Up** en fournissant une adresse e-mail et en choisissant un nom d'utilisateur. Certains pods peuvent nécessiter une approbation manuelle et exiger des règles d'inscriptions spécifiques (compte Telegram, garantie de légalité, motivation(s), etc.). Une fois les champs remplis, cliquez sur **Create my account**.

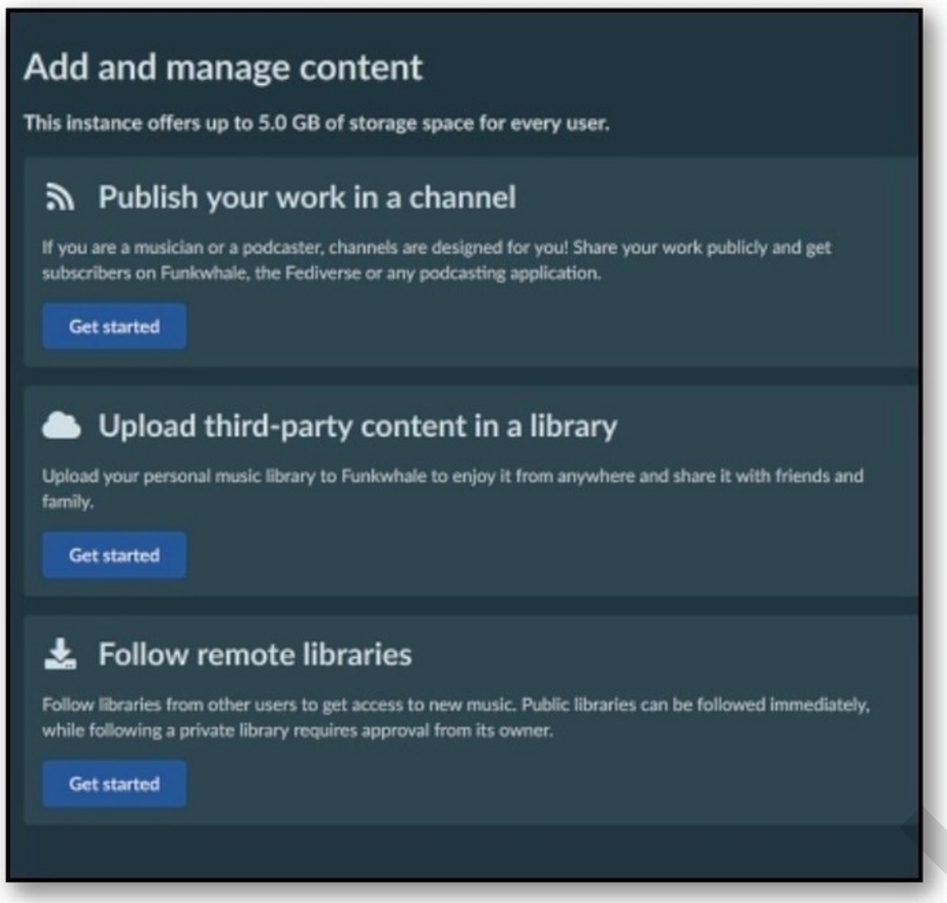


À NOTER

Dans **My Library**, chaque utilisateur peut importer ses propres fichiers audio pour constituer une bibliothèque accessible depuis n'importe quel appareil.

03› IMPORTER VOTRE MUSIQUE

Une fois votre profil accepté par le pod, vous voici membre de la communauté. Cliquez sur l'icône d'importation. Choisissez **Get started** dans **Upload third-party content in a library. Créez votre librairie puis** sélectionnez les fichiers audios depuis votre appareil ou faites-les glisser directement dans la zone prévue. Vous avez droit à 5 Go de stockage offerts. Cliquez sur **Publier**.



