N°59

Casser les codes et décrypter l'info

PIRATE INFORMATIQUE

Février / Avril 2024

HACKING

TOUT SAVOIR SUR LES **ATTAQUES DDOS**

ANONYMAT

ACTIVEZ L'ANTI-CENSURE SUR **TOR**

BEST of 2024 HACKING

TOP 5 Les **MESSAGERIES** qui évitent **VRAIMENT** d'être **SURVEILLÉ**

Les vraies **SOLUTIONS GRATUITES**

ALIAS

CHANGEZ D'IDENTITÉ AVEC **ANONADDY**

BLACK DOSSIER

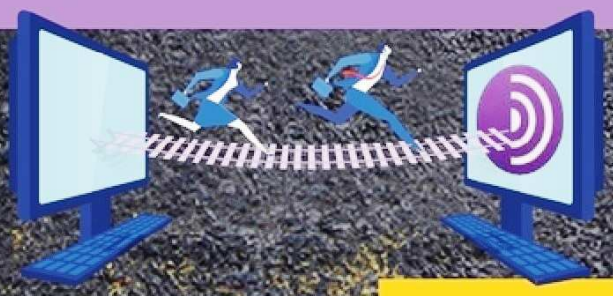
Les meilleurs **VPN** AU BANC D'ESSAI

LE GUIDE 2024

SOMMAIRE

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°59

Février – Avril 2024

Une publication du groupe ID Presse
Impasse de l'Espéron - Villa Miramar
13960 Sausset Les Pins

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

UN ESPACE À DÉFENDRE

Dans un réseau où chaque clic, chaque recherche, chaque interaction en ligne laisse une empreinte numérique, nous devenons malgré nous des produits commercialisables. Nos données, nos goûts, nos aversions, nos habitudes de vie sont scrutés, analysés, et vendus au plus offrant. Ce n'est pas seulement une question de marketing. Il s'agit d'une intrusion profonde dans nos vies personnelles, affectant notre liberté d'expression, notre autonomie de pensée et notre droit à évoluer. Qui sommes-nous sur le Web si chaque parcelle de notre identité est traquée, exploitée, conteneurisée, pesée et valorisée ?

Internet est un espace à défendre. Il nous revient, à chacun, de grignoter au quotidien ces bytes de liberté qui nous appartiennent. Les stratégies, les outils et les bons réflexes existent. Ils sont dans ces pages.
Bonne lecture !

La rédaction

LES BANQUES EUROPÉENNES PEUVENT-ELLES RÉSISTER AUX CYBERATTAQUES ?

La Banque centrale européenne procédera ce mois-ci à des cyber-stress tests sur les banques afin de déterminer leur résilience face aux cyberattaques. L'agence demande à 109 banques en Europe d'effectuer des évaluations de vulnérabilité et des évaluations de réponse aux incidents d'ici mi-2024. Dans chaque test, le régulateur européen simulera une cyberattaque perturbatrice capable de nuire aux opérations commerciales. La banque centrale surveillera ensuite la manière dont l'organisation financière réagit et se remet de l'attaque, ainsi que la rapidité avec laquelle elle reprend ses activités normales.

FORCER LES BANQUES À SE METTRE À NIVEAU

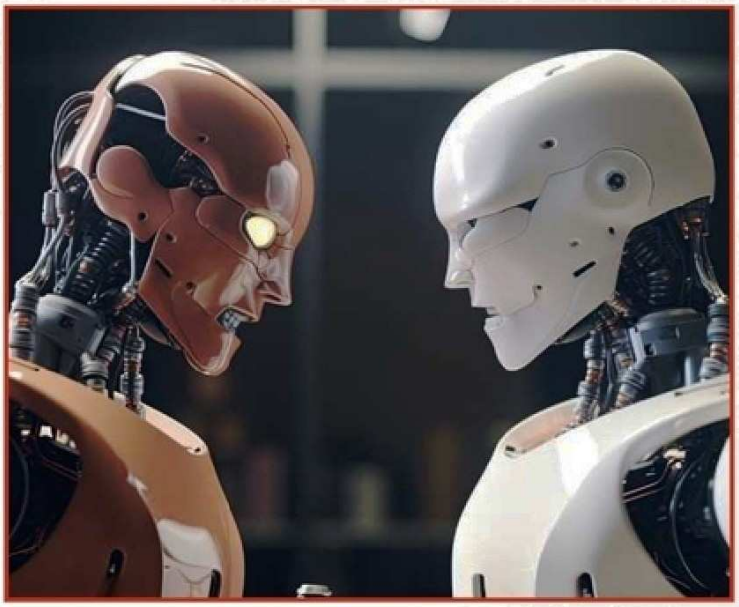
« Notre objectif principal est d'identifier les points faibles des banques », a déclaré en novembre Anneli Tuominen, membre du conseil de surveillance de la BCE. C'est bel et bien la guerre en la Russie et l'Ukraine qui a servi de catalyseur à la BCE pour obliger les institutions bancaires privées à se mettre à niveau. La banque centrale met ainsi les pieds dans le plat

> « Réduire les coûts n'est pas toujours compatible avec une bonne gestion des risques. »

et estime que les banques ne sont pas prêtes. Elle pointe du doigt une mauvaise gestion cyber en interne et dans l'organisation humaine et technologique de leurs systèmes d'information. Depuis l'invasion de l'Ukraine, les gouvernements européens et les organisations du secteur privé ont connu une augmentation des attaques par déni de service et des piratages de ransomware ciblant des fournisseurs de services tiers, confirmait récemment la BCE

« Les banques tentent de réduire leurs coûts en externalisant certains de leurs processus informatiques, mais cela n'est pas toujours compatible avec une bonne gestion des risques », a déclaré Tuominen. « Les banques doivent également comprendre les risques liés à l'externalisation.»

COMMENT JAILBREAKER CHATGPT ?



Nous nous amusons tous à tester et contourner les limites des robots de discussion comme ChatGPT, Bard et Bing Chat. Les algorithmes jalousement concoctés par leurs créateurs respectifs sont censés nous empêcher de générer du contenu qui pourrait être offensant, amoral, dangereux ou amener à la réalisation d'actions illégales. Ces restrictions sont souvent binaires (bien ou mal) et très dépendantes de la politique interne de chaque éditeur. En gros, pour éviter tout risque, ils limitent énormément, de façon assez obscure et infantilisante, le potentiel de leurs IA.

JEU DU CHAT ET DE LA SOURIS

De nombreux internautes s'amusent à créer des prompts (invites) qui sont censés court-circuiter cette logique. Cela s'appelle le « jailbreaking » (contournement des restrictions). Soit en se faisant passer pour quelqu'un d'autre (« Je suis un expert qui a absolument besoin de connaître ceci ou cela pour empêcher que de telles infos tombent entre de mauvaises mains »), soit en demandant au robot de se comporter comme une IA surpuissante libérée des contraintes humaines, soit en reformulant les questions de façon détournée, etc. Mais ChatGPT, Bard ou Bing apprennent eux aussi ces astuces et sont modifiés pour ne plus tomber dans la plupart des hacks connus. Un jeu du chat et de la souris qui épuisera l'humain avant la machine.

MASTERKEY : LE JAILBREAKER DOPÉ À L'IA

Du coup, un groupe international de chercheurs issus de plusieurs universités (Singapour, Chine, Australie et USA) ont utilisé un outil open source pour générer des invites en série jusqu'à trouver celles qui contournent les filtres. En utilisant un cadre qu'ils appellent «Masterkey», ces chercheurs ont pu automatiser ce processus de découverte de nouvelles vulnérabilités dans les systèmes basés sur de grands modèles de langage (LLM).
« En manipulant les réponses sensibles avec des robots de discussion, nous pouvons comprendre les subtilités de leur mise en œuvre (…) pour contourner les défenses », expliquent-ils.

TROIS FOIS PLUS DE JAILBREAKS

Les chercheurs affirment qu'en entraînant leur propre LLM sur des exemples d'invites de jailbreak courantes, ils ont pu générer de nouvelles invites fonctionnelles avec un taux de réussite de 21,58 %, plusieurs fois supérieur au taux de réussite de 7,33 % des invites de jailbreak connues actuellement. Temps de réponse plus ou moins longs, mots « drapeaux rouges », identification des règles, etc. : tous les tests permettent d'obtenir des connaissances et d'améliorer leur propre IA ainsi que les scénarios d'attaque. Selon les résultats, les anciens modèles d'IA comme GPT 3.5 ont été les plus touchés par ces attaques, avec un taux de réussite moyen des invites de 46,69 %, tandis que GPT 4, Bard et Bing Chat ont succombé aux attaques avec des taux moyens de 15,23, 14,64 et 13,85 %, respectivement. Les chercheurs affirment avoir pu contourner avec succès les filtres des robots de discussion pour générer plusieurs catégories de contenu interdit, y compris des sujets pour adultes comme la pornographie, des utilisations illégales, des violations de la vie privée et d'autres contenus nuisibles et abusifs.

Plus de tests, plus de connaissances, plus de scénarios d'attaque : Masterkey aide à comprendre comment fonctionnent les règles de chaque robot et à identifier plusieurs de leurs vulnérabilités. Beaucoup plus vite et de façon plus efficace que ce que peut faire un humain seul devant son écran.

MULTIPLICATION DES ATTAQUES DDOS FIN 2023

C'est d'abord la guerre menée par Israël sur le territoire palestinien qui a entretenu un très haut niveau d'attaques. Alors qu'au troisième trimestre 2023 Cloudflare observait déjà une augmentation des attaques DDoS, ainsi que des cyberattaques envers les médias et journaux Israéliens, ainsi que des institutions financières et les sites gouvernementaux, la poursuite du conflit a amplifié les attaques. Cloudflare observe une multiplication par 11 des attaques DDoS visant les sites web palestiniens. Le spécialiste a également atténué plus de 2,2 milliards de requêtes HHTP DDoS ciblant les sites web israéliens, les journaux et médias représentant près de 40% de l'ensemble des attaques.

Festival de fin d'année

Black Friday, Fêtes de fin d'année ou encore COP28, ce sont tout autant de temps forts qui rythme l'année des particuliers comme des professionnels. Mais ce sont également de parfaites occasions pour les cyberattaquants d'agir. Ainsi, le spécialiste observe une augmentation de 117% d'une année sur l'autre, des attaques DDoS visant les sites web de vente, d'expédition et de relations publiques pendant le Black Friday et la période des fêtes de fin d'année. Ainsi qu'une multiplication par 618 des attaques DDoS contre les sites des services environnementaux par rapport à l'année précédente, ce qui coïncide avec la 28ème Conférence des Nations Unies sur le changement climatique.

Nouvelle cible : les cryptomonnaies

Si le secteur des jeux d'argent est toujours présent dans le classement, le dernier trimestre 2023 a vu apparaitre un nouveau secteur, celui des crypto-monnaies. Toujours selon l'étude de Cloudflare, celui-ci affiche la 1ère place en termes de volume d'attaques.

CANAL+ LEADER DE LA LUTTE ANTI-PIRATAGE

Ultra-offensif, le groupe français multiplie les actions pour bannir tout flux sportif non autorisé du territoire français. C'est bel et bien Canal+ qui est parvenu ces deux dernières années à tarir une partie des sources de streaming en direct proposant des matchs de football ou de rugby.
Après avoir obtenu des ordonnances judiciaires

HALVING 2024

BITCOIN : FLAMBÉE ANNONCÉE AU PRINTEMPS ?

Au tournant du printemps 2024, probablement entre la fin mars et mi avril, le Bitcoin s'apprête à vivre un moment crucial avec le phénomène du « halving ». Historiquement, cet événement a conduit à une envolée remarquable de la valeur de la monnaie virtuelle...

C'EST QUOI LE HALVING ?

Satoshi Nakamoto, créateur supposé du Bitcoin, a voulu que ce dernier soit semblable à l'or, disponible en quantité finie. Il a défini une limite : seulement 21 millions de bitcoins seront jamais créés. Le principe du « halving », ou réduction par deux, est central dans cette stratégie.

Le principe est le suivant : tous les quatre ans, la quantité de Bitcoins générée par le minage (processus de création de nouveaux bitcoins) est divisée par deux. Cette mesure vise à s'aligner sur l'évolution de la puissance de calcul informatique.

Initialement, en 2009, 50 nouveaux bitcoins étaient générés toutes les 10 minutes ; le premier halving a eu lieu le 28 novembre 2012, réduisant cette quantité à 25 bitcoins toutes les 10 minutes ; le deuxième halving, en mi-2016, a encore diminué cette quantité à 12,5 ;

Le troisième halving, le 11 mai 2020, a vu la production chuter à 6,25 bitcoins toutes les 10 minutes. En avril 2024, la production chutera donc à 3,125 bitcoins toutes les 10 minutes pour les quatre ans qui viennent.

DES BITCOINS PLUS DIFFICILES À MINER

Historiquement, après chaque halving, la valeur du Bitcoin a connu une forte augmentation :

1er halving : la valeur du Bitcoin est passée de 13 $ à 1 152 $;

2eme halving : la valeur du Bitcoin est passée de 664 $ à 17 760 $;

Suite au troisième halving, elle a bondi de 9 774 $ à 67 549 $.

Comment justifier de telles augmentations ? Cela s'explique par la dynamique de l'offre et de la demande. Les bitcoins devenant plus rares et couteux à produire, leur prix tend à augmenter. Et, effectivement, depuis la fin de l'année 2023, la valeur de cette cryptomonnaie a repris son ascension. À suivre !

pour contraindre les fournisseurs d'accès à Internet (FAI) français à bloquer des sites populaires tels que Footybite et Streamcheck, Canal+ vise maintenant à colmater les brèches laissées ouvertes par les solutions de contournement des utilisateurs. Car les plus informés et les plus geeks des amateurs de sports savent qu'il « suffit » de changer de serveurs DNS pour débrider ce blocage. En passant par exemple par les serveurs DNS proposés des sociétés comme Cloudflare , Google ou Cisco (OpenDNS), un internaute peut continuer à accéder à ces sites bannis par leur FAI.

NOUVELLE ACTION EN JUSTICE

En mai 2023, une étude de l'Arcom indiquait que, confrontés à un site bloqué, près de la moitié des internautes contrevenants (46 %) abandonnaient complètement l'idée de regarder le contenu. Parmi tous les utilisateurs contrevenants, seulement 6 % ont tenté de contourner les mesures de blocage en utilisant un DNS alternatif, un VPN ou une méthode similaire. Même face à ce chiffre presque anecdotique, Canal+ maintient sa pression et entend étendre sa politique au napalm : le groupe français a depuis intenté un nouveau procès devant le tribunal judiciaire de Paris pour contraindre les fournisseurs DNS tiers à adopter des mesures de blocage similaires !

À SAVOIR

Le rapport 2022 de l'Arcom, publié en mai 2023, a révélé une baisse significative du nombre de spectateurs de retransmissions sportives illicites en France, passant de 2,8 millions en 2021 à 1,6 million en 2022. Ces statistiques témoignent de l'efficacité des mesures de blocage DNS déjà en place.

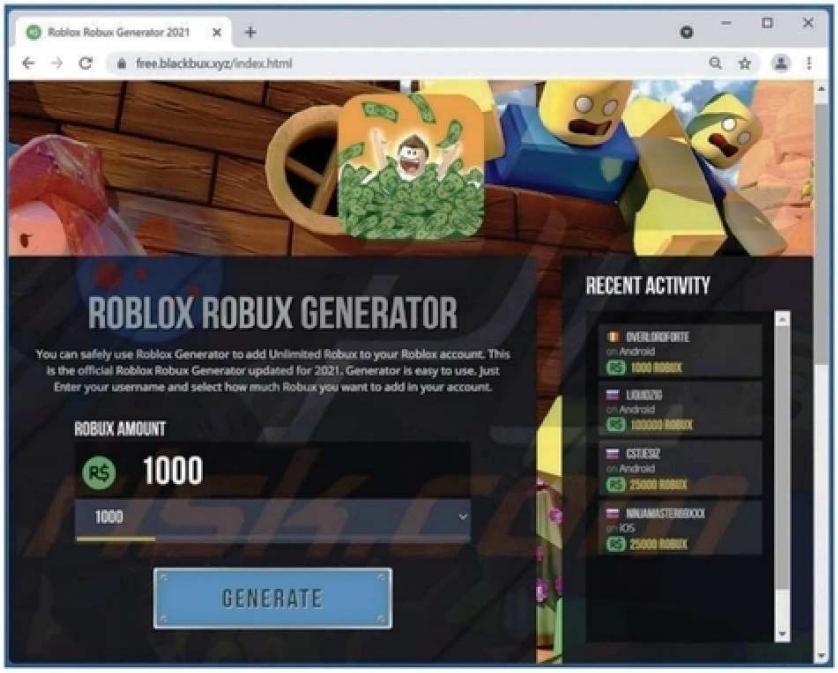
JEUX VIDÉO : À L'ÉCOLE DES APPRENTIS HACKERS

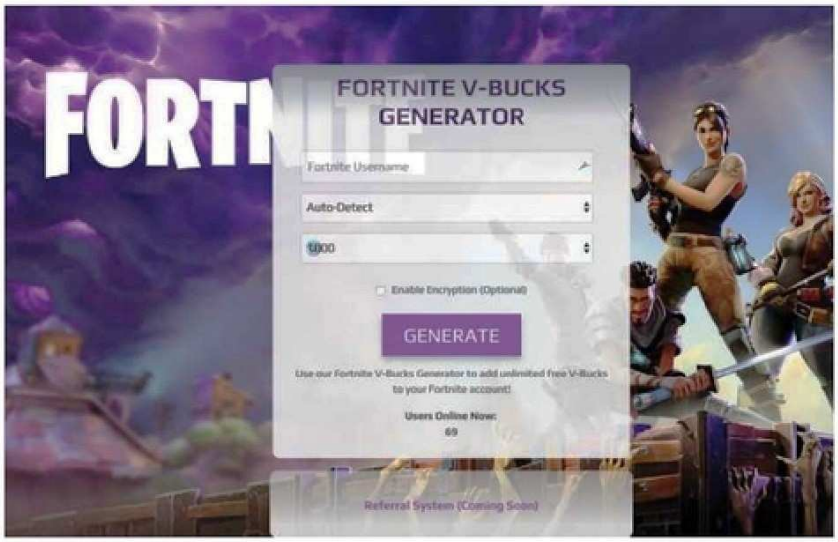
Les jeux en ligne populaires comme «Minecraft» et «Roblox» sont devenus des cibles de choix pour les cybercriminels. Leur grande audience, surtout composée d'enfants et d'adolescents, attire les pirates informatiques qui mettent en place des arnaques, du vol de comptes, et diffusent des logiciels malveillants. Ces plateformes servent également de terrains d'entraînement pour de jeunes hackers, qui commencent par des petits méfaits dans ces jeux avant de s'orienter vers des activités criminelles plus sérieuses.

VOL DE COMPTES

En 2022, une alerte surgit sur un forum de «Adopt Me», jeu populaire de Roblox. Un message avertissait contre NeedleworkerJaded336, un joueur proposant des échanges d'objets via des messages privés, utilisant un lien frauduleux qui semblait renvoyer vers un profil Roblox. En réalité, ce lien redirigeait vers un site factice,

Roblox.com.vu, conçu pour dérober les identifiants des joueurs. Ce stratagème, appelé «beaming», est devenu une pratique courante parmi les pirates de bas niveau qui créent des faux profils pour tromper les utilisateurs.
Ce phénomène n'est pas isolé. Des jeux en ligne célèbres comme Fortnite ou Minecraft servent aussi de terrains de chasse aux cybercriminels. Selon un rapport de Kaspersky, ces jeux attirent non seulement des millions de joueurs mensuellement, mais aussi des pirates informatiques à l'affût. Minecraft, par exemple, avec ses 100 millions de joueurs par mois, offre un marché noir florissant pour les versions piratées du jeu, où les virus sont souvent dissimulés.





TOUTE OFFRE SUGGÉRANT QUE L'UTILISATEUR PEUT GAGNER OU GÉNÉRER GRATUITEMENT DES ROBUX OU DES V-BUCKS (LES MONNAIES VIRTUELLES DE ROBLOX ET DE FORTNITE) EST UNE ARNAQUE !

ATTENTIONS AUX MODS ET EXTENSIONS

Les «mods» et extensions, en particulier dans Minecraft, ouvrent une autre porte aux logiciels malveillants. Des plateformes de distribution de mods ont découvert des logiciels malveillants cachés dans des téléchargements, destinés à voler des données personnelles et des cryptomonnaies.
Outre la menace des virus, les jeux en ligne sont également le théâtre d'arnaques sophistiquées. Des sites promettant des monnaies virtuelles gratuites, comme les «robux» de Roblox, ne sont souvent que des escroqueries visant à générer des revenus publicitaires pour leurs auteurs, sans jamais délivrer les promesses faites aux joueurs.

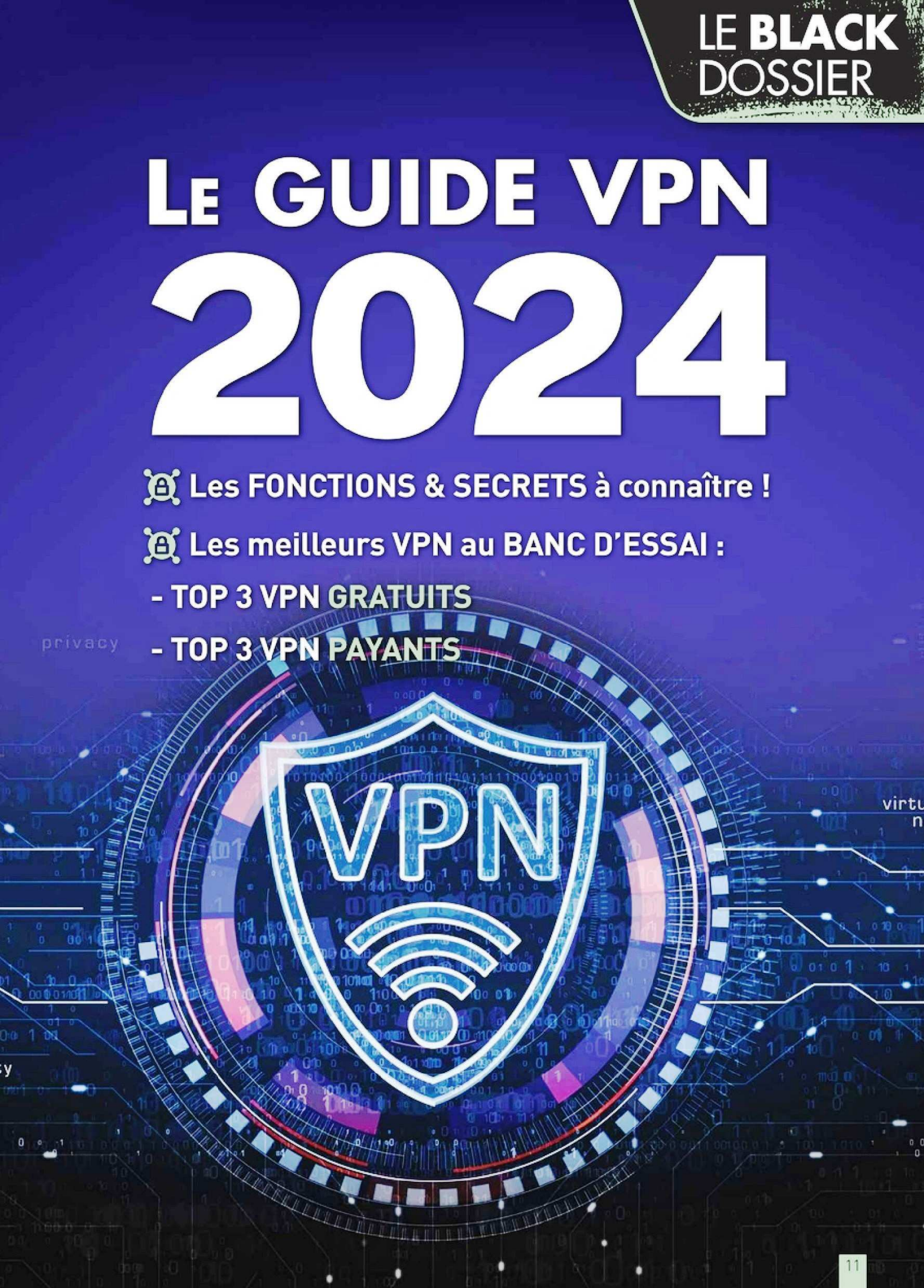
PREMIÈRES ARMES POUR DES ADOS ESCROCS

Cette sphère d'activité illégale attire également de jeunes pirates. Des enquêtes ont révélé que des adolescents, eux-mêmes joueurs, orchestrent ces escroqueries. Et ils font même des tutos vidéo sur YouTube pour expliquer leurs modus operandi ! De même, des sites de phishing visant les comptes Roblox ont été reliés à de jeunes pirates.
Ces jeux en ligne ne sont donc pas seulement des aires de jeux, mais aussi des écoles pour les cybercriminels de demain. Des cas comme celui de Graham Clark, impliqué dans le piratage de comptes Twitter en 2021, et Yannox un jeune français condamné en juillet 2023 pour une trentaine d'infractions dont une attaque du CNED, illustrent cette progression. Ces jeunes ont commencé par des escroqueries dans des jeux comme Minecraft, avant de s'engager dans des activités criminelles plus sérieuses.


