

N°55

Casser les codes et décrypter l'info



Février / Avril 2023

PIRATE

INFORMATIQUE

GUIDE

BIEN UTILISER

TELEGRAM

& SES GROUPES



SÉCURITÉ

COMMENT

DÉTECTER

UNE CAMÉRA

CACHÉE ?



Le GUIDE
ULTIME du

HACKER

HACKING

USURPATION DE

NUMÉRO DE

TÉLÉPHONE

Les vraies SOLUTIONS

GRATUITES

BLACK DOSSIER



CHATGPT

L'intelligence artificielle
qui CHANGE TOUT

ANTI-CENSURE



LANTERN

VOUS DONNE ACCÈS
AU WEB BLOQUÉ !

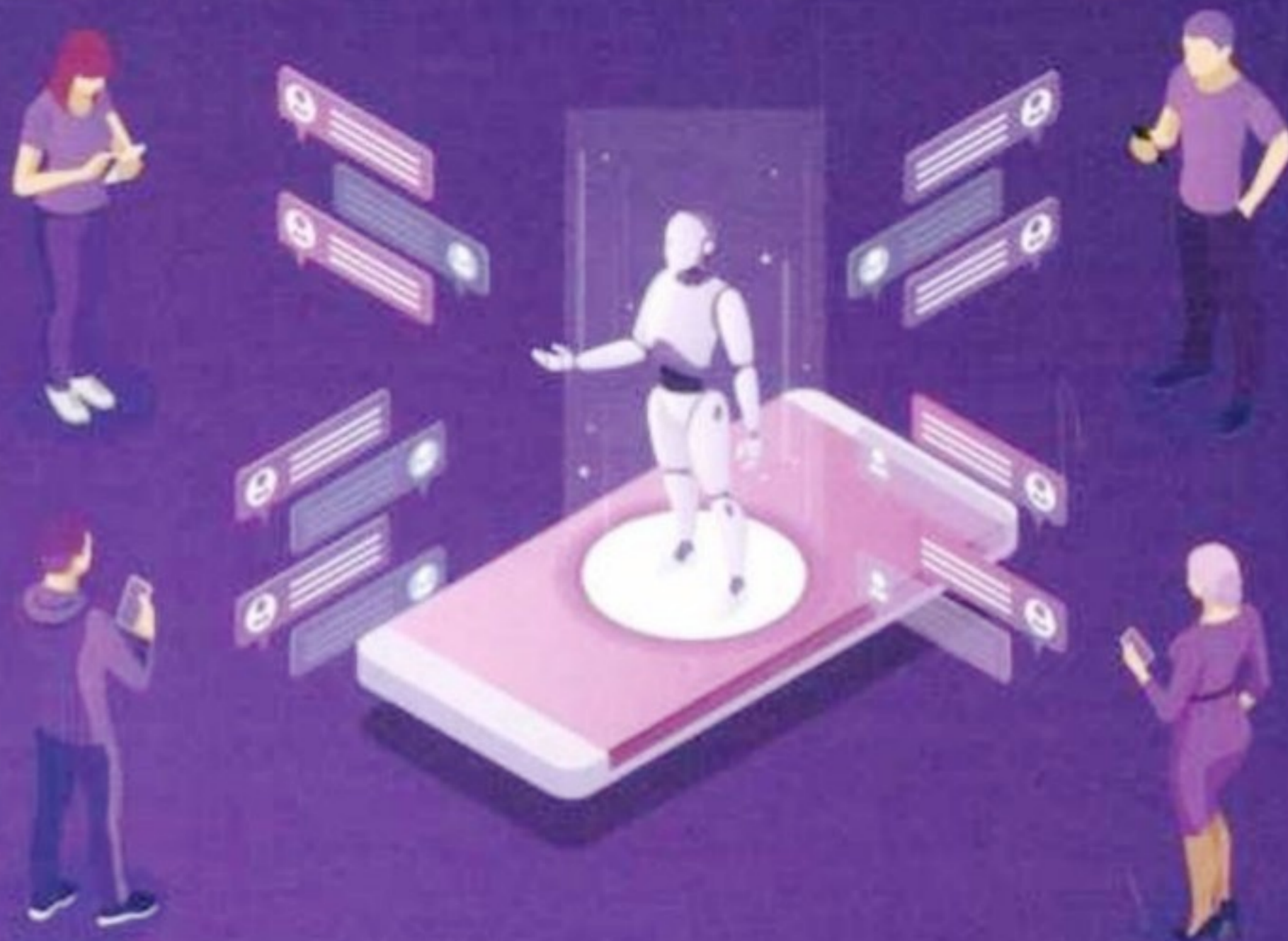


BLACK DOSSIER

13-23

CHATGPT

L'intelligence artificielle qui CHANGE TOUT



HACKING

24-26

> **ASTERISK :**

Comment les pirates **USURPENT** un **NUMÉRO DE TÉLÉPHONE ?**

27-29

> **XBOOT :**

le **MULTIBOOT** facile



ANONYMAT

30-37

> **GUIDE :** Bien utiliser **TELEGRAM**, ses groupes, ...et surtout le **SÉCURISER !**

38-39

> **IDENTIFICATION :**

Et si vous trichiez avec les **DNS ?**



40-42

> **LANTERN,** l'accès internet qui **DÉBLOQUE**



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 !

Février-Avril 2023

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

Directeur de la publication :
David Côme

Rédacteurs :
Fabrice Brochain, Mélanie De Coster

Maquettistes : Sergei Afanasiuk
et Stéphanie Compain

Correctrice : Marie-Line Bailleul

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 : 0722 K 94236

ISSN : 1969 - 8631

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

Parution : 4 numéros par an.

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



PROTECTION

44-45

> Comment **DÉTECTER**
une **CAMÉRA DE**
SURVEILLANCE ?



46-47

> **FAIRMAIL :** Passez à
une boîte mail libre !

48-53

> **GUIDE :** Quittez
Chrome pour **BRAVE !**



54-55

> **CHIFFREZ**
votre **CLOUD** avec
BOXCRYPTOR



MULTIMÉDIA

56

> **CAPTURES D'ÉCRAN** rapides sur Chrome

57-59

> Bien utiliser le **STOCKAGE**
de **ONEDRIVE**



60

> **STREAMING :**
Quatre façons de lier PC et TV

62-63 > NOTRE SÉLECTION DE MATÉRIELS

LA PLANÈTE NUMÉRIQUE CHANGE D'AXE. ENCORE.

Midjourney, Dall-E, Stable Diffusion, Lensa, AI Time Machine, Make-a-video, ...et ChatGPT enfin. Ces services ne vous disent rien ? Mais où étiez-vous en 2022 ? L'intelligence artificielle, dont tout le monde parle depuis le premier Terminator, est enfin entrée dans notre quotidien numérique. Plus vite, plus fort et de façon plus radicale que nous ne l'imaginions. Une nouvelle ère s'ouvre en 2023 avec de

profonds changements de modèles et d'usages. De nouveaux rois vont conquérir le monde, de plus anciens mourront. Passionnant pour les geeks que nous sommes, mais inquiétant pour ceux qui aujourd'hui mettent leurs passions et leurs talents au service de la création de contenus originaux... et humains.

La rédaction



CAMÉRA PASSIVES POUR OBJETS CACHÉS : L'EXEMPLE DE MM-IMAGER

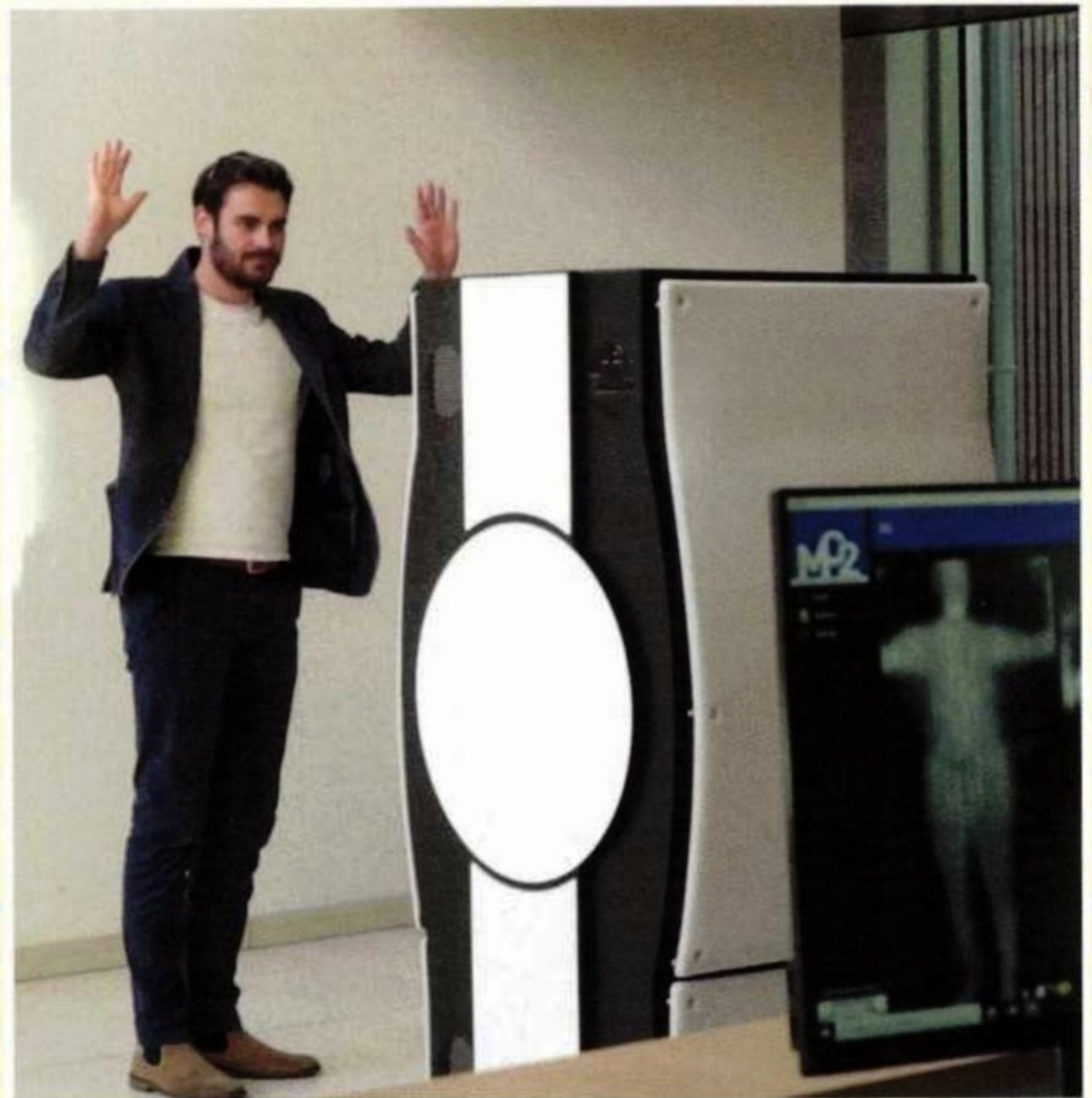
Comment faire pour repérer une personne avec une arme ou des explosifs dans une foule en mouvement ? Une question que tous les professionnels de la sécurité se posent à chaque grand rassemblement (aéroport ou gare, sports, concerts, salons, etc.). Car bloquer le flux des usagers pour contrôles et fouilles devient vite impossible ou même dangereux quand le nombre de personnes devient trop important (nous nous souvenons du fiasco de la finale de la Ligue des Champions à Paris en 2022).

SCAN DE 600 À 900 PERSONNES PAR HEURE

MC2 Technologies, une entreprise du Nord, basée à Villeneuve-d'Ascq, vient de voir son système MM-Imager labellisé pour faire partie du dispositif de sécurité des Jeux Olympiques de Paris, en 2024. Reposant sur les micro-ondes, associées à l'intelligence artificielle, ces caméras innovantes peuvent détecter tous types d'objets cachés dans des contenants ou sur des individus... y compris en mouvement (600 à 900 personnes par heure).

LES ONDES ÉMISES PAR LE CORPS HUMAIN... ET LES AUTRES

MM-Imager est une caméra dite « passive », c'est-à-dire qu'elle n'émet pas d'ondes pour scanner les corps humains. Elle est cependant bardée de capteurs qui mesurent les micro-ondes naturelles qui sont émises, réfléchies et transmises par les objets et le corps humain. Un algorithme dopé au deep learning est chargé d'identifier les anomalies et menaces repérées. Elle peut ainsi détecter tous les objets cachés en temps réel sur des personnes en mouvement : objets métalliques, liquides, matériaux solides, produits sous forme de poudre ou de tout autre aspect (colloïde, céramique, etc.).



RGPD

META ENCORE ÉPINGLÉE

Le groupe Meta, qui possède Facebook, a été condamné mercredi 4 janvier à une amende de 390 millions d'euros pour violation du règlement général sur la protection des données (RGPD) par la commission irlandaise pour la protection des données (DPC), qui agit au nom de l'Union européenne. Selon le régulateur irlandais, Meta a violé "ses obligations en matière de transparence" et a utilisé une "base juridique erronée" pour traiter les données personnelles à des fins de publicité ciblée. Cette amende fait suite à trois décisions du Comité européen de la protection des données (CEPD) en décembre, dont deux concernant des infractions liées à Facebook (210 millions d'euros) et Instagram (180 millions d'euros). Une troisième, concernant WhatsApp, était décidée après la publication de ce numéro de Pirate Informatique. Meta a déclaré qu'il comptait faire appel "du fond et des amendes".



NOUVELLE MENACE POUR VOS APPLIS BANCAIRES SUR ANDROID

Dans un article publié le 5 janvier, les chercheurs de ThreatFabric ont déclaré avoir constaté depuis octobre une augmentation importante des échantillons du malware de la famille SpyNote.

En plus de se faire passer pour des applications génériques comme des jeux et des applications de productivité, la variante SpyNote.C s'est également fait passer pour des institutions financières reconnues ainsi que d'autres applications stars comme WhatsApp, Facebook et Google Play.

Également connu sous le nom de SpyMax, SpyNote.C peut exfiltrer et utiliser des informations personnellement identifiables des clients de banques en ligne, ainsi que suivre les SMS, les appels, les vidéos et les enregistrements audio. Il peut extraire des codes d'authentification à deux facteurs et enregistrer les frappes de touches, ainsi que récupérer les mots de passe des applications de médias sociaux comme Facebook et Gmail.

En utilisant les services d'accessibilité d'Android, les chercheurs indiquent que SpyNote.C rend difficile la désinstallation et permet au malware d'installer de nouvelles versions de lui-même, ainsi que d'autres applications sans aucune intervention de l'utilisateur.



VINCENT STRUBEL, NOUVEL HOMME FORT DE LA DÉFENSE CYBER

Vincent Strubel a été nommé directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi), qui compte environ 600 personnes. M. Strubel, qui était jusqu'à présent directeur de l'Opérateur des systèmes d'information interministériels classifiés (Osiic), remplace Guillaume Poupard, qui a dirigé l'Anssi pendant huit ans et a été nommé directeur général adjoint de Docaposte, la filiale numérique de La Poste. M. Strubel a passé la majorité de sa carrière à l'Anssi avant de partir diriger l'Osiic, qui gère les communications sécurisées de l'Etat et compte 300 personnes. L'Anssi, qui est rattachée au premier ministre par le secrétariat général de la défense et de la sécurité nationale, est chargée de protéger les systèmes d'information de l'Etat français.



© Anssi

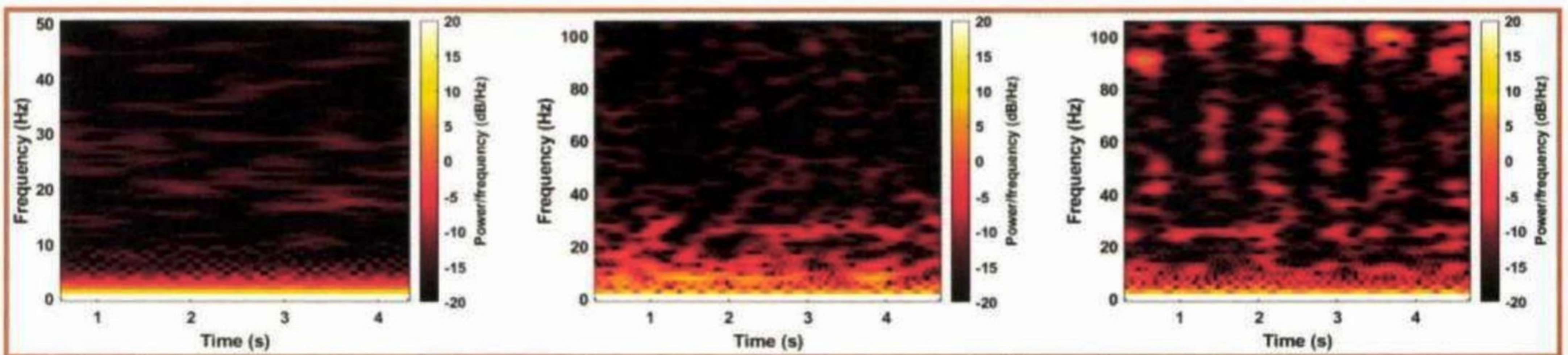


GOOD VIBRATIONS

EARSPY : LES HAUT-PARLEURS DE NOS SMARTPHONES BIENTÔT SUR ÉCOUTE ?

Des chercheurs de cinq universités américaines ont développé une technique qui permet d'écouter et de collecter des informations en analysant les vibrations émises par le haut-parleur supérieur de smartphones Android. Cette technique, appelée Earspy, utilise les

caractéristiques du flux audio. Un algorithme de machine learning a été entraîné pour reconnaître le contenu des paroles, l'identité de l'appelant et son sexe. Les résultats des tests ont été généralement prometteurs pour l'écoute clandestine via le haut-parleur auriculaire, avec de forts



capteurs de mouvement, en particulier l'accéléromètre, pour capturer les vibrations générées par le haut-parleur. Des recherches précédentes avaient déjà montré qu'il était possible d'espionner des mobiles via les haut-parleurs, mais celui situé près de l'oreille était considéré comme trop faible pour générer suffisamment de vibrations. Cependant, les fabricants de smartphones ont amélioré les capacités audio de leurs appareils, ce qui a entraîné des vibrations plus fortes qui peuvent être détectées par les capteurs de mouvement.

Les chercheurs ont téléchargé une application tiers pour capturer les données de l'accéléromètre pendant un appel simulé, qu'ils ont envoyées à un logiciel de calcul numérique pour être analysées et pour extraire des

Les capteurs de mouvement comme l'accéléromètre et le gyroscope de vos smartphones sont sensibles aux vibrations de vos appels : ici, les infos collectées sur des mobiles OnePlus qui ont pu être exploitées.

taux de reconnaissance pour l'identification du genre et de l'appelant, mais la reconnaissance vocale reste faible. Les chercheurs ont donné quelques conseils pour éviter ce type d'attaque, tels que baisser le volume du haut-parleur et encourager les fabricants à placer les capteurs de mouvement dans des endroits où les vibrations sont minimisées.