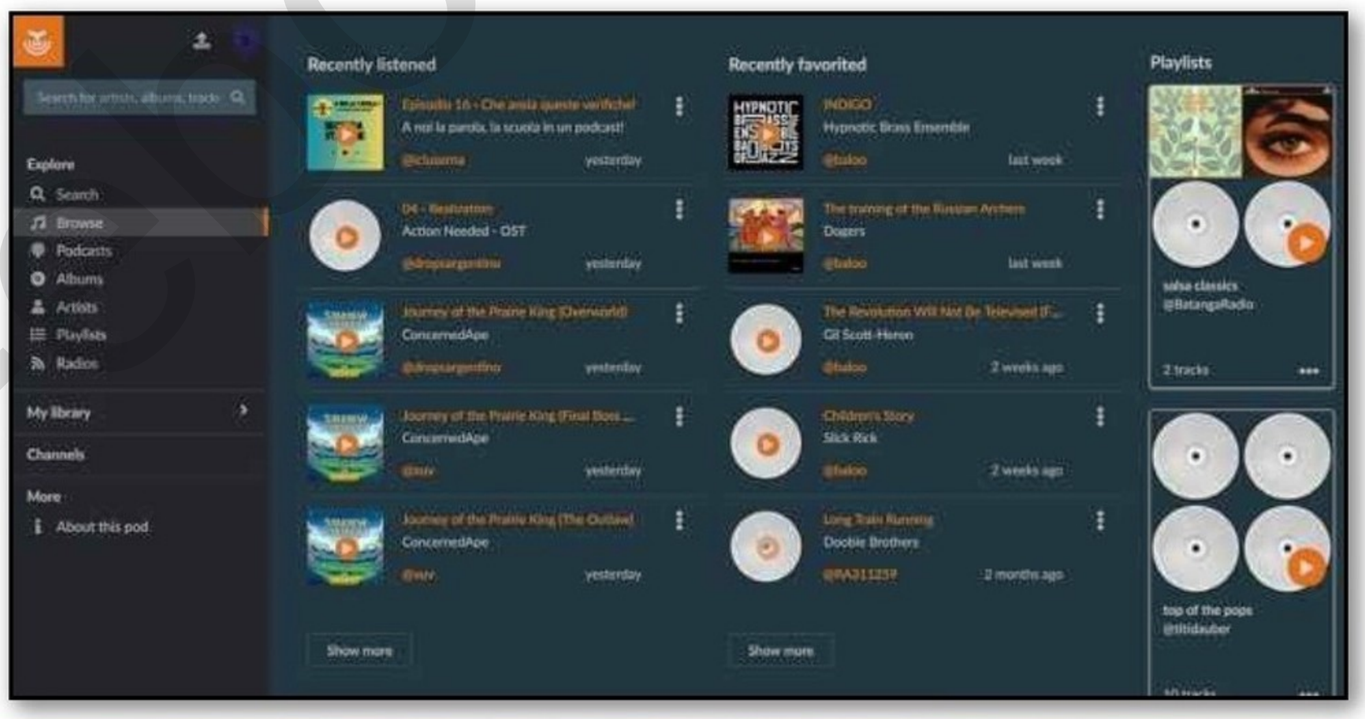
Une fois les fichiers téléversés, vous pouvez les organiser en albums, ajouter des balises (tags) et des descriptions.

À SAVOIR

Créée en 2015 par Agate Berriot, cette solution open source repose sur le protocole ActivityPub, également utilisé par Mastodon et PeerTube, pour interconnecter différentes instances appelées «pods». La compatibilité de Funkwhale avec Subsonic autorise l'intégration avec des applications tierces via l'API Subsonic, permettant une écoute sur diverses plateformes. Si vous possédez votre propre serveur (physique ou cloud exécutant Debian ou Ubuntu), vous pouvez aussi fédérer votre instance avec d'autres serveurs Funkwhale. Vous devrez disposer d'un nom de domaine pointant vers votre serveur ainsi que des connaissances de base en ligne de commande Linux.