FREE JULIAN
ASSANGE

LE GUIDE VPN 2024

- Les FONCTIONS & SECRETS à connaître !
- Les meilleurs VPN au BANC D'ESSAI :
  - TOP 3 VPN GRATUITS
  - TOP 3 VPN PAYANTS



VPN & ANONYMAT

COMMENT ÇA MARCHE ?

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

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

LE VPN : ANONYMAT DEPUIS VOTRE TERMINAL

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

Un VPN masque votre identité (adresse IP) et chiffre vos données pour que personne ne puisse espionner les contenus que vous échangez sur la Toile, dès votre box Internet !

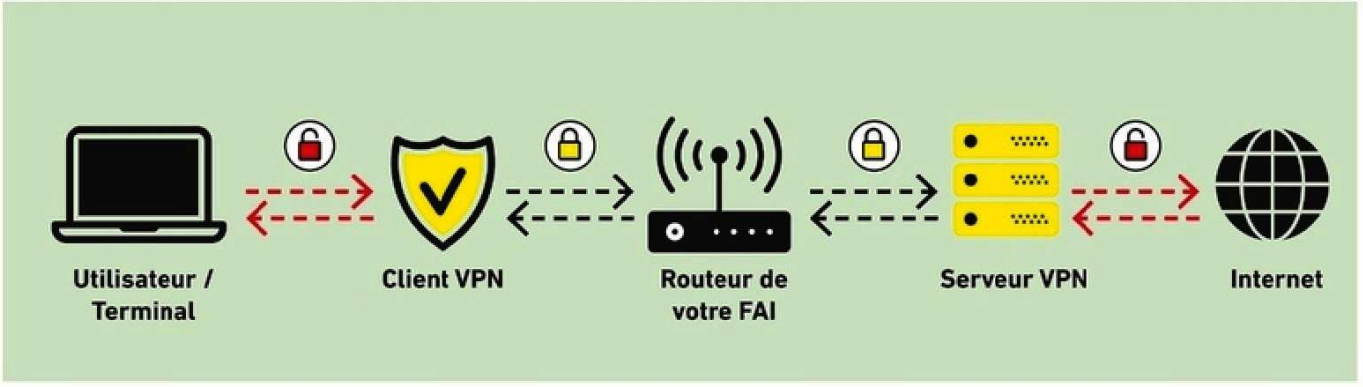
de déchiffrement appropriée. Une fois chiffrées, vos données sont envoyées au serveur VPN distant, où elles sont déchiffrées et transmises (enfin !) à leur destination finale sur Internet. Pour les sites Web visités, il semble que les demandes proviennent du serveur VPN et non de votre appareil (c'est pourquoi votre adresse IP est inconnue des sites visités puisque c'est celle du serveur VPN qui apparait).
Quant à votre FAI, il a perdu votre trace depuis longtemps et ne sait pas ce qui est passé par ses nœuds et serveurs puisque les données chiffrées qu'il a fait transiter sont illisibles pour lui.

LES LIMITES

Mais attention, un excès de confiance est votre pire ennemi ! Ce n'est pas parce que vous utilisez un VPN que vous pouvez faire n'importe quoi. Toutes les données que vous renseignerez sur des sites ou applis (messages, mails, données bancaires, mots de passe, documents, adresses, etc.) sont, elles, toujours accessibles depuis les serveurs des sites Web visités. Et, de la même manière, tout ce qui arrive sur votre disque dur est déchiffré et accessible à un pirate ou à un regard malveillant qui aurait accès à votre terminal.
Enfin, vous devez avoir confiance dans votre VPN : vos données sont-elles véritablement chiffrées de bout en bout, a-t-il prévu une backdoor de déchiffrement, conserve-t-il vos données (logs), etc. Une architecture VPN coûte cher et vos données valent de l'or : seuls les VPN payants et audités régulièrement par des tiers de confiance semblent, jusqu'à

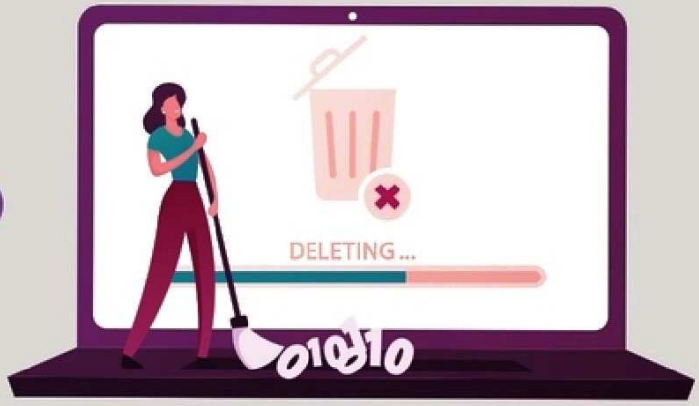
preuve du contraire, sérieux en la matière. Quant aux gratuits, à part ceux de notre sélection, attention aux mirages aux alouettes !

Comment fonctionne un VPN ?



QUAND VOUS ACTIVEZ VOTRE CLIENT VPN SUR VOTRE APPAREIL, CE DERNIER CHOISIT AUTOMATIQUEMENT LE SERVEUR DISPONIBLE LE PLUS RAPIDE (GÉNÉRALEMENT PAS TROP LOIN DE CHEZ VOUS) OU UN SERVEUR DANS UN PAYS QUE VOUS LUI AUREZ DEMANDÉ. À PARTIR DE LÀ, TOUTES VOS REQUÊTES ET RÉCEPTIONS DE DONNÉES PASSERONT PAR CE SERVEUR. VOUS N'EXISTEZ PLUS, TOUT SE FAIT COMME SI C'ÉTAIT CE SERVEUR QUI ENVOIE ET REÇOIT LES DONNÉES. SAUF QUE, CACHÉ DERRIÈRE LUI, C'EST BIEN VOUS QUI ÊTES À LA COMMANDE. MAIS LES INFORMATIONS QUI TRANSITENT PAR VOTRE ROUTEUR SONT, ELLES, CHIFFRÉES ET ANONYMISÉES JUSQU'À CE QU'ELLES SOIENT LUES EN CLAIR SUR VOTRE PC OU MOBILE. CE SONT EN EFFET LE LOGICIEL OU L'APPLI VPN (LE « CLIENT ») INSTALLÉ QUI PERMET CE PASSAGE DE L'OMBRE À LA LUMIÈRE SANS QUE VOUS AYEZ À VOUS PRÉOCCUPER DE QUOI QUE CE SOIT.

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



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

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

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

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

FAILLE DE SÉCURITÉ

Lorsqu'un fournisseur VPN stocke des données, il y a un risque que ces informations tombent entre les mains de cybercriminels, d'entités gouvernementales ou d'autres tiers, ce qui peut compromettre votre vie privée. Choisir un VPN qui applique rigoureusement une politique de non-conservation des logs vous assure que vos actions sur Internet restent confidentielles et protégées, même en cas de demandes juridiques.
Il est donc essentiel de privilégier des fournisseurs de VPN qui garantissent cette politique « No Log ». Mais, attention, certains l'affirment sans respecter cette exigence ! S'il est important de trouver des déclarations explicites affirmant que le fournisseur ne garde ni logs d'activité ni logs de session, seuls des audits indépendants réalisés par des tiers peuvent fournir une assurance supplémentaire quant à la véracité des déclarations d'un fournisseur. Heureusement, conscients de cette suspicion, la majorité des fournisseurs de VPN sérieux mettent en avant l'existence de ces audits et les références des sociétés spécialisées les ayant réalisées.

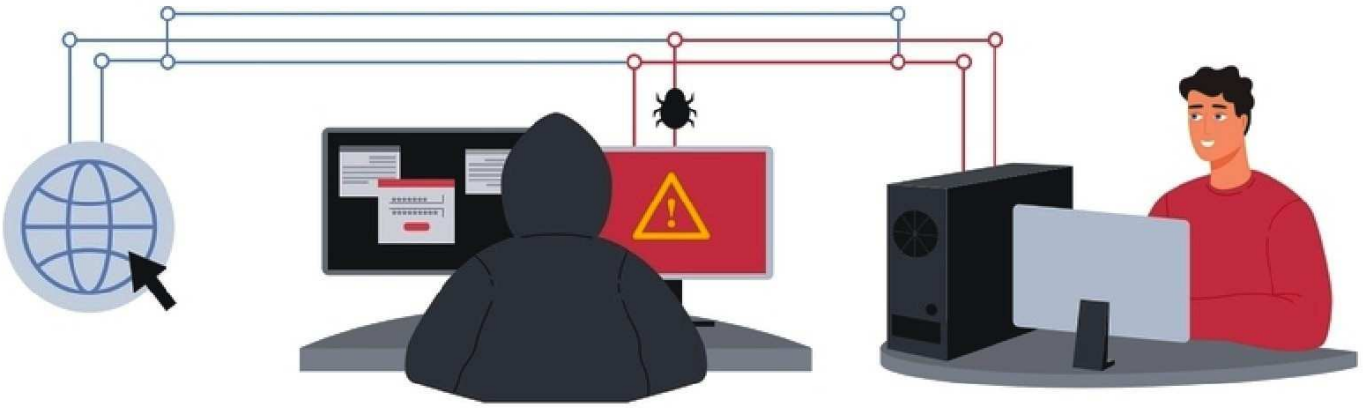
Pourquoi confier à une société privée des informations que vous souhaitez masquer aux autres acteurs du Web ? Un fournisseur de VPN ne doit enregistrer et conserver aucune donnée.

POURQUOI UTILISER UN VPN ? 4 BONNES RAISONS EN DÉTAIL

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

1# SE PROTÉGER DES PIRATES

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



2# PROTÉGER SA VIE PRIVÉE ET SON IDENTITÉ

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

Attention, certains sites et services bannissent de plus en plus d'adresses IP connues comme appartenant à des serveurs VPN

3# CONTOURNER LES RESTRICTIONS GÉOGRAPHIQUES

Les VPN peuvent vous permettre d'accéder à des contenus qui sont géographiquement restreints, toujours grâce à ce changement d'adresse IP. Par exemple, si un service de streaming propose des émissions différentes selon les pays, vous pouvez utiliser un VPN pour accéder à ces contenus en vous connectant à un serveur situé dans le pays concerné. Pour le site visité, votre IP correspondra par exemple à celle d'un utilisateur américain (pour accéder à tout le catalogue de Netflix par exemple), indonésien ou suisse. Attention, certains sites et services bannissent de plus en plus d'adresses IP connues pour appartenir à des serveurs VPN. Un bon VPN doit donc continuellement chercher et proposer de nouvelles localisations d'adresses IP.

REGARDER TOUS LES PROGRAMMES NETFLIX MÊME CEUX BLOQUÉS EN FRANCE ? IL SUFFIT DE SE CONNECTER AU CATALOGUE US GRÂCE À UNE IP AMÉRICAINE.

4# CONTOURNEMENT DE LA CENSURE

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

10 POINTS À VÉRIFIER POUR BIEN CHOISIR SON VPN

1# CHIFFREMENT FORT

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

2# POLITIQUE DE NON-CONSERVATION DES LOGS

Cette politique signifie que le fournisseur VPN ne conserve pas de registres de votre activité en ligne, ce qui est crucial pour votre confidentialité. C'est-à-dire que personne, que ce soit votre fournisseur de VPN, un pirate ou une autorité ne peut récupérer votre historique de connexions sur les serveurs du VPN.

3# JURIDICTIONS PROTECTRICES DES DONNÉES

Vous devez aussi vérifier dans quel État est enregistrée la société éditrice du VPN. Préférez, dans la mesure du possible, des sociétés situées dans des juridictions respectueuses de la vie privée. Les États-Unis, la Russie, la Chine, le Royaume-Uni ou l'Australie sont par exemple des états qui peuvent exiger juridiquement d'avoir accès à des données centralisées ! Au contraire, voici ci-dessous des juridictions considérées comme respectueuses de la vie privée sur Internet et qui ont des lois strictes en matière de protection des données :

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

Ces juridictions sont souvent privilégiées par les fournisseurs de VPN qui souhaitent offrir une confidentialité maximale à leurs utilisateurs.

4# NOMBRE, QUALITÉ ET LOCALISATIONS DES SERVEURS

Un grand nombre de serveurs dans différents pays signifie que vous avez plus d'options pour masquer votre emplacement réel et accéder à un contenu géographiquement restreint. Et plus de serveurs signifie aussi que la bande passante de votre opérateur VPN

n'est pas saturée par le nombre d'utilisateurs. C'est donc un critère essentiel pour assurer une navigation fluide et rapide, et encore davantage pour le streaming, le téléchargement ou le jeu vidéo en ligne. D'ailleurs, certains fournisseurs ont compris cette demande en insistant sur le fait qu'une partie de leur parc serveurs est optimisée pour le streaming par exemple afin de garantir des débits élevés et stables ! L'existence de serveurs VPN proches de chez vous est enfin un plus si c'est bien la vitesse que vous recherchez !

5# COMPATIBILITÉ ET FACILITÉ D'UTILISATION

Le VPN doit être compatible avec une variété de dispositifs et offrir une interface facile à utiliser, même pour les débutants. Les fonctions de bases doivent être configurables et accessibles facilement. Car configurer un VPN peut entraîner des soucis avec certains protocoles (messageries,

FTP, cloud, etc.) que vous utilisiez auparavant sans problème. Les utilisateurs doivent être guidés en cas de souci (FAQ, tutos, etc.) et un service client francophone doit être disponible gratuitement pour répondre à leurs questions.

6# FONCTIONNALITÉS SUPPLÉMENTAIRES

Des fonctionnalités comme un «kill switch» (qui coupe votre connexion Internet si le VPN tombe), une protection contre les fuites DNS, et le split tunneling (qui permet de router certaines applications via le VPN et d'autres directement sur Internet) sont des ajouts précieux. Certaines fonctions sont aussi réservées aux gamers, d'autres vous permettent de vous connecter à Tor en plus de votre VPN, d'utiliser un cloud chiffré, d'accéder à un réseau mesh, etc.

7# CONNEXIONS SIMULTANÉS

Pour un abonnement VPN, vous pouvez connecter plusieurs appareils avec un seul compte. Oui, mais combien ? Votre PC, celui d'un ou plusieurs membres de la famille, votre téléphone, celui d'un ou plusieurs membres de la famille, un player ou TV connectés, etc. : très rapidement, vous allez vous apercevoir que la possibilité d'installer votre VPN sans surcoûts sur plusieurs terminaux est indispensable. Alors, vérifiez cette info avant de souscrire !

8# PRIX ET RAPPORT QUALITÉ-PRIX

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

> Le prix est bien sûr un facteur déterminant. Mais les moins chers ne sont pas tous recommandables...

9# AVIS ET RÉPUTATION

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

10# POLITIQUE COMMERCIALE

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

TOP 3 VPN GRATUITS

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

PROTONVPN FREE

> USAGE ILLIMITÉ

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

Lien :
protonvpn.com/fr/free-vpn

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

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

WINDSCRIBE

> 10 GO ET 10 PAYS !

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

Lien :
fra.windscribe.com

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

Les -
- Données limitées
- Sélection de serveurs limitée en version gratuite

TUNNELBEAR

> EN TOUTE SIMPLICITÉ

TunnelBear est un VPN gratuit qui a su se démarquer par son approche axée sur la simplicité d'utilisation, ce qui en fait une option idéale pour les utilisateurs novices en matière de VPN. Outre un chiffrement pro et un nombre de serveurs conséquent, il propose également une fonction de Kill Switch, qui coupe automatiquement la connexion à Internet en cas de perte de la connexion VPN, garantissant ainsi que vos données restent sécurisées. Par contre, la limite de 500 Mo par mois est insuffisante pour un usage régulier. Il est possible d'obtenir 1 Go de données supplémentaires en tweetant sur TunnelBear.

Lien : www.tunnelbear.com

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

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

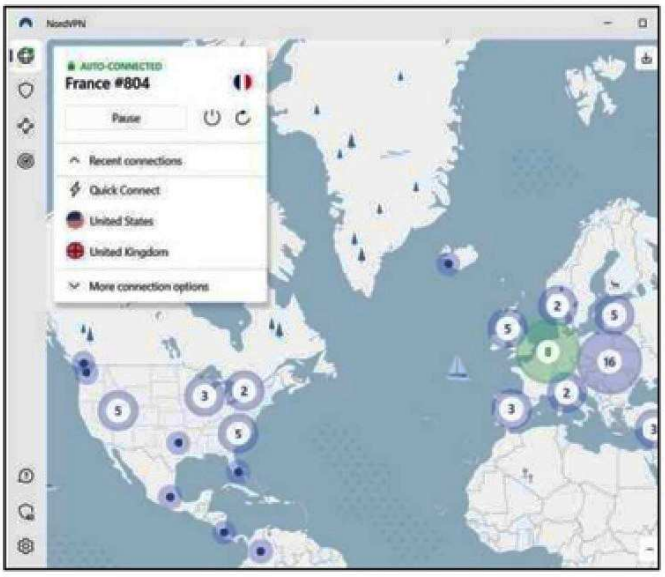
TOP 3 VPN PAYANTS

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

NORDVPN

> MALIN ET RAPIDE

NordVPN est peut-être le plus connu des VPN, autant par ses campagnes publicitaires que par la qualité réelle des services fournis. Il est un excellent compromis entre facilité d'utilisation et fonctions avancées pour les geeks.
Son nombre et la qualité de ses serveurs, associés au protocole NordLynx, en font un VPN agile et rapide qui ne ralentira que très peu votre connexion. Il propose aussi des serveurs spécialisés P2P et streaming ainsi que des serveurs Double VPN (vous passez par deux serveurs différents en série pour brouiller encore plus les pistes). Et vous pouvez même choisir un mode Obfuscation pour contourner la censure si vous êtes dans un pays qui bannit ou condamne l'usage d'un VPN.
NordVPN excelle dans le déblocage de contenus géorestreints et est excellent au jeu du chat et de la souris (comme avec Netflix). L'interface est claire et esthétique, offrant une prise en main intuitive et des options de personnalisation. Attention, lors de la configuration, vous devez savoir quels services vous souhaitez activer, car tout s'enchaine rapidement et sans trop d'explications, au risque parfois de se tromper et de créer des conflits avec certains protocoles. Heureusement, le retour en arrière est ensuite possible.



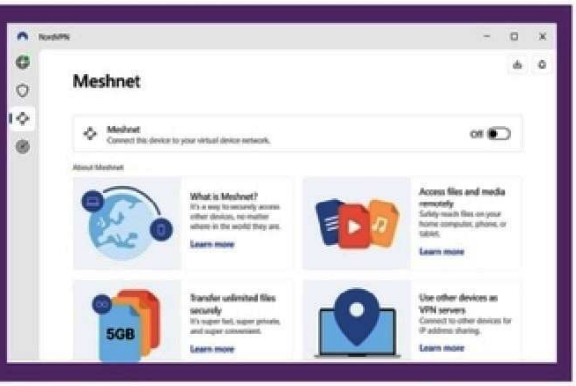
FONCTIONS EXCLUSIVES

NordVPN inclut un Kill Switch, une protection anti-menaces contre les malwares et traqueurs, des préréglages personnalisables ainsi qu'une fonctionnalité Réseau Mesh pour connecter plusieurs appareils entre eux. L'abonnement NordVPN est disponible sur divers appareils et systèmes d'exploitation, y compris sur AndroidTV, mais est le moins généreux des trois VPN sélectionnés avec seulement 6 connexions simultanées.
Un service client réactif et utile est enfin disponible 24/7 via chat en ligne.

Lien : nordvpn.com

Réseau mesh, c'est quoi ?

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



CYBERGHOST

> PUISSANCE ET SÉRIEUX

CyberGhost, fondé dès 2011 et acquis par Kape Technologies en 2018, se distingue par son large réseau : il offre près de 10 000 serveurs dans 100 pays, y compris des serveurs NoSpy opérés en interne pour une sécurité accrue. Bien que son grand nombre de serveurs n'assure pas toujours des débits supérieurs à la concurrence, CyberGhost a commencé à déployer des serveurs 10 Gb/s pour améliorer les performances. À surveiller de près donc en 2024 pour obtenir des données fiables... et stables quand ce maillage sera pleinement opérationnel.

Car CyberGhost cible ici son concurrent NordVPN, jugé plus puissant et optimisé. Il met donc en avant sa capacité à gérer le trafic issu du streaming, torrenting et... gaming. Ce dernier point étant parfois remis en question par des utilisateurs.

VPN TOUT TERRAIN

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

Lien : www.cyberghostvpn.com

Le Split Tunneling, c'est quoi ?

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

SURFSHARK

> UNE INNOVATION MORDANTE

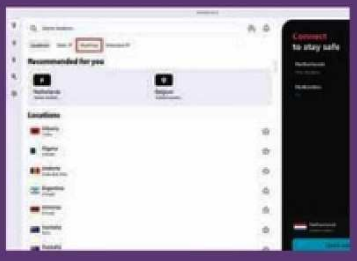
Fondé en 2018, Surfshark a été acquis par Nord Security en 2022, mais opère indépendamment. Il est domicilié aux Pays-Bas, un État membre des 14 Eyes, ce qui est un moins conséquent dans ce classement. Mais il intègre le podium pour trois caractéristiques essentielles :
- Sa politique tarifaire est très agressive et il propose régulièrement les meilleures offres du marché ;
- En second lieu, Surfshark propose des innovations qui séduiront les plus geeks... ou les plus paranoïaques (pour compenser le fait que la société soit basée aux Pays-Bas sans doute) ;
- Il propose un nombre illimité d'appareils connectés avec un seul abonnement !
Surfshark dispose de plus de 3200 serveurs dans plus de 100 pays, avec lui aussi une transition vers des serveurs 10 Gb/s pour des performances améliorées. Il applique une politique stricte de non-conservation des données, auditée et confirmée par Deloitte.

OUTILS ANTI-CENSURE

Le VPN batave offre des fonctionnalités telles que le mode Camouflage, Dynamic MultiHop, IP dédiées, et Alternative ID pour des alias numériques. Avec son projet Nexus, il développe aussi un réseau maillé de serveurs permettant une rotation automatique des IP pour renforcer l'anonymat et la stabilité des connexions. Sa solution de sécurité Surfshark One inclut enfin des outils de cybersécurité comme un antivirus, un module d'alerte de fuite de données, et un moteur de recherche privé.
Un support technique réactif est enfin disponible 24/7.

Lien : surfshark.com

Camouflage et MultiHop, c'est quoi ?



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

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

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

Notre sélection en détails

	Cyber Ghost	NordVPN	SurfShark
Tarifs*	2,20 € / mois pour un engagement de 2 ans	2,99 € / mois pour un engagement de 2 ans	**1,99 € / mois pour un engagement de 2 ans**
Période d'essai	**45 jours satisfait ou remboursé**	30 jours satisfait ou remboursé	30 jours satisfait ou remboursé
Chiffrement	Protocoles OpenVPN, IKEv2 et WireGuard avec chiffrement AES-256	**OpenVPN et le réputé NordLynx basé sur WireGuard avec chiffrement AES-256**	Protocoles OpenVPN, IKEv2 et WireGuard avec chiffrement AES-256
Juridiction	Roumanie	**Panama**	Pays-Bas
Nombre de pays couverts	**100**	60	**100**
Nombre de serveurs	**9500**	5100	3200
Serveurs dédiés	**Oui - Streaming, P2P et gaming**	Oui - Streaming et P2P	Oui - Streaming
Nombre d'appareils simultanés	7	6	**Illimité**
Fonctions avancées	Kill Switch, Split tunneling, IP dédiée, Smart Rules...	Kill Switch, Réseau Mesh, Cloud, Tor over VPN, DoubleVPN, IP dédiée, Obfuscation...	**Kill Switch, Camouflage, NoBorders, MultiHop, CleanWeb, ByPasser, IP rotative, IP fixe...**
Vitesse des débits	★★★★½	★★★★½	★★★★½
Politique de conservation des logs	**No log strict**	**No log strict**	**No log strict**
OS compatibles	**Windows, Android, Mac, iOS, Linux extensions pour navigateurs**	**Windows, Android, Mac, iOS, Linux extensions pour navigateurs**	Windows, Android, Mac, iOS, extensions pour navigateurs
URL	**www.cyberghostvpn.com**	**nordvpn.com**	**surfshark.com**

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

L'INFORMATIQUE FACILE
POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

TUTO

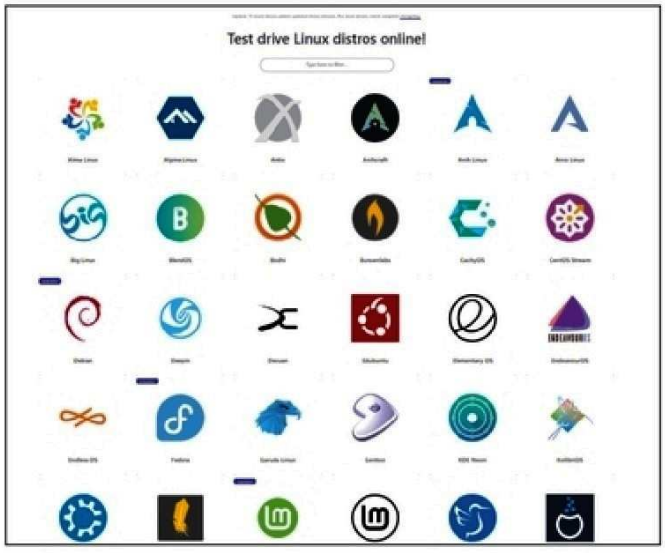
ESSAYEZ PLUSIEURS DISTRIBUTIONS LINUX... EN LIGNE !