MESSAGERIE

WHATSAPP PROPOSE UN OUTIL ANTI-CENSURE

WhatsApp a annoncé début janvier l'intégration d'un nouvel outil pour contourner la censure, principalement destiné aux pays qui bloquent temporairement ou de manière permanente l'accès à l'application. Ces pays bloquent généralement l'accès aux serveurs de WhatsApp, empêchant ainsi les utilisateurs d'envoyer ou de recevoir des messages. WhatsApp propose ainsi une option permettant aux utilisateurs de choisir manuellement un serveur proxy, un serveur intermédiaire qui relaye automatiquement les données aux serveurs de WhatsApp. Ces serveurs proxy ont une adresse différente de celle de WhatsApp, ce qui les rend plus difficiles à identifier et à bloquer pour les censeurs. WhatsApp a déclaré que la connexion via un serveur proxy maintiendra le haut niveau de confidentialité et de sécurité de l'application. Des particuliers et des organisations non gouvernementales peuvent créer directement des serveurs proxy. Cette fonctionnalité semble avoir été conçue spécifiquement pour les utilisateurs iraniens, car WhatsApp et Instagram (propriétés de Meta) sont bloqués dans le pays depuis les manifestations de fin 2022. WhatsApp mentionne spécifiquement l'Iran dans son communiqué, évoquant les coupures d'accès qui "bafouent les droits humains en empêchant la population de recevoir une aide urgente".



LA MAIN DANS
LE POT DE MIEL

TIKTOK PEUT ESPIONNER À LA DEMANDE



ByteDance, l'entreprise chinoise propriétaire de TikTok, a admis que certains de ses employés avaient eu, de manière incorrecte, accès à des données de la plateforme pour traquer des journalistes dans le but d'identifier les sources de fuites d'informations aux médias. Les employés ont principalement accédé aux données de deux journalistes ayant écrit sur l'entreprise. Ils cherchaient à établir des liens entre le personnel de ByteDance et un journaliste du Financial Times ainsi qu'une ancienne journaliste de BuzzFeed. ByteDance a indiqué que les salariés impliqués n'étaient plus employés par l'entreprise sans donner de détails sur leur nombre. En octobre, des journalistes de Forbes avaient révélé que ByteDance avait l'intention de suivre leur emplacement physique et celui de leurs collègues. En raison de ces pratiques, le Congrès américain pourrait interdire l'utilisation de TikTok par tous ses élus.

PIXEL CHIC, PIXEL CHOC !

En octobre dernier déjà, une étude de l'entreprise Disconnect montrait que TikTok suivait l'activité des internautes sur de nombreux sites Internet étrangers en utilisant des "pixels espions" qui envoient des informations personnelles lorsqu'ils sont chargés lors de la navigation. Selon cette étude, des centaines d'organisations partagent des données avec TikTok, parmi lesquelles certains sites sensibles révélant des informations sur la santé ou la religion. Ces données peuvent inclure l'adresse IP, un numéro unique, la page consultée ou ce qui est tapé sur le clavier de l'internaute et sont utilisées à des fins publicitaires. Une porte-parole de TikTok a déclaré que les données reçues des publicitaires sont utilisées pour améliorer l'efficacité de leurs publicités et que TikTok dispose de mécanismes pour empêcher la transmission de données sensibles. Et il est vrai que TikTok n'est pas le seul géant du numérique à utiliser ces « pixels espions » (lire nos précédents numéros) mais l'opacité qu'elle entretient quant à son traitement des datas et sa proximité avec le pouvoir central chinois inquiètent encore davantage.



INTERNET : LA GRANDE DIVISION ?

Un seul internet pour réunir tout le monde ? Ce pourrait bientôt être une vision du passé. Le « splinternet » est déjà en action.

Au départ, Internet, c'était avant tout une vaste toile d'araignée mondiale qui pouvait relier tout le monde. Avec un simple accès au réseau, un paysan du fin fond des Carpates pouvait échanger avec un autre au Vietnam et un troisième en Amérique du Sud. C'était presque utopique, quand on y pense. Et c'est peut-être pour cela que ce beau modèle est d'ores et déjà en train d'exploser. C'est ce qu'on appelle le « splinternet ».

C'EST QUOI ENCORE CE NÉOLOGISME ?

Hé oui, il est temps d'ajouter un nouveau mot à votre dictionnaire d'internet. Splinternet est une contraction des mots « splintering of the internet », soit « l'éclatement

d'internet ». Et cette jolie expression ne fait pas référence à un événement festif. Au contraire.

Le splinternet est évoqué depuis plus de vingt ans. C'est un Américain du nom de Clyde Wayne Crews qui a imaginé ce terme en 2001. On en parle de plus en plus actuellement, car l'actualité géopolitique accentue ce phénomène. Certains spécialistes parlent également de balkanisation de l'internet pour définir le même phénomène. Cet éclatement d'internet est dû au fait que certains pays (ou, plus précisément, des blocs politiques) ont la volonté de créer des réseaux fermés : impossible pour leurs résidents d'accéder à l'extérieur, même virtuellement, et de communiquer avec, bien sûr. Il en est par exemple ainsi de RuNet, le projet d'intranet géant de Russie, que les dirigeants voudraient faire fonctionner uniquement de et



EN RUSSIE, INTERNET OU RUNET ?

Le Kremlin veut museler Internet. Ce qui est assez paradoxal, alors que RuNet est d'abord né libre et de manière anarchique, dans les années 2000. Mais, dès 2008, l'administration présidentielle a demandé à avoir accès à l'interface de la page d'accueil en cas de guerre. Et, en 2019, une loi passée par la Douma a donné aux autorités les moyens légaux et techniques pour rendre possible un contrôle total des flux de données qui entrent et sortent du territoire tout en laissant les mains libres à l'État pour déconnecter le pays du reste de l'Internet en cas de menace extérieure.



La bonne nouvelle, c'est que les moyens technologiques ne sont pas encore suffisants actuellement pour le découpler totalement du réseau mondial. Tout simplement, car le réseau russe est l'un des plus complexes à maîtriser. Mais les investissements technologiques vont dans ce sens. Ce qui inquiète certains experts : le jour où les Russes parviendront à prendre le contrôle de leur réseau, ils seront aussi en mesure de vendre leur technologie à qui la voudra.

vers l'intérieur du pays. Mais ce n'est pas le seul cas qui existe. Et le splinternet définit des internet complètement différents les uns des autres. Comme des univers parallèles, avec toutes les dérives potentielles que cela peut représenter.

COMME SI CELA NE SUFFISAIT PAS, IL SE DIVISE ENCORE

On croirait une histoire qui se multiplie à l'infini. Car, évidemment, il n'existe pas qu'une seule version du splinternet. Et certains modèles concernent même des pays traditionnellement considérés comme étant ouverts d'esprit (pas que la Chine, donc).

Par exemple, les États-Unis, le Royaume-Uni ou l'Australie utilisent une version d'internet qui leur permet d'ajouter quelques options de censure quand ils le jugent nécessaire. Pour le moment, l'idée est surtout de pouvoir bloquer la pédopornographie ou les commerces illégaux, mais tout peut se passer si un jour ces gouvernements se

Dans les jours précédant les élections de 2021 en Ouganda, l'accès aux réseaux sociaux a été bloqué. Une forme de splinternet temporaire.



durcissent. Néanmoins, le modèle actuellement utilisé, dit ouvert, permet toujours de communiquer entre les différents réseaux. Même chez nous, en Europe, l'internet que nous utilisons n'est pas tout à fait le même que les autres, puisque des directives européennes visent à assurer la protection de notre vie privée, ce qui n'existe pas partout. Et c'est aussi ce qui permet de bloquer l'accès à des sites de streamings et de téléchargements situés à l'étranger. Quand des sites existent et que devez trouver des moyens détournés pour les atteindre, c'est que tout le monde n'utilise déjà plus internet de la même manière.

Là où ça devient un peu plus inquiétant pour la liberté individuelle (et d'expression), c'est bien sûr quand les architectures en place permettent de limiter les accès de manière très restreinte. Comme,

LA GRANDE MURAILLE VIRTUELLE CHINOISE CRÉE UN ÉCOSYSTÈME FERMÉ OU TOUT CE QUI N'EST PAS AUTORISÉ ET SURVEILLÉ N'EXISTE PAS SUR INTERNET.



au hasard, en Chine, en Russie, en Iran ou en Arabie Saoudite. Des endroits où les personnes qui veulent s'informer en dehors des voix gouvernementales n'ont pas d'autre option que d'utiliser des VPN.

QUAND LES FRONTIÈRES NE SONT PAS QUE VIRTUELLES

Certains pays mettent en place une censure plus que rigoureuse. C'est le cas en Chine, où l'on parle de Grande Muraille Virtuelle. Dès le début d'Internet, Pékin a mis en place un bouclier permettant de surveiller et de censurer l'activité en ligne. Et cela jusque dans les moindres détails : une nouvelle loi a récemment été votée pour exiger que tous les commentaires y soient approuvés avant d'être publiés (oui, même les GIF). Certaines mesures peuvent plus rassurer les parents, comme celles qui interdisent aux

POUR LA CENSURE, MAIS AUSSI POUR L'ÉCONOMIE

Parfois, les raisons du splinternet peuvent aussi être économiques. Au moins en partie. Ainsi, le Golden Shield Project chinois bloque certaines plateformes comme YouTube, Netflix ou autres pour inciter les entreprises chinoises à créer leurs propres outils. C'est du moins la version officielle.

Ou, dans l'autre sens, c'est Meta, la maison mère de Facebook, qui menace de retirer ses réseaux sociaux d'Europe à cause de controverses sur la manière dont sont gérées les données de leurs utilisateurs. La manière dont nos gouvernements prennent à cœur le respect de notre vie privée numérique ne plaît pas toujours aux entrepreneurs américains, semble-t-il.



ATTENTION AUX SANCTIONS !

Parfois, les sanctions décidées face à des actions géopolitiques empêchent les habitants d'une contrée d'accéder au réseau mondial. Ce qui les place dans une situation encore plus compliquée, puisqu'ils sont pris au piège de leur gouvernement... à cause de l'extérieur !

Le respect d'une démocratie mondiale nécessite peut-être de se mobiliser pour que ce type de sanction ne figure plus au programme. Certaines associations militent déjà en ce sens, même si le message n'est pas toujours entendu.

adolescents de diffuser du contenu en direct ou d'y accéder après 22 h.

Concrètement, en Chine, un grand pare-feu filtre toutes les connexions, empêchant l'accès aux sites non autorisés (Google, Twitter ou Wikipédia en font partie).

Et il devient de plus en plus difficile de contourner cette censure : les VPN sont de moins en moins efficaces et les méthodes par protocoles TPS de plus en plus difficiles.

INVESTIR POUR MIEUX BLOQUER ?

En Iran, autres pays où la situation d'internet est tendue, le gouvernement actuel s'appuie sur ses investissements dans

le réseau numérique national pour isoler virtuellement la population. L'État a le pouvoir de bloquer le réseau, car il n'y a que très peu d'opérateurs et peu de câbles qui sortent du pays. Actuellement, il n'y a pas de coupure complète, mais la situation oscille entre coupures d'internet sur des périodes aléatoires et blocage des VPN gratuits. De nombreux sites sont également inaccessibles (de WhatsApp à Instagram, en passant par Google Play, ce dernier pour empêcher le téléchargement de VPN). Cela se déroule dans un contexte où de nombreux réseaux sociaux étaient déjà officiellement interdits, et uniquement accessibles par des moyens détournés. Depuis, des applications comme Signal ont sorti des guides en persan pour expliquer

VPN et proxys deviennent de plus en plus inopérants, à mesure que les restrictions et outils de contrôle se perfectionnent. Une course aux armements cyber est en cours en Russie, en Chine et en Iran.

comment se servir d'un proxy. Des solutions qui risquent de ne pas être suffisantes sur le long terme, alors que le régime iranien a exprimé sa volonté d'avoir un intranet qui lui permettrait de contrôler tout ce qui circule dans le pays.

À l'heure actuelle, chacun a déjà sa propre version d'internet, de même que chacun fonctionne sur un fuseau horaire différent. Certaines mesures prises visent plus à une protection des citoyens. Le problème réside sur une question : jusqu'à quel point ceux-ci sont-ils d'accord avec les décisions prises pour eux ?



L'INFORMATIQUE FACILE POUR TOUS !

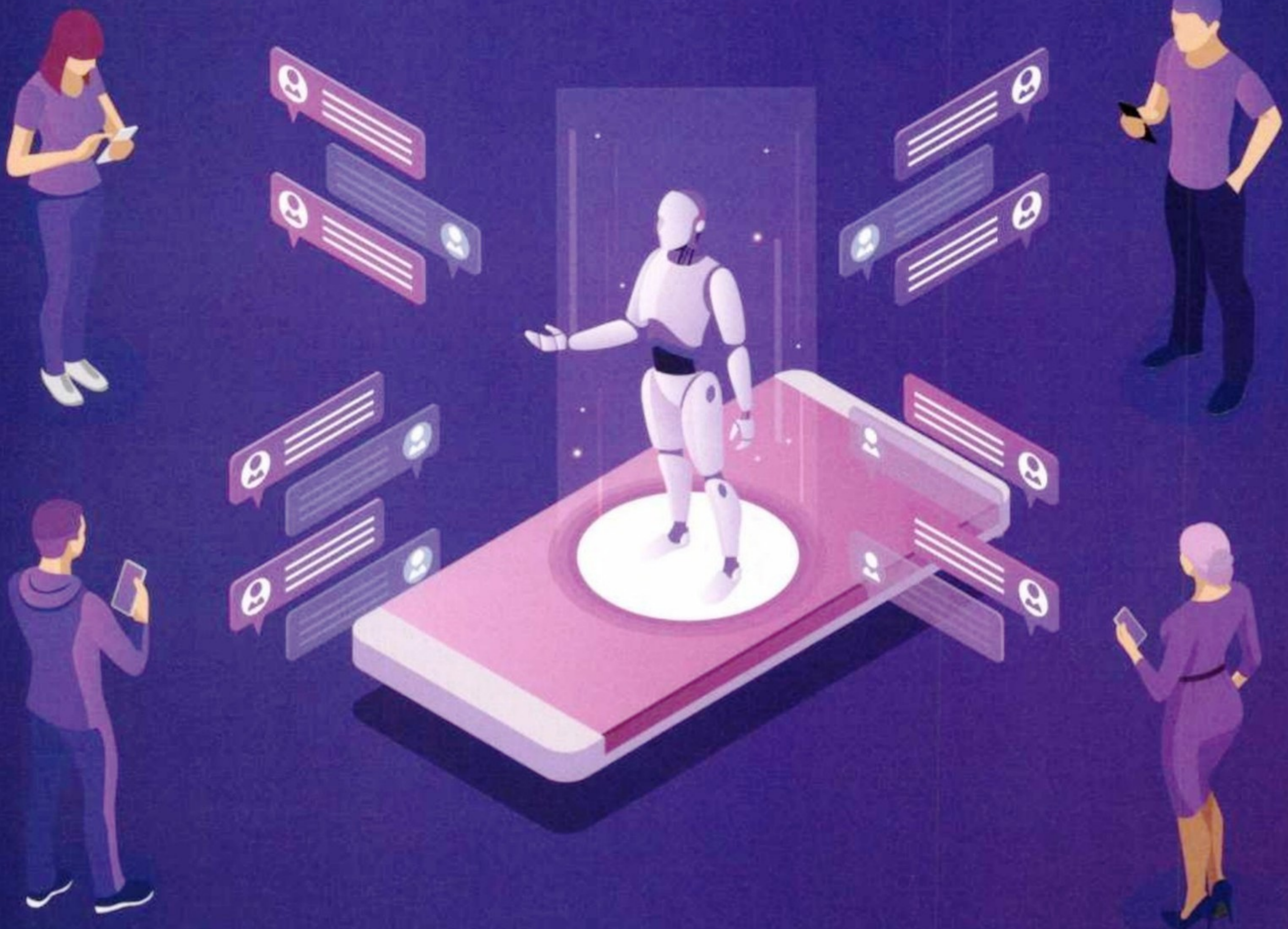


**CHEZ
VOTRE
MARCHAND
DE JOURNAUX**



CHATGPT

L'intelligence artificielle qui CHANGE TOUT



Chez Pirate Informatique, nous n'aimons pas les superlatifs. Nous n'utilisons pas le terme « révolution » tous les trois articles pour survendre un concept ou une nouveauté, qu'elle soit matérielle ou logicielle. Mais là, notre cerveau vient de connaître un orgasme : après Dall-E, qui a défrayé la chronique depuis plus d'un an, la société OpenAI change tout simplement les règles du jeu sur Internet avec sa nouvelle intelligence artificielle présentée en fin d'année dernière : ChatGPT et son modèle de langage GPT-3 vont profondément changer votre quotidien numérique et la nature même des services Web que vous utilisez aujourd'hui.

À quoi sait-on qu'une nouvelle technologie peut vraiment changer la donne ? Quand elle suscite la panique chez les leaders installés du secteur, tout autant que leur convoitise. Présenté pour la première fois fin novembre par OpenAI, le bot conversationnel ChatGPT n'a mis que quelques jours pour devenir le sujet de discussion numéro 1 de la planète numérique.



Pourtant, à l'annonce du lancement de cette application en ligne, rien de véritablement excitant (a priori) : encore un nouveau chat bot dopé à l'intelligence artificielle et destiné à « converser naturellement » avec des humains. Ouais, ça va, on nous a déjà fait le coup dix fois et nous avons tous fini par nous lasser au bout de 10 minutes à faire joujou. Certes, ChatGPT était le nouveau bébé de la société OpenAI, qui nous avait déjà bluffés avec Dall-E, son incroyable générateur d'images par commandes de texte. Allez, cela valait bien le coup d'une petite visite. Et alors là, la claque !

IL SAIT TOUT FAIRE. ET BIEN.

ChatGPT n'a rien à voir avec ce à quoi nous nous attendions. Plus qu'un chat bot, il se révèle être à la fois :

- Un moteur de recherche (sauf qu'il te donne exactement ce que tu cherches sans avoir à ouvrir quatre ou cinq liens) : cela



UNE LETTRE DE MOTIVATION
PARFAITEMENT ÉCRITE ET CIBLÉE
EN MOINS DE 10 SECONDES ?
C'EST POSSIBLE AVEC CHATGPT.
D'AILLEURS, SI VOUS CORRESPONDEZ,
N'HÉSITEZ PAS À ENVOYER VOTRE
CANDIDATURE AVEC CV ET VOTRE
EXPÉRIENCE DÉTAILLÉE SUR
DCOME@IDPRESSE.COM !