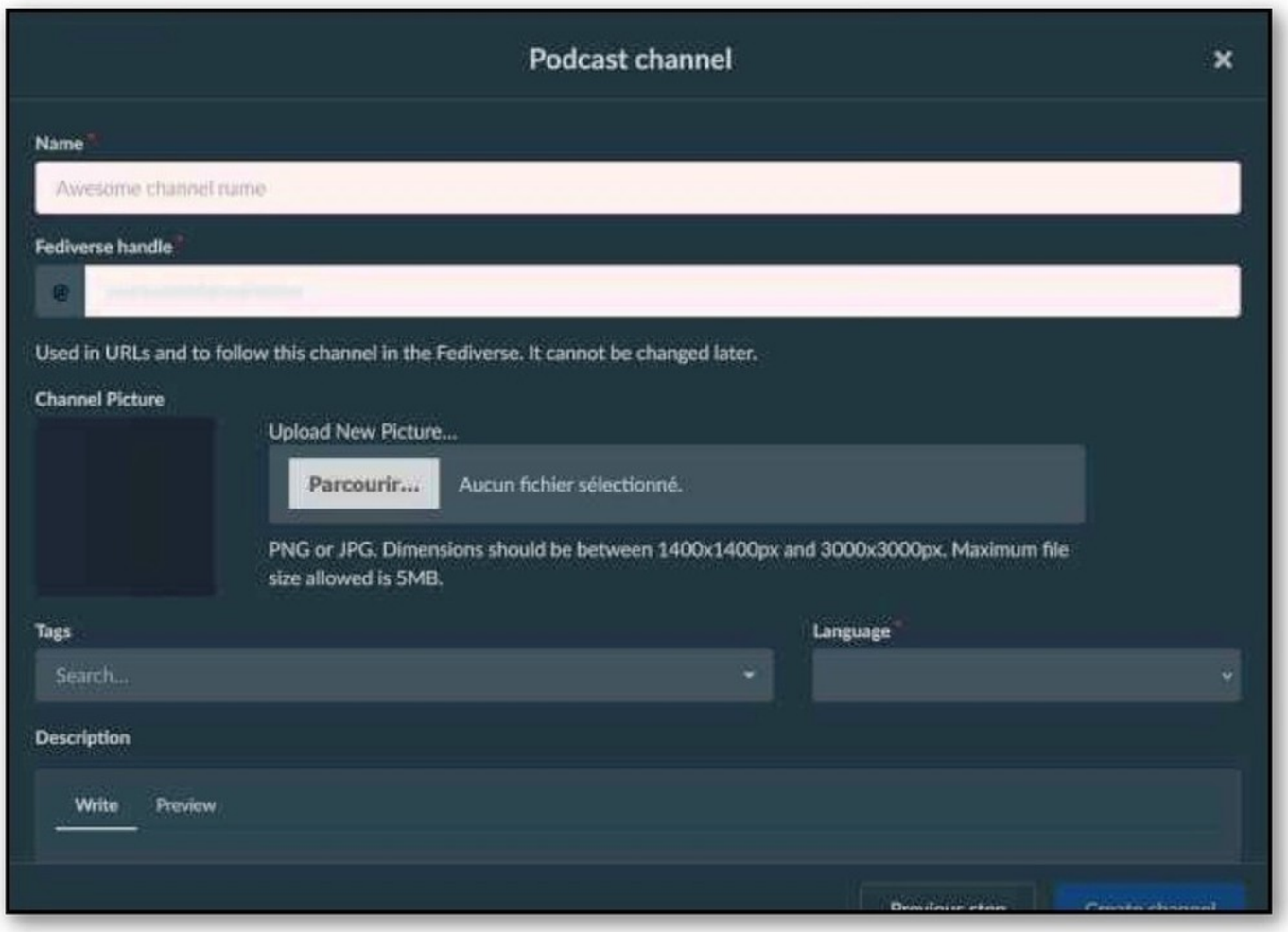
04› EXPLORER ET ÉCOUTER

Utilisez les fonctions de recherche (**Search, Browse, Albums, Artists, Playlists, Radios**) via le volet à gauche pour découvrir de la musique partagée par les autres utilisateurs du ou des pods desquels vous êtes membres. Ajoutez des morceaux à vos favoris ou créez des playlists personnalisées.