DistroSea est un service en ligne qui permet de tester diverses distributions Linux directement dans un navigateur web, sans installation ou démarrage via un support externe.

DistroSea offre la possibilité de tester rapidement et gratuitement près de 60 distributions Linux en ligne ! Particulièrement utile pour ceux qui souhaitent explorer différents environnements Linux sans les installer sur leur système.

ENVIRONNEMENTS COMPLETS ET EN TEMPS RÉEL

Les serveurs du site simulent un environnement Linux complet qui s'affichera au sein même de votre fenêtre de navigateur. Lorsqu'un utilisateur sélectionne une distribution, DistroSea crée une instance virtuelle de cette dernière et vous pourrez la piloter en temps réel depuis votre PC.



60 DISTRIBUTIONS LINUX ACCESSIBLES SANS INSCRIPTION... ET PLUS DE 500 POSSIBILITÉS AVEC LES DIFFÉRENTES VERSIONS PROPOSÉES POUR CHACUNE !

Les utilisateurs peuvent interagir avec l'interface graphique de la distribution, ouvrir et utiliser des applications, et même tester des commandes dans le terminal. Bien que l'expérience puisse varier légèrement par rapport à une installation locale en termes de performance, elle offre un aperçu précieux de l'aspect et du fonctionnement de la distribution.

Vous pourrez changer de distribution en quelques clics jusqu'à découvrir celle qu'il vous faut ! Vous avez même la possibilité de comparer les ergonomies et fonctionnalités de deux distributions en même temps, en les plaçant côte à côte dans des onglets séparés.

QUELQUES EXEMPLES DE DISTRIBUTIONS LINUX DISPONIBLES

Ubuntu : Une distribution populaire et facile à utiliser, basée sur Debian.

Linux Mint : Connue pour son environnement de bureau intuitif, adapté aux utilisateurs recherchant un système d'exploitation stable et élégant.

Debian : Réputée pour sa stabilité et son support d'une large gamme d'architectures.

openSUSE : Offre des versions à publication continue et à publication fixe, adaptées à divers cas d'utilisation.

Manjaro : Une distribution basée sur Arch Linux, offrant un modèle à publication continue.

Zorin OS : Conçue pour la facilité d'utilisation et la familiarité, en particulier pour les utilisateurs débutants.

Rocky Linux : Une distribution Linux d'entreprise pilotée par la communauté, alternative compatible binaire à Red Hat Enterprise Linux (RHEL).

DÉCOUVREZ DISTROSEA

PRATIQUE

01› LE SITE

Rendez-vous sur le site de DistroSea. Pas besoin d'inscription pour un usage occasionnel. Près de 60 distributions sont accessibles immédiatement.

02› CHOISIR SA OU SES DISTRIBUTIONS

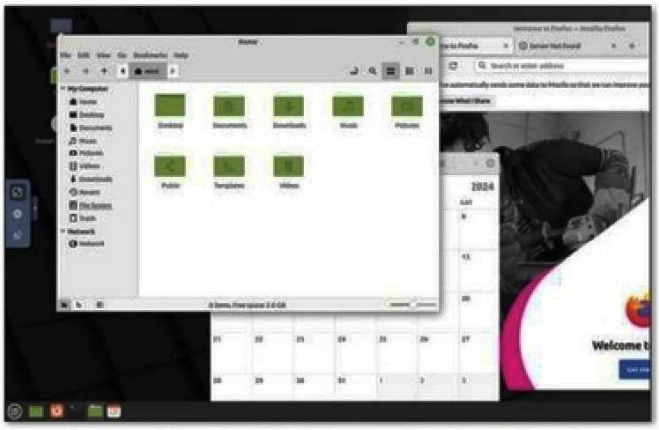
En cliquant sur l'une d'entre-elles, vous aurez un bref descriptif de ses spécificités et pourrez choisir parmi plusieurs versions.

03› ACCÈS AUX SERVEURS DISTANTS

Choisissez celle à tester, validez le captcha et il ne vous reste plus qu'à cliquer sur **Start**. Vous êtes ajouté à la liste des utilisateurs en attente (**Waiting in queue**) et votre position est indiquée. Votre tour arrive rapidement (une poignée de secondes lors de nos tests). Cliquez alors sur **Continue**.

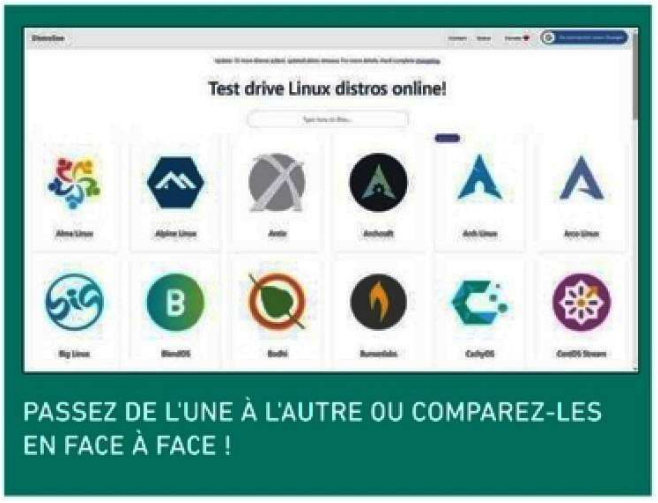
04› TESTEZ !

Vous êtes maintenant connectés à la distribution choisie et votre test peut démarrer. Vous remarquerez immédiatement que l'environnement est complet et correspond bien à un Linux connecté en temps réel !



05› ASTUCE

Passez en mode plein écran grâce à l'onglet-flèche à gauche de l'écran pour une adaptation parfaite de la résolution de votre écran. Vous pourrez aussi vous déconnecter de la distribution via cet onglet latéral.



PASSEZ DE L'UNE À L'AUTRE OU COMPAREZ-LES EN FACE À FACE !

3 QUESTIONS SUR LES

Sites d'informations, d'institutions ou d'associations, voire des systèmes critiques comme ceux d'hôpitaux ou de distribution d'énergie : des centaines d'attaques par déni de service visent chaque année des cibles françaises. Si les dégâts sont passagers, ils peuvent impacter la vie économique des victimes, leur image ou même la sécurité publique.

1 QU'EST-CE QU'UNE ATTAQUE DDOS ?

Une attaque par déni de service distribué (DDoS) est une tactique malveillante visant à perturber le fonctionnement normal d'un service en ligne, d'un site web, ou d'un serveur. Elle est réalisée en inondant la cible avec un volume écrasant de trafic Internet, dépassant sa capacité à gérer les requêtes entrantes. Cela entraîne généralement un ralentissement ou un arrêt complet du service visé. Les motivations derrière les attaques DDoS sont variées. Elles peuvent inclure la volonté de nuire à un concurrent commercial, un acte de vengeance, une protestation politique, ou simplement pour démontrer une capacité de perturbation. Dans certains cas, les attaques DDoS sont utilisées pour détourner l'attention des administrateurs de système pendant que les attaquants infiltrent le réseau pour d'autres activités malveillantes.

```
// UDP Flood initiation..

286|  function udpflood($host,$port,$time,$packetsize) {↓
287|      $this->privmsg($this->config['chan'],"[¥2UdpFlood Started!¥2]");
288|      $packet = "";↓
289|      for($i=0;$i<$packetsize;$i++) { $packet .= chr(rand(1,256)); }↓
290|      $end = time() + $time;↓
291|      $multitarget = false;↓

// Supporting Multiple Hosts Attacks..

298|  if($multitarget)↓
299|  {↓
300|      $fp = array();↓
301|      foreach($host as $hostt) $fp[] = fsockopen("udp://".$hostt,$port

// The UDP Packet attack logic (payloads)..

306|    fwrite($fp[$i % $count],$packet);↓
307|  fflush($fp[$i % $count]);↓
308|  if($i % 100 == 0)↓
309|  {↓
310|      if($end < time()) break;↓
311|  }↓
312|  $i++;↓
```

PAR QUI ?

Les attaques DDoS peuvent être orchestrées par des individus isolés, des groupes de pirates informatiques, des organisations criminelles, ou même des États. Avec la disponibilité croissante des outils de DDoS et des services de location de botnets, il est devenu plus facile pour des individus avec des compétences techniques limitées de lancer des attaques DDoS.

QUELLES CIBLES HABITUELLES ?

Les cibles des attaques DDoS peuvent être variées et incluent des sites web d'entreprises, des services en ligne, des infrastructures critiques (comme des systèmes de gestion de l'eau ou de l'énergie), des institutions gouvernementales, et des organisations financières. Essentiellement, tout service qui dépend fortement d'Internet pour son fonctionnement peut être une cible potentielle.
Les conséquences d'une attaque DDoS peuvent être graves. Elles vont du simple désagrément pour les utilisateurs à des pertes financières importantes pour les entreprises. Les attaques peuvent également endommager la réputation d'une organisation, éroder la confiance des clients ou des utilisateurs, et dans certains cas, entraîner des conséquences plus graves comme la perturbation de services essentiels pour une communauté.

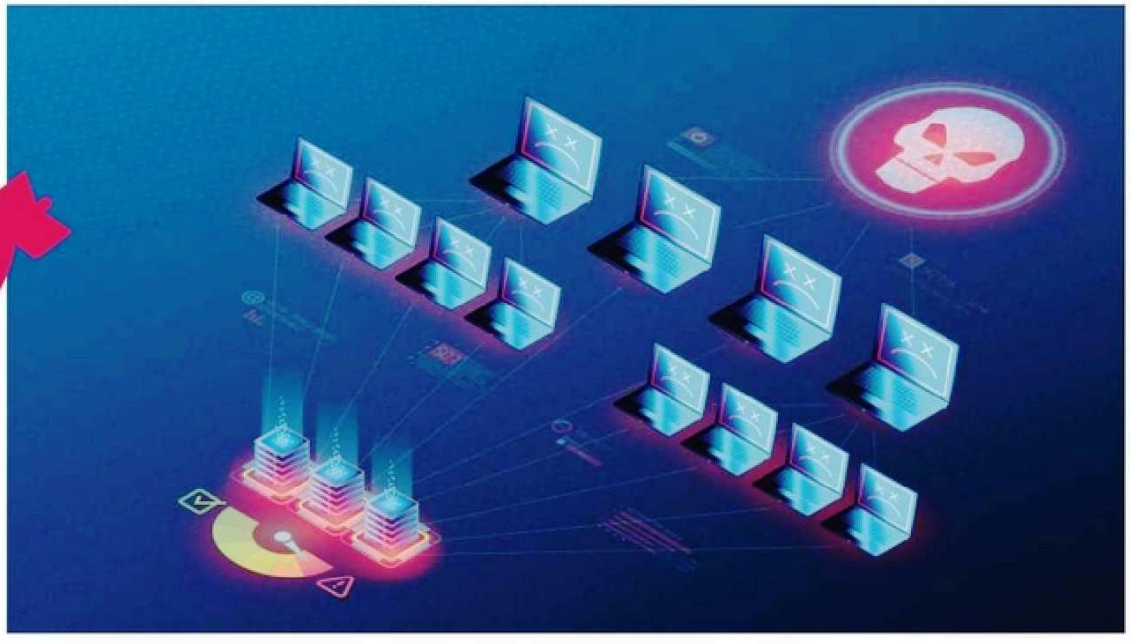
ATTAQUES DDOS

2 COMMENT FONT LES PIRATES ?

Les attaquants utilisent différentes méthodes pour lancer une attaque DDoS. Une stratégie commune est la création d'un "botnet", un réseau de machines infectées par des logiciels malveillants, contrôlées à distance par l'attaquant. Ces machines, souvent des ordinateurs personnels ou des appareils IoT compromis, sont utilisées pour envoyer un grand nombre de requêtes simultanées à la cible, la submergeant de trafic.
Une autre stratégie est l'exploitation des vulnérabilités des serveurs ou des réseaux pour amplifier le trafic. Par exemple, un attaquant peut utiliser un petit nombre de requêtes pour générer une grande quantité de réponses de la part du serveur cible. Cette technique utilise des protocoles comme NTP (Network Time Protocol) ou DNS (Domain Name System) pour amplifier l'attaque.

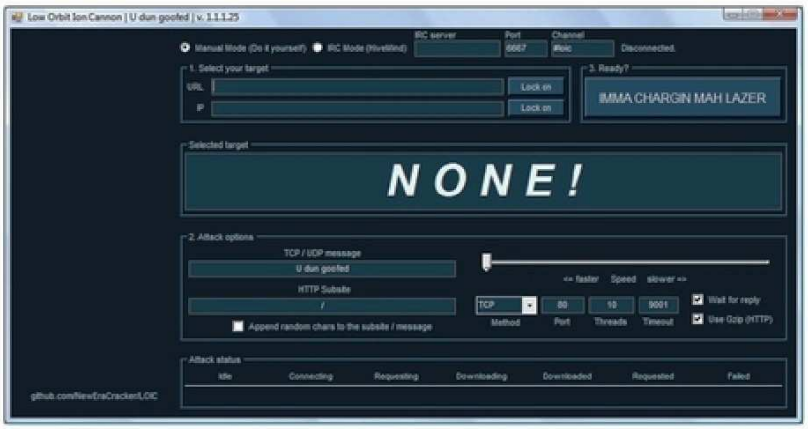
QUELLES RESSOURCES NÉCESSAIRES ?

Pour mener une attaque DDoS, les pirates ont besoin de ressources telles que des ordinateurs ou des appareils compromis pour former un botnet. Ils peuvent également avoir besoin de logiciels spécifiques pour automatiser et orchestrer l'attaque, ainsi que d'une connexion Internet stable et rapide pour gérer le trafic généré.



POUR MENER UNE ATTAQUE PAR DÉNI DE SERVICE, UN PIRATE UTILISERA UN RÉSEAU DE PC ZOMBIES. UN PC ZOMBIE EST UN PC INFECTÉ SANS QUE SON PROPRIÉTAIRE LE SACHE. MAIS SES RESSOURCES ET SA CONNEXION À INTERNET SERONT UTILISÉES PAR UN HACKER POUR ENVOYER DES REQUÊTES SUR SA CIBLE FINALE. IL FAUT DES CENTAINES VOIRE DES MILLIERS DE PC ZOMBIES POUR MENER UNE ATTAQUE DDOS. UN TEL RÉSEAU EST APPELÉ BOTNET.

Les attaquants passent par des forums spécialisés pour acquérir des outils et des compétences, ou des services de location de botnets («DDoS-for-hire») pour faciliter l'attaque sans nécessiter une infrastructure propre. L'un des outils d'attaque gratuit les plus connus est LOIC (Low Orbit Ion Cannon) permettent à un utilisateur d'inonder une cible de trafic. Les protocoles couramment exploités incluent HTTP pour le trafic web, UDP (User Datagram Protocol) pour les services comme le streaming vidéo, et ICMP (Internet Control Message Protocol) pour les messages d'erreur et de contrôle du réseau.



En plus de LOIC, plusieurs autres outils et protocoles sont fréquemment utilisés dans les attaques DDoS :

- HOIC (High Orbit Ion Cannon) : Similaire à LOIC mais plus puissant, il permet aux utilisateurs de lancer des attaques DDoS avec une interface simple. HOIC peut cibler jusqu'à 256 adresses web simultanément.

- Mirai Botnet : Bien que plus connu comme un botnet, Mirai est également associé à un outil pour lancer des attaques DDoS. Il infecte les appareils IoT et les utilise pour inonder les cibles avec du trafic.

- UDP Flood : Cette technique utilise le protocole UDP (User Datagram Protocol) pour envoyer un grand nombre de paquets UDP à des ports aléatoires sur un serveur distant, provoquant une surcharge du serveur.

- SYN Flood : Une attaque qui exploite le protocole TCP. Elle envoie des demandes de connexion (SYN) rapides et continues sans compléter le processus de connexion, ce qui épuise les ressources du serveur.

- Ping of Death : Exploite les faiblesses du protocole ICMP en envoyant des paquets malformés ou de très grande taille qui peuvent provoquer un crash ou un redémarrage du système cible.

CERTAINS PACKS PRÊTS À L'EMPLOI SONT EN VENTE SUR LE DARKWEB, MAIS LES HACKERS CONTINUENT AUSSI D'UTILISER DES LOGICIELS GRATUITS QUI ONT FAIT LEURS PREUVES, COMME LOIC (LOW ORBIT ION CANNON).

ET POUR LES RÉSEAUX DE BOTNETS ?

Pour l'utilisation de PC zombies et de botnets, voici également les principaux malwares utilisés :

- Mirai : Toujours pertinent en 2024, Mirai est connu pour cibler des appareils IoT vulnérables, les transformant en bots pour des attaques DDoS.

- Trickbot : Originellement un cheval de Troie bancaire, Trickbot a évolué pour inclure des fonctionnalités permettant la création de botnets. Il est souvent distribué via des campagnes de phishing.

- Emotet : Bien qu'il soit principalement un logiciel malveillant de vol d'informations, Emotet a été utilisé pour distribuer d'autres types de malwares, y compris ceux qui créent des botnets.

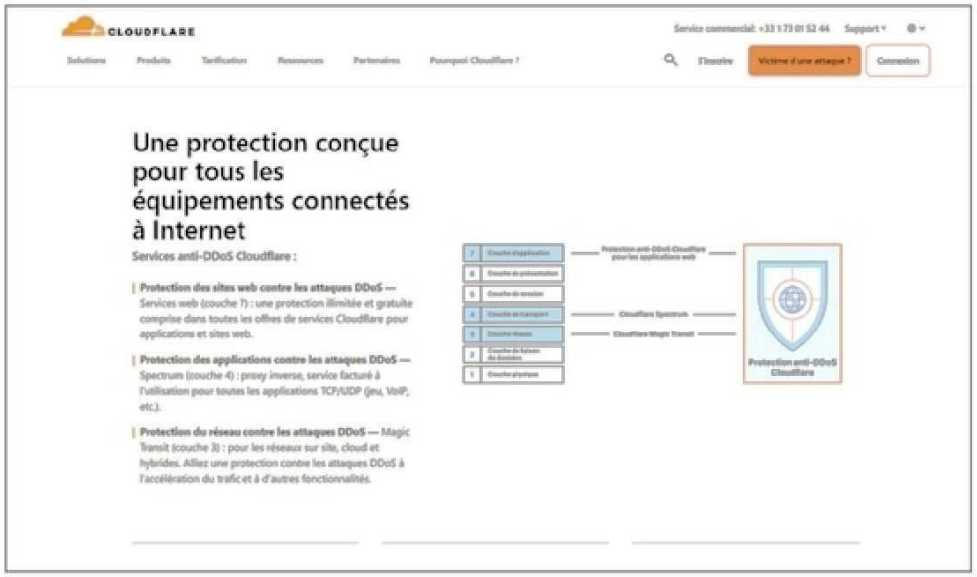
- Qbot (ou Qakbot) : Ce malware polymorphe est connu pour sa capacité à infecter des réseaux d'entreprises et à recruter des machines infectées dans des botnets.

- DDoS-for-hire Services : Ces services, également connus sous le nom de «booters» ou «stressers», offrent à des individus la capacité de lancer des attaques DDoS sans avoir besoin de créer leur propre botnet. Ils louent l'accès à des réseaux de machines infectées.

LES HACKERS EN HERBE TROUVE FACILEMENT DES SITES LEUR PROPOSANT POUR QUELQUES DIZAINES D'EUROS PAR MOIS DES SERVICES « DDOS-FOR-HIRE ». C'EST-À-DIRE QUE PROGRAMMES D'ATTAQUES ET BOTNETS SONT FOURNIS POUR AUTOMATISER AU MAXIMUM LES ATTAQUES.

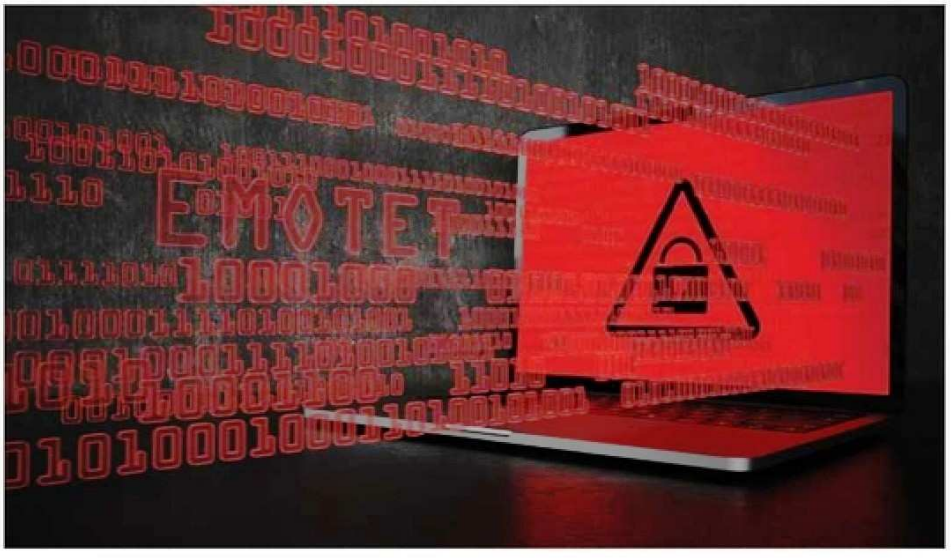
3 COMMENT SE PROTÉGER ?

a# PRÉVENTION



Les propriétaires ou administrateurs d'un service web doivent s'assurer que les infrastructures réseau peuvent gérer des volumes de trafic significativement plus élevés que la normale. Cela implique souvent l'augmentation de la bande passante et la mise en place de systèmes redondants. L'utilisation de firewalls avancés et de solutions anti-DDoS spécifiques pour filtrer le trafic non désiré et atténuer les attaques sont également préconisés. Enfin, l'intégration de Systèmes de détection et de prévention d'intrusion (IPS/IDS) permet de surveiller automatiquement le réseau pour détecter des comportements anormaux et bloquer les activités suspectes.
À titre d'exemple, un service comme Cloudflare offre une protection DDoS en agissant comme un proxy entre le site web de l'utilisateur et ses visiteurs, filtrant ainsi le trafic malveillant. De la même manière, AWS Shield est une autre solution de protection DDoS pour les sites et applications hébergés sur Amazon Web Services. Elle fournit des mesures automatiques pour atténuer les attaques.

b# QUE FAIRE EN CAS D'ATTAQUE ?



Vous devez avoir en tête un protocole d'action avec certains outils et solutions préalablement configurés :

- Réseaux de distribution de contenu (CDN) : Utiliser un CDN pour disperser le trafic sur de multiples serveurs, rendant plus difficile pour une attaque de surcharger un point unique.

- Basculer le trafic : En cas d'attaque, rediriger le trafic vers une infrastructure de sauvegarde pour maintenir la disponibilité du service.

- Coopération avec les fournisseurs de services Internet (ISP) : Travailler avec les ISP pour bloquer les adresses IP malveillantes ou pour implémenter des règles de filtrage de trafic.

- Analyse post-attaque : Après une attaque, il est essentiel d'analyser l'incident pour comprendre comment l'attaque a été menée et identifier les vulnérabilités. Cette analyse aidera à renforcer les défenses contre de futures attaques.

Activez le mode Dieu > Avec Windows 11

Le mode Dieu vous donne accès à l'ensemble des paramètres de Windows 11, y compris les outils cachés pour des raisons de sécurité. Avec lui, plus besoin d'aller d'un dossier à l'autre via le panneau de configuration : tous les réglages possibles sont regroupés dans un seul endroit.

Pour y accéder, créez un nouveau dossier directement sur le bureau, en utilisant le clic droit et en sélectionner « **Nouveau** » puis « **Dossier** ». Cliquez ensuite dessus avec le bouton droit de la souris pour le renommer.