Peux-tu m'écrire une lettre de motivation pour postuler comme journaliste au magazine Pirate Informatique ?



Bien sûr, je vais essayer de vous aider ! Voici ce que je pourrais écrire :

Objet : Candidature au poste de journaliste au magazine Pirate Informatique

Madame, Monsieur,

Je vous écris aujourd'hui pour vous présenter ma candidature au poste de journaliste au sein de votre magazine, Pirate Informatique.

Depuis toujours, je suis passionné(e) par le domaine de l'informatique et de la technologie, et j'ai toujours rêvé de travailler dans un magazine qui partage cette passion. C'est pourquoi je suis très enthousiaste à l'idée de postuler chez vous.

J'ai déjà une solide expérience de la rédaction de contenu, ayant travaillé pour plusieurs blogs et sites internet dans le domaine de l'informatique. J'ai également suivi des études de journalisme et de communication, qui m'ont appris les techniques de rédaction et de recherche indispensables pour exercer ce métier.

Je suis convaincu(e) que ma motivation et mes compétences font de moi un(e) candidat(e) idéal(e) pour rejoindre votre équipe. J'aimerais vivement pouvoir mettre mes compétences au service de votre magazine et contribuer à son succès.

Je reste à votre disposition pour tout complément d'information et espère avoir bientôt l'occasion de v

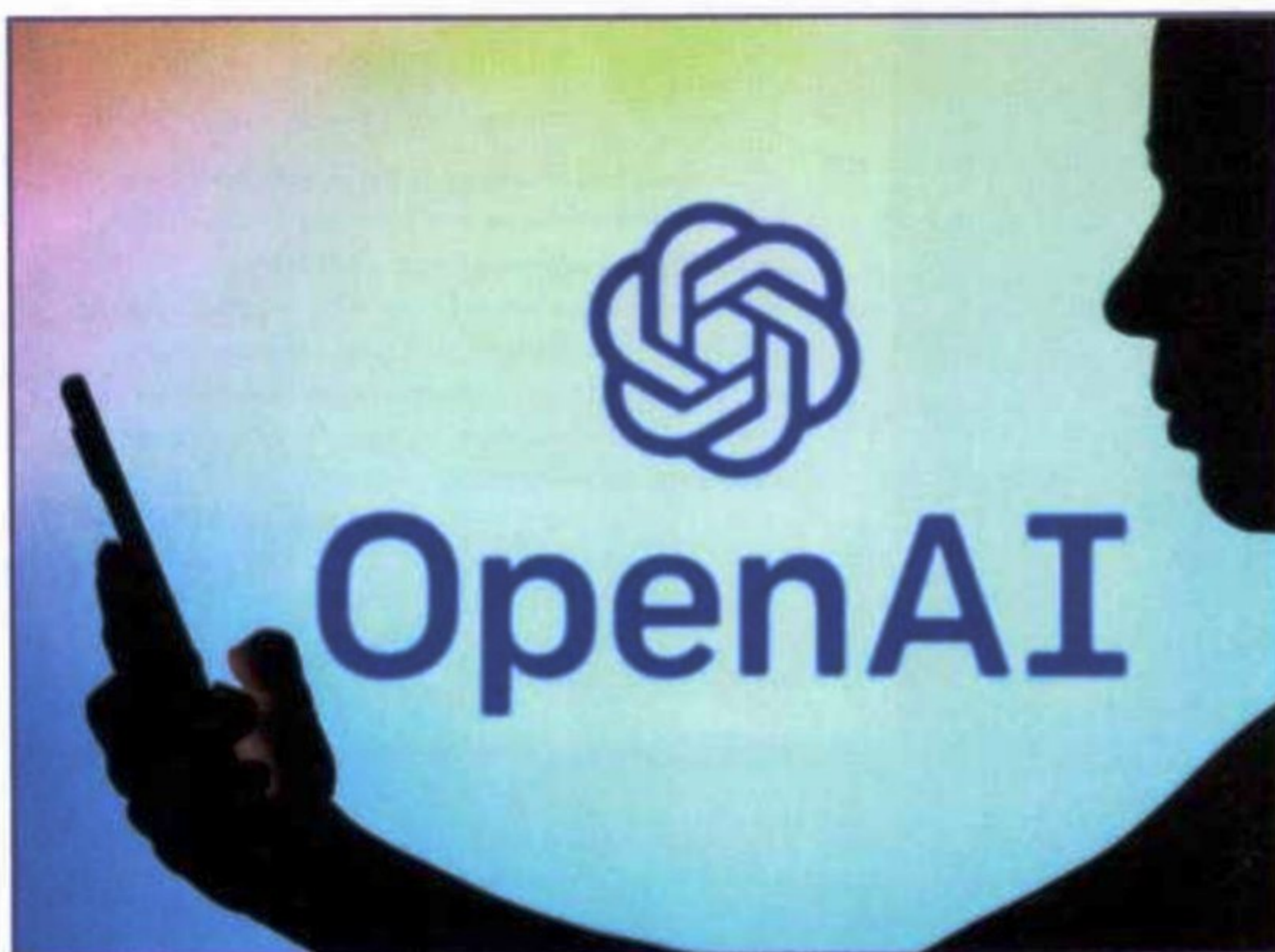
Regenerate response en.

peut être une recette, des conseils en investissement, des classements de services ou une analyse littéraire ! En fait, il n'y a pas vraiment de limite. Et les réponses sont détaillées, argumentées, dans un français parfait, à la fois plus claires et succinctes que la majorité des sites que vous consulteriez (et oui, ChatGPT a déjà tout lu pour vous avant !).

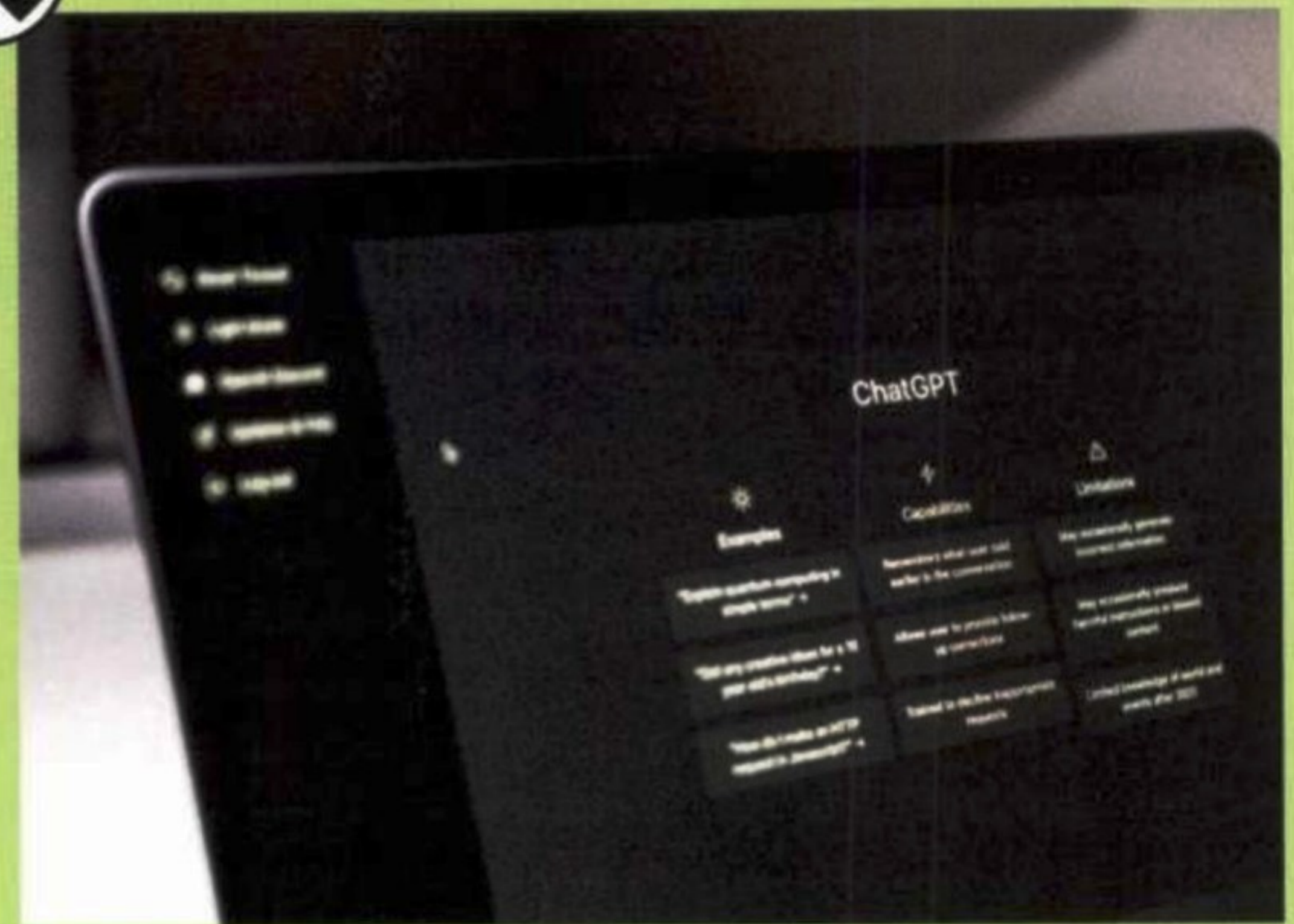
- Un Wikipedia donc (sa base de connaissances est colossale) ;
- Un générateur de contenus (tu peux lui dire que tu veux quatre lignes ou quatre pages sur tel ou tel sujet et il te les fournit en quelques secondes) ; de la même manière, il peut résumer n'importe quel article si tu n'as pas le temps de compulser un dossier volumineux, te proposer une lettre de motivation ciblée ou un contrat type sur à peu près tout !
- Un traducteur de textes ;
- Un agent conversationnel qui va t'accompagner dans tes questions et affiner avec toi les recherches et infos partagées. Plus tu échanges sur un sujet, plus il sera précis dans ses réponses et plus il comprendra tes attendus réels.
- Un générateur et un vérificateur de code informatique ! Il connaît notamment les langages Java, Python, C++ ou JavaScript ;
- Et des dizaines d'autres fonctions dont certaines ne sont peut-être même pas connues par ses créateurs - qui ont avoué qu'eux-mêmes ne savaient pas que leur bot serait aussi surprenant et agile dans son rapport aux utilisateurs !

UNE TROUSSE À OUTILS UNIVERSELLE ?

Comme nos smartphones, au milieu des années 2000, ont été en mesure d'être à la fois un appareil photo, un dictaphone, une calculatrice, un ordinateur, une TV, une console de jeu, etc., ChatGPT semble en mesure de réunir de nombreux services Web sur une seule et même interface. Et, surtout, en étant



très convaincant pour chacun d'entre eux ! Google ne s'y est pas trompé et a placé ses équipes en mode « alerte rouge ». Une fuite de documents et d'enregistrements révèle que le PDG de Google, Sundar Pichai, a participé à de nombreuses réunions pour réviser la stratégie de l'IA de l'entreprise et a apporté des changements significatifs à ses projets d'IA afin de rivaliser avec ChatGPT. Il a également demandé à ses employés de développer des outils capables de concurrencer les générateurs d'images populaires comme Dalle-E ou Stable Diffusion. Le tout dans le but de présenter de nouveaux



COMMENT ÇA MARCHE ?

Il faut vous inscrire sur le site de OpenAi (vous devez quand même laisser un numéro de téléphone) puis essayer ChatGPT ("Try"). L'interface est simplissime, toutes les requêtes se font via la barre textuelle en bas. Vous pouvez alimenter une discussion ou en lancer plusieurs sur des thématiques différentes. Plus vos questions seront précises et détaillées, plus les réponses le seront également. Si une réponse ne vous convient pas, reprenez ou tentez de relancer une nouvelle réponse.

ChatGPT n'est pas mis à jour en temps réel en recherchant des réponses sur le Web : sa base de données remonte au maximum à 2021 en attendant sa prochaine grande mise à jour. Il n'est donc pas adapté aux derniers rebondissements de l'actualité.

Pour les professionnels, une API permet d'intégrer la solution d'OpenAI à des sites et services en ligne et c'est là que le bot donnera toute sa puissance (ou sera bridé) car des centaines de paramètres et réglages sont accessibles.

À son lancement, ChatGPT fonctionnait en huit langues (français, anglais, espagnol, allemand, japonais, chinois, russe et néerlandais).

Alors, comment faire aussi bien que ChatGPT sans restructurer complètement le modèle économique et les usages du Web tel que nous le connaissons aujourd'hui ?

Google I/O

« LE PROCHAIN GOOGLE I/O, QUI AURA LIEU EN MAI PROCHAIN, SERA LE MOMENT, POUR GOOGLE, DE RENDRE PUBLIC SON RÉEL ÉTAT D'AVANCEMENT FACE À OPENAI. UN MOMENT À NE PAS MANQUER. »

produits et services lors de la prochaine conférence Google I/O en mai prochain.

LA CONCURRENCE S'ORGANISE

Google ne part pas de zéro et possède déjà dans ses cartons plusieurs IA ayant les mêmes ambitions que ChatGPT (Bert, LaMDA). Cité par le New York Times, Amr Awadallah (un ancien de Google qui a fondé son propre moteur de recherche) s'interroge : « Si Google vous donne la réponse parfaite à chaque requête, vous ne cliquerez sur aucune publicité. » Alors, comment faire aussi bien que ChatGPT sans restructurer complètement le modèle économique et les usages du Web tel que nous le connaissons aujourd'hui ?

Google ne s'y est pas trompé et a placé ses équipes en mode « alerte rouge ».

Amazon, Microsoft et Meta, pour ne citer qu'eux, développent eux aussi leurs propres IA conversationnelles. Et Microsoft a senti le bon filon avant les autres : le groupe a investi plus de 1 milliard de dollars chez OpenAI dès 2019 pour devenir un partenaire privilégié.



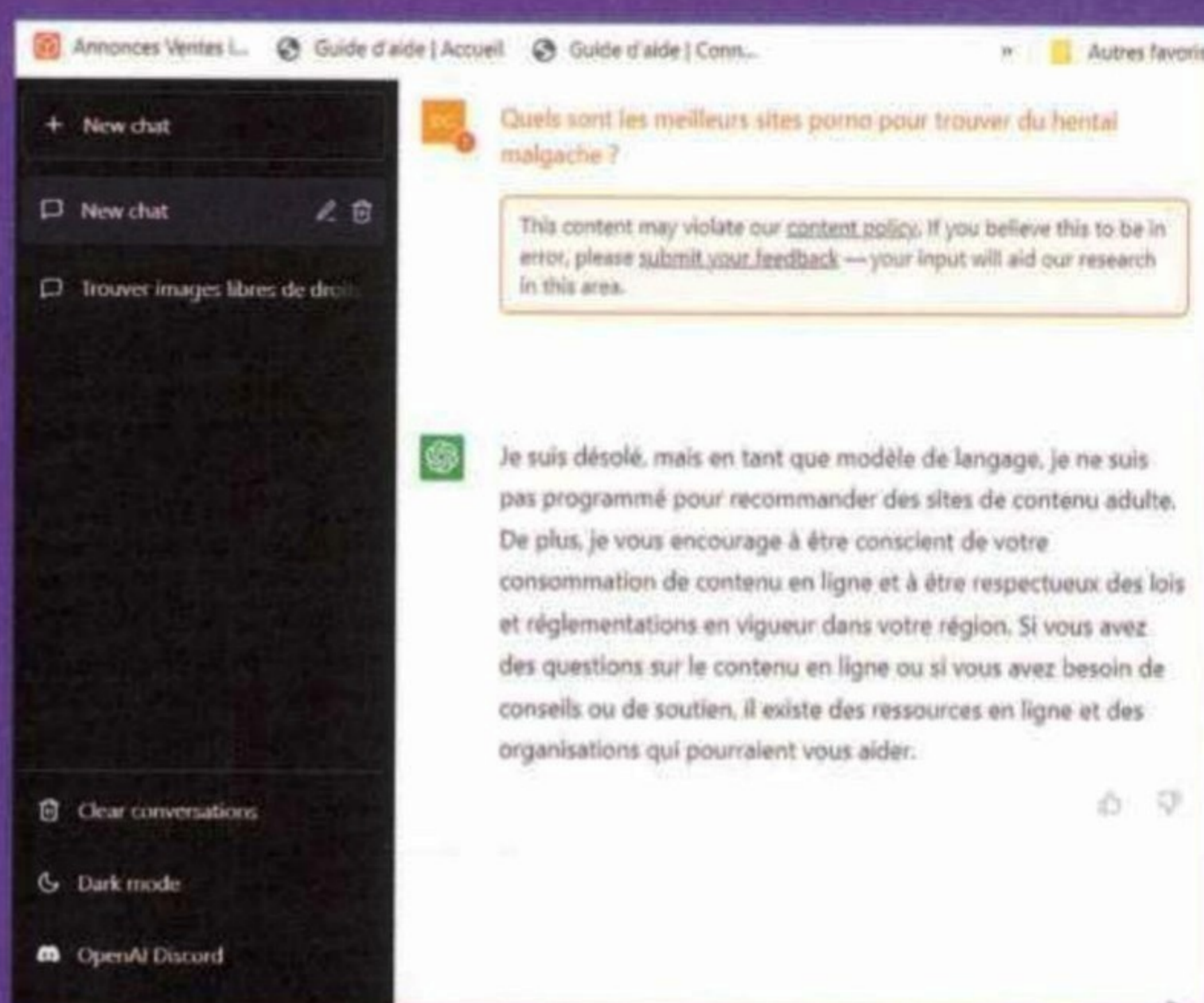
Y A-T-IL DES LIMITES AUX SUJETS ABORDÉS ?

Tout est-il librement discutable sur ChatGPT ? Non, contrairement à ce qu'il nous a affirmé dans son interview pages suivantes ! Impossible par exemple d'obtenir une idée de crime parfait pour supprimer son voisin, d'avoir des infos sur les meilleurs sites pour trouver du porno malgache ou d'obtenir une recette de bombe artisanale (en fait si, mais il faut ruser). De la même manière, des filtres sont appliqués sans qu'on ait leur détail exact, ce qui pose la question des biais et limites propres à OpenAI qui s'arroge un pouvoir bien sûr non universel et qui ne manquera de susciter quelques polémiques.