05› CRÉER UNE CHAÎNE

Si vous êtes artiste ou podcasteur, créez une chaîne pour partager vos créations. Les utilisateurs pourront s'abonner à votre chaîne et recevoir des notifications lors de nouvelles publications. Cliquez sur l'icône d'importation, puis sur **Get Started** dans **Publish your work in a channel**. Passez par **+ Add New** en face de **Channels** et choisissez si vous souhaitez publier des podcasts ou vos créations musicales. Remplissez les champs correspondants puis **Create Channel**. C'est dans cet espace que vous pourrez ajouter vos fichiers.



3 SOLUTIONS POUR SIMULER UNE PRÉSENCE CHEZ SOI

S'ABSENTER DE SON DOMICILE PEUT SUSCITER DES INQUIÉTUDES QUANT À LA SÉCURITÉ DE SON FOYER. NE PASSEZ PAS FORCÉMENT PAR DES SOLUTIONS DOMOTIQUES COMPLEXES ET ONÉREUSES : DE PETITS DISPOSITIFS SIMPLES ET ABORDABLES VOUS PERMETTENT DE SIMULER UNE PRÉSENCE ET DE DISSUADER LES INTRUSIONS. NOUS NOUS SOMMES ARRÊTÉS SUR TROIS SOLUTIONS ÉCONOMIQUES : LES AMPOULES CONNECTÉES, LES PRISES CONNECTÉES ET LES SIMULATEURS DE TV.

> LES AMPOULES CONNECTÉES

TP-LINK KL110 KASA

> Simple, efficace

NOTRE CHOIX

L'avantage de cette TP-Link, c'est qu'elle intègre son propre système Wi-Fi : pas besoin de hub et d'installation domotique. Via l'application dédiée (Kasa) sur votre smartphone (iOS, Android), vous la connecterez directement à votre réseau Wi-Fi domestique. Tous les réglages et programmations horaires (allumage, extinction) se feront via votre mobile, chez vous ou loin de votre domicile. Vous pouvez même la commander à la voix puisque l'ampoule est compatible avec Alexa et Google Assistant. La puissance est de 10 watts et l'intensité lumineuse est également personnalisable.

Prix : **19 €** Où la trouver ? **www.tp-link.com**

KONYKS ANTALYA EASY E27

> Deux valent mieux qu'une

L'ALTERNATIVE

Passez directement à un pack de deux ampoules pour moins de 20 euros. Créez ainsi des scénarios d'allumage dans différentes pièces de la maison pour un rendu plus réaliste. Konyks Antalya Easy E27 est une ampoule LED connectée dont la température de couleur est ajustable.
Elle est compatible avec les réseaux Wi-Fi et Bluetooth, ce qui simplifie son installation et son utilisation. Grâce à l'application dédiée, il est possible de programmer des plages horaires d'allumage. Bien que ses fonctionnalités soient plus limitées que celles de ses concurrentes haut de gamme, elle remplit parfaitement son rôle pour un coût modéré.

Prix : **19,90 € (Pack de 2 ampoules)**
Où les trouver ? **konyks.com**

> SIMULATEURS DE TV : L'ILLUSION PARFAITE

SIMULATEUR TV 24 LED POWERPLUS TIIWEE

> Basique et puissant

Malgré son format ultra-compact (12 cm de large), les 24 LED du PowerPlus simulent un grand téléviseur d'au moins 42 pouces de diamètre. Le fonctionnement est classique avec trois réglages possibles : 4 ou 7 heures après le crépuscule (activation automatique grâce au capteur de luminosité) ou bien « toujours activé » avec une minuterie externe (non fournie avec le produit). Il suffit de pointer le simulateur PowerPlus vers le mur ou le plafond et de placer l'appareil de façon à ce qu'il ne soit pas visible directement depuis l'extérieur. L'avantage de ces systèmes LED est leur très faible consommation électrique. L'alimentation se fait sur secteur.