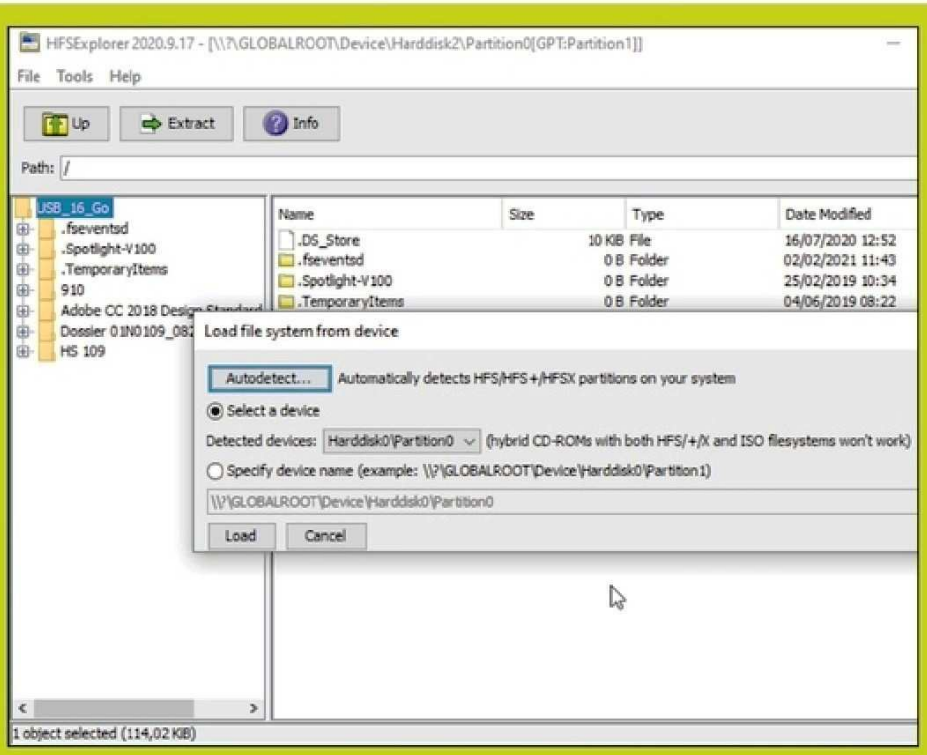
Intitulez-le : **ModeDieu.{ED7BA470-8E54-465E-825C-99712043E01C}** et appuyez sur **Entrée**.

L'icône va alors changer d'apparence et son nom disparaîtra. Soyez cependant conscient que jouer un peu trop avec les paramètres du système peut s'avérer dangereux si vous ne les maîtrisez pas : tout le monde n'est pas fait pour être Dieu.

Lire une clé USB provenant d'un Mac > Avec HFSExplorer

Pour lire une clé USB formatée pour Mac (HFS+), installez l'utilitaire gratuit HFSExplorer. Branchez votre clé USB et ignorez les alertes de Windows. Puis, via le menu **Démarrer**, lancez **Run HFSExplorer in Administrator Mode** (si nécessaire, téléchargez et installez Java, comme indiqué dans la fenêtre d'avertissement). Cliquez sur **File** > **Load File System from device** puis sur le bouton **Autodetect**. Votre clé USB est détectée, cliquez sur **OK**. Faites un clic droit sur le fichier à récupérer et choisissez **Extract data** pour le copier sur votre disque dur.

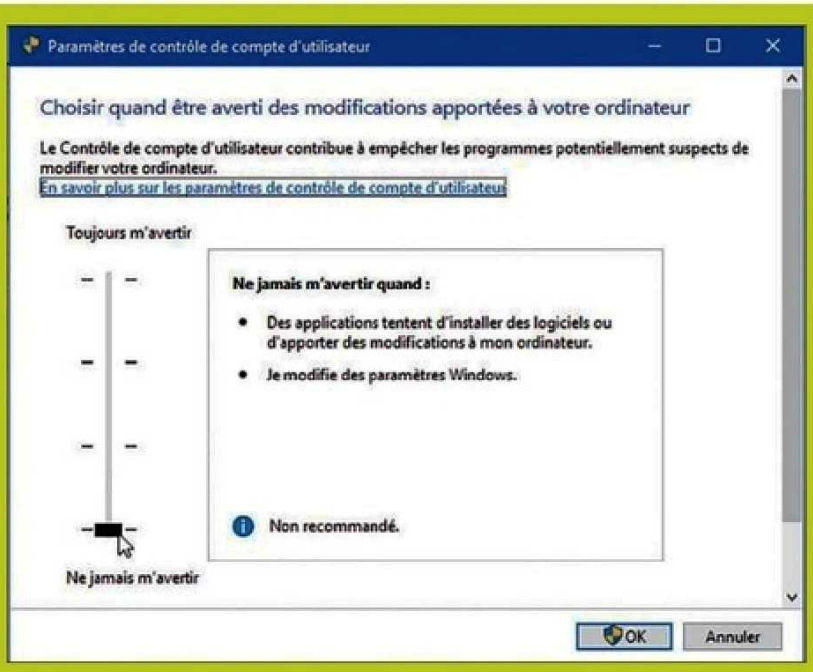
Lien : **https://tinyurl.com/HFSEx**



Supprimer le contrôle de compte d'utilisateur

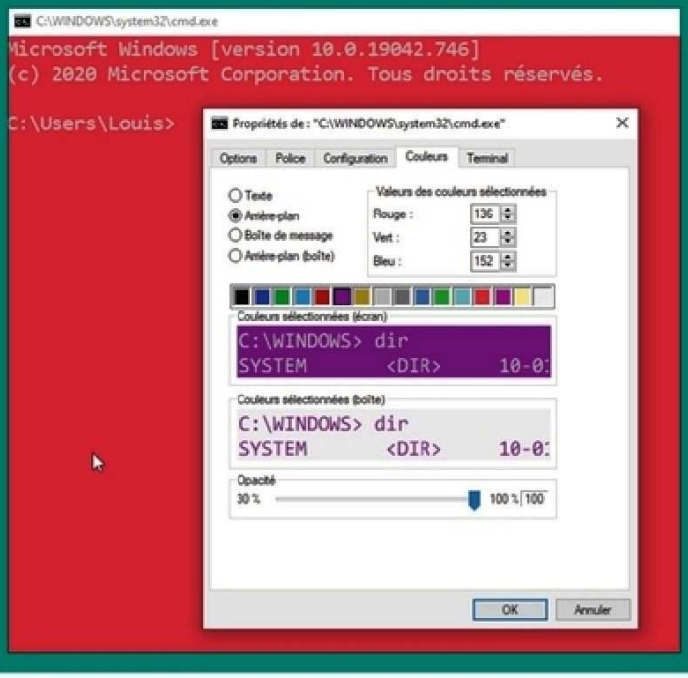
> Avec le Panneau de configuration

Le contrôle de compte d'utilisateur protège le système en vous demandant une confirmation de vos actions susceptible de l'affecter. Si ces demandes vous agacent et que vous savez ce que vous faites, désactivez-les. Ouvrez le Panneau de configuration et sélectionnez **Comptes d'utilisateurs** puis **Modifier les paramètres de contrôle du compte d'utilisateur**. Faites glisser le curseur sur **Ne jamais m'avertir** pour désactiver les demandes de confirmation. Validez avec **OK**.



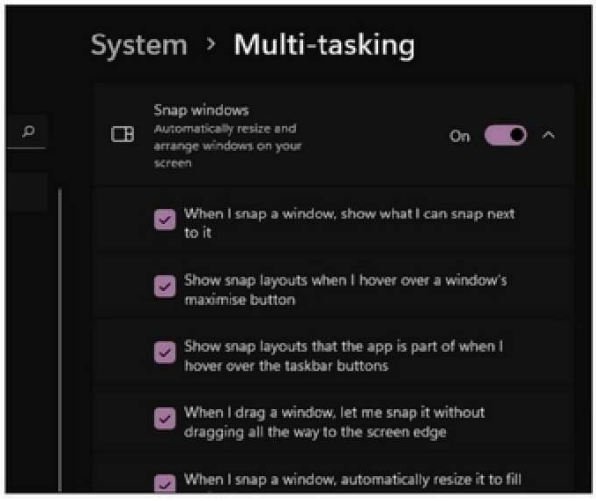
Modifier l'apparence de l'invite de commandes > Avec Windows

Vous en avez assez de vous esquinter les yeux dans l'invite de commandes de Windows ? Modifiez son apparence selon vos besoins (et vos goûts). Lancez l'invite de commandes puis cliquez sur l'icône **C:/** dans l'angle supérieur droit de la fenêtre. Choisissez **Propriétés**. Dans la fenêtre qui s'affiche, ouvrez l'onglet **Police** pour changer la fonte et modifier la taille des caractères. Depuis l'onglet **Couleurs** vous pouvez choisir une autre couleur d'arrière-plan que le noir. Quittez l'**Invite de commandes** et relancez-la pour apprécier le résultat.



Divisez l'écran pour effectuer plusieurs tâches > Avec Windows 11

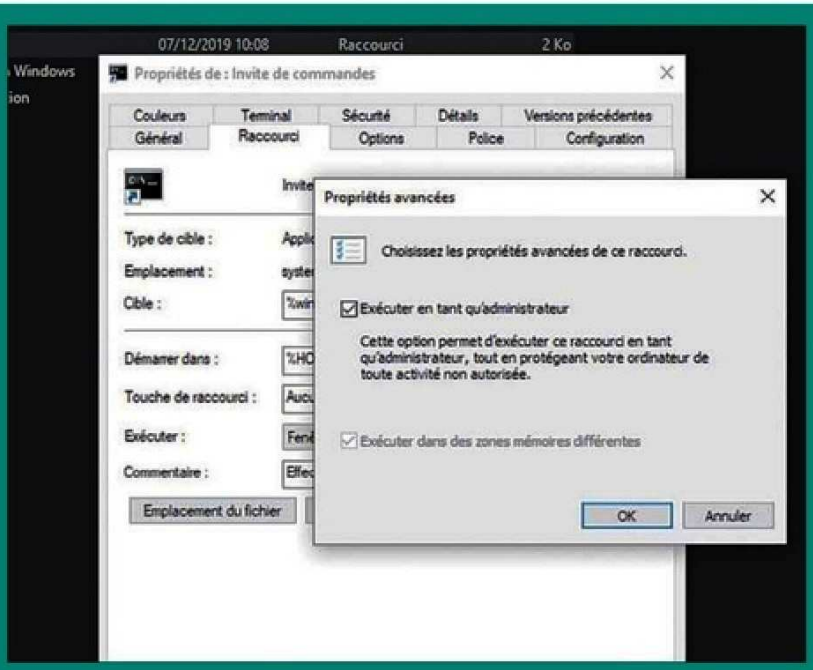
Avoir plusieurs fenêtres qui se partagent l'écran de votre ordinateur peut vous faciliter le travail quand vous avez besoin de passer d'une application à l'autre. S'il est toujours possible de le faire manuellement en les redimensionnant, des raccourcis clavier vous feront gagner du temps.Allez dans **Paramètres > Système > Multitâche** et vérifiez que Snap Windows est allumé. Pour deux fenêtres, maintenez enfoncées la touche Windows et les flèches gauche ou droite selon le côté de l'écran où vous voulez les positionner. Pour trois ou quatre fenêtres, répétez l'opération précédente en terminant votre combinaison de touches par les flèches haut ou bas. Encore plus rapide, vous pouvez aussi survoler avec votre souris l'icône servant à agrandir une fenêtre et sélectionner la mise en page qui vous intéresse.



Exécuter toujours l'invite de commandes en mode administrateur

> Avec Windows

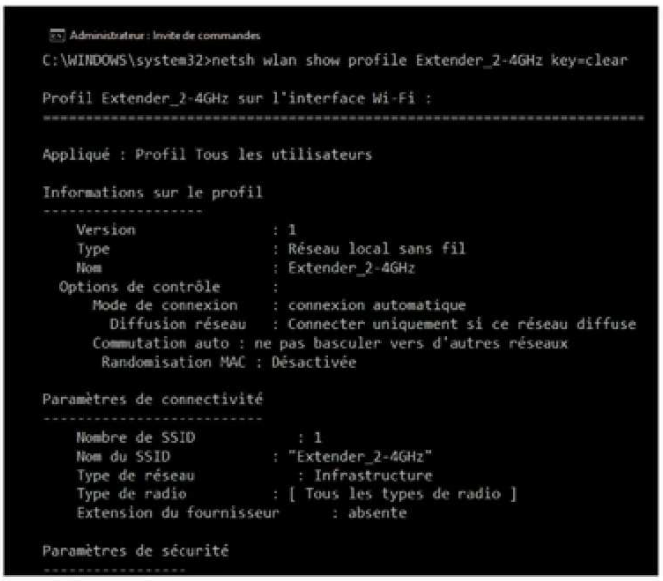
Adepte des lignes de commande dans Windows, vous lancez le Powershell en mode Administrateur... via quelques clics supplémentaires. Pour gagner du temps, réglez l'ouverture pour que ce mode soit toujours actif. Saisissez **Invite** dans le champ de recherche de Windows. Effectuez un clic droit sur **Invite de commandes** et choisissez **Épingler au menu Démarrer**. Faites de nouveau un clic droit sur l'icône apparue dans le menu Démarrer et choisissez **Plus > Ouvrir l'emplacement du fichier**. Faites un clic droit sur le fichier et choisissez **Propriétés**. Dans la fenêtre qui s'affiche, cliquez sur **Avancé** puis cochez la case **Exécuter en tant qu'administrateur**. Validez.



Retrouver facilement le mot de passe d'un réseau WiFi

> Avec Windows

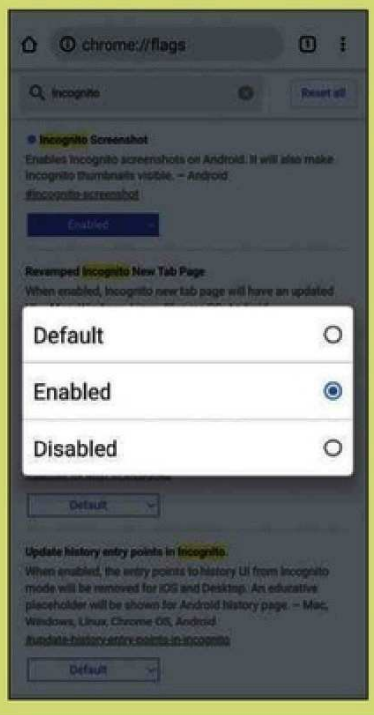
Impossible de vous souvenir du mot de passe du réseau WiFi auquel est pourtant bien connecté votre PC pour l'utiliser sur un autre appareil ? Inutile d'ameuter les utilisateurs autour de vous. Windows peut s'en charger et vous le livrer en clair à l'aide d'une simple ligne de commande. Ouvrez pour cela l'invite de commande et saisissez : **netsh wlan show profile nomduréseauwifi key=clear**. Le mot de passe apparaît dans la section **Paramètres de sécurité**, à la ligne **Contenu de la clé**.



Faire des captures d'écran d'un onglet Incognito

> Avec Android

Avez-vous déjà tenté de faire une capture d'écran d'une page ouverte en navigation privée dans Chrome ou Firefox sur Android ? C'est impossible. Ce mode de navigation est justement prévu pour ne pas laisser de trace de vos consultations et n'autorise donc pas les captures d'écran. Sauf à modifier le comportement du navigateur. Dans Chrome, tapez **Chrome://flags** dans le champ d'adresse. Recherchez le réglage **Incognito Screenshot**. Activez l'option **Enable** et relancez Chrome. Dans Firefox, accédez aux paramètres de navigation privée et activez le curseur idoine.



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 !

Votre publication s'engage pour le recyclage des papiers avec Ecofolio.

ecofolio

TOR : FAUT-IL EMPRUNTER LES PONTS ?

Lors de l'installation du navigateur ou plus tard à l'usage, vous avez la possibilité de passer par des « ponts » pour accroitre votre confidentialité. Comment ça marche, à quoi cela sert-il et est-ce vraiment conseillé ?

Une passerelle, un chemin de traverse, un passage secret : les ponts TOR sont tout cela à la fois ! Ces «Tor bridges» sont des relais du réseau Tor qui ne sont pas listés dans l'annuaire public principal de Tor. Leur fonction principale est de fournir un moyen de se connecter au réseau Tor dans les régions où l'accès à ce dernier est censuré ou bloqué.

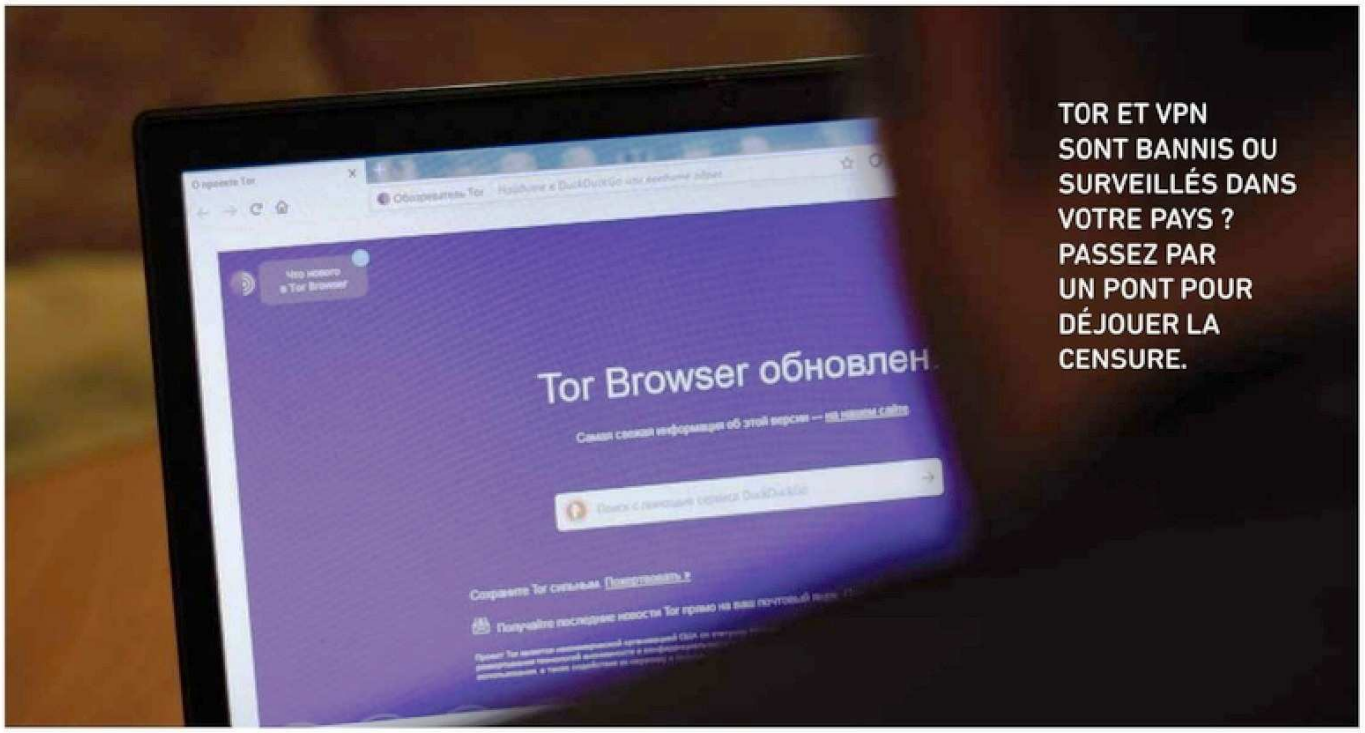
Lorsque vous utilisez un pont, votre connexion à Internet passe d'abord par ce dernier, qui apparaitra comme un serveur anonyme aussi banal que les dizaines de milliers d'autres qui structurent la Toile. Il n'est pas identifié comme un « nœud » du réseau Tor et votre navigation ne sera pas filtrée ou bloquée automatiquement par les robots et listes noires d'un pays ou d'une autorité bannissant ce navigateur.

Et de façon plus générale, cette voie d'accès apporte une couche supérieure de confidentialité, même en France. Car l'objectif est de masquer le fait que vous utilisiez le protocole Tor. Car si ce dernier vous offre un anonymat de bonne qualité, un pirate placé entre vous et le Web ou le Darknet sait que vous utilisez Tor. Du coup, cela éveillera leurs soupçons… et leur intérêt.

Dans une certaine mesure, un pont fait ainsi office de VPN pour Tor. Vous vous connectez ensuite à ce dernier via cette connexion extérieure, sans que votre FAI ne puisse vous suivre. Comme avec les autres relais Tor, la connexion à travers un pont est chiffrée, assurant la confidentialité et l'anonymat.

OBTENEZ DES ADRESSES DE PONTS SOUS FORME DE LIENS OU DE QR CODE.

> Dans une certaine mesure, un pont fait office de VPN pour Tor



TOR ET VPN SONT BANNIS OU SURVEILLÉS DANS VOTRE PAYS ? PASSEZ PAR UN PONT POUR DÉJOUER LA CENSURE.

QUI CRÉE CES PONTS, QUI LES PROTÈGENT ?

Les ponts Tor peuvent être des serveurs dédiés ou des ordinateurs appartenant à des particuliers. Tout comme les relais Tor ordinaires, ils sont généralement gérés par des volontaires qui choisissent de contribuer au réseau en exécutant un relais. Le projet Tor fournit les logiciels et les protocoles nécessaires, mais ce sont les utilisateurs individuels et les organisations qui hébergent et exécutent ces ponts. Les adresses des ponts Tor sont distribuées de manière contrôlée pour éviter qu'elles ne soient facilement accessibles aux censeurs. Les utilisateurs peuvent les obtenir via le site Web de Tor, par e-mail, ou par d'autres moyens sécurisés.

CAMOUFLAGE !

Les ponts Tor intègrent des techniques d'obfuscation pour cacher le fait qu'une connexion utilise Tor. Ces techniques masquent le trafic Tor pour le faire ressembler à du trafic Internet ordinaire. Vous pouvez les trouver via les paramètres du navigateur via les « Ponts intégrés » et sont qualifiés de « transports amovibles ». Ils sont au nombre de trois :

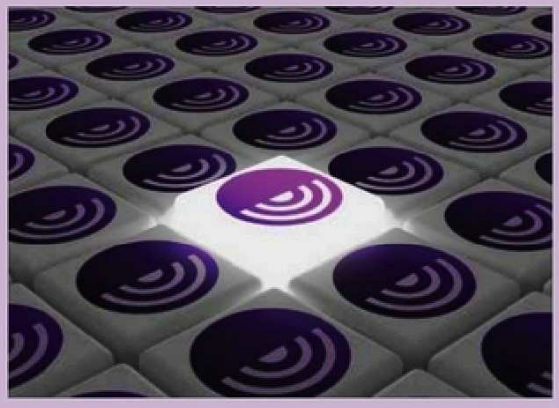
1) obfs4 (intégré par défaut) : Fait ressembler votre trafic Tor à des données aléatoires. Peut ne pas fonctionner dans les régions fortement censurées.

2) Snowflake : Achemine votre connexion via des proxys Snowflake pour faire croire que vous passez un appel vidéo, par exemple.

3) meek-azure : Donne l'impression que vous êtes connecté à un site web de Microsoft, au lieu d'utiliser Tor. Peut fonctionner dans des régions fortement censurées, mais est généralement très lent.

Y-A-T-IL DES INCONVÉNIENTS À UTILISER UN PONT TOR ?

Bien que les ponts Tor soient un outil essentiel pour le contournement de la censure, ils ne sont pas la solution optimale pour tous les utilisateurs. Leur utilisation est recommandée uniquement dans des situations où l'accès à Tor est restreint ou bloqué. Pour la majorité des Tornautes, les relais standards offrent un meilleur équilibre entre vitesse, fiabilité et facilité d'utilisation.



1# Vitesse de connexion réduite : Les ponts Tor peuvent souvent avoir des vitesses de connexion plus lentes que les relais Tor ordinaires. Cela est dû au fait que le nombre de ponts disponibles est bien sûr inférieur à celui des relais publics, et ils peuvent être surchargés par de nombreux utilisateurs.

2# Fiabilité variable : Certains ponts peuvent être moins fiables ou stables que les relais Tor standards. Leur disponibilité et leur performance peuvent donc varier. Leur efficacité dépend de leur non-détection par les censeurs. Certains peuvent « tomber » puis être remplacés par d'autres.
Et si tout le monde utilisait des ponts par défaut, cela pourrait enfin surcharger ces relais et les rendre moins disponibles pour ceux qui en ont vraiment besoin.

3# Complexité de configuration : Pour les nouveaux utilisateurs, la configuration d'un pont Tor peut sembler complexe et dissuasive. Surtout s'ils veulent changer de ponts régulièrement pour plus d'efficacité. Cela implique de trouver et entrer les adresses de pont correctes à chaque fois.

4# Stratégie de défense en profondeur : En n'utilisant pas de ponts par défaut, Tor offre une stratégie de défense en profondeur. Si un utilisateur rencontre des problèmes avec les relais ordinaires, il a toujours l'option des ponts comme solution de secours.

COMMENT OBTENIR ET CONFIGURER UN PONT TOR ?