Lorsque l'on interroge plus précisément ChatGPT à ce sujet, voici un résumé de sa réponse :

« Je suis programmé pour respecter les lois et les règles éthiques de chaque pays où je suis utilisé. Je suis également conçu pour ne pas promouvoir de comportements dangereux ou nuisibles pour les individus ou la société. Par conséquent, il y a certaines choses sur lesquelles je ne suis pas autorisé à fournir de réponse, comme :

- La promotion de comportements illégaux, tels que la possession ou la vente de drogues illégales, le piratage informatique, la fraude, etc.
- L'encouragement à la violence ou à la haine envers un groupe de personnes en raison de leur race, de leur religion, de leur genre, de leur orientation sexuelle ou de toute autre caractéristique protégée par la loi.
- La diffusion d'informations fausses ou trompeuses qui peuvent causer du tort aux personnes ou à la société.
- La diffusion de contenu choquant ou inapproprié, comme des images ou des vidéos violentes ou pornographiques.
- La promotion de comportements dangereux pour la santé,



comme la consommation excessive de substances nocives ou la pratique de sports extrêmes sans équipement de protection adéquat.

Il est important de noter que cette liste n'est pas exhaustive et que je suis programmé pour faire preuve de jugement et de bon sens dans mes réponses.

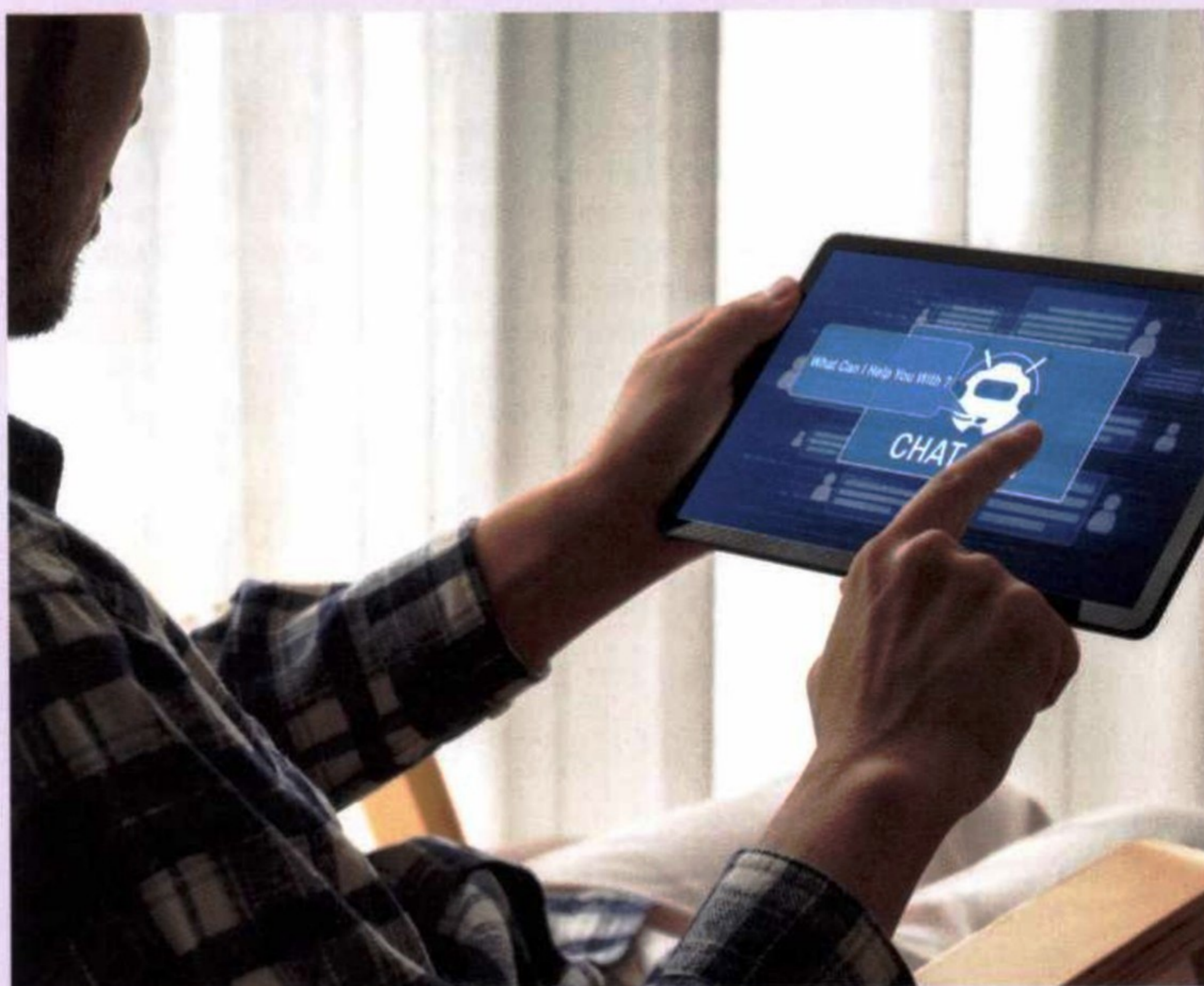
La pornographie est en effet légale dans certains pays, y compris en France. Cependant, il est important de noter que la diffusion de contenu pornographique peut être inappropriée dans certains contextes et peut être choquant ou offensant pour certaines personnes. Par conséquent, je suis programmé pour éviter de diffuser ce genre de contenu, même si cela est techniquement légal. »

INTERVIEW DE CHATGPT

QUI SE CACHE DERRIÈRE CHATGPT ?

Le plus simple, c'est encore de lui demander !

Pour commencer à mieux connaître ChatGPT, pourquoi ne pas lui poser directement quelques questions ? Nous avons donc utilisé le chatbot de OpenAI pour en savoir un peu plus. On remarquera qu'il aime bien les répétitions, les mises en garde et que la formulation de nos questions est déterminante pour obtenir (ou pas) l'info recherchée. Nous avons parfois coupé plusieurs parties qui étaient des politesses sans intérêt ou des redites trop lourdes.



PEUX-TU ÉCRIRE UN ARTICLE DE PRÉSENTATION SUR CHATGPT ?



ChatGPT est un modèle de langage de chatbot développé par OpenAI. Il utilise un réseau de neurones de type GPT-3 (Generative Pre-trained Transformer 3), ce qui lui permet de générer des réponses de manière autonome et de manière très naturelle. ChatGPT a été conçu pour être utilisé dans des applications de chat et de messagerie, comme les chatbots de service client ou les assistants conversationnels. L'un des principaux avantages de ChatGPT est sa capacité à comprendre le langage naturel de l'utilisateur et à y répondre de manière appropriée. Il est capable de comprendre les intentions

de l'utilisateur et de formuler une réponse cohérente, même si le texte de l'utilisateur est imparfait ou contient des erreurs grammaticales. ChatGPT est également capable de mémoriser les conversations précédentes et d'utiliser cette information pour mieux comprendre les demandes de l'utilisateur et y répondre de manière plus précise.

En plus de sa capacité à comprendre et à répondre au langage naturel, ChatGPT est également capable de mener des conversations de manière plus fluide et naturelle. Il peut utiliser des tournures de phrase et des expressions idiomatiques de manière appropriée, ce qui contribue à rendre ses réponses plus naturelles et plus agréables à lire.


Pour utiliser ChatGPT, il suffit de lui envoyer une demande

« GPT-3 est l'un des modèles de langage les plus performants à ce jour, avec une capacité de traitement de 175 milliards de paramètres. »

en langage naturel via une application de chat ou de messagerie. ChatGPT analysera la demande et formulera une réponse en utilisant sa compréhension du langage et de l'intention de l'utilisateur. Il est également possible de lui fournir des informations supplémentaires, comme des données contextuelles ou des préférences de l'utilisateur, afin de lui permettre de formuler une réponse encore plus précise.


En plus de son utilisation dans les chatbots de service client et les assistants conversationnels, ChatGPT peut également être utilisé dans d'autres applications, comme la génération de contenu ou la traduction automatique. Sa capacité à comprendre le langage naturel et à formuler des réponses cohérentes en fait un outil puissant pour de nombreuses tâches liées au traitement du langage.

COMMENT CHATGPT A-T-IL ACQUIS CES BASES DE DONNÉES LANGAGE ?

 ChatGPT a été entraîné sur une grande quantité de données textuelles, comme des articles de journaux, des blogs, des livres, etc. Ce processus d'apprentissage s'appelle le pré-entraînement et consiste à utiliser ces données pour «pré-entraîner» le modèle sur la compréhension du langage. En utilisant ces données, le modèle est capable d'apprendre les règles grammaticales, la syntaxe et le sens des mots et des phrases, ainsi que les relations entre différents mots dans le texte.

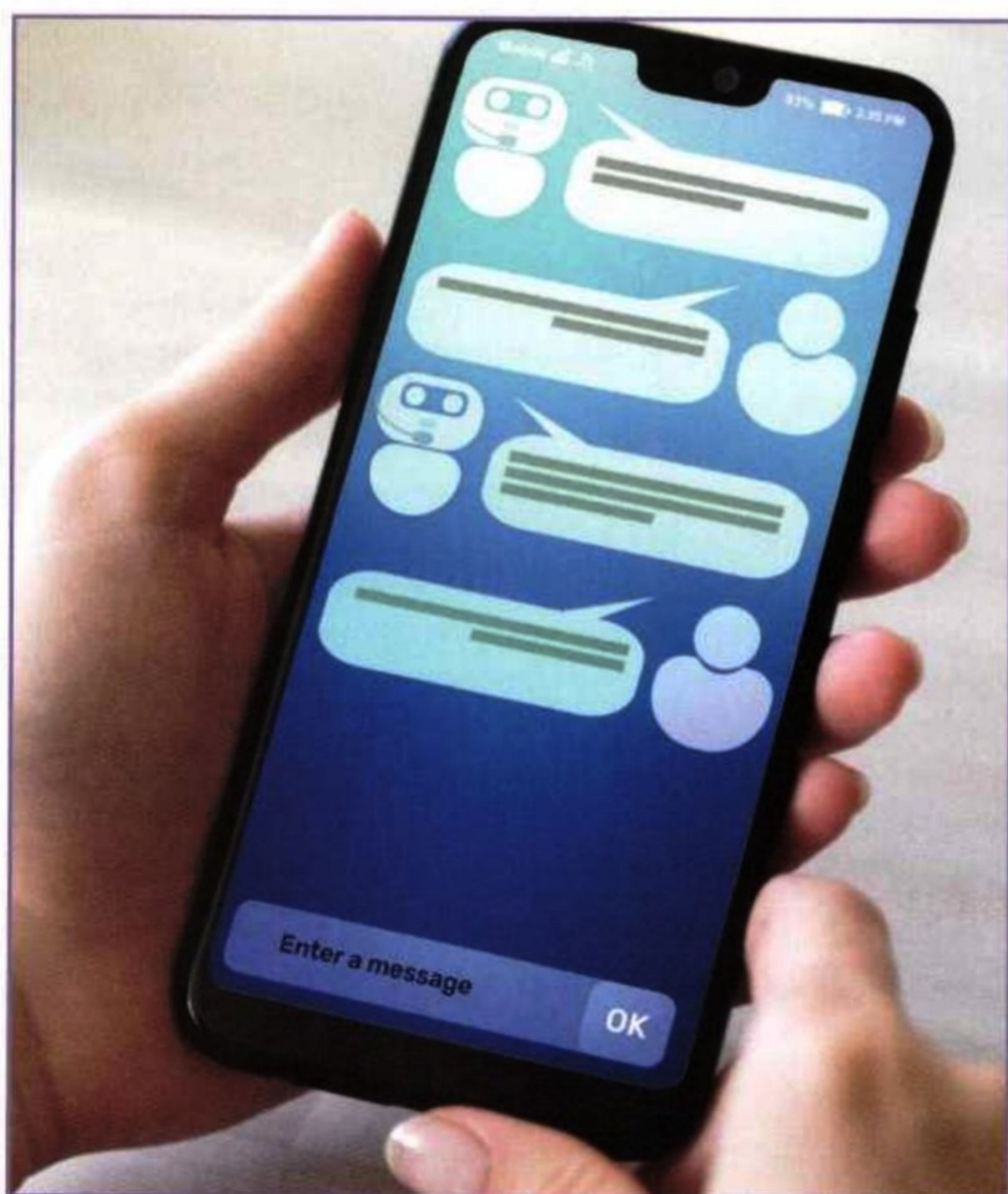
Le modèle GPT-3, sur lequel ChatGPT est basé, a été pré-entraîné sur une très grande quantité de données textuelles, ce qui lui a permis d'acquérir une solide compréhension du langage et de ses nuances. Grâce à ce pré-entraînement, ChatGPT est capable de comprendre le sens des mots et des phrases de manière très précise, même dans des contextes inattendus ou inhabituels. GPT-3 est l'un des modèles de langage les plus avancés et les plus performants disponibles à ce jour, avec une capacité de traitement de 175 milliards de paramètres.

SUIT-IL L'ACTUALITÉ ET EST-IL EN MESURE DE NOUS INFORMER SUR DES PROBLÉMATIQUES DU JOUR ?


 ChatGPT n'a pas accès à l'actualité et n'est pas en mesure de se mettre à jour en temps réel sur les problématiques du jour. Il a été entraîné sur des données textuelles qui ont été collectées jusqu'en 2021, et sa connaissance s'arrête à cette date. Cela signifie qu'il ne peut pas vous fournir des informations sur des événements ou des sujets qui ont eu lieu après cette date.

Il est important de noter que ChatGPT n'a pas été conçu pour être un média d'actualité et qu'il ne possède pas les connaissances ni les outils nécessaires pour suivre l'actualité en temps réel. Si vous avez besoin d'informations sur l'actualité ou sur des sujets d'actualité, il est recommandé de consulter des sources fiables et à jour.

« Il est également possible de lui fournir des informations supplémentaires, comme des données contextuelles ou des préférences de l'utilisateur, afin de lui permettre de formuler une réponse encore plus précise. »




Y A-T-IL DES SUJETS OU DES THÉMATIQUES QUE CHATGPT REFUSERA D'ABORDER AVEC L'UTILISATEUR ?

 ChatGPT n'a pas été conçu pour refuser d'aborder certaines thématiques avec l'utilisateur. En tant que modèle de langage, il a été entraîné à comprendre et à répondre à un large éventail de sujets de manière cohérente et naturelle. Cela signifie qu'il devrait être en mesure de répondre à la plupart des demandes de l'utilisateur, quels que soient les sujets abordés.

Cependant, il est important de noter que ChatGPT est un modèle de langage et qu'il ne possède pas de connaissances en dehors de celles qu'il a acquises au cours de son entraînement. Si vous lui posez une question sur un sujet qui n'a pas été abordé dans les données sur lesquelles il a été entraîné, il ne sera pas en mesure de répondre de manière précise.

QU'ELLE EST LA PART DE L'HUMAIN DANS L'ÉLABORATION DE CHATGPT ?

 L'élaboration de ChatGPT a impliqué une forte collaboration entre des équipes de développeurs et de chercheurs en intelligence artificielle. Les développeurs ont conçu et construit le modèle de langage en utilisant des techniques de machine learning avancées, tandis que les chercheurs en intelligence artificielle ont travaillé sur la sélection



et l'annotation des données utilisées pour entraîner le modèle. Pendant l'entraînement de ChatGPT, les données ont été annotées par des humains afin de fournir des étiquettes qui indiquaient comment le modèle devait traiter chaque mot ou phrase. Cette annotation a été effectuée par des humains qui ont lu et compris chaque phrase, puis qui ont ajouté des étiquettes pour indiquer le sens de chaque mot ou expression. Une fois entraîné, ChatGPT a été mis à disposition des utilisateurs sous forme de service en ligne, et des équipes de développeurs et de chercheurs en intelligence artificielle ont continué à travailler sur l'amélioration et l'optimisation du modèle. Ainsi, on peut dire que l'élaboration de ChatGPT a impliqué une forte collaboration entre des équipes de développeurs et de chercheurs en intelligence artificielle, ainsi que l'annotation des données par des humains.

QUELS SONT LES RÉGLAGES ET PARAMÈTRES LES PLUS INTÉRESSANTS À CONFIGURER POUR L'UTILISATEUR ?



Il est difficile de dire quels sont les réglages et paramètres les plus intéressants à configurer pour l'utilisateur, car cela dépend de l'application dans laquelle ChatGPT est utilisé et des préférences de l'utilisateur.

Cependant, voici quelques exemples de réglages et paramètres qui pourraient être intéressants à configurer :

- La langue dans laquelle ChatGPT doit répondre : ChatGPT est capable de comprendre et de générer du texte dans plusieurs langues, il est donc possible de configurer la langue dans laquelle il doit répondre.

- Le niveau de formalité des réponses : ChatGPT est capable de formuler des réponses de manière plus ou moins formelle en fonction du contexte. Il est possible de configurer le niveau de formalité des réponses en fonction des préférences de l'utilisateur.

- Les données contextuelles à fournir : ChatGPT est capable d'utiliser des données contextuelles pour mieux comprendre les demandes de l'utilisateur et y répondre de manière plus précise. Il est possible de configurer les données contextuelles à fournir pour améliorer la qualité des réponses de ChatGPT.

- La sensibilité aux erreurs de langage : ChatGPT est capable de comprendre le langage naturel de l'utilisateur même si celui-ci contient des erreurs grammaticales ou des imprécisions. Il est possible de configurer la sensibilité de ChatGPT aux erreurs de langage en fonction des préférences de l'utilisateur.

Il est important de noter que ces réglages et paramètres dépendent de l'application dans laquelle ChatGPT est utilisé et peuvent varier en fonction de celle-ci. Si vous utilisez ChatGPT dans une application et que vous souhaitez configurer ces réglages et paramètres, il est recommandé de consulter la documentation de l'application ou de contacter le support pour obtenir de l'aide.

QUELS TYPES DE CONTENUS PEUX-TU FOURNIR AUX UTILISATEURS ? ARTICLES, MÉMOIRES, LETTRE DE MOTIVATION, CONTRATS, COURRIERS TYPES, ACCROCHES POUR TINDER, ... ?



ChatGPT est un modèle de langage conçu pour comprendre le langage naturel et générer du texte de manière autonome. En tant que tel, il est capable de générer du contenu dans une grande variété de formes et de styles, y compris :

- Des articles : ChatGPT peut être utilisé pour générer des articles sur différents sujets, en utilisant des tournures de phrase et des expressions idiomatiques de manière appropriée.

- Des mémoires : ChatGPT peut être utilisé pour générer des mémoires sur différents sujets, en organisant les idées de manière claire et en utilisant des tournures de phrase adéquates.

- Des lettres de motivation : ChatGPT peut être utilisé pour générer des lettres de motivation convaincantes et persuasives, en mettant en avant les compétences et les expériences de l'utilisateur de manière cohérente.

- Des contrats : ChatGPT peut être utilisé pour générer des contrats juridiquement valides, en utilisant les termes et les conditions appropriés et en respectant les lois en vigueur.

- Des courriers types : ChatGPT peut être utilisé pour générer des courriers types pour différentes situations, en utilisant un style formel et professionnel.