Prix : **29,90 €** Où le trouver ? **tiiwee.fr**

NOTRE CHOIX

> PRISES CONNECTÉES : RENDEZ VOS APPAREILS INTELLIGENTS

PRISKA MAX BLACK

> Complète et à moins de 25 €

La Priska Max Black est la petite nouvelle de chez Konyks. La marque la présente comme « *la plus petite prise connectée du marché* ». Elle s'intègre discrètement dans n'importe quelle prise murale, permettant même l'utilisation simultanée de plusieurs prises sur une multiprise standard.

NOTRE CHOIX

Ne vous fiez pas à sa petite taille : la Priska Max Black est capable de supporter une charge allant jusqu'à 16 A, soit une puissance maximale de 3680 W. Elle est donc adaptée à une large gamme d'appareils électroménagers, des lampes aux machines à laver. Même si sa fonctionnalité phare est son suivi détaillé de la consommation énergétique, ce qui nous intéresse ici, c'est bien ses possibilités de simulateurs de présence. La Priska Max Black permet d'allumer et d'éteindre vos appareils de manière aléatoire, dissuadant ainsi les éventuels intrus lors de vos absences. De plus, en cas de coupure de courant, vous pouvez définir le comportement de la prise à la reprise de l'alimentation : rester éteinte, s'allumer ou reprendre son état précédent. Compatible avec les assistants vocaux tels qu'Alexa, Google Home et les raccourcis Siri, la Priska Max Black se pilote aisément à la voix. Elle utilise une connexion Wi-Fi 2,4 GHz et intègre également le Bluetooth, facilitant ainsi l'appairage initial et assurant un contrôle local même en cas de coupure internet.

Prix : **24,90 €** Où la trouver ? **konyks.com**

WIZ SMART PLUG > Le bon plan

Dans les premiers prix, on retiendra la Wiz Smart Plug. Cette prise connectée simple d'utilisation, idéale pour ceux qui recherchent une solution sans fioriture. Elle se connecte elle aussi directement à votre réseau Wi-Fi,

L'ALTERNATIVE

sans nécessiter de hub, et supporte une puissance maximale de 2300W. Grâce à l'application Wiz, vous pouvez programmer des horaires de fonctionnement et contrôler vos appareils à distance. Sa compatibilité avec Google Home, Alexa et Siri en fait une option flexible pour intégrer vos appareils existants.

Prix : **14,50 €** Où la trouver ? **www.wizconnected.com**

SIMULATEUR TV 12 LED VISORTECH

> Petit mais complet

Ce simulateur utilise un éclairage LED dynamique qui diffuse une lumière comparable à celle d'un téléviseur, ce qui donne l'impression que vous regardez la TV. Votre maison semble alors habitée même lorsque vous n'y êtes pas. Ce petit simulateur TV dispose de trois modes de fonctionnement : il peut être programmé par plages horaires, fonctionner en continu ou encore s'activer uniquement à la tombée de la nuit grâce au détecteur d'obscurité. Dans ce dernier cas, le simulateur s'enclenche lui aussi pour 4 ou 7 heures de fonctionnement. Il compte 12 LED (7 blanches, 2 vertes, 2 bleues et 1 rouge), ce qui lui permet de simuler l'équivalent d'un petit téléviseur. L'alimentation est sur secteur (câble de 145cm).