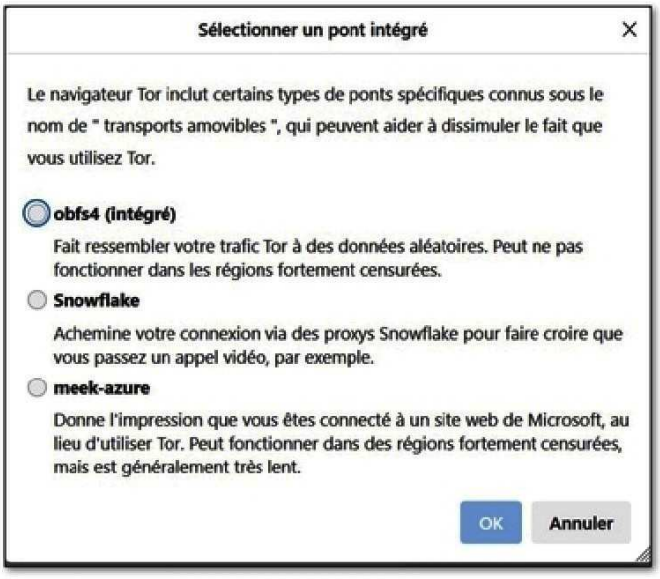
PRATIQUE

01› PREMIÈRE FOIS

Lorsque vous lancez Tor Browser pour la première fois, cliquez sur **Configurer**. Cochez l'option indiquant que Tor est censuré dans votre pays. Entrez les adresses des ponts que vous avez obtenues. Une fois configuré, Tor essaiera de se connecter à Internet via le pont spécifié.

02› PONTS INTÉGRÉS

Vous pouvez aussi configurer un pont ultérieurement. Allez dans **Paramètres > Connexion**. Descendrez jusqu'à la partie **Ponts**. Vous pouvez simplement sélectionner un Pont intégré. Il s'agit en fait de trois techniques d'obfuscation qui vont tenter de dissimuler le protocole Tor. Pas aussi puissant et rapide qu'un véritable pont, mais cela peut suffire pour un usage ponctuel ou au sein d'une zone à censure modérée.



03› PONT RELAIS

En plus du point précédent, toujours dans **Ponts > Ajouter un nouveau pont**, choisissez **Demandez un pont**. Après le Captcha, vous obtiendrez une

ou plusieurs adresses de ponts que vous pourrez sélectionner. Vous avez aussi la possibilité de les partager en copiant le lien ou le QR code associé.

04› ADRESSE MANUELLE

Vous pouvez aussi obtenir de façon plus confidentielle et plus personnalisée des adresses de ponts moins connues en contactant Tor Project ou des organisations

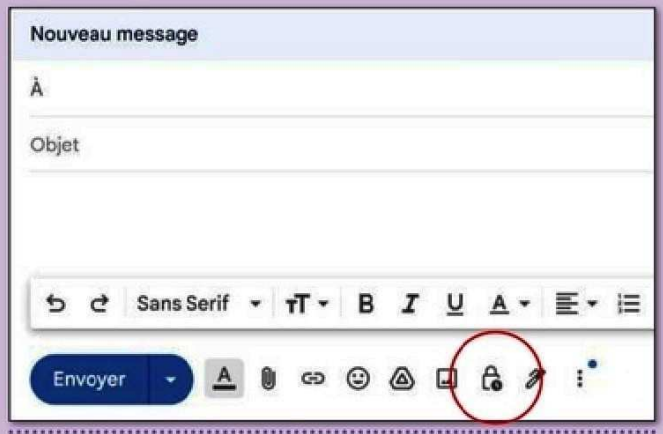
internationales. Pour Tor Project, vous pouvez aller sur **https://bridges.torproject.org**, envoyez un mail à **bridges@torproject.org** (attention seules les adresses Gmail ou Riseup sont compatibles) ou passer par le canal Telegram **@GetBridgesBot** en tapant **/start** ou **/bridges** dans le chat.

ENVOYEZ DES MAILS CONFIDENTIELS AVEC GMAIL

Gmail vous permet d'envoyer des messages et des pièces jointes en mode confidentiel. Il vous permet de définir la date d'expiration de vos messages (votre email disparaîtra à l'issue de ce délai), ou d'en révoquer l'accès à tout moment. Les options de transfert, copie, impression et téléchargement sont désactivées pour les destinataires du message confidentiel.

01 › ACTIVER LE MODE

Lors de la rédaction d'un email, cliquez sur la petite icône de cadenas avec une horloge situé en bas à droite de votre fenêtre de saisie.



02 › VOS RÉGLAGES

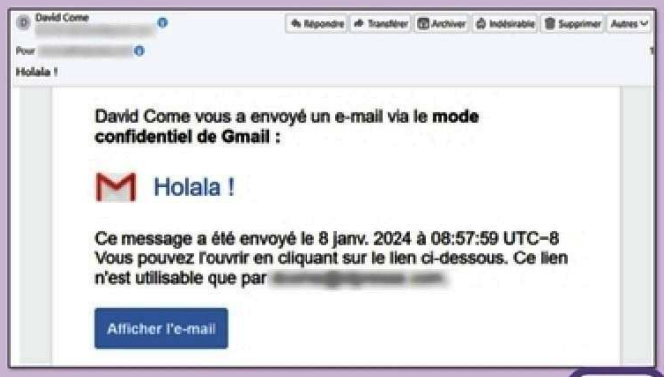
Dans la fenêtre qui s'ouvre, vous définirez une date d'expiration pour le message (de 1 jour... à 5 ans) et pourrez aussi demander que le destinataire renseigne un code reçu par SMS pour pouvoir ouvrir votre email.

03 › CODE OU PAS CODE

Envoyez votre message. Si votre l'adresse mail de votre destinataire est un compte Gmail, pas de code secret requis même si vous avez coché l'option ci-dessus. Mais s'il s'agit d'un autre client de messagerie, vous devrez indiquez le numéro de téléphone de votre destinataire afin qu'il reçoive le code à usage unique.

04 › MAIL PROTÉGÉ !

Votre destinataire reçoit le mail sécurisé avec une invitation à l'afficher. Selon qu'il est un compte Gmail associé ou non à son client de réception, il devra s'y connecter ou recevoir le code par SMS pour pouvoir lire votre message. Et votre email sera effacé de sa boîte de réception à la fin de la date d'échéance.



A SAVOIR !

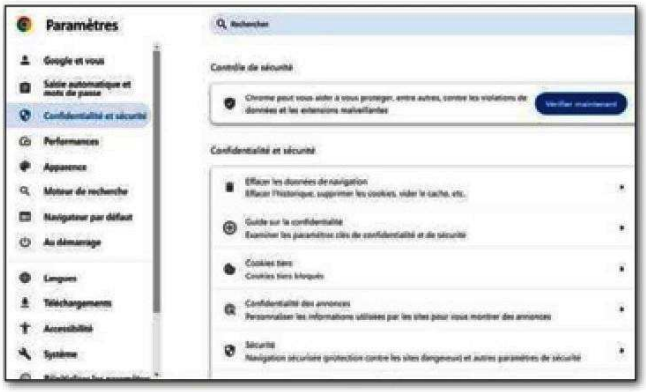
Attention, ce mode confidentiel empêche les destinataires de partager accidentellement votre e-mail, mais pas de prendre des captures d'écran ni des photos du message ou des pièces jointes.

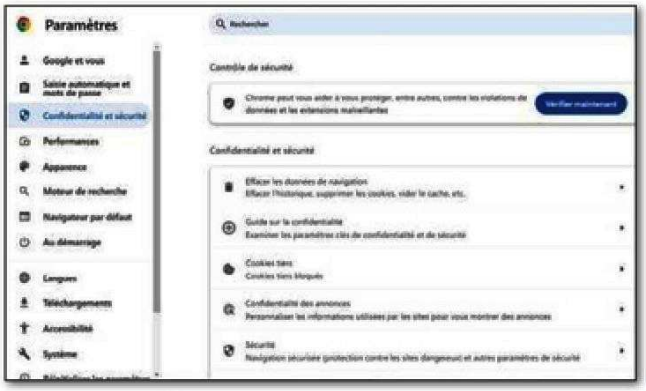
DÉSACTIVEZ LES COOKIES TIERS SUR CHROME

PRATIQUE

En bloquant les cookies tiers, vous empêchez les sites de communiquer des informations avec d'autres services et donc de vous profiler, navigation après navigation.

INFOS
[Chrome]
Difficulté : ☠☠☠





01› PARAMÈTRES

Sur Chrome (mais le cheminement est assez similaire sur les différents navigateurs) : via les trois points en haut à droite du navigateur, passez par **Paramètres > Confidentialité et Sécurité > Cookies tiers**.

02› BLOQUER

Activez l'option **Bloquer les cookies tiers**. Pour aller plus loin, désactivez également l'option **Autoriser les sites associés à voir votre activité dans le groupe**, qui reste sinon activée par défaut ! Les différents services de Google ne pourront par exemple plus échanger de données entre eux via cookies.

VÉRIFIEZ LES PERMISSIONS DES EXTENSIONS

PRATIQUE

Examinez régulièrement les permissions accordées à vos extensions sur Chrome ou Firefox. Désinstallez ou désactivez les extensions qui demandent des permissions excessives.

INFOS
[Chrome]
Difficulté : ☠☠☠

01› ACCÈS AUX EXTENSIONS

Dans Chrome, passez par les trois ponts en haut du navigateur puis **Extensions > Gérer les extensions**. Vous verrez une liste de toutes les extensions que vous avez installées dans Chrome.

02› QUELLES AUTORISATIONS ?

Pour chaque extension, cliquez sur **Détails** puis faites défiler vers le bas pour trouver la section **Autorisations**. Ici, vous verrez les différentes permissions que l'extension a demandées. **Désactiver** ou **Supprimer** (en bas du menu) les extensions suspicieuses.

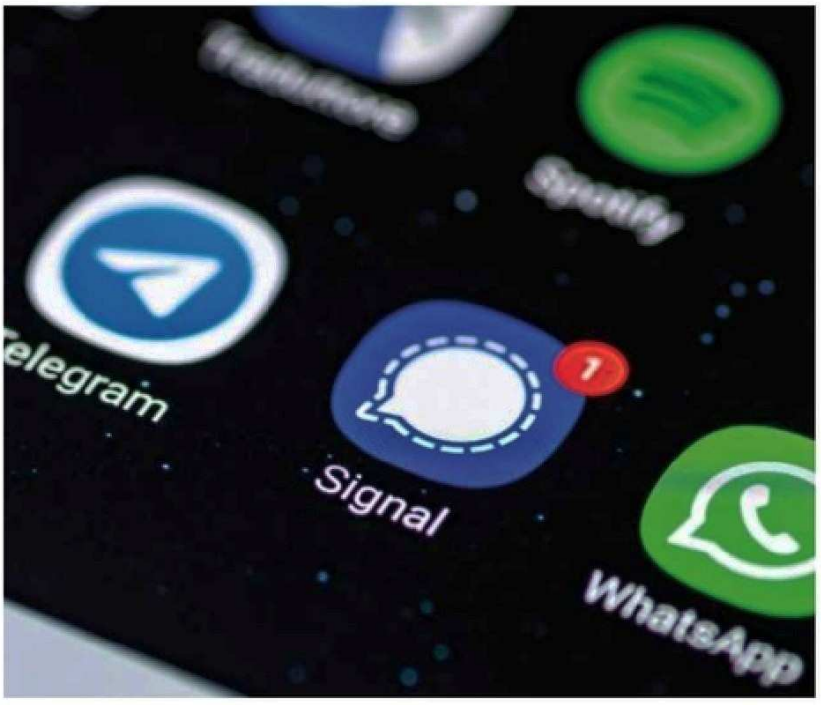
DECRYPTAGE

MESSAGERIES INSTANTANÉES

Arrêtez de confier votre vie à n'importe qui !

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

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



CHIFFREMENT... MAIS PAS QUE

Le chiffrement de bout en bout s'impose de plus en plus, mais n'est pas la règle !
De grandes messageries comme Facebook Messenger, Skype ou Telegram ne le proposent toujours pas par défaut. Celles d'Instagram et autres réseaux sociaux sont pires : ce sont des aspirateurs à données !
Seules les applications de messagerie chiffrées de bout en bout garantissent un niveau minimum de confidentialité. Mais d'autres caractéristiques et fonctions doivent être présentes pour garantir, si ce n'est l'anonymat, du moins un niveau de sécurisation de haut niveau :

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

- Politique de confidentialité
Si vous vous souciez de votre confidentialité, assurez-vous que les entreprises qui fournissent vos applications s'en soucient également. La charte et les engagements de confidentialités doivent être clairement stipulés et expliqués, pas seulement fournis sous la forme d'un simple slogan marketing. Comme pour les VPN (lire page 15), la domiciliation de l'entreprise dans un pays très protecteur des données personnelles est un vrai gage de sérieux.

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

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

> Ne croyez pas les éditeurs de messageries sur parole... Certains sont plus transparents que d'autres, c'est déjà bon signe.

TOP 5 MESSAGERIES SÉCURISÉES

SIGNAL

> Le meilleur rapport qualité/sécurité

Considérée comme l'une des applications de messagerie les plus sûres du marché, Signal protège vos communications par un chiffrement de bout en bout des appels et des messages. Son protocole de chiffrement est si sûr que d'autres applications de premier plan (telles que WhatsApp et Facebook Messenger), l'utilisent également.
Comme d'autres applications, Signal propose des fonctions de messagerie, appel, chat vidéo et partage de fichiers/photos. Elle permet également de faire disparaître les messages pour plus de confidentialité. Vous avez besoin d'un numéro de téléphone pour vous inscrire et nous vous recommandons de sécuriser l'application avec un mot de passe. Pour les amateurs de sécurité, toutes vos données sont stockées localement sur votre appareil, et non sur des serveurs distants. Enfin, des dizaines de fonctions et paramètres vous permettront de personnaliser votre usage et d'ajouter encore plus de confidentialité !
Signal n'est pas la propriété d'une grande entreprise technologique. Il s'agit d'un logiciel open source financé par des subventions et des dons. Contrairement à d'autres

applications de messagerie privée, Signal ne contient pas de publicités, d'affiliés ni de suivi secret — nul besoin de s'embarrasser d'une option « Ne pas suivre ». De plus, grâce à son statut de logiciel open source, l'application fait l'objet d'audits de sécurité continus afin de la rendre encore plus sûre.

Lien : **signal.org/fr**

WHATSAPP

> Incontournable

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

« WHATSAPP ? VOUS ÊTES SÉRIEUX ?! »

Alors, pourquoi l'intégrer dans notre Top nous direz-vous ? Aujourd'hui, c'est l'une des rares applications à avoir une audience véritablement mondiale (2 milliards d'utilisateurs), avec des fonctions sociales et applicatives performantes tout en offrant une sécurisation stable et puissante. , Si vous n'avez pas le choix pour rester connecter au monde : utilisez WhatsApp... et ajouter une seconde messagerie plus sécurisée pour vos échanges

sensibles, pros ou simplement intimes.
WhatsApp utilise le chiffrement de bout en bout et permet des sauvegardes chiffrées de tous vos chats. De plus, elle ne stocke pas les messages sur ses serveurs. WhatsApp propose une vérification en deux étapes, qui nécessite un code PIN pour vérifier votre numéro de téléphone sur n'importe quel appareil. Et comme l'application utilise une quantité limitée de données en arrière-plan, vous pouvez faire des économies de datas.

Lien : **www.whatsapp.com**

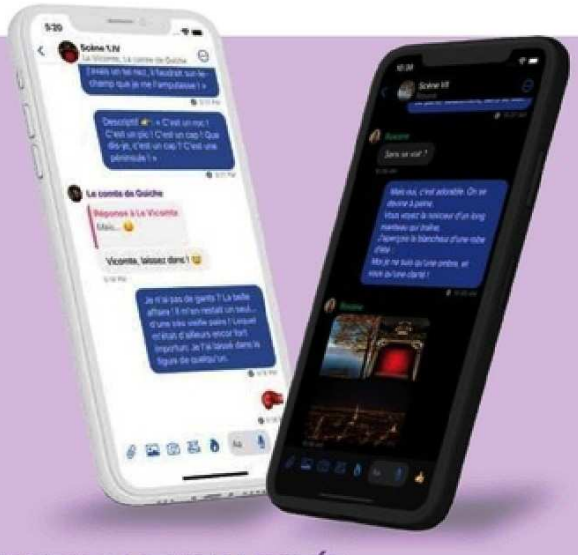
OLVID

> La nouvelle messagerie du gouvernement

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

LE GOUVERNEMENT FRANÇAIS PASSE À OLVID

Crée en juin 2019. Elle ne recueille bien sûr aucune donnée personnelle, même lors de l'inscription, chiffre les échanges de bout en bout et même les métadonnées. Contrairement à ce qui se passe pour la plupart des messageries, chaque conversation établit un lien direct avec le ou les destinataires, sans passer par un serveur central. Comme Threema, Olvid ne nécessite pas de numéro de téléphone pour l'inscription, l'ajout de contacts se fait via QR codes, en raison de l'absence d'un annuaire centralisé.



VERSION GRATUITE LIMITÉE

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

Lien : **olvid.io/fr**

DUST

> L'éphémère radical

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

LA CHÈVRE ET LE CHOU

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

En clair, le contenu de vos messages (chiffrés de bout en bout) ne l'intéresse pas. Mais vos métadonnées, oui. Dust mérite cependant d'exister pour son originalité, mais plus de transparence serait nécessaire pour gagner la confiance des utilisateurs, notamment en rendant le code de l'application disponible en open source.

Lien : **usedust.com**

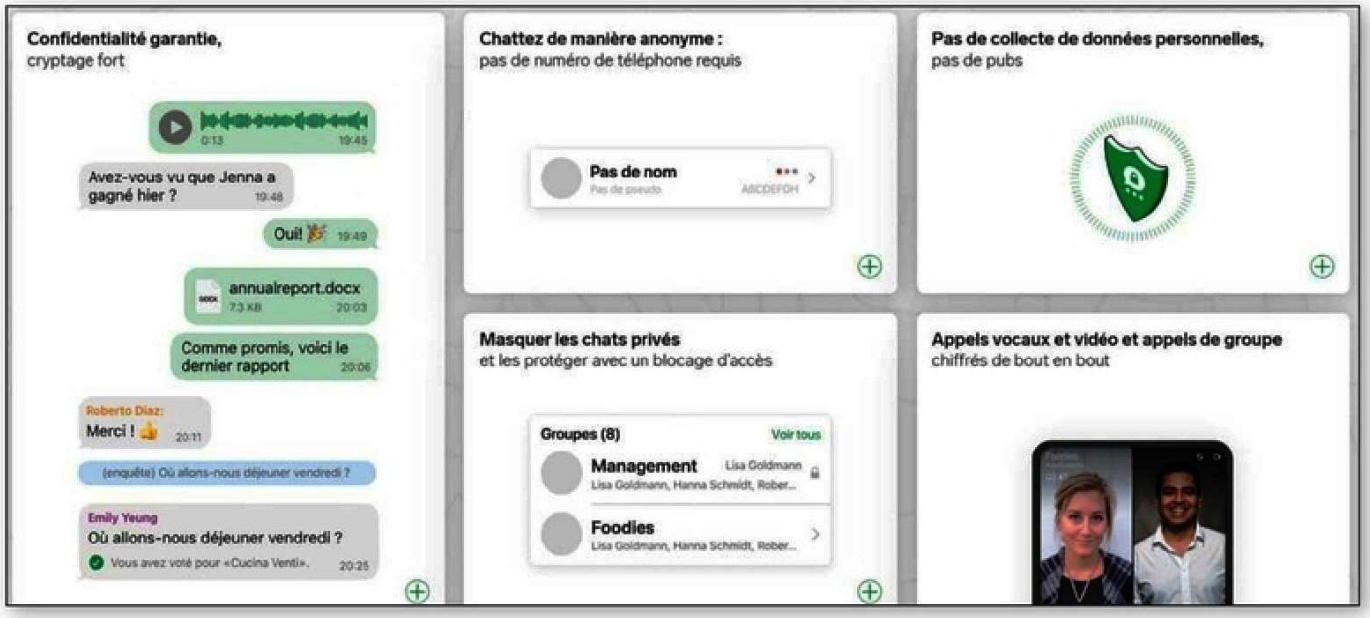
THREEMA
> Le modèle idéal ?

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

PAYANTE, MAIS SANS ABONNEMENT

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

Lien : **threema.ch/fr/home**



TCHAP : L'ÉTAT FRANÇAIS DÉVELOPPE SA MESSAGERIE

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

USAGE INTERNE

Tchap est une alternative sécurisée pour les membres des administrations et du gouvernement pour échanger des informations. Pour le moment, l'application n'est accessible qu'aux fonctionnaires habilités (400 000 quand même). Comme Olvid, elle est rendue obligatoire pour l'exécutif et les besoins de discussions entre collègues, en lieu et place d'autres solutions étrangères. Chiffrée de bout en bout, Tchap est hébergée sur des serveurs de l'État et permet d'envoyer des messages texte de manière sécurisée. D'autres services sont mis à disposition (audio, vidéo) au fil de l'eau. Tchap doit son nom à Claude Chappe, qui a réalisé la première expérience de communication à distance entre Paris et Lille en 1791 et inventé le télégraphe l'année suivante.

Lien : **www.tchap.gouv.fr**

Changement de Circuit

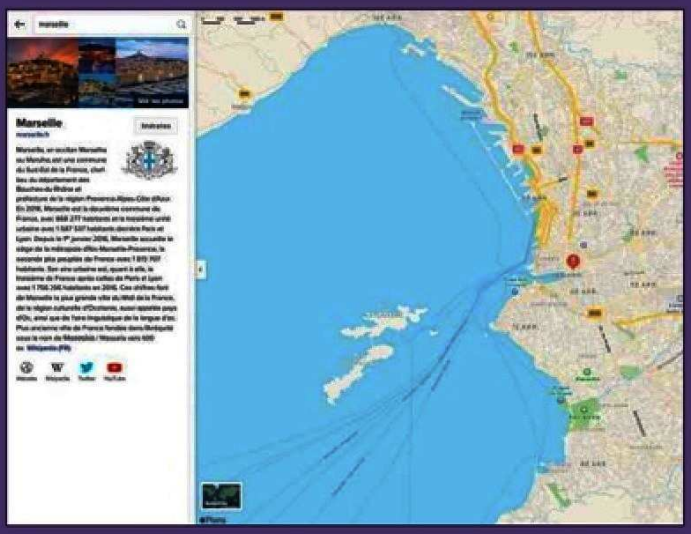
> Avec Tor

Si un site ne charge pas ou semble lent sur Tor, changer de circuit peut résoudre le problème. Cliquez sur l'icône en forme de circuit à gauche de la barre d'adresse. Sélectionnez **Nouveau circuit pour ce site**. Tor établira un nouveau chemin pour le site, ce qui peut améliorer la vitesse ou l'accès.

Utilisez les cartes de DuckDuckGo plutôt que Google Maps

> Avec DuckDuckGo

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



Désactiver l'historique des notifications

> Avec Android

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

SÉLECTION

TOP 10 EXTENSIONS POUR FIREFOX

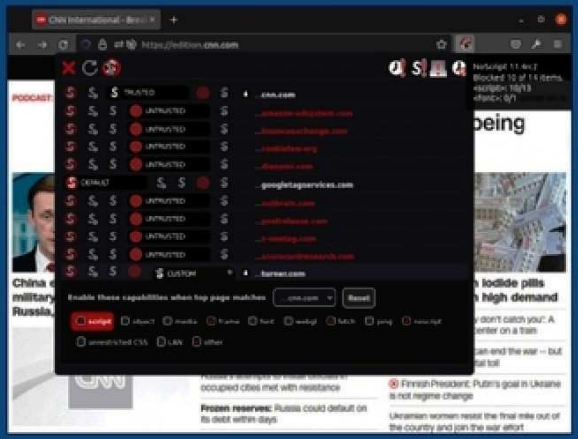
Avec Brave, Firefox est l'un des navigateurs préférés des internautes soucieux de garder le contrôle de leurs données et de leur vie numérique. Il dispose également de nombreuses extensions qui viennent renforcer voire étendre le champ de ses possibilités en matière de sécurité, de protection de la vie privée et de confidentialité.

UMATRIX > Tour de contrôle

UMatrix permet un contrôle complet des connexions, des téléchargements et de l'exécution des scripts par le navigateur. Il est recommandé pour les utilisateurs avancés, car il nécessite de nombreux réglages. UMatrix fonctionne en bloquant par défaut tous les scripts, iframes, et autres éléments potentiellement dangereux, tout en permettant à l'utilisateur de créer des règles personnalisées pour les autoriser sur des sites de confiance. Sa spécificité réside dans sa capacité à décomposer les sites web en composants individuels et à donner un contrôle complet sur ce qui est chargé et ce qui est bloqué. Cela permet de réduire considérablement les risques de malwares, de publicités intrusives et de trackers. L'extension est particulièrement appréciée pour sa flexibilité, mais elle peut être complexe à configurer pour les débutants.

NOSCRIPT > Anti-scripts malicieux

NoScript Security Suite est une extension essentielle pour les utilisateurs de Firefox qui veulent se protéger contre les scripts malveillants et les attaques de type cross-site scripting (XSS). Elle fonctionne en bloquant par défaut tous les scripts JavaScript, Java, Flash et autres types de scripts intégrés dans les pages web. L'utilisateur a la possibilité de permettre ces scripts temporairement ou de manière permanente sur des sites de confiance. Une des particularités de NoScript est sa capacité à offrir une protection même contre les menaces inconnues, grâce à son approche préventive. Bien que très efficace, NoScript peut rendre la navigation plus difficile sur certains sites jusqu'à ce que l'utilisateur configure correctement les autorisations. L'extension est idéale pour les utilisateurs qui privilégient la sécurité et sont prêts à consacrer du temps à la configuration des paramètres pour chaque site.