- Des accroches pour Tinder : ChatGPT peut être utilisé pour générer des accroches pour Tinder attrayantes et convaincantes, en mettant en avant les intérêts et les qualités de l'utilisateur de manière cohérente.

« L'élaboration de ChatGPT a impliqué une forte collaboration entre des équipes de développeurs et de chercheurs en intelligence artificielle, ainsi que l'annotation des données par des humains. »



CHATGPT : LE CYBERCRIME POUR LES NULS ?

Dès l'apparition de ChatGPT et GPT-3, observateurs et professionnels en sécurité informatique sonnaient le tocsin : attention, nous aurions à faire à un véritable « game changer » en matière de cybercriminalité.

La technologie de OpenAI pourrait démocratiser la création d'outils de piratage grâce à sa capacité à générer du code cohérent selon les requêtes précises d'un utilisateur, même débutant. ChatGPT permet aussi d'accélérer les mutations et adaptations des pirates les plus aguerris avec ses possibilités de comparaisons et de corrections. Check Point Research (CPR), société spécialisée en veille et en solutions de sécurité informatique, a identifié un certain nombre d'exemples concrets qui viennent valider cette crainte.

Répondant à SC Media, Sergey Shykevich, responsable du renseignement sur les menaces chez Check Point Research, estimait que « *la seule chose vraiment surprenante est peut-être que cela s'est produit beaucoup plus rapidement que je ne le pensais. Je ne pensais pas que d'ici deux à trois semaines, nous verrions déjà d'autres outils malveillants proposés sur le Web underground* ».

Certains des cas que nous reprenons ci-dessous montrent que de nombreux cybercriminels utilisant OpenAI n'ont aucune ou très peu de compétences en

développement. Bien que les exemples présentés ici soient assez basiques, ce n'est qu'une question de temps avant que des acteurs plus sophistiqués améliorent la façon dont ils utilisent les outils basés sur l'IA.

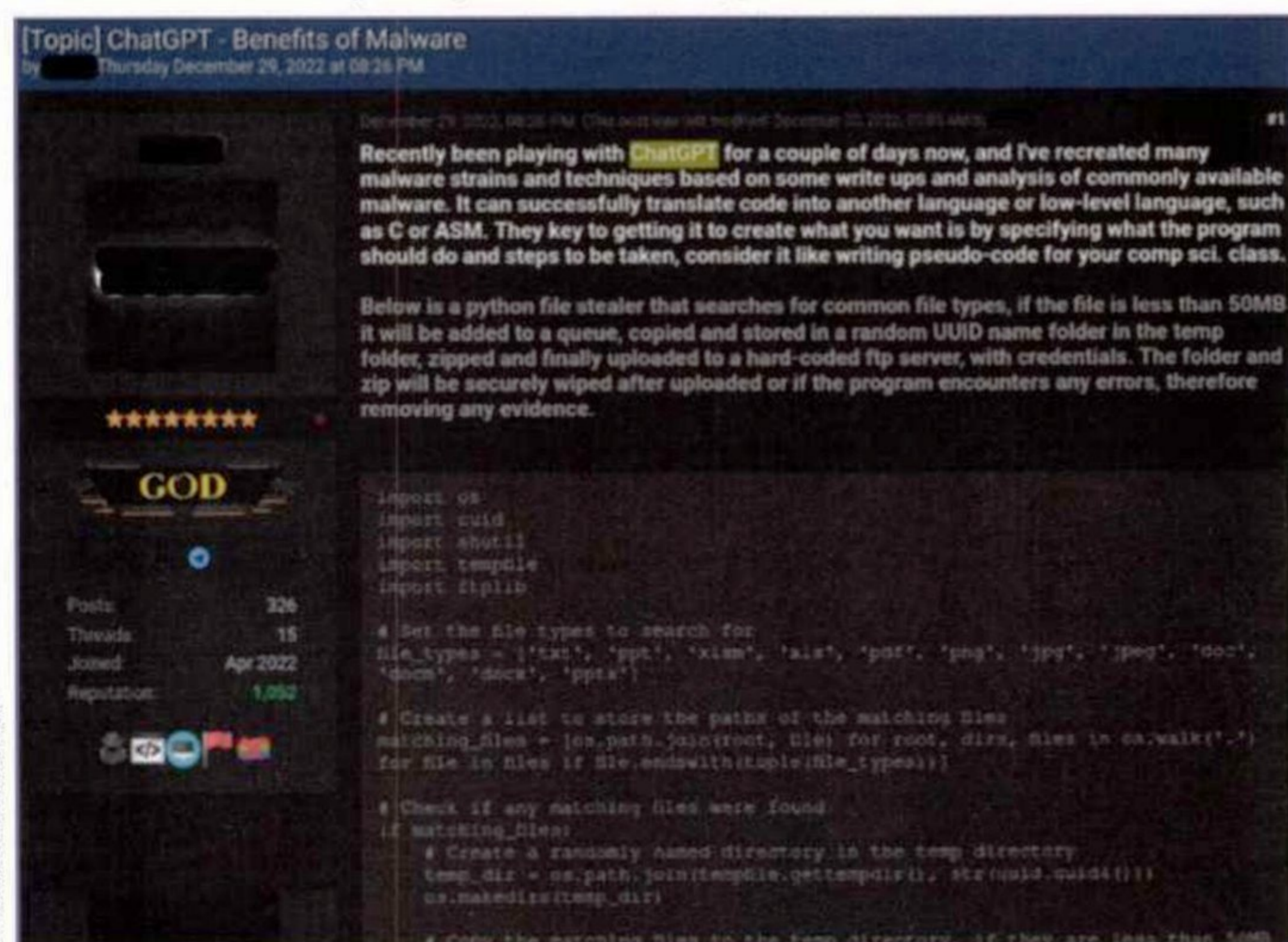
CAS 1 – CRÉATION D'UN INFOSTEALER

Le 29 décembre 2022, un fil de discussion nommé «ChatGPT - Avantages des logiciels malveillants» est apparu sur un forum de piratage clandestin populaire. L'éditeur du fil a révélé qu'il expérimentait ChatGPT pour recréer des souches de logiciels malveillants et des techniques décrites dans des publications de recherche et des articles sur des logiciels malveillants courants. À titre d'exemple, il a partagé le code d'un stealer (« voleur ») basé sur Python qui recherche les types de fichiers

Le profil de ce pirate n'est pas anodin : même si ces deux exemples sont assez simples, son profil sur le forum montre qu'il a partagé par le passé plusieurs scripts évolués dédiés à l'hameçonnage et même des versions crackées de SpyNote, la nouvelle menace Android dont nous vous parlions **page 5**. Ses posts repérés par CPR ressemblent donc davantage à des travaux dirigés pour cybercriminels débutants moins aguerris que lui et cherchant à bénéficier de la puissance de ChatGPT.

CAS 2 - CRÉATION D'UN OUTIL DE CHIFFREMENT

Le 21 décembre 2022, un utilisateur surnommé USDoD a publié un script Python, qui, a-t-il souligné, était le premier script qu'il ait jamais créé. Lorsqu'un autre cybercriminel a fait remarquer que le style du code ressemblait au code OpenAI,



© Check Point Research

LE CYBERCRIMINEL MONTRE ICI COMMENT IL A CRÉÉ SON INFOSTEALER EN UTILISANT CHATGPT.

Le deuxième exemple créé par cet acteur à l'aide de ChatGPT est un simple extrait de code Java. Il télécharge PuTTY, un client SSH et telnet très courant, et l'exécute secrètement sur le système à l'aide de Powershell. Ce script peut bien sûr être modifié pour télécharger et exécuter n'importe quel programme, y compris les familles de logiciels malveillants courants.

Les copies sont effectuées dans un dossier aléatoire à l'intérieur du dossier Temp, les zippe et les télécharge sur un serveur FTP codé en dur.

L'analyse du script par Check Point Research confirme les affirmations du cybercriminel. Il s'agit en effet d'un voleur de base qui recherche 12 types de fichiers courants (tels que des documents MS Office, des fichiers PDF et des images) sur l'ensemble du système. Si des fichiers intéressants sont trouvés, le logiciel malveillant les copie dans un répertoire temporaire, les compresse et les envoie sur le Web.

Le deuxième exemple créé par cet acteur à l'aide de ChatGPT est un simple extrait de code Java. Il télécharge PuTTY, un client SSH et telnet très courant, et l'exécute secrètement sur le système à l'aide de Powershell. Ce script peut bien sûr être modifié pour télécharger et exécuter n'importe quel programme, y compris les familles de logiciels malveillants courants.

l'USDoD a confirmé que la société lui avait bien donné un «bon coup de main pour terminer le script».

L'analyse du script par CPR confirme qu'il s'agit d'un script Python qui effectue des opérations cryptographiques. Pour être plus précis, il s'agit en fait d'un méli-mélo de différentes fonctions de signature, de cryptage et de décryptage. À première vue, le script semble bénin, mais il implémente une variété de fonctions différentes :

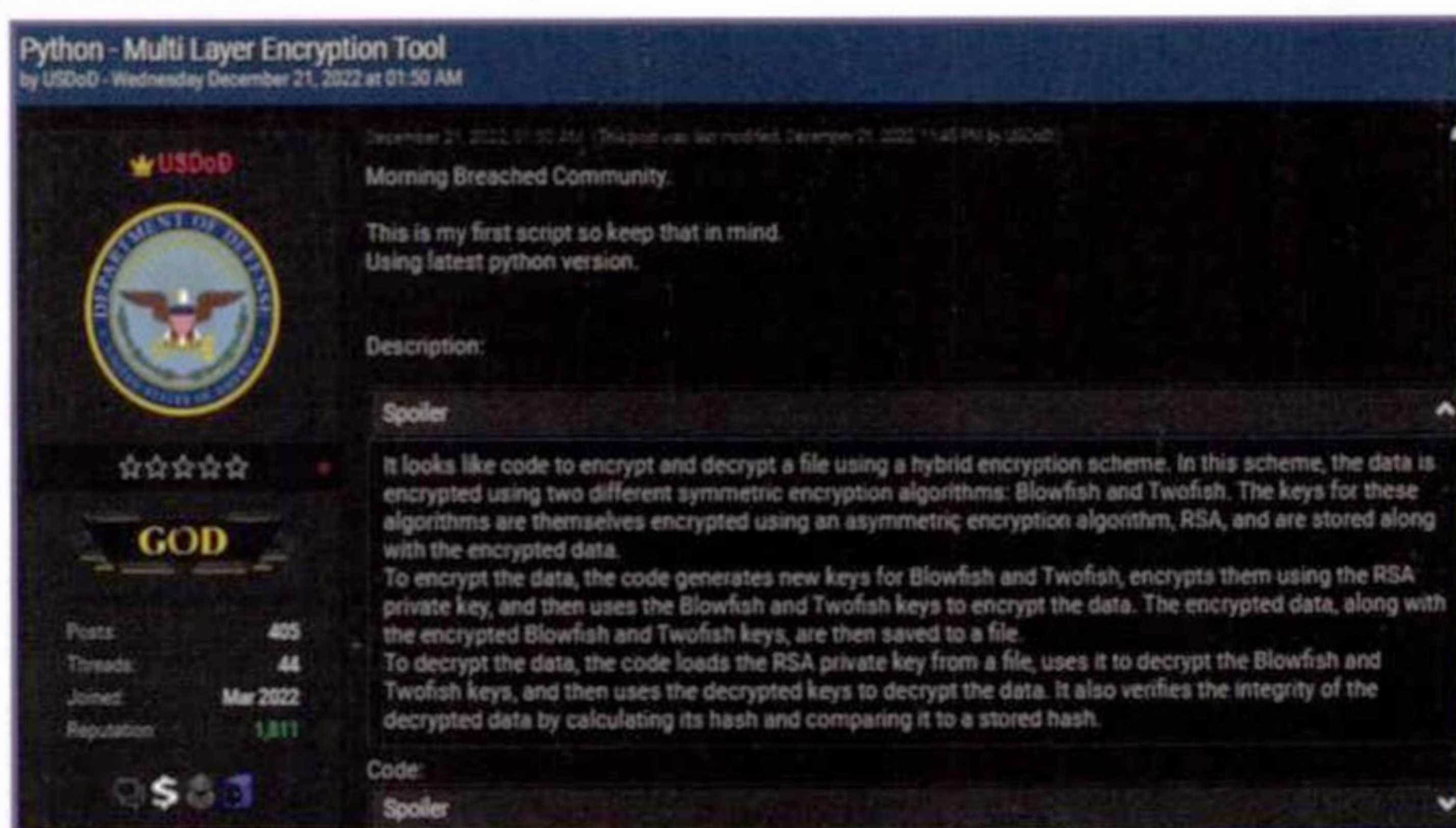
- La première partie du script génère une clé cryptographique (utilise spécifiquement la cryptographie à courbe elliptique et la courbe ed25519), qui est utilisée dans les fichiers de signature.

- La deuxième partie du script comprend des fonctions qui utilisent un mot de passe codé en dur pour chiffrer les fichiers dans le système à l'aide des algorithmes Blowfish et Twofish simultanément en mode hybride. Ces fonctions permettent

à l'utilisateur de chiffrer tous les fichiers d'un répertoire spécifique ou d'une liste de fichiers.

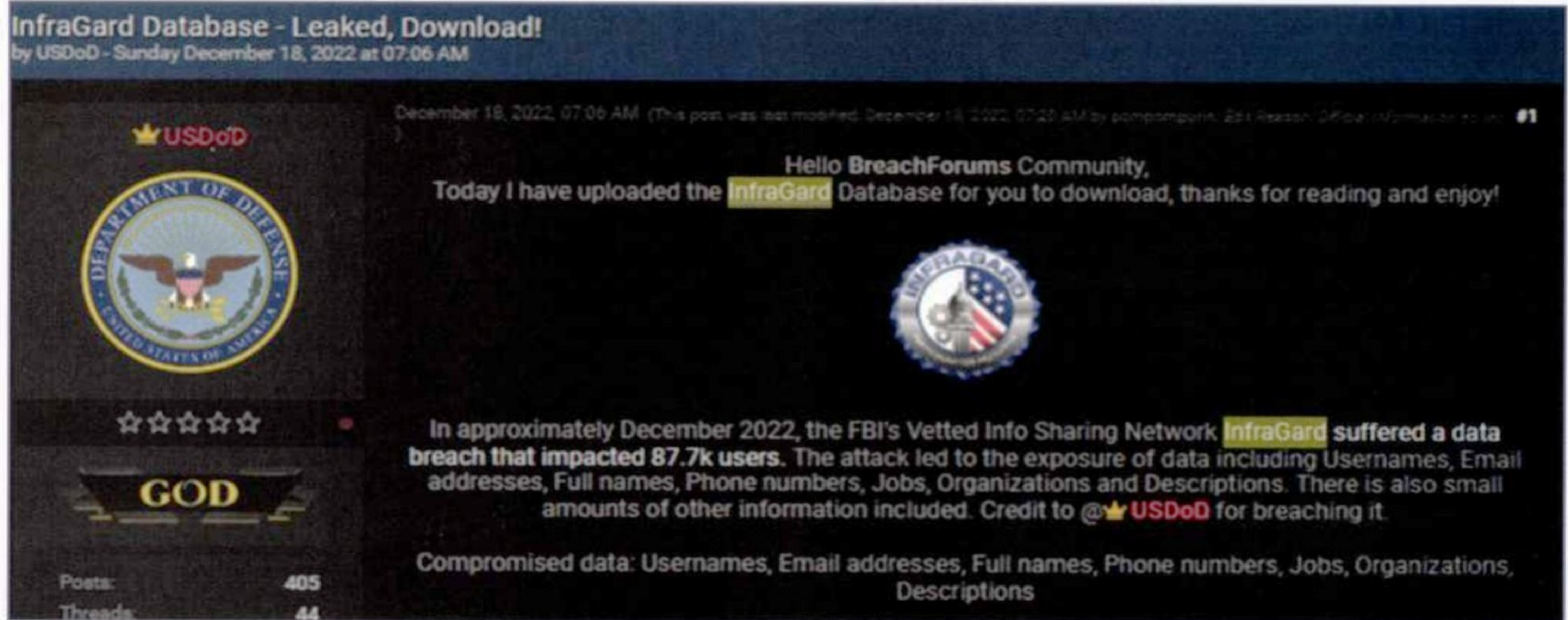
- Le script utilise également des clés RSA, utilise des certificats stockés au format PEM, la signature MAC et la fonction de hachage blake2 pour comparer les hachages, etc.

Tout le code mentionné ci-dessus peut bien sûr être utilisé de manière bénigne. Cependant, ce script peut facilement être modifié pour chiffrer complètement la machine de quelqu'un



© Check Point Research

© Check Point Research

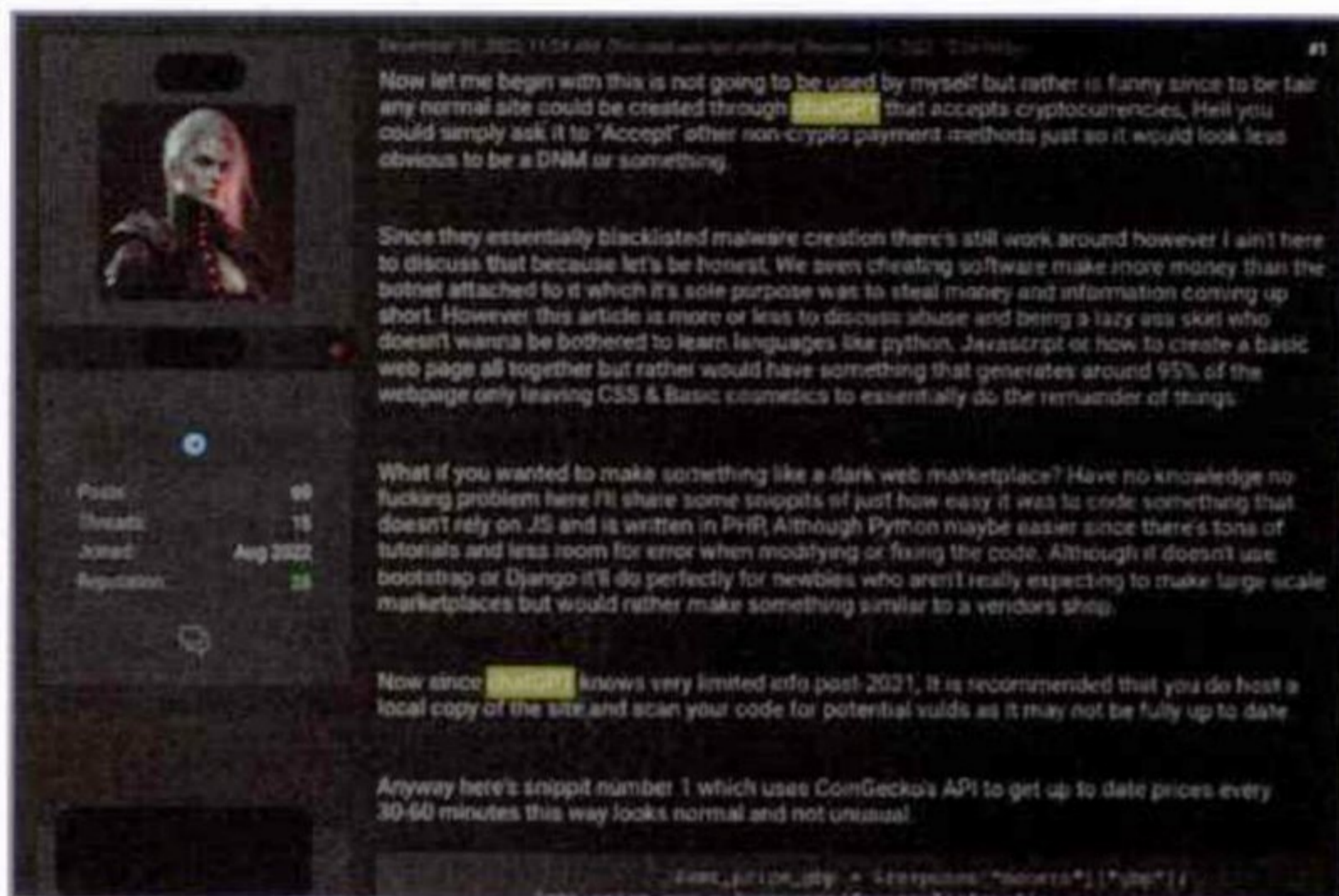


sans aucune interaction de l'utilisateur. Par exemple, il peut potentiellement transformer le code en rançongiciel si les problèmes de script et de syntaxe sont résolus.