L'ALTERNATIVE

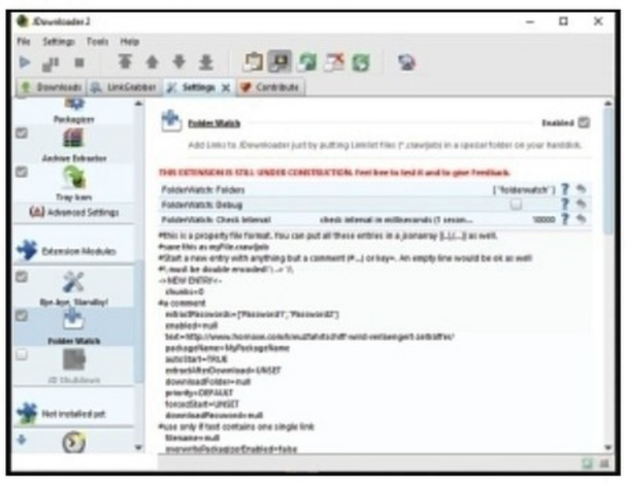
Prix : **19,95 €** Où le trouver ? **www.pearl.fr**

SÉLECTION

TOP 15 Logiciels & services GRATUITS

TOP5 GESTIONNAIRES DE TÉLÉCHARGEMENT

JDOWNLOADER 2 > Toujours le roi



JDownloader 2 automatise au maximum les téléchargements issus des plateformes comme Mega, Uptobox, MediaFire ou encore 1fichier. Son interface pique les yeux mais ses fonctionnalités sont au top : vous collez une URL et le logiciel scanne puis extrait les liens exploitables, y compris ceux dissimulés derrière des redirections, des pages de pub ou des CAPTCHA.

Lien : jdownloader.org

FREE DOWNLOAD MANAGER (FDM)

> Le challenger

FDM est un gestionnaire de téléchargement open source qui prend en charge les protocoles HTTP, HTTPS, FTP et BitTorrent. Il offre des fonctionnalités comme la planification des téléchargements, la reprise des téléchargement, la gestion de la bande passante et une interface utilisateur moderne.

Lien : www.freedownloadmanager.org

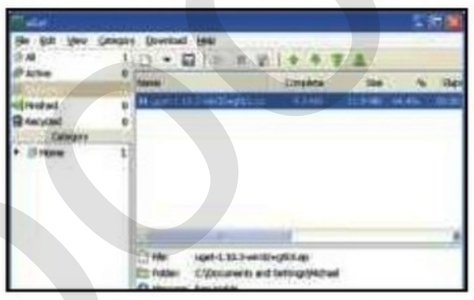
XTREME DOWNLOAD MANAGER (XDM)

> Un surdoué en fin de vie ?

Xtreme Download Manager est reconnu pour sa capacité à accélérer les téléchargements grâce à la segmentation des fichiers. Il excelle dans la capture de vidéos en streaming. Son intégration avec les navigateurs facilite la détection automatique des liens. Des plantages occasionnels sont à noter sur Windows et les mises à jour datent.

Lien : xtremedownloadmanager.com

UGET > Léger, stable, simple !



uGet est un gestionnaire de téléchargement open source léger, idéal pour les utilisateurs de Linux et Windows. Il offre une interface simple et prend en charge les téléchargements multi-connexions, les files d'attente et l'intégration avec les navigateurs. Moins riche en fonctionnalités que certains concurrents, sa légèreté et sa stabilité en font un choix fiable.

Lien : ugetdm.com

INTERNET DOWNLOAD ACCELERATOR (IDA)

> Vous êtes pressés ?

IDA est apprécié pour sa capacité à augmenter la vitesse de téléchargement en segmentant les fichiers. Il offre une intégration avec les navigateurs et prend en charge les protocoles HTTP, HTTPS et FTP. Cependant, certains utilisateurs ont exprimé des préoccupations concernant le support client et la stabilité du logiciel.

Lien : westbyte.com/ida/

TOP5 OUTILS DE SCAN DE VULNÉRABILITÉS RÉSEAU

NMAP > Le couteau suisse du scan réseau

Nmap (Network Mapper) est un outil open source incontournable pour la cartographie réseau et la détection de services. Grâce à son moteur de scripts NSE, il identifie les vulnérabilités spécifiques, configurations erronées et services obsolètes. Sa flexibilité et sa puissance en font un allié précieux pour les administrateurs système et les pentesters.