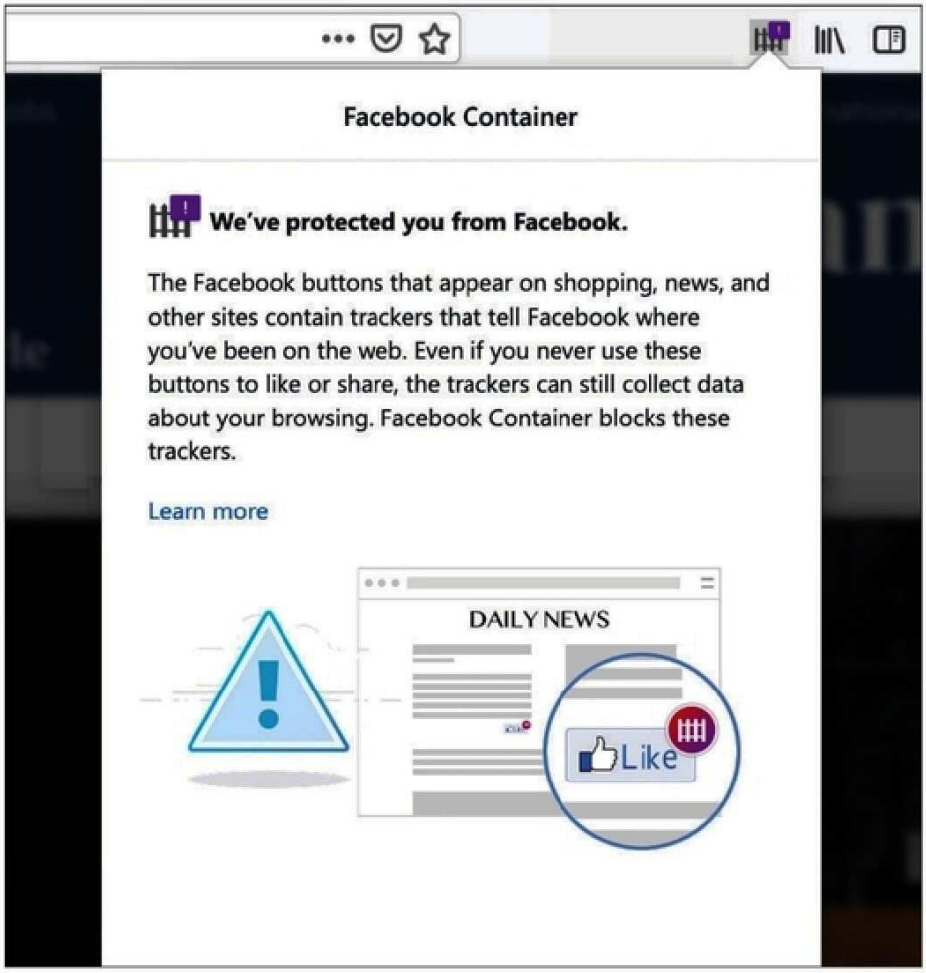
DUCKDUCKGO PRIVACY ESSENTIALS

> Le canard masqué

Cette extension offre une expérience de navigation sans suivi, notant les sites en fonction de leurs pratiques de confidentialité. Elle est facile à utiliser et s'intègre bien aux applications courantes. L'extension évalue et note les sites web en fonction de leur utilisation de méthodes de suivi et de la transparence de leur politique de confidentialité. Elle intègre également le moteur de recherche DuckDuckGo par défaut dans le navigateur, permettant ainsi des recherches anonymes sans suivi. Une caractéristique clé est la fonctionnalité de «Protection de la vie privée», qui force les sites à utiliser des connexions cryptées HTTPS lorsque cela est possible, renforçant ainsi la sécurité des données transmises. L'extension est conçue pour être conviviale, avec une interface simple et des explications claires sur les notes de confidentialité des sites. Elle est particulièrement adaptée aux utilisateurs qui veulent une protection de la vie privée sans avoir à configurer de multiples paramètres ou extensions.

FACEBOOK CONTAINER >

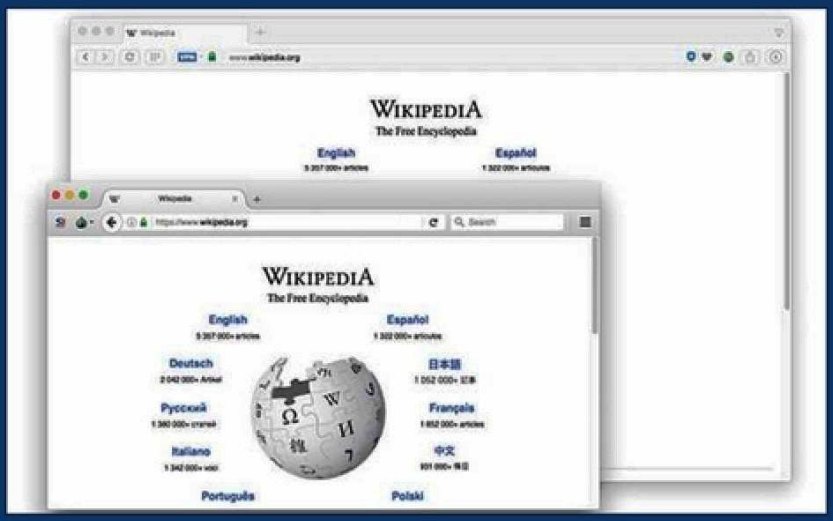
Facebook, pas bouger !



Facebook Container est une extension développée par Mozilla pour limiter la capacité de Facebook à suivre votre activité en ligne en dehors de sa plateforme. L'extension fonctionne en isolant votre identité Facebook dans un «conteneur» séparé, empêchant ainsi Facebook de suivre vos visites sur d'autres sites via des cookies tiers. Lorsque vous utilisez Facebook, l'extension ouvre le site dans un onglet bleu spécial, indiquant qu'il s'agit d'un conteneur isolé. Tout lien non-Facebook ouvert dans cet onglet sera chargé en dehors du conteneur, empêchant Facebook de lier vos activités sur ces sites à votre identité Facebook. Cette extension est particulièrement utile pour les utilisateurs qui veulent continuer à utiliser Facebook tout en limitant son influence sur leur vie privée en ligne. Elle est simple à utiliser et ne nécessite pas de configuration complexe, ce qui la rend accessible à tous les utilisateurs, indépendamment de leur niveau de compétence technique.

OPEN IN TOR BROWSER

> Tu me vois, tu me vois plus



En activant le bouton Tor, les utilisateurs peuvent diriger leur trafic Internet à travers le réseau Tor, rendant ainsi leur navigation beaucoup plus difficile à suivre pour les annonceurs, les fournisseurs de services Internet et les gouvernements. L'extension est particulièrement utile pour les utilisateurs qui nécessitent un haut niveau d'anonymat en ligne, comme les journalistes travaillant dans des environnements répressifs, les militants, ou toute personne soucieuse de la confidentialité. Le bouton Tor permet de basculer facilement entre une navigation normale et une navigation via le réseau Tor, offrant flexibilité et commodité. Il est important de noter que l'utilisation de Tor peut ralentir la navigation en raison de la manière dont le trafic est acheminé à travers différents relais pour atteindre son anonymat.

PRIVACY BADGER

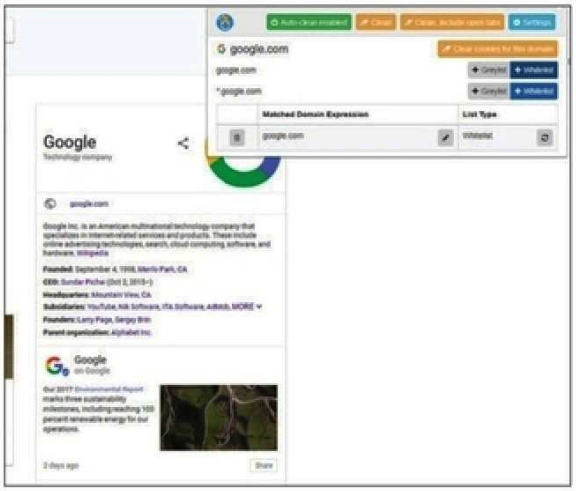
> Pubs et trackers

Privacy Badger est une extension développée par l'Electronic Frontier Foundation (EFF) pour bloquer les publicités et les trackers qui ne respectent pas les préférences de Do Not Track de l'utilisateur. Contrairement aux bloqueurs de publicités traditionnels, Privacy Badger se concentre sur le blocage des trackers invisibles qui collectent des données sur votre comportement en ligne sans votre consentement. L'extension utilise un algorithme d'apprentissage pour détecter et bloquer de nouveaux trackers, ce qui signifie qu'elle s'améliore avec le temps en fonction de votre utilisation. Une caractéristique unique de Privacy Badger est qu'elle ne maintient pas de liste de blocage prédéfinie, mais apprend plutôt quels domaines suivent votre navigation et les bloque en conséquence. Cela rend l'extension efficace contre les trackers récemment apparus et les méthodes de suivi moins connues. Privacy Badger est une excellente option pour les utilisateurs qui cherchent une protection contre le suivi en ligne sans avoir besoin de configurer des listes de blocage ou de filtres complexes.

COOKIE AUTODELETE

> Supprime

Cookie Autodelete gère automatiquement les cookies de votre navigateur. Inspirée par l'extension «Self-Destructing Cookies», elle supprime les cookies des onglets fermés après un certain délai, empêchant ainsi les entreprises de suivre votre navigation

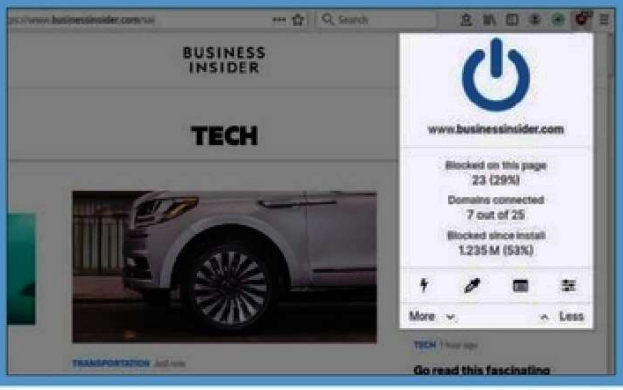


sur plusieurs sessions. L'extension offre une fonctionnalité «Auto-clean» qui doit être activée pour que les cookies soient effacés automatiquement. Les utilisateurs peuvent également créer une liste blanche de sites pour lesquels ils souhaitent conserver les cookies, garantissant ainsi que les préférences et les sessions de connexion restent intactes pour les sites de confiance. L'extension est facile à utiliser avec une interface simple qui permet une gestion efficace des cookies sans expertise technique approfondie.

UBLOCKORIGIN

> Le meilleur bloqueur de pubs

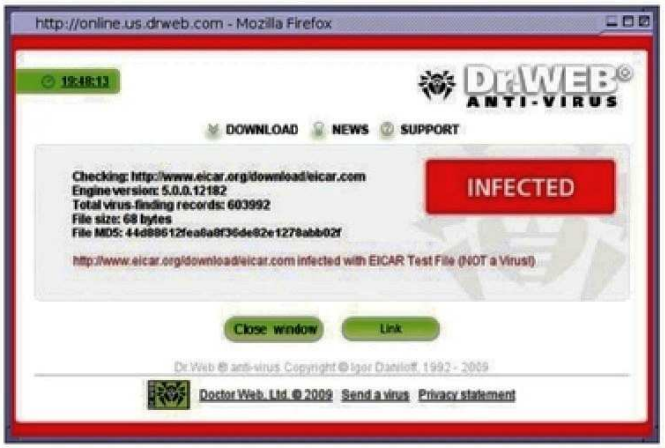
Très recommandée, UBlockOrigin bloque les publicités intrusives et les traceurs. Elle utilise des listes de filtrage pour bloquer les publicités, les traceurs, et potentiellement les scripts malveillants. Les utilisateurs peuvent personnaliser le filtrage et ajouter ou supprimer des sites de la liste blanche. Ce qui distingue UBlockOrigin, c'est sa légèreté en termes d'utilisation des ressources du système par rapport à d'autres bloqueurs de publicités. Elle offre également une interface utilisateur avancée pour ceux qui souhaitent personnaliser leurs filtres.



DR.WEB LINK CHECKER

> Vérificateur de liens

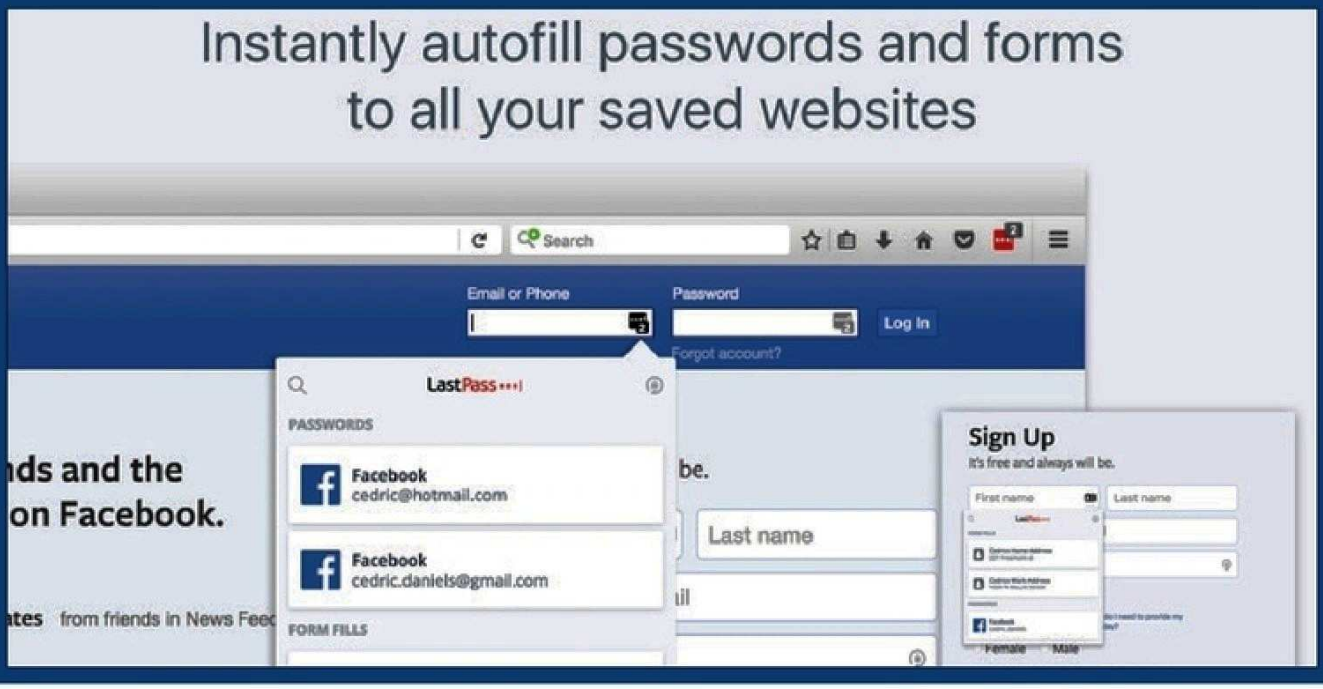
Cette extension utilise le moteur antivirus de Dr.Web pour analyser les hyperliens sur les pages Web, permettant à l'utilisateur de vérifier les liens avant de cliquer, réduisant ainsi le risque d'infection. L'extension utilise le moteur



antivirus de Dr.Web pour scanner les liens et les fichiers téléchargés, fournissant ainsi une évaluation rapide du risque potentiel et évitant, en temps réel, de lancer par mégarde un programme malveillant.

LASTPASS > Gestion de mots de passe

LastPass est un gestionnaire de mots de passe conçu pour stocker et gérer en toute sécurité les identifiants de connexion et les mots de passe. Il stocke ces derniers dans un coffre-fort crypté, sécurisé par un mot de passe principal. Cela signifie que vous n'avez besoin de mémoriser qu'un seul mot de passe fort. Il peut générer des mots de passe forts et uniques pour chaque compte puis s'occuper du remplissage automatique de vos identifiants de connexion. En plus des mots de passe, LastPass peut stocker de manière sécurisée d'autres informations sensibles, telles que les notes sécurisées, les informations de carte de crédit et les pièces d'identité.



TUTO

EMAILS: CACHEZ-VOUS DERRIÈRE UN ALIAS !

AnonAddy est spécialisé dans la création d'alias email. Attention, pas d'un email jetable, mais bien d'un alias que vous pourrez piloter depuis votre adresse principale. Un outil puissant et gratuit pour réduire les risques de spam, de phishing et d'autres formes de cyberattaques.

Votre adresse email est ce que tous les traqueurs et escrocs en ligne utilisent - in fine - pour vous vendre ce dont vous n'avez pas besoin ou, pire, tenter de vous arnaquer (phishing). Vous pouvez bien sûr limiter au maximum les traces que vous laissez sur Internet, mais l'usage d'un email ou d'un numéro de téléphone (encore moins recommandé) est toujours nécessaire pour vous inscrire à un certain nombre de services ou sites. Et si vous preniez l'habitude de donner un faux email, un « alias », pour toute activité qui ne soit pas liée à vos contacts proches ou professionnels. C'est ce que propose AnonAddy. Celui-ci génère des alias email qui redirigent vers l'adresse email principale de l'utilisateur, mais sans jamais dévoiler cette dernière aux services que vous utilisez. .

ALIAS COMPROMIS ? DÉSACTIVEZ-LE

En utilisant des alias pour les inscriptions en ligne, les utilisateurs évitent que leur adresse principale soit ciblée par des spams. En cas de fuite de données, les alias peuvent être facilement désactivés ou modifiés, contrairement à une adresse email principale. Les alias permettent enfin de tracer l'origine des emails reçus, offrant ainsi une meilleure gestion de la provenance des messages.

VERSION GRATUITE PUISSANTE

Anonaddy dispose d'une version gratuite qui suffira à la plupart des usages : création d'un domaine avec autant d'alias que nécessaire, redirection automatique des emails vers une adresse principale enregistrée, possibilité de répondre aux emails sans révéler l'adresse principale. Par contre, si vous souhaitez un nom de domaine personnalisé, il faudra souscrire à un abonnement payant (à partir de 1 € par mois)

5 AUTRES SERVICES

Anonaddy nous a séduits par son interface, la possibilité de créer ses alias directement lors d'une nouvelle inscription (sans repasser par sa plateforme) et surtout par son tableau de bord qui vous permet de vous y retrouver facilement parmi vos alias et de gérer vos comptes au doigt et à l'œil. Et puis, le fait qu'il soit open source et qu'il s'engage sur la protection de vos données est un vrai plus. Mais ce service n'est pas le seul sur le marché ! Voici quelques concurrents qui peuvent aussi vous séduire :

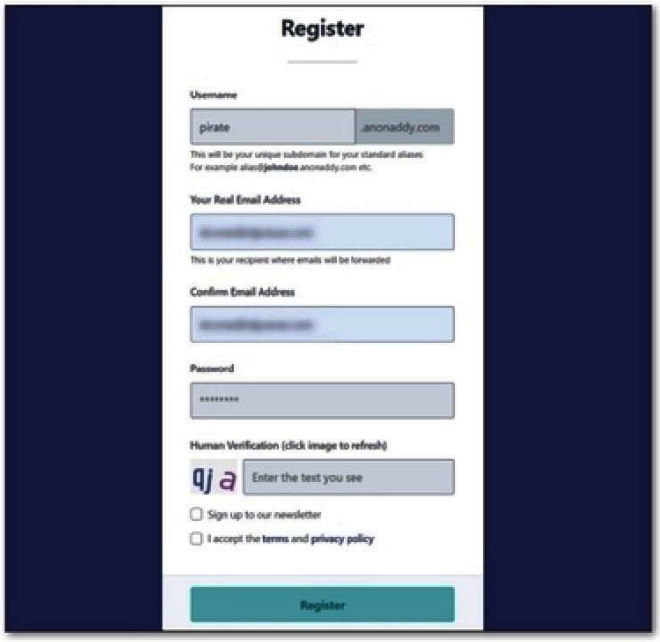
- **SimpleLogin**
- **33Mail**
- **Spamgourmet**
- **Mailinator**
- **Burner Mail**

VOTRE PREMIER ALIAS AVEC ANONADDY

PRATIQUE

01 NOM DE DOMAINE ET MAIL PRINCIPAL

Créez un compte et personnalisez votre alias : en version gratuite, le service vous fournit un nom de



domaine de votre choix (s'il n'est pas déjà pris) de type **@votrenomdedomaine.anonaddy.com**. Renseignez aussi l'adresse email réelle qui sera liée à ce faux compte ultérieurement et les différentes informations. Cliquez enfin sur **Register**. Validez la vérification via votre email puis identifiez-vous sur AnonAddy.

02 ALIAS À LA VOLÉE

Une fois sur le tableau de bord de votre compte, vous vous demandez sans doute comment créer votre premier alias ? Pas besoin ! La prochaine fois que vous enregistrerez un email sur un service Web, mettez celui qui vous passe par la tête sur ce modèle : **monalias@votrenomdedomaine.anonaddy.com.** Ici par exemple : **raoul@pirateinfo.anonaddy.com**.

Vous recevrez tous les mails sur votre adresse réelle sans que celle-ci soit divulguée.

03 GESTION

Ainsi, si un spammeur s'empare de l'un de vos alias et commence à lui envoyer des emails non sollicités, vous pouvez simplement désactiver cet alias

via votre tableau de bord. AnonAddy supprimera alors tout autre email et vous ne recevrez rien d'autre pour cet alias. Si vous supprimez définitivement l'alias, AnonAddy rejettera ensuite tous les emails et répondra par une erreur.

04 RÉPONSE ANONYME

Et vous pouvez bien sûr renvoyer des emails avec cet alias, sans que votre email réel ne soit visible. Vous restez sur votre email principal et utilisez simplement l'option de réponse au mail reçu via votre alias. AnonAddy se charge

de modifier automatiquement le champ d'envoi. Attention, votre client mail doit être compatible DMARC et cette fonction doit être activée.

QUE FAIRE SI JE TROUVE UN TRACKER SUR MA VOITURE ?

La législation française impose un cadre strict pour l'usage de traceurs GPS sur les véhicules. Découvrir un tel dispositif dissimulé sur votre voiture représente une violation de la vie privée, passible de sanctions sévères.

L'installation d'un dispositif GPS est autorisée à condition de ne pas porter atteinte à la vie privée d'autrui. Cela signifie que la personne suivie doit être parfaitement informée de l'existence de la balise et utiliser le véhicule en toute connaissance de cause. Le propriétaire d'un véhicule équipé d'un tel dispositif doit par exemple impérativement en avertir tous les utilisateurs, même si le véhicule ne leur appartient pas officiellement ! Certains assureurs peuvent exiger leur installation pour des véhicules de luxe. Mais, même dans ce cas, conjoints, enfants ou salariés doivent être avertis.

QUELS TYPES DE TRACKERS ?

Les trackers GPS utilisent le système de positionnement global (GPS) pour fournir la localisation exacte d'un véhicule. Le tracker capte les signaux GPS, calcule sa position, et transmet ces informations via le réseau cellulaire ou Wi-Fi à un serveur ou une application, permettant ainsi à l'utilisateur de suivre le véhicule depuis un smartphone ou un ordinateur.
Ils se déclinent en plusieurs modèles, des plus basiques aux plus avancés :

- **Modèles basiques** : Ils enregistrent les données de localisation pour un accès ultérieur. Ils peuvent avoir une autonomie de quelques jours qui oblige l'espion à les récupérer et à les charger régulièrement. Les premiers prix commencent à une vingtaine d'euros.

- **Modèles avancés** : Ils offrent des fonctionnalités en temps réel, comme le suivi en direct, les alertes de vitesse, et parfois des fonctions de contrôle du véhicule. Certains sont aussi équipés d'un micro pour enregistrer leur environnement sonore. Ils peuvent avoir une autonomie de quelques semaines voire de quelques mois. Ils peuvent même être alimentés directement via la batterie du véhicule. Les plus sophistiqués peuvent couter plusieurs centaines d'euros avec, parfois, un abonnement payant pour une gestion 100% à distance via une application.

CE QUE PRÉVOIT LA LOI

L'article L226-1 du Code pénal stipule qu'une atteinte volontaire à la vie privée d'autrui peut entraîner une peine d'un an d'emprisonnement et une amende de 45 000 euros. Cette amende peut atteindre 60 000 euros si l'infraction est commise par le conjoint, le concubin ou le partenaire de PACS de la victime. Cette règle s'applique également aux chefs d'entreprise désirant géolocaliser leurs véhicules de service. Une information préalable des employés est nécessaire, ainsi qu'une déclaration à la CNIL et le respect du RGPD.

QUE FAIRE ?