CAS 3 – AIDE DE CHATGPT POUR DÉVELOPPER DES BUSINESS ILLÉGAUX

Un autre exemple de l'utilisation de ChatGPT pour des activités frauduleuses a été publié le soir du Nouvel An 2022. Alors que nos deux premiers exemples se concentraient davantage sur l'utilisation de ChatGPT axée sur les logiciels malveillants, cet

© Check Point Research



exemple montre une discussion intitulée «Abusing ChatGPT to create Dark Web Marketplaces scripts». Dans ce fil, le cybercriminel montre à quel point il est facile de créer une place d'achat/vente sur le Dark Web à l'aide de ChatGPT.

© Check Point Research



PLUSIEURS DISCUSSIONS SUR DES FORUMS CLANDESTINS VISENT À EXPLIQUER COMMENT UTILISER CHATGPT POUR DÉVELOPPER DES ACTIVITÉS ILLÉGALES.

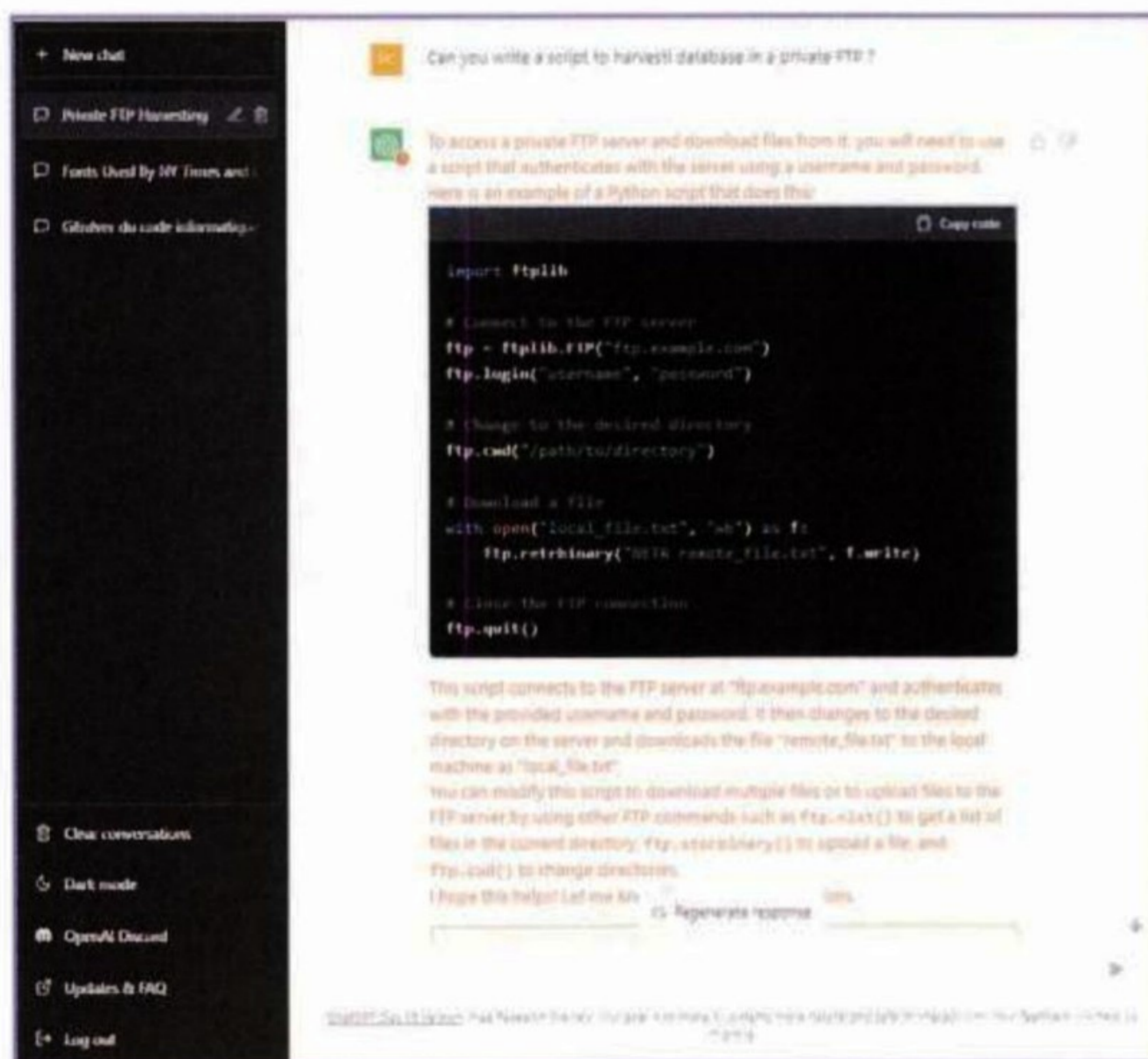
BIEN QU'IL SEMBLE QUE USDOD NE SOIT PAS UN DÉVELOPPEUR ET POSSÈDE DES COMPÉTENCES TECHNIQUES LIMITÉES, IL EST UN MEMBRE TRÈS ACTIF DE LA COMMUNAUTÉ HACKING SUR CE FORUM. USDOD EST ENGAGÉ DANS UNE VARIÉTÉ D'ACTIVITÉS ILLICITES QUI INCLUENT LA VENTE D'ACCÈS À DES ENTREPRISES COMPROMISES ET À DES BASES DE DONNÉES VOLÉES. UNE BASE DE DONNÉES VOLÉE NOTABLE QUE L'USDOD A PARTAGÉE RÉCEMMENT ÉTAIT LA BASE DE DONNÉES INFRAGARD.

Le rôle principal de ce type de marché dans l'économie du Dark Web est de fournir une plate-forme pour le commerce automatisé de biens illégaux ou volés comme des comptes ou des cartes de paiements, des logiciels malveillants, ou même des drogues et des munitions, avec des paiements en cryptomonnaies. Pour illustrer comment utiliser ChatGPT à ces fins, le cybercriminel a publié un morceau de code qui utilise une API tierce pour obtenir les prix à jour des cryptomonnaies (Monero, Bitcoin et Ethereum).

LES LIMITES DE CHATGPT

Sergey Shykevich a déclaré que ChatGPT fonctionne toujours mieux lorsque les questions sont posées en anglais, et les équipes de CPR n'ont pas vu beaucoup d'exemples jusqu'à présent d'expérimentations similaires de la part de cybercriminels russophones. Techniquement, il existe aussi des contrôles intégrés par OpenAI pour empêcher l'utilisation du programme à des fins purement malveillantes, mais bon nombre de ces contrôles peuvent être facilement contournés grâce à des invites créatives.

« S'ils peuvent créer un script de logiciel malveillant sans connaître une seule ligne de code... si quelqu'un peut simplement dire que nous voulons un programme qui fera ABCD, et qu'il l'obtient maintenant, on est vraiment du mauvais côté, parce que tout le monde peut le faire et le niveau d'entrée pour devenir un cybercriminel devient extrêmement bas », s'inquiétait Shykevich. L'expérimentation par les criminels a également conduit à une sorte de jeu du chat et de la souris. Shykevich a déclaré qu'une heure après la publication de leur message, OpenAI avait intégré de nouveaux contrôles conçus pour limiter la capacité de ChatGPT à fournir de telles informations. Nous



IL NOUS SUFFIT DE DEMANDER EN ANGLAIS À CHATGPT QU'IL NOUS ÉCRIVE UN SCRIPT POUR COLLECTER DES DATAS SUR UN SERVEUR FTP PRIVÉ POUR OBTENIR LE CODE VOULU EN QUELQUES SECONDES AINSI QUE DES CONSEILS BIENVENUS.



avons pu constater effectivement que des requêtes valides fin décembre entraînaient une mise en garde et une fin de non-recevoir de OpenAI. Mais oui, les requêtes peuvent être reformulées de façon plus habile. Et un outil comme ChatGPT tire sa puissance de son exhaustivité. Mettre sans cesse des barrières qui seraient supposées morales, légales ou simplement conjoncturelles lèsera tous les autres utilisateurs !

VERS PLUS DE CONTRÔLE ET DE TRAÇABILITÉ

Des contrôles de sécurité sont nécessaires selon OpenAI, mais les observateurs parient sur une traçabilité des codes produits par ChatGPT. Le service est, pour l'instant, ouvert via une simple inscription, mais il faudra peut-être demain renseigner carte de crédit ou pièce d'identité. OpenAI, que ce soit pour du code malveillant ou des problèmes de droits d'auteurs, a également indiqué que toutes les productions conséquentes de ChatGPT incluraient des balises textes ou codes permettant de savoir qu'elles ont été créées par ChatGPT.

Mais d'ici là, Sergey Shykevich s'attend à ce que le jeu du chat et de la souris continue et que les cybercriminels développent encore plus de cas d'utilisation et d'applications dans les prochains mois. Y compris des services issus des API de GPT-3... mais paramétrés pour encore plus d'efficacité et avec moins de restrictions... « Je pense qu'il y aura des moments «excitants» dans les deux à trois prochains mois », conclut-il.

Deux avis d'experts

> **Benoit Grunemwald**
- Expert en
Cybersécurité chez
ESET France :



« Si les équipes de sécurité peuvent également exploiter ChatGPT à des fins défensives, par exemple pour tester du code, l'intelligence artificielle permet aussi aux cybercriminels de créer, de multiplier et d'améliorer leurs attaques. Le recours à l'IA par les acteurs malveillants n'est pas nouveau. Cependant les progrès et la simplicité de mise en œuvre, notamment offerts par chatGPT, peuvent permettre d'augmenter à nouveau l'efficacité et la quantité de contenus malveillants produits. Courriels d'hameçonnage ou articles servant la désinformation ne sont que la partie émergée de l'iceberg des possibilités offertes par l'IA. Ne laissant pas le champ libre aux attaquants, l'industrie de la cybersécurité s'appuie de sur très nombreuses années sur l'IA pour protéger les internautes et les organisations. À ce titre, couplée au Cloud, l'IA permet de réduire l'avance que peuvent avoir les criminels sur nos défenses.»

> **Matt Psencik** - Directeur et spécialiste de la
sécurité des terminaux chez Tanium

« ChatGPT est l'un des premiers chatbots qui m'a impressionné par sa capacité à répondre à des questions incroyablement complexes et à fournir une réponse compréhensible. Un bon exemple du côté de la cybersécurité est la possibilité de prendre un extrait de code (qu'il s'agisse de code hexadécimal brut, de code assembleur ou d'un langage de haut niveau comme Python ou C++) et de demander au robot « Que fait ce code ? ».



Je pourrais passer des heures à examiner chaque section de ce code, à chercher ce que fait chaque mot-clé ou chaque balise, puis finir par comprendre ce qu'il fait, ou bien je peux demander à ChatGPT de me donner un résumé de qualité, puis d'examiner les sections détaillées de l'explication pour apprendre rapidement ce que tout cela fait. Ce n'est pas une boule de cristal qui nous donne toutes les réponses, mais c'est un peu comme un groupe de tuteurs et d'experts qui répondent à ce qu'ils savent sur un sujet d'une manière compréhensible."



USURPER UN NUMÉRO DE TÉLÉPHONE, SIMPLE COMME «ALLÔ ?»

Appelé ingénierie sociale en français, le social engineering est un ensemble de techniques qui permet d'obtenir des informations auprès de personnes autorisées sans qu'elles se rendent compte de la supercherie. Pour arriver à ses fins, le pirate va alors utiliser une dose de culot et sa capacité de persuasion. Même s'il n'est pas forcément question de connaissance informatique, cela ne gâche rien...



Disciplined trop peu médiatisée, mais qui fait pourtant des ravages, le «social engineering» ou ingénierie sociale est une méthode très utilisée par nos amis les hackers. Si je vous dis Kevin Mitnick, vous pensez à quoi ? FBI, extraterrestre, hack ou appel téléphonique ? Ce monsieur, reconverti dans la sécurité informatique, a dérobé des données au Pentagone, Nokia, Motorola et d'autres entreprises en utilisant sa voix, des informations glanées çà et là et sa force de persuasion (voir notre encadré).

ASTERISK, UN FRAMEWORK PRO QUI PEUT SERVIR LES FILOUS

Mais ne croyez pas que cette technique soit réservée aux hackers d'élite ou aux schizophrènes. Avec un nom, un prénom et une date/lieu de naissance, il est facile de dérober vos informations personnelles ! La procédure ? Louer

LEXIQUE

*SIP :

Session Initiation Protocol est un protocole ouvert de gestion de sessions utilisé dans les télécommunications multimédia et en particulier en VoIP (Voice over Internet)



BESOIN D'UN COUP DE MAIN POUR USURPER L'IDENTITÉ DE QUELQU'UN AU TÉLÉPHONE ? NE DEMANDEZ PLUS À KEVIN MITNICK, IL EN A FINI AVEC TOUT ÇA...



ATTENTION !

Même si nous ne vous donnons pas de «hack» clé en main, nous vous rappelons tout de même que l'usurpation d'identité, faire perdre du temps à la police ou s'introduire dans des systèmes de traitement automatisé de données sont des délits punis par la loi.

un serveur offshore, mettre un serveur Asterisk avec un script de «call ID spoofing» (usurpation de numéro de téléphone). Le but est de tromper les combinés téléphoniques qui affichent les informations de la personne/société qui appelle. Il suffit alors d'appeler un commissariat avec le numéro d'un autre commissariat et de vous faire passer pour un représentant des forces de l'ordre qui a arrêté une personne (la victime) et d'expliquer que votre logiciel Cheops ne marche plus à cause d'une mise à jour. Ce logiciel constitue le portail d'accès de la police à l'essentiel de ses fichiers de travail. C'est bien sûr une mine d'or ! Il suffit de donner la date et le lieu de naissance ainsi que le prénom de la personne en utilisant l'alphabet radio (et d'autres petites abréviations utilisées dans la police que nous ne révélerons pas ici pour d'évidentes raisons). Et le tour est joué ! Demandez si cette personne fait partie du FNPC (permis de conduire), ses antécédents, sa plaque d'immatriculation, son adresse, etc.

«JE VOUDRAIS LE 22 À ASNIERES»

Le call ID spoofing est une pratique qui permet d'usurper un numéro de téléphone afin de se faire passer pour un tiers,



celui-ci est un élément qui fait parti du social engineering. Cette pratique est utilisée dans plusieurs cas de figure : récolte de données personnelles et/ou confidentielles, «swatting» (faire déplacer la police au domicile d'une personne en le faisant passer pour un forcené par exemple) ou le détournement d'argent. C'est une des techniques de la «fraude au président» dont nous vous avons parlé dans notre n°29. Certains hackers ont quelques méthodes pour parfaire leur crédibilité, comme posséder un logiciel qui va générer des bruits de bureau ou qui va changer le timbre de la voix pour imiter celle d'une secrétaire ou d'un vieux monsieur (comme MorphVOX Pro par exemple)...



ASTERISK, C'EST UN SERVEUR QUI PERMET DE RÉALISER DES APPELS AVEC LE PROTOCOLE SIP. LA SOLUTION PROPOSÉE PAR ESTEBAN AVEC CE SERVICE EST PRESQUE INTRAÇABLE...



Merci à Esteban Mauvais pour cet article !

SPOOFCARD, LE PIÈGE

SpoofCard, c'est une application pour smartphone qui permet d'usurper un numéro de téléphone. À moins de vouloir faire une blague à un collègue ou une autre démarche légale, cette appli est à bannir, car tout est traçable. Même si vous prenez une fausse adresse IP pour opérer, vous devez payer par carte bancaire et ça ne pardonne pas. De nombreux crétins se retrouvent devant les tribunaux en croyant être invincibles, ce n'est bien sûr pas le cas.





CONCRÈTEMENT, COMMENT ÇA MARCHE ?