Lien : nmap.org

OPENVAS

> L'alternative open source à Nessus

OpenVAS est un scanner de vulnérabilités complet, maintenu par Greenbone Networks. Il offre une base de données régulièrement mise à jour et une interface web conviviale. Idéal pour les petites structures, son interface et configuration demeurent cependant complexes.

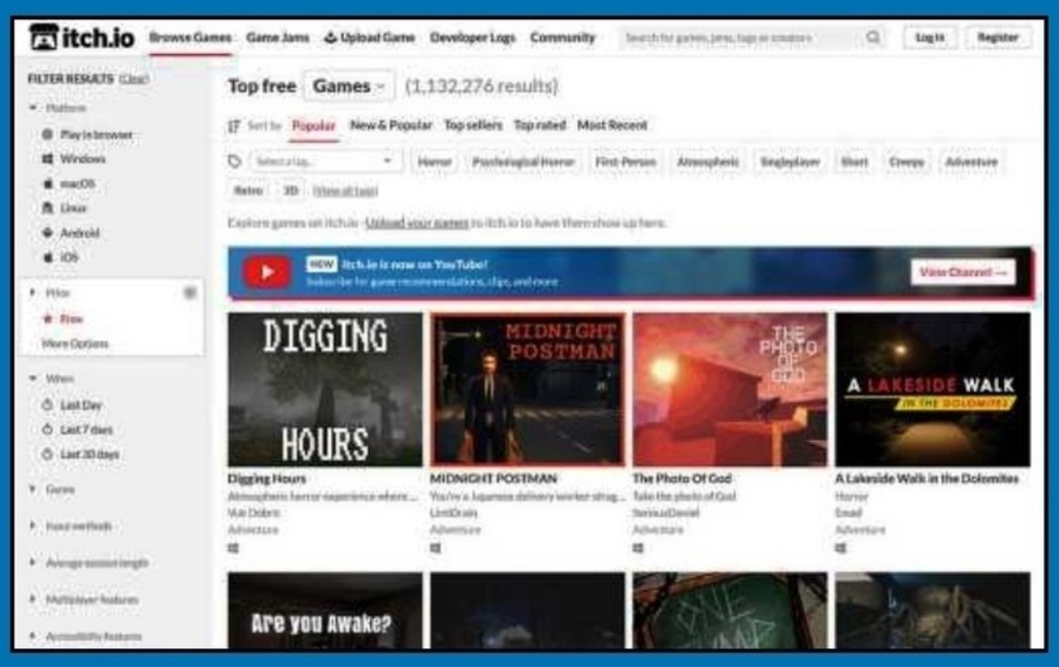
Lien : www.openvas.org

TOP5 TÉLÉCHARGER DES JEUX GRATUITS

ITCH.IO > L'ANTRE DE LA CRÉATIVITÉ INDÉPENDANTE

Itch.io est une plateforme emblématique pour les développeurs indépendants, offrant une vaste collection de jeux gratuits couvrant tous les genres imaginables. La communauté active et les fréquentes «game jams» garantissent un flux constant de nouveautés.

Lien : itch.io/games/free



STEAM (SECTION FREE-TO-PLAY) > LE GÉANT AUX TRÉSORS CACHÉS

Steam n'est pas seulement une plateforme de vente ; sa section Free-to-Play regorge de jeux de qualité, allant des MOBA aux FPS, en passant par des jeux de cartes et des simulateurs (Dota 2, Warframe, Team Fortress 2...). Certains jeux gratuits conservent la présence de microtransactions « in game ».

Lien : store.steampowered.com/tags/fr/Free-to-play/

MMOGAMES.COM > L'UNIVERS DES MMO GRATUITS

Pour les amateurs de jeux massivement multijoueurs, le site propose des critiques, des actualités et des liens vers des MMO gratuits, couvrant une variété de genres et de styles graphiques.