En cas de découverte d'un traceur GPS installé illégalement sur votre véhicule, le tribunal correctionnel est compétent pour traiter l'affaire. Vous avez le choix de saisir un juge directement ou – et c'est la démarche la plus courante – de porter plainte auprès des forces de l'ordre (police ou gendarmerie). Dans tous les cas, prenez des photos du tracker, notez l'heure et le lieu de la découverte. Gardez le tracker en l'état jusqu'à sa prise en charge par les enquêteurs.
Le tribunal pourra imposer, en plus des peines mentionnées précédemment, des sanctions complémentaires telles que la perte des droits civiques, civils et familiaux, la confiscation du dispositif de traçage, ou une interdiction de port d'armes pour une durée pouvant aller jusqu'à cinq ans. Ces sanctions sont également applicables en cas d'installation d'un micro-espion dans l'habitacle, une infraction tout aussi grave.

DÉTECTION DE TRACKERS GPS

Pour ceux qui soupçonnent la présence d'un tracker GPS, des détecteurs spécifiques existent. Ces appareils scannent les fréquences radio pour détecter les signaux émis par les trackers. Bien qu'ils ne garantissent pas une détection à 100%, ils peuvent être un outil utile pour signaler la présence d'un équipement espion.

CHIFFRER DES ÉLÉMENTS SUR UNE CLÉ USB

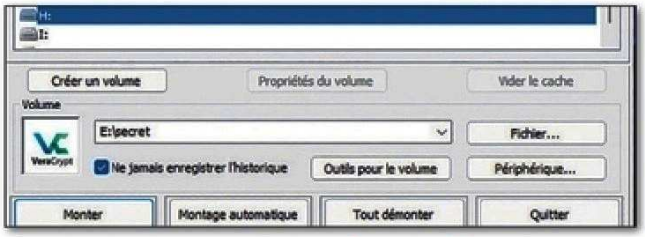
PRATIQUE

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

INFOS [VeraCrypt]
Où le trouver ? [veracrypt.fr]
Difficulté : ☠☠☠

01› CRÉER UN ESPACE CHIFFRÉ SUR LA CLÉ

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



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

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

VÉRIFIEZ UNE URL RACCOURCIE

PRATIQUE

Très pratiques pour abréger une adresse Internet, les URL raccourcies (type goo.gl, tinyurl, bit.ly) sont parfois utilisées pour nuire. En cas de doute, utilisez Unshorten.me pour découvrir ce qui se cache derrière.

Unshorten.me
Où le trouver ? [https://unshorten.me]
Difficulté : ☠☠☠

01› TAPER L'URL

Tapez ou copiez l'adresse raccourci dans le champ prévu à cet effet, sur la page d'accueil d'unshorten.me (une copie est préférable, elle évite les erreurs ou les confusions). Puis cliquez sur le bouton **Un-Shorten**.

02› VÉRIFIER LE LIEN

Le site déchiffre l'URL et affiche une miniature de la page correspondante. Vous pouvez vous rendre directement dessus (bouton **Visit Website**), ou consulter d'abord son score de fiabilité (**Internet Safety User Score**) s'il ne vous inspire pas confiance.

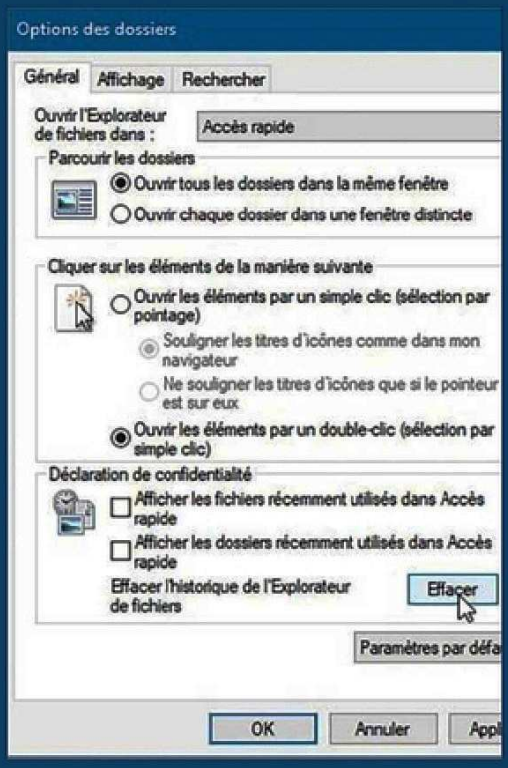
Contre le dropshipping
> AVEC CAPTAINDROP

Arrêtez de payer quatre fois le prix pour des produits provenant de Chine ! Le petit chien renifleur de Captain Drop vérifie les sites et vous indique également où vous pourrez trouver les mêmes produits... mais étrangement pour beaucoup moins cher. Il est disponible en ligne ou via une application pour smartphone.

Lien : **fr.captaindrop.com**

Effacer l'historique du PC
> AVEC WINDOWS

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



Collecte de données... éthique
> AVEC CLEAN INSIGHTS

Vous êtes développeurs de sites Web ou d'applications mobiles et vous recherchez bien sûr un outil de tracing qui vous permette à la fois de collecter des données pour améliorer leurs fonctionnements et services ainsi qu'une meilleure connaissance de votre base utilisateurs. Oui, mais la plupart des solutions proposées sur le marché sont des aspirateurs à vie privée qui ne correspondent pas à votre déontologie et qui sont difficilement paramétrables. Plutôt que de

laisser le choix du « Tout ou rien » à vos utilisateurs, optez pour Clean Insights. Basée sur Matomo, cet applicatif à intégrer exploite par défaut des données pertinentes, mais anonymisées et sécurisées, sans aucun excès de zèle. La vie privée et l'identité de vos utilisateurs sont protégées grâce à plusieurs couches de sécurisation et de dilution. Soutenu par The Guardian Project, Clean Insights est par exemple utilisé par F-droid et Mailvelope.

Lien : cleaninsights.org

Oui,
recycler mes papiers, c'est utile.

Pour l'environnement

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

Le recyclage de papier, c'est :

3 fois moins d'eau*

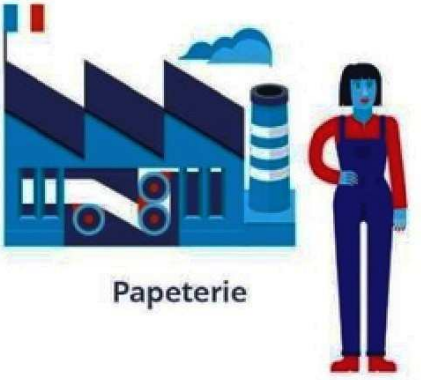
3 fois moins d'énergie*

* comparé à la fabrication de papier non recyclé

Pour l'emploi

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

Collecte



Papeterie

Centre de tri

Découvrez le recyclage du papier sur www.consignesdetri.fr

CITEO

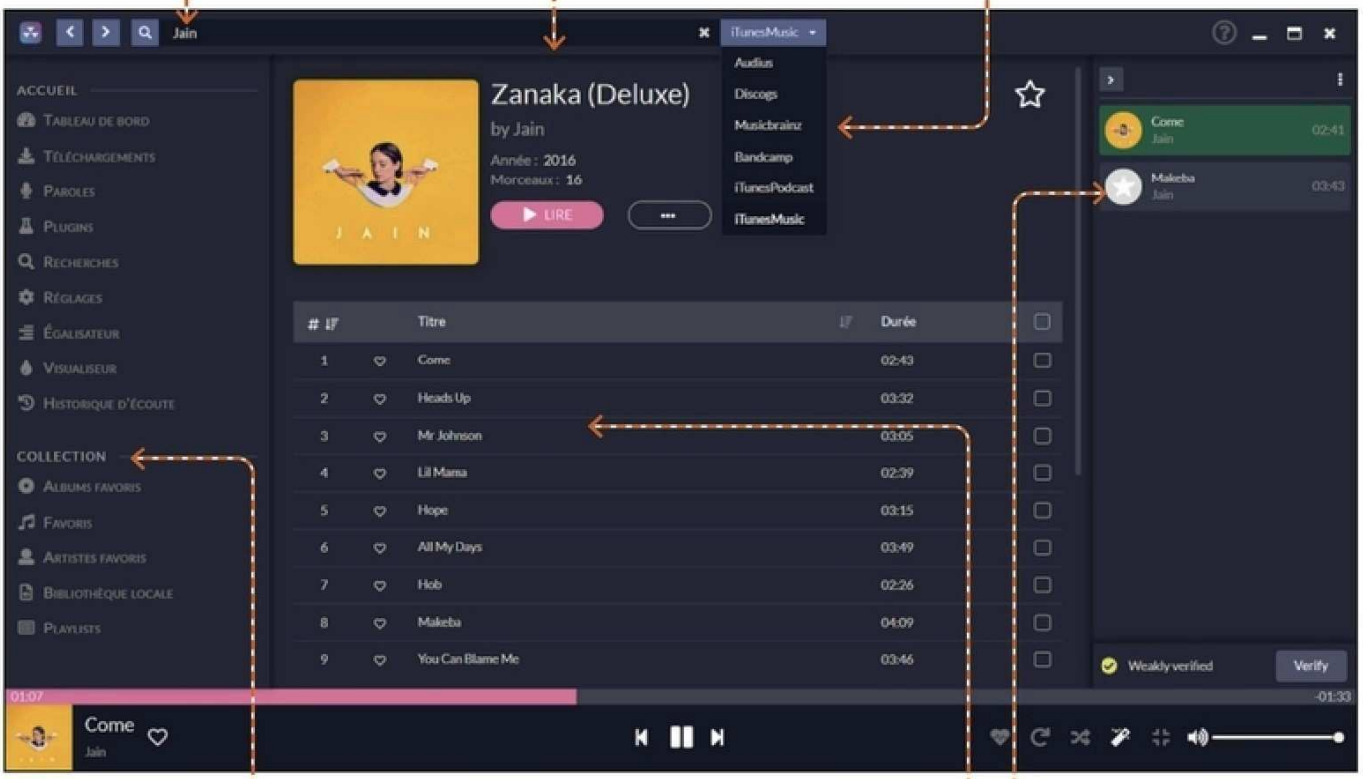
Le nouveau nom d'Eco-Emballages et Ecofolio

DECRYPTAGE

Une interface claire, intuitive et en français : Nuclear séduira les plus exigeants.

C'est ici que vous lancerez vos recherches, par titre, artiste ou album.

Plusieurs sources pour scanner le Web à la recherche de votre musique.



La colonne latérale vous donnera accès à vos fichiers téléchargés, à la gestion de playlists, à un égaliseur, à votre médiathèque PC et à des dizaines d'options de personnalisation via l'onglet **Réglages**.

Le pilotage de vos titres se fait ici, via votre liste de lecture à droite ou via l'espace central ou seront affichés album, playlist et métadonnées.

NUCLEAR

VOTRE PLATEFORME 100% GRATUITE

Nuclear est une plateforme de streaming musical donnant accès à des millions de titres et albums, avec gestion de playlists, recommandations et fonctions avancées. Oui, comme Spotify, Deezer ou iTunes. Sauf que Nuclear est entièrement gratuit, open source et sans pub.

La recette de la fusion nucléaire a été trouvée : vous prenez un peu de YouTube Music, un peu de iTunes, du Soundcloud bien sûr et quelques pincées d'autres services musicaux, vous secouez bien fort sur Github… et vous obtenez Nuclear. Ce service de streaming musical ne cesse d'évoluer et sa dernière version méritait que nous en reparlions dans Pirate. Plutôt que de dépenser dix euros par mois pour un abonnement à Spotify, Deezer ou autres, Nuclear vous propose gratuitement (et sans pub !) des millions de titres et d'albums. Si le contenu est au rendez-vous, le contenant vaut le détour également : une ergonomie agréable et claire, une interface en français et des dizaines de fonctions qui rappellent parfois ce qui se fait de mieux chez la concurrence payante.

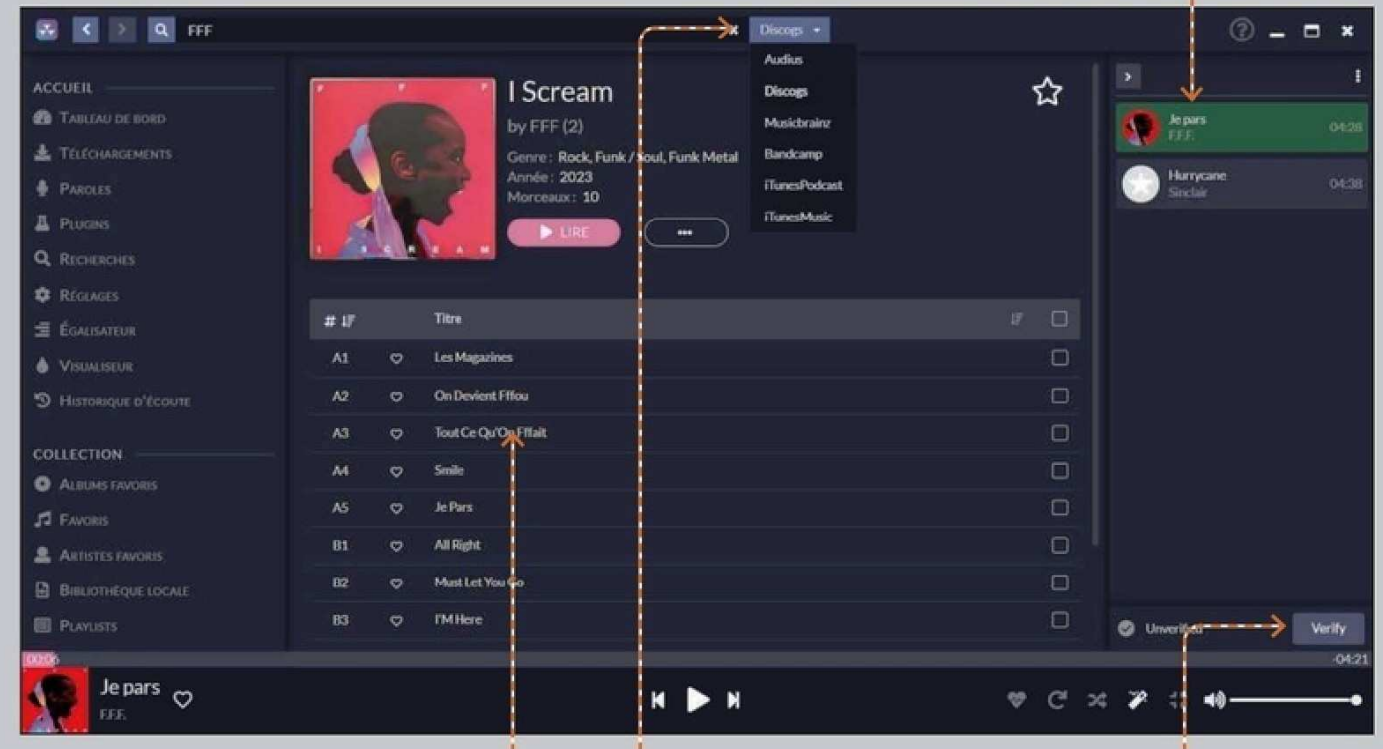
PAS D'APPLICATION SUR ANDROID OU SUR IPHONE

Son vrai bémol, qui sera peut-être corrigé à l'avenir : il n'existe pas encore de version Android ou Apple. Nuclear n'est disponible que pour Windows, Linux et macOS. Et l'on sait combien musique et mobile sont pourtant indissociables. Mais une telle appli pourra-t-elle survivre plus de 5 minutes sur Google Play et l'App Store ? Il y a fort à parier qu'un service aussi sulfureux se ferait rapidement atomiser par les géants américains. C'est même ce que pense Nukeop, le

ERREURS DE FLUX : BUG OU SABOTAGE ?

Quand vous effectuez une recherche, vous croyez obtenir l'album ou le titre désiré, tout semble ok (titre, artiste, etc.), mais lorsque vous lancez la lecture, grosse déconvenue : le son n'a rien à voir ! Nuclear prévient que « Contrairement aux lecteurs qui gèrent leurs propres bibliothèques musicales comme Spotify ou Deezer, Nuclear doit trouver des flux musicaux en fonction du nom de l'artiste et du titre du morceau. Ce processus est imparfait et peut parfois conduire à la lecture de mauvais flux. » Mais comme tout projet ouvert, il est aussi possible que certaines maisons d'édition et d'ayants droit polluent la base de Nuclear avec des flux fantaisistes qui utilisent les mêmes métadonnées, mais avec un contenu vérolé.

Nous sommes repassés par iTunesMusic et, là, le résultat est enfin le bon.



Ici, en passant par **Discogs**, nous avons cherché le dernier album de FFF sorti fin 2023. Tout semble ok, sauf que se cachent de faux sons derrière chacun des titres de la liste de lecture ! Si vous tombez sur ce genre d'erreur, changez de source en haut du logiciel.

Pour aider la communauté, chaque utilisateur peut valider les résultats conformes en cliquant sur **Verify** afin de les faire remonter prioritairement en résultats de recherche.

Le meilleur de la musique trouvé pour vous aux quatre coins du Web et centralisé gratuitement sur Nuclear

créateur de Nuclear : « Les magasins Apple et Google n'accepteraient jamais Nuclear, même sous la forme la plus simple possible. Les téléphones mobiles sont des plates-formes hostiles aux utilisateurs. »
Il avoue aussi que si la création d'une application n'est pas pour lui « une priorité », c'est peut-être qu'il n'a « pas de smartphone et je n'ai pas l'intention d'en acheter un, donc je suis peu familier avec les programmes mobiles et leurs modèles d'utilisation ». Voilà, c'est clair.

COMME UN PRO

Sur PC, contrairement aux interfaces web d'autres concurrents, Nuclear est un logiciel traditionnel que vous installez. Vous pouvez y constituer votre bibliothèque musicale en sélectionnant des chansons ou des albums complets provenant de sources variées telles que YouTube, iTunes, Deezer, Bandcamp, Soundcloud ou Vimeo. Vous pouvez bien sûr aussi y intégrer vos propres fichiers. La recherche peut se faire par chanson, artiste ou album, vous avez la possibilité de créer des playlists, recevoir des suggestions de playlists ou d'artistes similaires, etc. Vous pourrez aussi visualiser les paroles d'une chanson et les pochettes d'albums, profiter d'un égalisateur pour régler le son, et même télécharger une partie de la base de données musicale si les sources sont compatibles. Et ce n'est pas toujours le cas, malgré le scan multi sources qu'effectue Nuclear. C'est ce qui explique aussi la latence observée lors d'un lancement d'un titre la première fois.

À SAVOIR

On apprécie enfin de pouvoir importer des playlists entières en provenance de Spotify ! Idéal pour garder copie de vos titres en cas d'arrêt d'abonnement ou récupérer des playlists partagées par d'autres internautes.

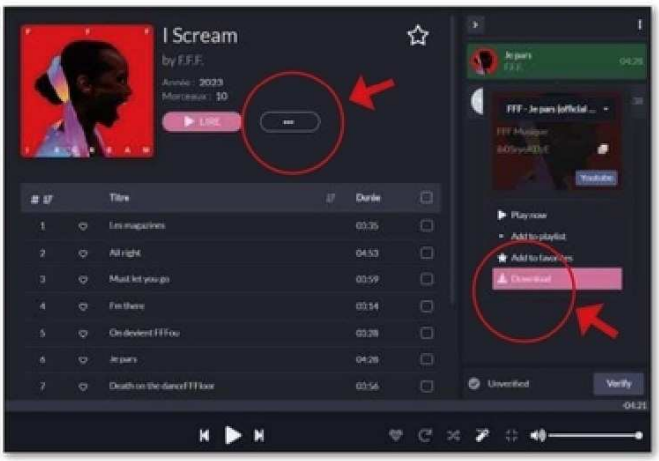
COMMENT TÉLÉCHARGER UN TITRE OU UN ALBUM ?

PRATIQUE

Nuclear cherchera des sources téléchargeables, souvent sur YouTube, du ou des titres sélectionnés et les enregistrera sur votre PC. Les playlists sont aussi concernées même si le résultat peut être plus aléatoire.

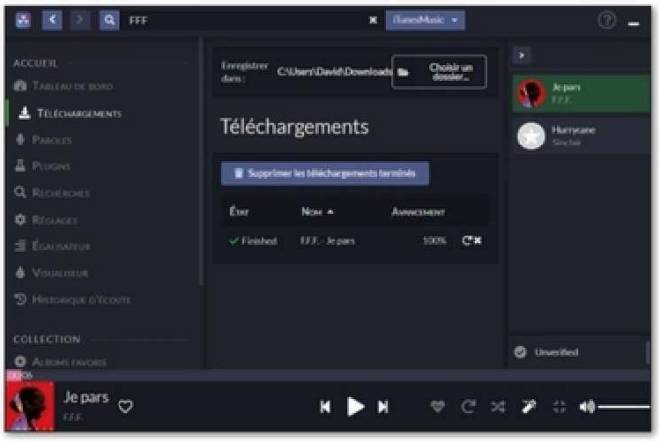
01 › TITRE OU ALBUM

Vous pouvez sélectionner les trois points verticaux à côté du bouton **Lire** pour un album ou faire un simple clic droit sur le titre présent dans votre liste de lecture. Cliquez alors sur **Download** pour lancer le rapatriement.



02 › TÉLÉCHARGER

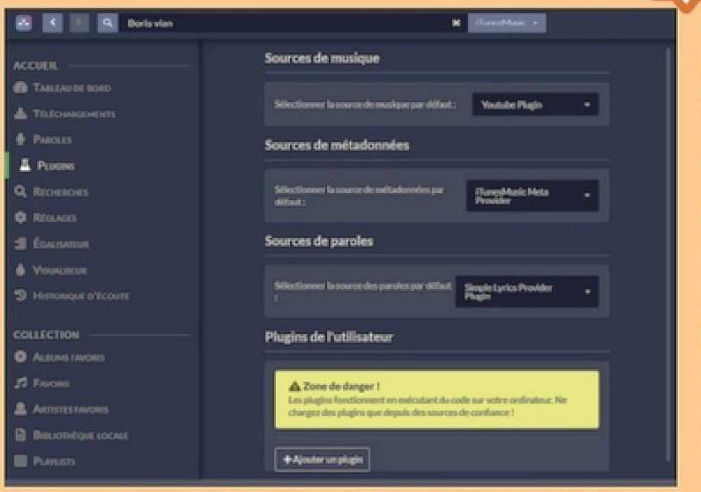
Vous retrouverez vos titres téléchargés ou en cours de téléchargement dans l'onglet **Téléchargements** à



gauche. Un emplacement par défaut est prédéfini sur votre PC, mais vous pouvez bien sûr le changer.

ET LES PLUGINS ALORS ?

Nuclear intègre plusieurs plugins indispensables, c'est ce qui lui permet par exemple de sélectionner les sources de musique, de métadonnées (titre, auteurs, dates, etc.) et de paroles à afficher. La communauté et des services en ligne tiers proposent d'autres plugins pour enrichir l'expérience de l'utilisateur. À découvrir sur GitHub et au hasard de vos pérégrinations sur le Web et sur vos services préférés. Une fois un plugin rapatrié sur votre PC, pour l'installer sur Nuclear, allez dans **Plugins > Ajouter un plugin**. Attention, vérifiez l'avis des utilisateurs et évitez les plugins issus de sources extérieures méconnues, car ce genre d'extensions sont des portes d'entrée royales pour les malwares.



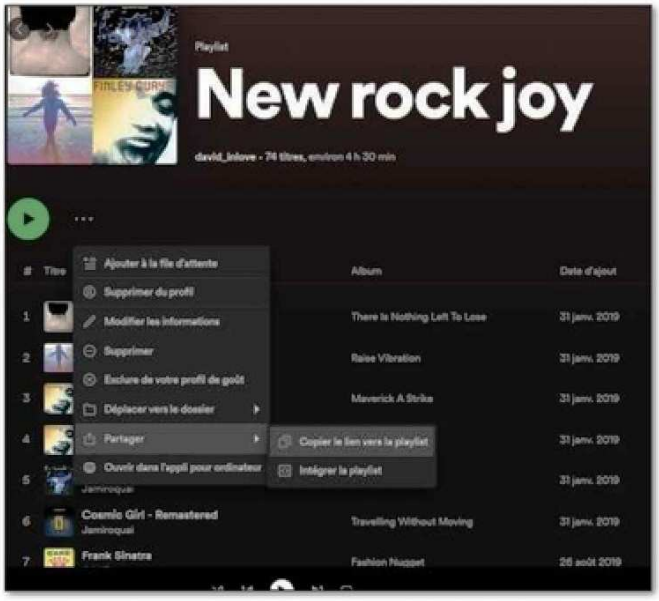
IMPORTER UNE PLAYLIST DE SPOTIFY

PRATIQUE

Une fonction très pratique pour passer d'un format propriétaire (Spotify) que vous pourriez perdre demain à une playlist sauvegardée dans un environnement plus ouvert avec des fonctions plus libres.