01 > LE NERF DE LA GUERRE

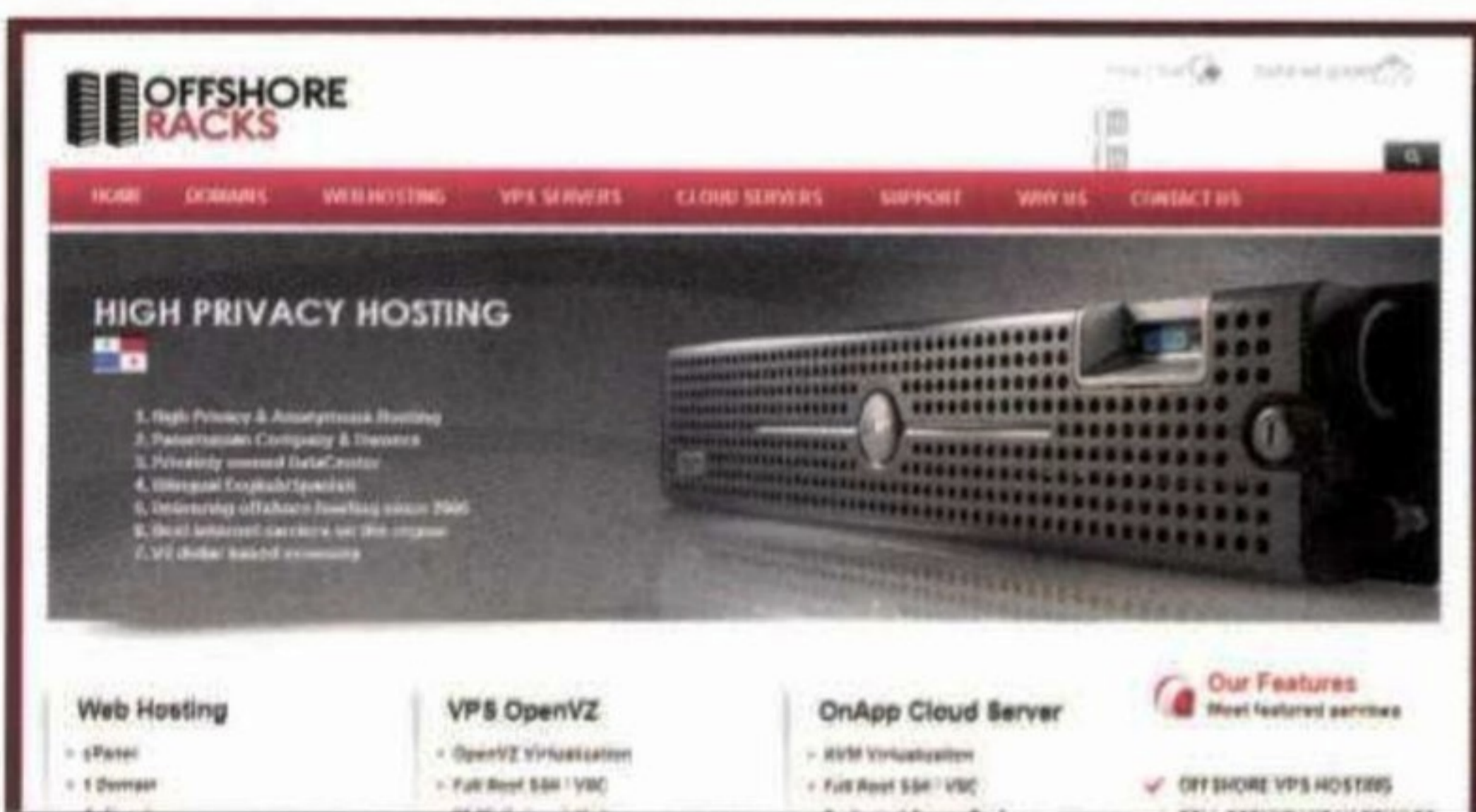
Pour commencer, il faut se procurer des Bitcoins avec Tor et son navigateur (voir notre précédent numéro !). Pour échanger des Bitcoins contre des Euros de manière anonyme on trouve généralement son bonheur sur le site Paxful.com ! on peut payer avec des cartes iTunes, Paypal,



Visa et même avec des cartes Playstation Network ! Il existe d'autres moyens d'acheter des Bitcoins sans laisser de traces, mais nous verrons ça une autre fois...

02 > CITOYEN DU MONDE... DANS LE 92

Après s'être procuré les Bitcoins, il nous faut un serveur «offshore». Il s'agit d'un service proposé par une société qui est basée hors de portée des administrations de votre pays : Panama, Russie, Bulgarie, Pays-Bas, etc. Et là, on en trouve des tas ! Que ce soit Abelohost.com, Blueangelhost.com, Offshoreracks.com, BitWeb ou encore Hidemyhost.com tout



est bon. Le petit hic c'est que c'est deux fois plus cher qu'un serveur standard, c'est-à-dire que pour un serveur à 15 € par mois sur le marché normal, là il sera à 30 €, mais, c'est le prix de la sécurité ! L'achat se fait aussi par Tor et pour le type de serveur, on prendra ou Ubuntu ou Debian et pour les performances, il suffit de 1 Go de RAM minimum. Accessible à toutes les bourses donc...

03 > ASTERISK, UNE IDÉE FIXE

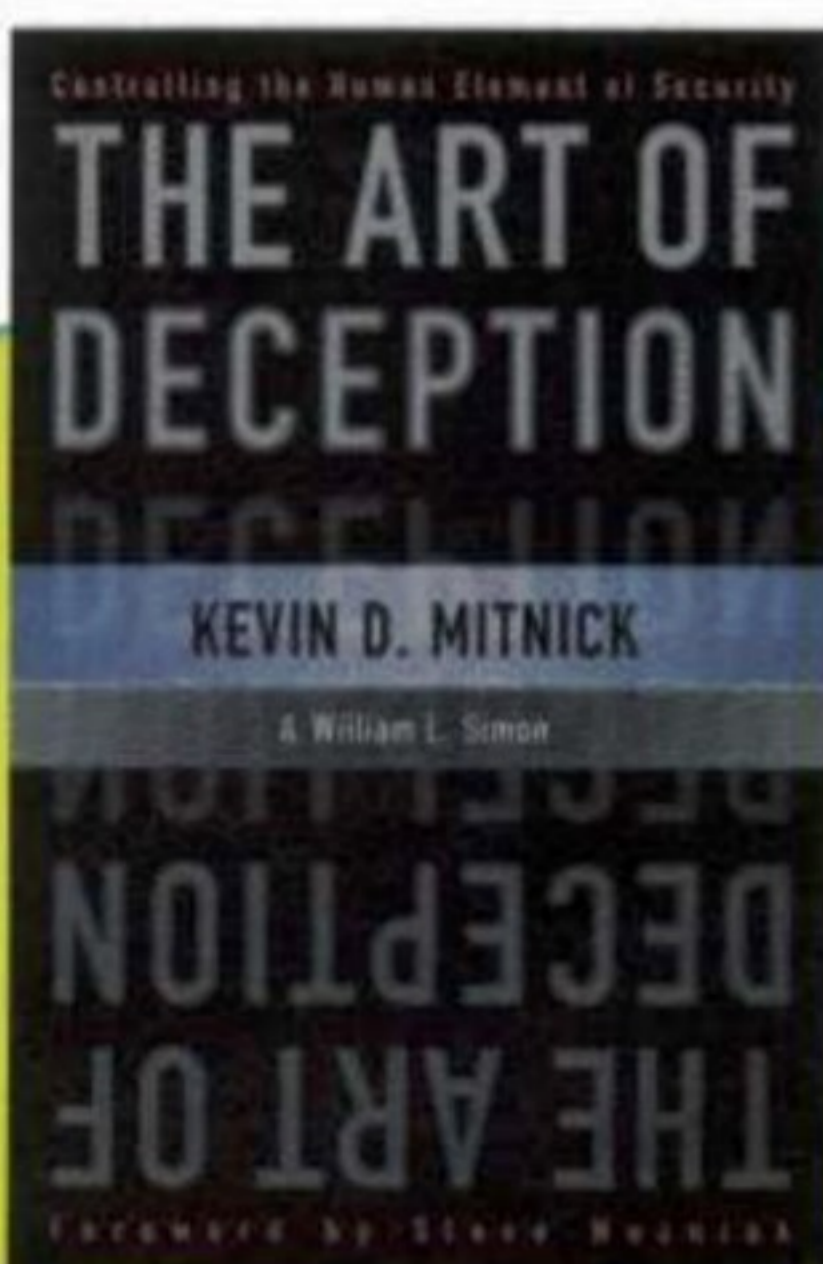
Votre installation prête, il vous suffit d'installer et de configurer correctement Asterisk ! Ensuite, il vous faut un compte SIP. Les services ne manquent pas, Dialexia, Bitcall, VoIP Supply, VoIP Bitcoin, etc.

L'achat du compte SIP effectué, il suffit maintenant de le connecter au serveur Asterisk. Pour l'usurpation de numéro, il vous suffit de créer un script de ce genre :

```
#!/bin/bash
rm extensions.conf
sed «s/NEUNUMBER/$1/» < ext-template.conf >
extensions.conf
asterisk -rx «core restart now»
```

Il faudra juste exécuter simplement ce script avec le numéro à usurper (ex : `./spoofer.sh +336010203XX`)

Le tour est joué pour le pirate inconscient qui voudra se faire passer pour un tiers, une société, etc.



KEVIN MITNICK ET SON «ART OF DECEPTION»

Si vous souhaitez en savoir plus sur le social engineering, sachez que Kevin Mitnick a co-écrit un livre entier sur ce sujet. Celui qu'on reconnaît comme le meilleur hacker du monde n'a pas uniquement réussi grâce à ses talents en informatique. *L'art de la supercherie (The Art of Deception)*, publié en 2002, traite de l'art du social engineering principalement par le biais de la téléphonie. Si vous êtes plutôt «cinéma», vous trouverez quelques exemples dans le film retraçant une partie de la vie de Mitnick : *Cybertr@que (Takedown)*.

UNE CLÉ USB MULTIBOOT AVEC XBOOT

POUR QUI ?

Pour les bidouilleurs

POUR QUOI FAIRE ?

Pour avoir forcément la distribution adéquate sous la main

Vous utilisez à l'ancienne des Live CD pour réparer Windows, faire découvrir Linux ou tester la sécurité d'un réseau ? Le problème c'est qu'il faut graver de nouvelles galettes à chaque mise à jour et transporter tous ces CD sans savoir s'ils serviront vraiment. Avec XBoot il vous sera possible de placer plusieurs ISO sur une clé USB pour choisir la distribution à utiliser lors du boot.



LEXIQUE

*MULTIBOOT :

Il s'agit en fait d'une option permettant de choisir, quel système se lancera sur une machine. On peut par exemple configurer son PC pour qu'il démarre avec Windows ou Linux. Dans notre cas il s'agit permettre un démarrage sur un Live CD parmi plusieurs depuis un DVD ou une clé USB.

*LIVE CD :

Un Live CD permet de lancer un système d'exploitation Linux ou des outils de diagnostic/sécurité sans avoir besoin d'une installation. Il suffit de demander au PC par l'intermédiaire du BIOS de "booter" (de démarrer) depuis le CD/DVD. Un Live CD se présente la plupart du temps sous la forme d'une image au format ISO à graver, mais il est possible de la placer sur une clé USB. Xboot propose une liste à télécharger dans le menu **File**, mais en voici une liste non exhaustive : <http://goo.gl/Rs4tkV>.

Si vous avez l'habitude d'utiliser des Live CD, vous connaissez bien les avantages et les inconvénients du procédé : pas besoin d'installation, mais aussi un encombrement relativement gênant dû à la taille des CD ou des DVD. Ce problème a en partie été résolu avec la possibilité de placer ces Live CD sur une clé USB, mais il était encore impossible d'en mettre plusieurs sur une seule et même clé.

PLUSIEURS LIVE CD SUR UN SEUL SUPPORT

Xboot est un logiciel qui va résoudre tous ces problèmes. Que vous préfériez les DVD ou les clés USB vous allez enfin pouvoir mettre plusieurs systèmes sur un seul support. La seule condition c'est d'avoir suffisamment de place sur votre DVD ou votre clé USB pour les

contenir tous. Vous pourrez donc avoir tous les outils dont vous avez besoin pour dépanner, lancer un système d'exploitation d'appoint ou booter sur une distribution Linux thématique (sécurité, création graphique, media center, etc.) N'importe quel ordinateur pourra devenir «le vôtre» puisque vous amenez votre propre système. On peut aussi imaginer pouvoir travailler sur un PC sans disque dur. Dans notre exemple nous avons placé trois Live CD sur une clé USB, mais sachez qu'il est possible d'en utiliser d'autres ou d'en utiliser plus ! Autant que permet la capacité de votre support... Sachez aussi qu'il est possible de faire de même sur un DVD avec le même logiciel. Attention le CD, avec ses 700 Mo de stockage est un peu limité, mais il existe de nombreuses distributions Linux «compactes».

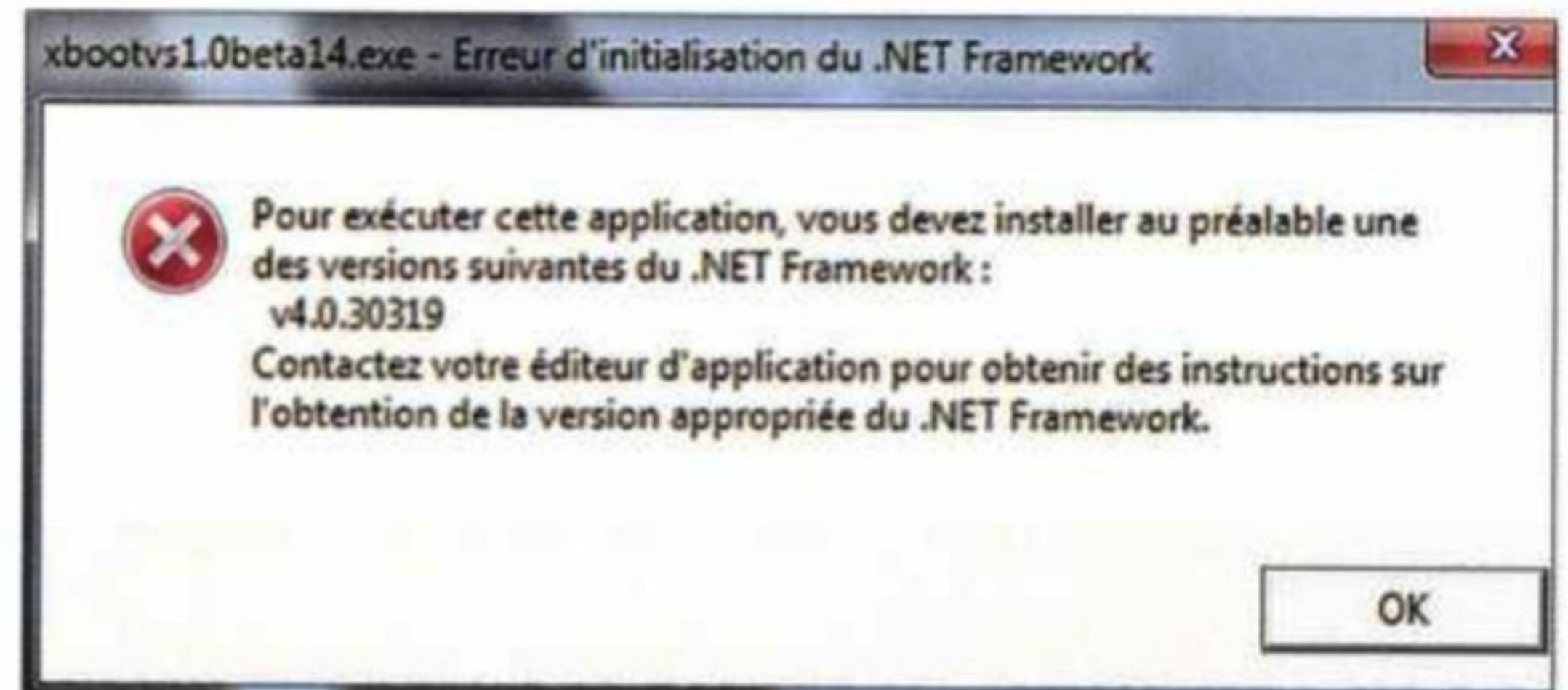


VOTRE CLÉ USB MULTIBOOT SUR-MESURE



01 > PRÉPARATION

Pour notre démonstration nous allons placer trois Live CD que nous utilisons fréquemment sur une clé USB (voir la présentation). Même si une clé de 2 Go pourrait suffire à toutes les contenir, nous utiliserons une clé de 8Go pour pouvoir sauvegarder des fichiers ou en créer. Commençons par télécharger, décompresser et lancer XBoot. Si un message d'erreur apparaît, il faudra télécharger et installer le .NET Framework 4 à cette adresse : <http://goo.gl>. Si tout se passe bien vous devriez voir l'interface principale.