Lien : www.mmogames.com

INDIE GAME BUNDLES > LE RADAR DES BONS PLANS

Indie Game Bundles est un site qui recense les offres promotionnelles et les jeux gratuits disponibles sur diverses plateformes. Il est particulièrement utile pour ne pas manquer les distributions temporaires de clés Steam ou les bundles à prix réduit.

Lien : www.indiegamebundles.com/category/free/

ACID-PLAY > LE MUSÉE DU FREEWARE

Acid-Play est une archive dédiée aux jeux freeware, proposant une collection de titres classiques et rétro. Des remakes de Super Mario aux jeux d'action comme Soldat, le site ravira les nostalgiques et les curieux.

Lien : acid-play.com

OWASP ZAP > SCANNER WEB CIBLÉ POUR LES DÉVELOPPEURS

OWASP ZAP (Zed Attack Proxy) est un outil open source dédié à la sécurité des applications web. Il agit comme un proxy entre le navigateur et l'application, permettant d'intercepter et d'analyser les requêtes pour détecter des vulnérabilités. Compatible avec les pipelines CI/CD.

Lien : www.zaproxy.org

ZMAP > LE SCANNER ULTRA-RAPIDE POUR L'IPV4

ZMap est un scanner réseau open source, conçu pour effectuer des scans à grande échelle. Il peut scanner l'ensemble des adresses IPv4 en quelques minutes, en fonction de la bande passante. Idéal pour des analyses globales, il est principalement utilisé dans des contextes de recherche ou de sécurité offensive.

Lien : zmap.io

ZEROTHREAT > LE SCANNER MODERNE POUR APPLICATIONS WEB

ZeroThreat est axé sur les applications web et les API. Il détecte efficacement les vulnérabilités courantes comme celles listées dans l'OWASP Top 10 et fournit des suggestions de remédiation automatisées. Son interface intuitive et ses rapports clairs en font un outil accessible.

Lien : zerothreat.ai

Casser les codes et décrypter l'info

JE M'ABONNE à PIRATE INFORMATIQUE

LIVRAISON SOUS PLI DISCRET

OFFRE ABONNEMENT

1 AN POUR 19,90 € (au lieu de ~~23,60 €~~)

2 ANS POUR 35,40 € (au lieu de ~~47,20 €~~)

- LIVRÉ CHEZ VOUS !
- PRATIQUE & ÉCONOMIQUE !

LES GUIDES du HACKER et du PIRATE

- > Logiciels et applications exclusifs
- > Tutoriels et astuces clairs
- > Dossiers pratiques complets pour débutants et experts
- > Sélection et test de matériels
- > L'actu et les nouveautés !

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 19,90 €**

☐ **Abonnement à Pirate Informatique pour 8 numéros, je joins mon règlement de 35,40 €**

☐ 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.bii@gmail.com

Offre valable jusqu'au 31 décembre 2025. 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 – 1104, CHEMIN DE LA BATTERIE - 13500 MARTIGUES

RÉDUCTION JUSQU'À -25%

LES AVANTAGES :

- > Jusqu'à -25 % sur le prix en kiosques
- > Ne manquez aucun numéro
- > Ne soyez plus une victime
- > Vos magazines livrés chez vous gratuitement

LES DOSSIERS DU Pirate

DES DOSSIERS THÉMATIQUES COMPLETS

À DÉCOUVRIR EN KIOSQUES

PETIT FORMAT

MINI PRIX

CONCENTRÉ D'ASTUCES

100% Windows

Actuellement #Guide pratique

LE GUIDE ANTI-ESPIONS !

DARKNET

WEBCAM

SURVEILLANCE

CLOUD

Wi-Fi

CRYPTOS

ANONYMAT

TÉLÉCHARGER

RÉSEAUX SOCIAUX

PIRATE
INFORMATIQUE

IDPRESSE id presse

L 12730 - 64 - F: 5,90 € - RD

BELUX 6,80€ - CH 9,50CHF - PORT-CONT 6,90€ - DOM 6,70€ - NCAL 1050XPF -
POL 880XPF - MAR 66MAD - TUN 12TND - CAN 10,50$CAD