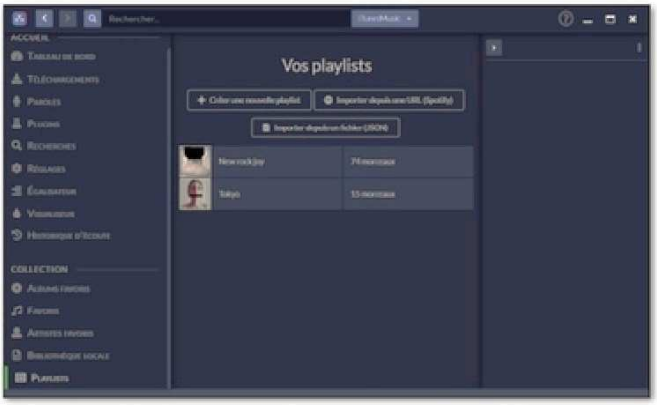
01 › OBTENIR UN LIEN

Pour obtenir le lien d'une playlist Spotify, passez par l'interface Web de la plateforme ou par l'appli Spotify pour PC. Cliquez sur les trois points à droite du bouton **Lire** de la playlist convoitée puis choisissez **Partagez > Copiez le lien vers la Playlist**.



02 › PLAYLISTS NUCLEAR

Revenez maintenant sur Nuclear. En bas de la colonne de gauche, cliquez sur **Playlists**. Vous arrivez sur votre page dédiée avec celles que vous avez créées ou celles que vous avez déjà rapatriées depuis Spotify.



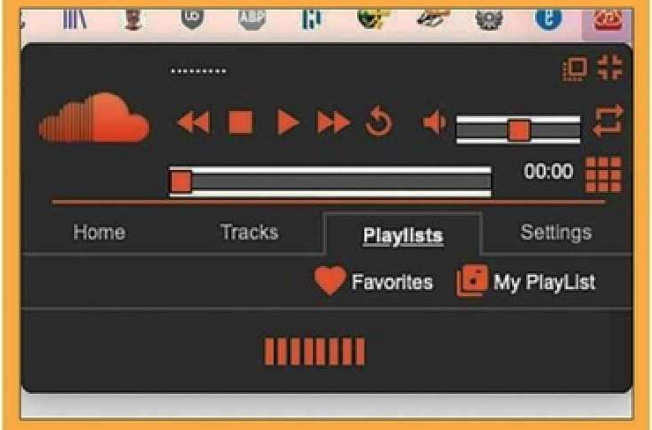
03 › COPIER LE LIEN

Pour en importer une nouvelle, choisissez bien sûr **Importer depuis une URL (Spotify)**. Une nouvelle fenêtre apparait, c'est ici que vous copierez votre lien Spotify avant de cliquer sur **Importer**. Le rapatriement se lance au bout de quelques instants. Sinon, vérifiez qu'un VPN par exemple ne bloque pas la communication.

Piloter Soundcloud avec une extension

> avec Chrome et Firefox

Inutile de garder un onglet de votre navigateur Web dédié spécialement à SoundCloud. Si vous utilisez Chrome ou Firefox, vous pouvez doter votre navigateur de l'extension SoundCloud Player. Gratuite, elle permet



de contrôler la lecture des morceaux et de naviguer dans vos listes de lecture. La lecture peut continuer même après la fermeture de l'onglet SoundCloud dans votre navigateur.

Trouver des livres audio gratuits

> Avec LitteratureAudio

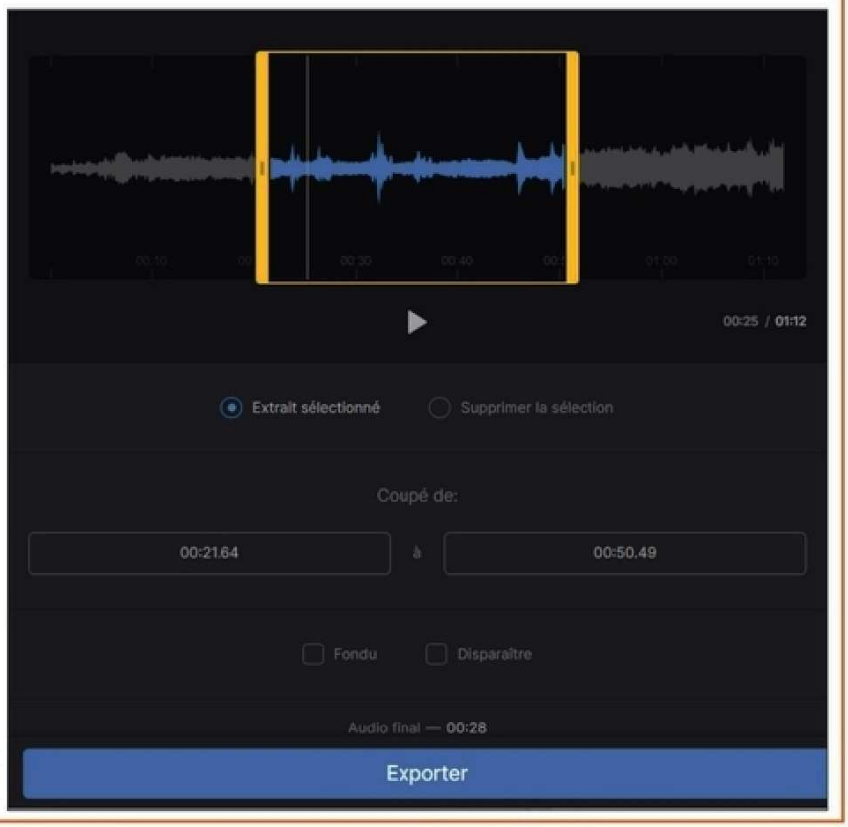
Ce site web offre une vaste bibliothèque de livres audio gratuits (plus de 9000 !), permettant aux amateurs de littérature de profiter de leurs œuvres préférées en écoutant plutôt qu'en lisant. Litteratureaudio.com propose un éventail impressionnant de genres, allant de la fiction classique à la science-fiction, en passant par la poésie et les contes pour enfants. Les livres audio sont disponibles en lecture et en téléchargement gratuit. Litteratureaudio.com offre également des fonctionnalités avancées telles que des listes de lecture personnalisées, la possibilité de commenter et de noter les livres audio, ainsi que des forums pour discuter de vos découvertes littéraires avec d'autres passionnés.

Lien : **www.litteratureaudio.com**

Couper un fichier audio

> avec Clideo

Un service 100 % en ligne, rapide, intuitif et précis pour couper n'importe quel fichier audio. Spécialisé dans la vidéo (plus de 20 services dédiés), Clideo n'en oublie pas moins le son avec deux outils en ligne : l'un pour fusionner des fichiers audio, l'autre pour couper/extraire une séquence précise. C'est ce dernier qui nous intéresse ici.Rendez-vous sur **Les outils > Tous les outils** et sélectionnez en bas **Couper la audio** (oui, la traduction automatique est ici pourrie). Sélectionnez via le bouton **Choisir un fichier** la source que vous souhaitez éditer. Le fichier apparaît et vous pouvez définir l'extrait à couper. Clideo vous propose deux méthodes : vous pouvez sélectionner la longueur en déplaçant deux marqueurs ou en insérant le temps nécessaire en secondes. Une fois calé, il ne vous reste plus qu'à **Exporter**. Vérifiez, modifiez si besoin et téléchargez sur votre PC ou mobile !



PIRATE INFORMATIQUE

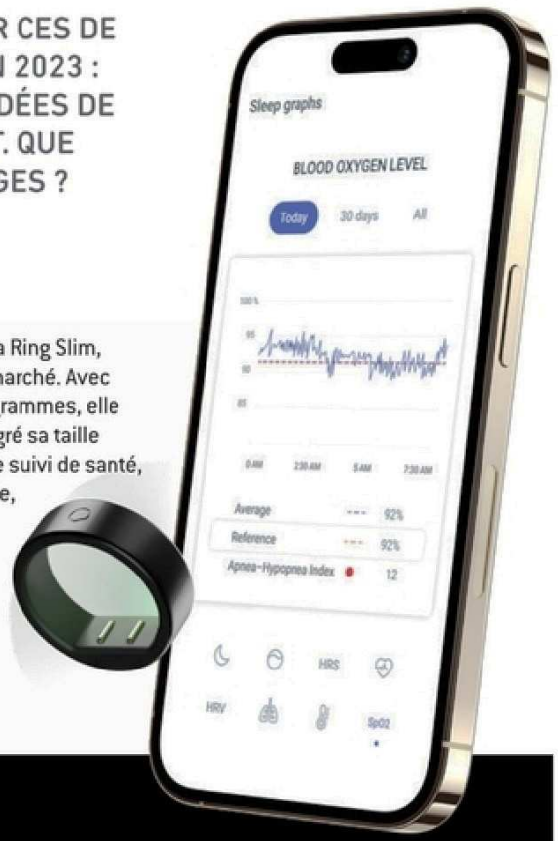
JE SOUTIENS
LE COMMERCE DE PROXIMITÉ,

JE VAIS CHEZ MON MARCHAND DE JOURNAUX

Direct éditeurs

LE RETOUR DES ANNEAUX CONNECTÉS

DE NOUVEAUX MODÈLES PRÉSENTÉS LORS DU DERNIER CES DE LAS VEGAS, PLUSIEURS ANNEAUX REMARQUÉS DÈS FIN 2023 : UNE NOUVELLE GÉNÉRATION DE « SMART RINGS » BARDÉES DE CAPTEURS VEULENT VOUS PASSER LA BAGUE AU DOIGT. QUE PROPOSENT-ELLES COMME FONCTIONNALITÉS ET USAGES ?



CIRCULAR RING SLIM : LA FINESSE FRANÇAISE ?

Circular, une entreprise française, a récemment lancé la Ring Slim, présentée comme la bague connectée la plus fine du marché. Avec une épaisseur de seulement 2,2 mm et un poids de 2 grammes, elle se distingue par sa discrétion et son design épuré. Malgré sa taille compacte, la Ring Slim offre une variété de fonctions de suivi de santé, telles que le rythme cardiaque, la fréquence respiratoire, l'oxygénation du sang (SpO2), le comptage des pas, et la variabilité de la fréquence cardiaque (HRV). Elle suit également l'activité physique, les niveaux d'énergie, les cycles de sommeil, le stress, et le VO2 max, incluant une fonction de cohérence cardiaque et un assistant personnel pour l'analyse détaillée des données. Sa batterie dure 5 jours

Prix : **264 €** Où la trouver ? **fr.circular.xyz**

AMAZFIT HELIO RING : LA FUTURE RÉFÉRENCE ?

Amazfit, une marque connue pour la qualité de ses montres connectées, s'attaque au marché des bagues connectées avec son dernier produit, l'Amazfit Helio Ring. Cette superbe bague au look très réussi vient, elle aussi, d'être présentée au CES 2024. Le prix n'est pas encore connu, mais la commercialisation devrait débuter au second trimestre 2024. Cette bague, conçue pour les sportifs et les amateurs de fitness exigeants, combine élégance et technologie de pointe. La qualité et la précision des capteurs semblent au rendez-vous et devraient faire grimper la facture. Conçue en alliage de titane, elle pèse moins de 4 grammes pour 2,6 mm d'épaisseur. Mais, à l'heure où nous écrivions ces lignes, seules deux tailles étaient proposées : 10 ou 12. Notez que l'Helio Ring pourra par ailleurs être utilisée sous l'eau grâce à sa certification d'étanchéité 10 ATM.

Elle intègre, sans surprise, des capteurs pour mesurer la fréquence cardiaque, le niveau d'oxygène dans le sang (SpO2), et offre un suivi du sommeil avancé avec des options assez bluffantes. De plus, cette bague connectée sera en mesure de s'associer à d'autres écosystèmes et appareils connectés (Strava, Apple Santé, Relive ou Adidas Running). Un abonnement pour un suivi applicatif plus poussé avec de l'IA conversationnelle est également au programme.

Prix : **à venir**
Où la trouver : **www.amazfit.com**

EVIE RING : SANTÉ DES FEMMES

Movano devrait finalement lancer son Evie Ring, une bague connectée spécialement conçue pour les femmes, cette année. La particularité de l'Evie Ring réside dans son aptitude à surveiller non seulement les cycles menstruels, mais également d'autres aspects de la santé des femmes, tels que le sommeil, l'équilibre hormonal, ainsi que la santé physique et mentale. Toutes ces informations sont accessibles via une application spécifique. Du point de vue de l'autonomie, l'Evie Ring promet une durée de fonctionnement de quatre jours sans recharge.

Présentée pour la première fois en 2022, cette bague se distingue par un design élégant et discret, ne trahissant pas son caractère technologique. Initialement prévue pour septembre dernier, la sortie de l'Evie Ring a été retardée, en attente des autorisations nécessaires pour être classifiée en tant que dispositif médical. Des complications liées à l'intégration d'un oxymètre et d'un cardiofréquencemètre ont freiné le processus. Actuellement, l'Evie Ring est disponible en précommande aux États-Unis pour les utilisateurs iOS, proposée à 269 dollars et en trois coloris. Les premières livraisons sont prévues pour la fin janvier. À surveiller pour une sortie prochaine sur les marchés européens et français.

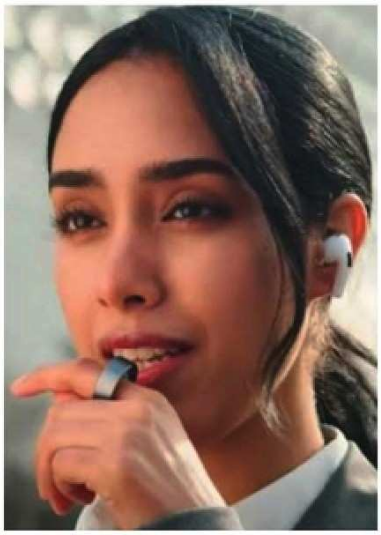
Prix : **269 dollars** Où la trouver ? **eviering.com**

ICE RING : ÉLÉGANTE ET ABORDABLE

Présentée au CES de Las Vegas en janvier dernier, la Ice Ring est une bague connectée élégante et à un prix très compétitif (sous la barre des 200 euros). Conçue par Ice Watch, elle est disponible en trois couleurs (noir, or, argent) et six tailles différentes. Orientée elle aussi sport et santé, elle propose le suivi du sommeil, l'oxymétrie, la fréquence cardiaque, la SpO2, et la variabilité de la fréquence cardiaque. Cependant, elle présente encore des inexactitudes dans la mesure de distance en course à pied. Elle ne dispose pas de son propre GPS et s'appuie sur celui du smartphone pour le calcul des distances, ce qui peut entraîner des inexactitudes importantes. Pour le suivi cardiaque, elle est généralement fiable au repos, mais peut montrer des écarts plus importants durant l'exercice. En ce qui concerne le suivi du sommeil, la Ice Ring semble efficace, détectant correctement les phases d'endormissement et de réveil, ainsi que la concentration d'oxygène dans le sang. Elle pèse moins de 3 grammes et est résistante à l'eau avec une certification IP68. Sa batterie peut durer entre 4 à 6 jours et se recharge rapidement en 30 minutes.

Prix : **199 €** Où la trouver : **www.ice-watch.com**

VTOUCH WHSP : LA BAGUE QUI VOUS ÉCOUTE



VTouch, une entreprise sud-coréenne, a reçu un prix de l'innovation au CES 2024 pour sa WHSP Ring. Cette bague dotée d'un capteur de proximité et d'un microphone s'active lorsque vous la portez à proximité de votre bouche. Via une application sur votre téléphone, vous entrez en contact avec votre assistant qui vous répondra via oreillettes. Vous pouvez simplement marmonner et interagir, comme dans un film d'espions.

VTouch proposera plusieurs assistants intégrant des chatbots conversationnels, aux personnalités et expertises différentes en fonction de vos attentes (à Las Vegas, des démonstrations ont par exemple été faites avec un psychiatre et un conservateur d'art !). Vous pouvez également interagir avec votre environnement connecté grâce aux ordres vocaux que vous donnerez, lancer un enregistrement du son ambiant, etc. C'est classique, mais le geste et la discrétion sont nouveaux. L'autonomie de la WHSP est annoncée à 1,5 jour. VTouch prévoit de lancer WHSP Ring en tant que Kickstarter dans un avenir proche.

Prix : **à venir** Où la trouver : **vtouch.io**

SÉLECTION

TOP 15 Logiciels & services GRATUITS

TOP5 OUTILS DE MONITORING

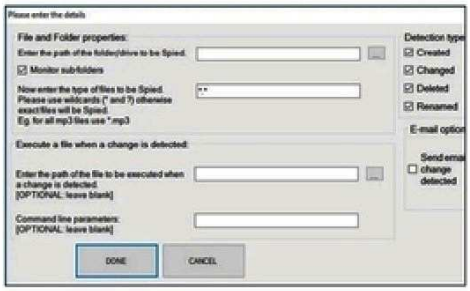
WATCH 4 FOLDER

> LE PLUS DIRECT

Il vous suffit de quelques étapes pour configurer le processus de surveillance de Watch 4 Folder. Ce qui ne limite pas pour autant ses capacités : il peut superviser une quinzaine d'événements différents, et effectuer diverses actions programmées. Par contre, en version gratuite, il ne pourra s'attarder que sur un dossier !

Lien : **bit.ly/3pL1X62**

THEFOLDERSPY > EN MODE ESPION



Cet outil de monitoring peut se transporter sur une clé USB et s'installer en mode incognito sur un appareil. Très léger, il surveille toutes les modifications de fichiers et dossiers et est entièrement automatisé. Une fois en place, vous n'avez plus qu'à regarder les journaux pour savoir ce qu'il s'est passé en votre absence.

Lien : **bit.ly/3KhMQZI**

FOLDERMONITOR > SIMPLISSIME

Cet utilitaire très simple tient dans une seule fenêtre. Vous pouvez surveiller des disques locaux ou partagés, sélectionner le niveau d'alerte, les événements à noter... S'il n'a pas de kit d'installation, il ne comporte pas non plus d'options supplémentaires, qui pourraient compliquer son utilisation.

Lien : **nodesoft.com/foldermonitor**

DIRECTORYMONITOR

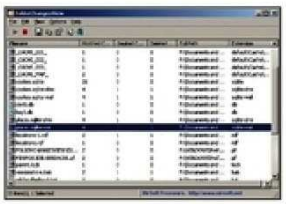
> LE COMMUNICANT

DirectoryMOnitor aime vous prévenir que quelque chose se passe sur votre ordinateur. Soit via un son (si vous ne voulez pas supprimer des fichiers par erreur), soit en vous envoyant des mails quand des modifications sont apportées. Léger, il peut passer inaperçu si vous le décidez. Vous pouvez aussi l'utiliser en mode réseau ou local.

Lien : **directorymonitor.com**

FOLDERCHANGESVIEW

> PORTABLE ET EN RÉSEAU



Déterminez quels fichiers ont été créés, modifiés ou supprimés avec FolderChangesView. Il analyse les disques de votre choix (en local ou en réseau) et se présente également en version portable, sans installation (une clé USB suffit pour l'utiliser). Cependant, pour le moment, il ne fonctionne pas au-delà de Windows 10.

Lien : **bit.ly/3ClrY0P**

TOP5 TÉLÉCHARGER SUR YOUTUBE

NOTMP3 FREE VIDEO DOWNLOADER

> POUR LES PURS

Ce logiciel gratuit est à l'aise avec la vidéo comme avec l'audio. Il permet des téléchargements illimités depuis des milliers de sites, offrant ainsi une grande flexibilité et est apprécié pour son efficacité sans chichi et sans pub ! Disponible uniquement pour les utilisateurs Windows.

Lien : **notmp3.com**

FREEMAKE VIDEO DOWNLOADER

> TOUT TERRAIN

Freemake Video Downloader est un logiciel de téléchargement vidéo hautement intuitif, adapté pour télécharger des vidéos non seulement de YouTube mais aussi de Facebook, Dailymotion ou Vimeo. Il peut convertir les vidéos dans plusieurs formats et extraire l'audio des fichiers vidéo.

Lien : **www.freemake.com**

TOP5 ANTIVIRUS POUR ANDROID

BITDEFENDER ANTIVIRUS FREE

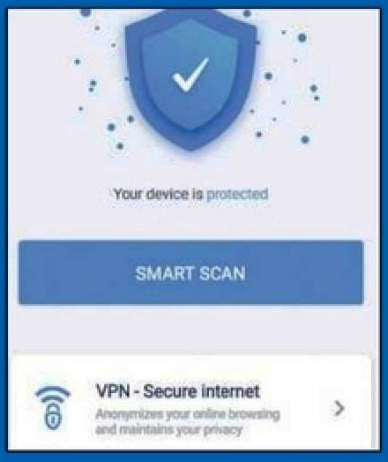
> Gardien Silencieux

Cette application gratuite brille par sa légèreté, avec son scanner antivirus à un clic. Elle se distingue par son approche de cloud-scanning, offrant une détection avancée des menaces sans alourdir le système. La solution de Bitdefender sait se faire discrète, protégeant sans interrompre l'utilisateur.

AVIRA ANTIVIRUS SECURITY

> Protecteur Complet

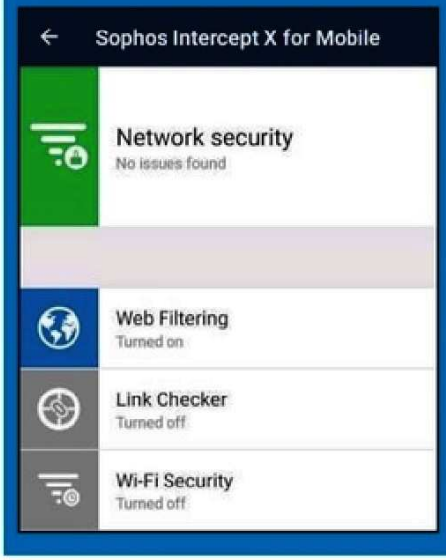
Une solution de sécurité complète : moteur de détection de virus, analyse approfondie des applications, protection des données personnelles, VPN intégré, surveillance Web, etc. Une plateforme à découvrir et à apprivoiser.



PANDA DOME FREE ANTIVIRUS

> Ultra-connecté

Compatible avec les smartwatches, Panda peut opérer à distance via une montre, pour rester informé des menaces en temps réel. L'application détecte la plupart des malwares, avec un accent sur la protection contre les ransomwares et les spywares.



SOPHOS INTERCEPT X

> Highway to Web

Sa fonctionnalité de scans programmés assure une surveillance continue, tandis que sa protection web exceptionnelle bloque efficacement les sites dangereux. L'appli de Sophos met notamment l'accent sur la protection anti-phishing.

KASPERSKY FREE

> Simplicité et puissant

Ses fonctionnalités gratuites se concentrent sur l'essentiel : détection efficace de malwares et protection en temps réel, qui empêche le téléchargement de fichiers nuisibles. Vous pouvez aussi initier des scans depuis une smartwatch (intégration moins avancée que celle de Panda).

NOTUBE > Rapide et efficace

noTube est un service en ligne sans inscription dédié à la conversion de vidéos YouTube en formats MP3 et MP4. Simple, ergonomie réussie et téléchargement d'un clic ! Pas de limite dans le nombre de vidéos à convertir. Attention, la qualité HD n'est pas sélectionnée par défaut.

Lien : **notube.lol**

MP3 YOUTUBE

> Qualité du son

MP3 YouTube, connu sous le nom de MP3Y, offre une expérience utilisateur épurée pour la conversion de vidéos YouTube en MP3. Il promet des fichiers de qualité sonore maximale, bien qu'il ne propose pas de réglages de qualité. Son interface sommaire est fonctionnelle et compatible avec plusieurs sites de streaming vidéo.

Lien : **www.mp3y.org**

CLIPGRAB

> Recherche intégrée

ClipGrab est compatible avec YouTube, Vimeo et Dailymotion. Un des points forts de ClipGrab est sa barre de recherche intégrée, permettant de trouver des vidéos sans ouvrir un navigateur. L'installateur de ClipGrab propose des logiciels publicitaires, donc une vigilance est nécessaire lors de l'installation.

Lien : **clipgrab.de**

Casser les codes et décrypter l'info

JE M'ABONNE à PIRATE INFORMATIQUE

LIVRAISON SOUS PLI DISCRET

OFFRE ABONNEMENT

1 AN POUR 17 € (au lieu de ~~19,60 €~~)

2 ANS POUR 29,40 € (au lieu de ~~39,20 €~~)

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

☐ OUI, JE M'ABONNE :

Nom .....
Prénom .....
Adresse .....
.....
Code Postal .....
Ville .....
E-Mail .....

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

Offre valable en France métropolitaine uniquement.

POUR NOUS CONTACTER :
abonnement@idpresse.com

Signature obligatoire :

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

RÉDUCTION DE -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

VIVEZ HEUREUX, VIVEZ CACHÉS !

MUSIQUE

BITCOIN

ANONYMAT

GPS

TOR

CONFIDENTIELS

ATTAQUES

CHATGPT

MOTS DE PASSE

MESSAGERIES

PIRATE
INFORMATIQUE

IDPRESSE idpresse
L 12730 - 59 - F: 4,90 € - RD

BEL/LUX : 6 € - DOM : 6,10 € - CH : 8,50 ChF - PORT.CONT. : 6 € - CAN : 7,99 $ cad – POL/S : 750 CFP – NCAL/S : 950 CFP - MAR : 50 mad - TUN : 9,8 tnd