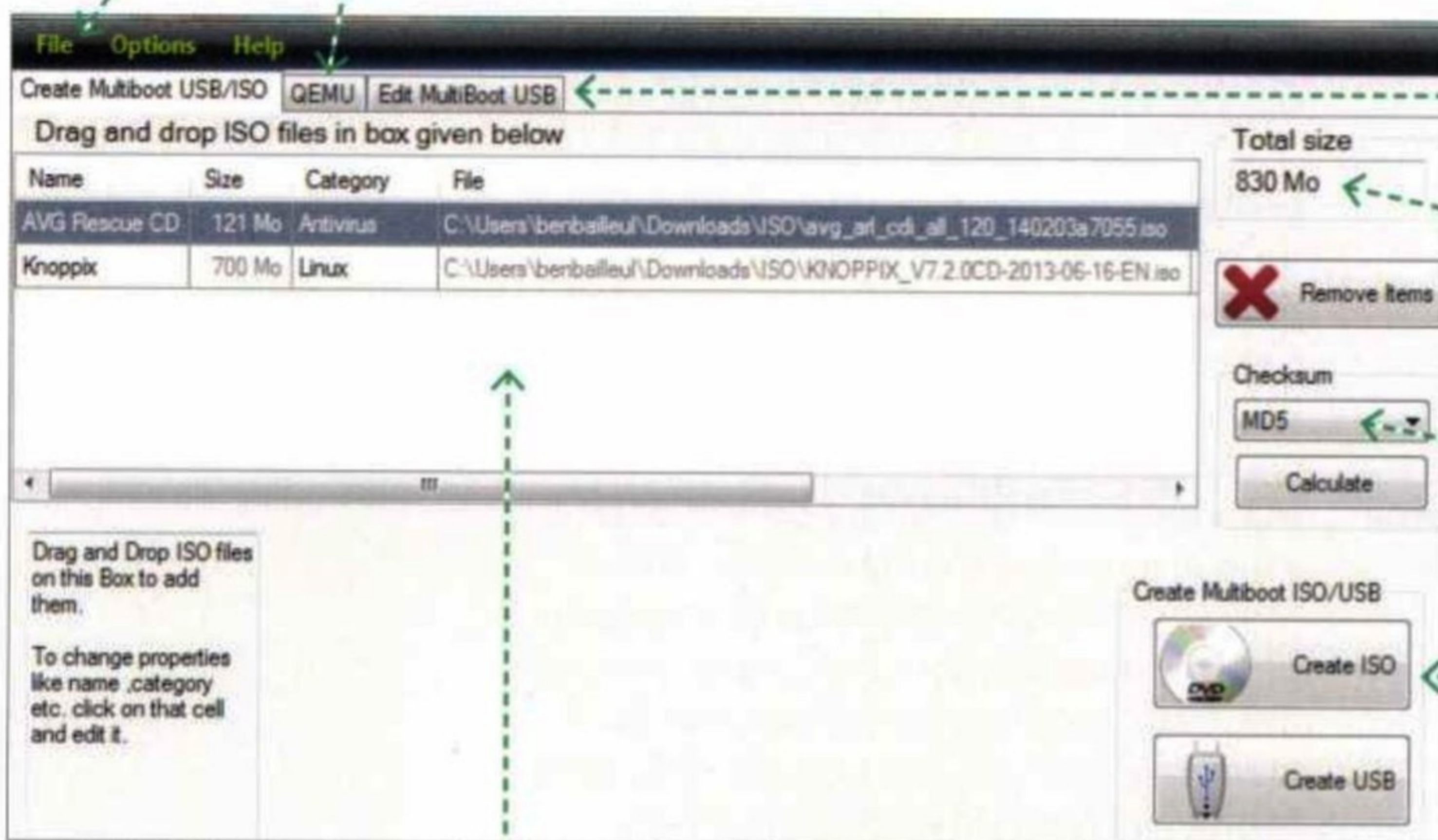
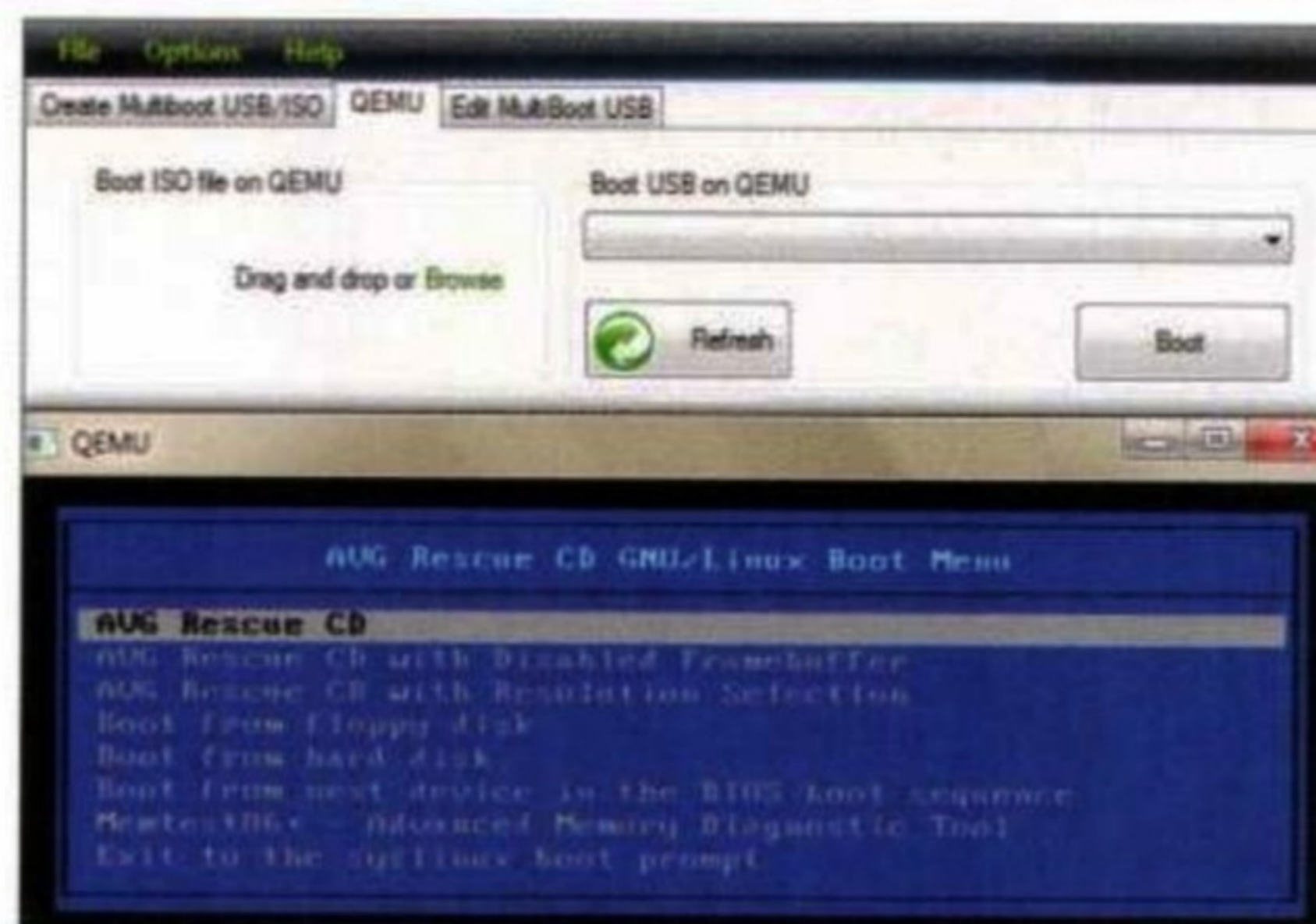


02 > L'INTERFACE

Dans **File>Download** vous trouverez pas loin d'une cinquantaine d'emplacements pour télécharger des Live CD, des utilitaires ou des antivirus prêts à être montés sur votre clé USB.



Onglet permettant de vérifier le bon fonctionnement de vos ISO. Glissez-déposez votre fichier et regardez-le se lancer dans un environnement émulé.



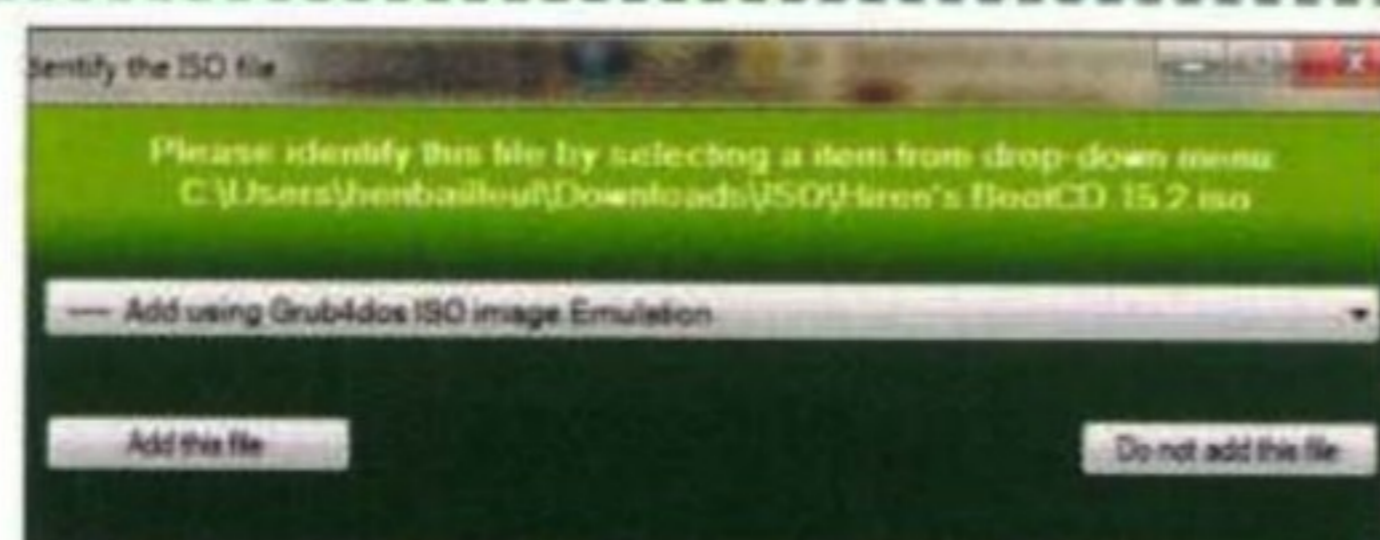
Outil d'édition du multiboot pour les clés USB (pour les utilisateurs avancés)

Taille totale des fichiers ISO

Vérifiez l'intégrité de vos fichiers ISO avec les checksums MD5 ou SHA. Si le chiffre mis dans le presse-papier (faites **coller** dans un fichier texte !) correspond au checksum inclus dans les fichiers du téléchargement, c'est que tout est bon.

C'est ici qu'il faudra cliquer pour préparer votre ISO final ou votre clé USB multiboot

Glissez-déposez vos ISO dans cette fenêtre. Si votre fichier n'est pas reconnu, il faudra choisir **Add using Grub4dos ISO image** dans le menu déroulant et cliquer sur **Add this file**.





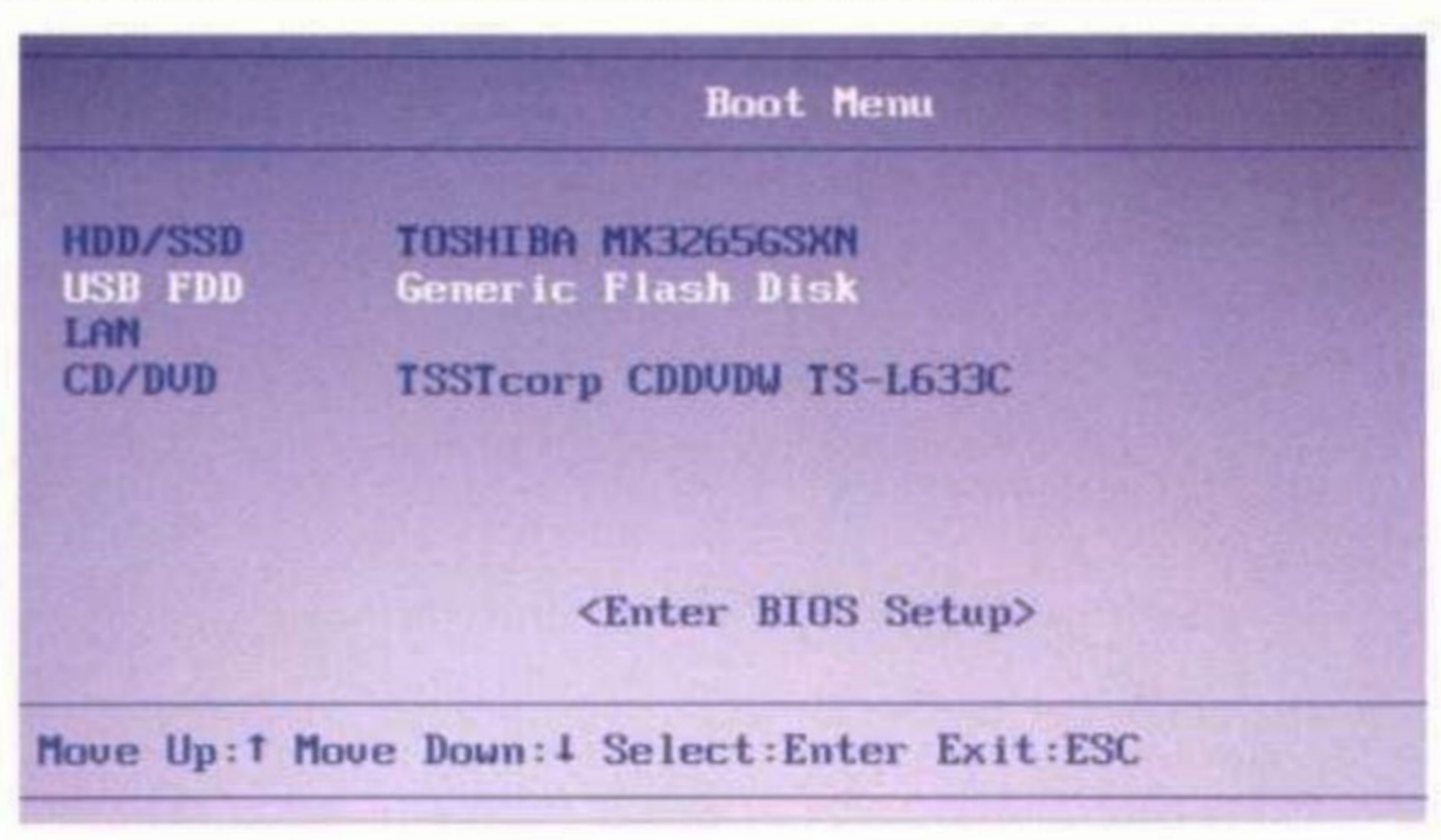
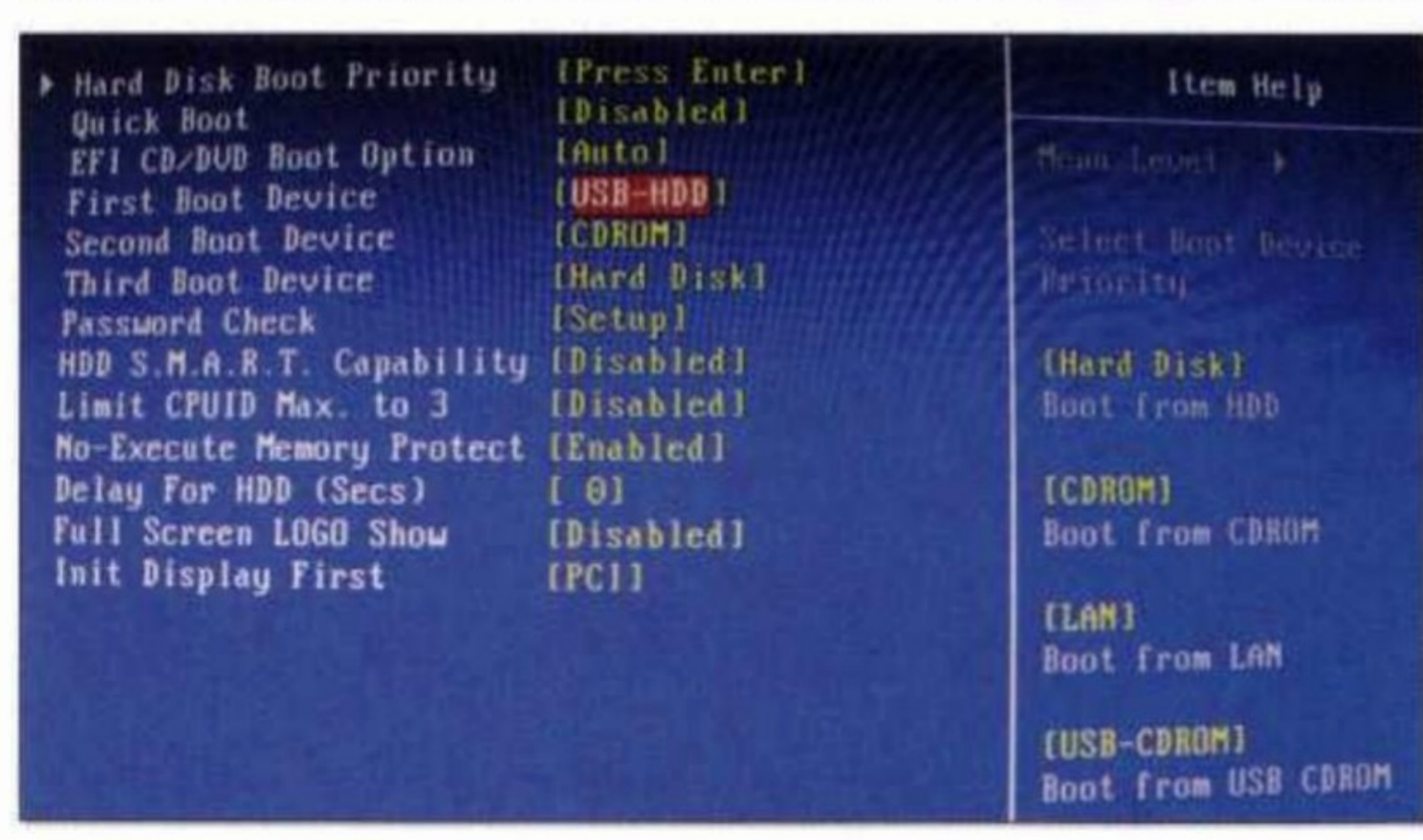
03 > CRÉATION DE LA CLÉ

Une fois que les vérifications ont été faites et que tous vos ISO ont été sélectionnés, il suffit de brancher votre clé USB vierge et de cliquer sur **Create USB**. Sélectionnez votre périphérique dans le menu et laissez le bootloader (le menu permettant de sélectionner son Live CD lors du boot) par défaut. Laissez alors faire le logiciel (le temps dépendra de la taille et du nombre d'ISO). Xboot vous demandera alors si vous voulez lancer votre création virtuellement pour voir si tout fonctionne bien (bizarrement cela ne fonctionne pas à tous les coups). Si vous préférez les DVD, le logiciel regroupera les ISO en un seul prêt à graver et intégrera un menu multiboot.



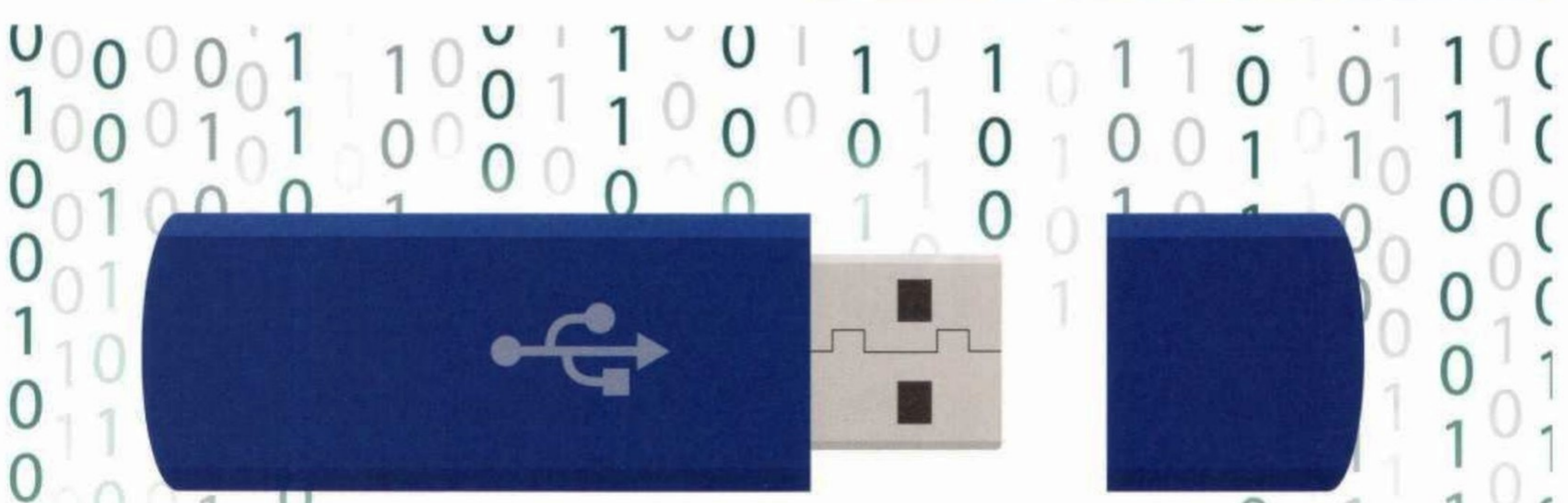
04 > UTILISEZ VOTRE CLÉ

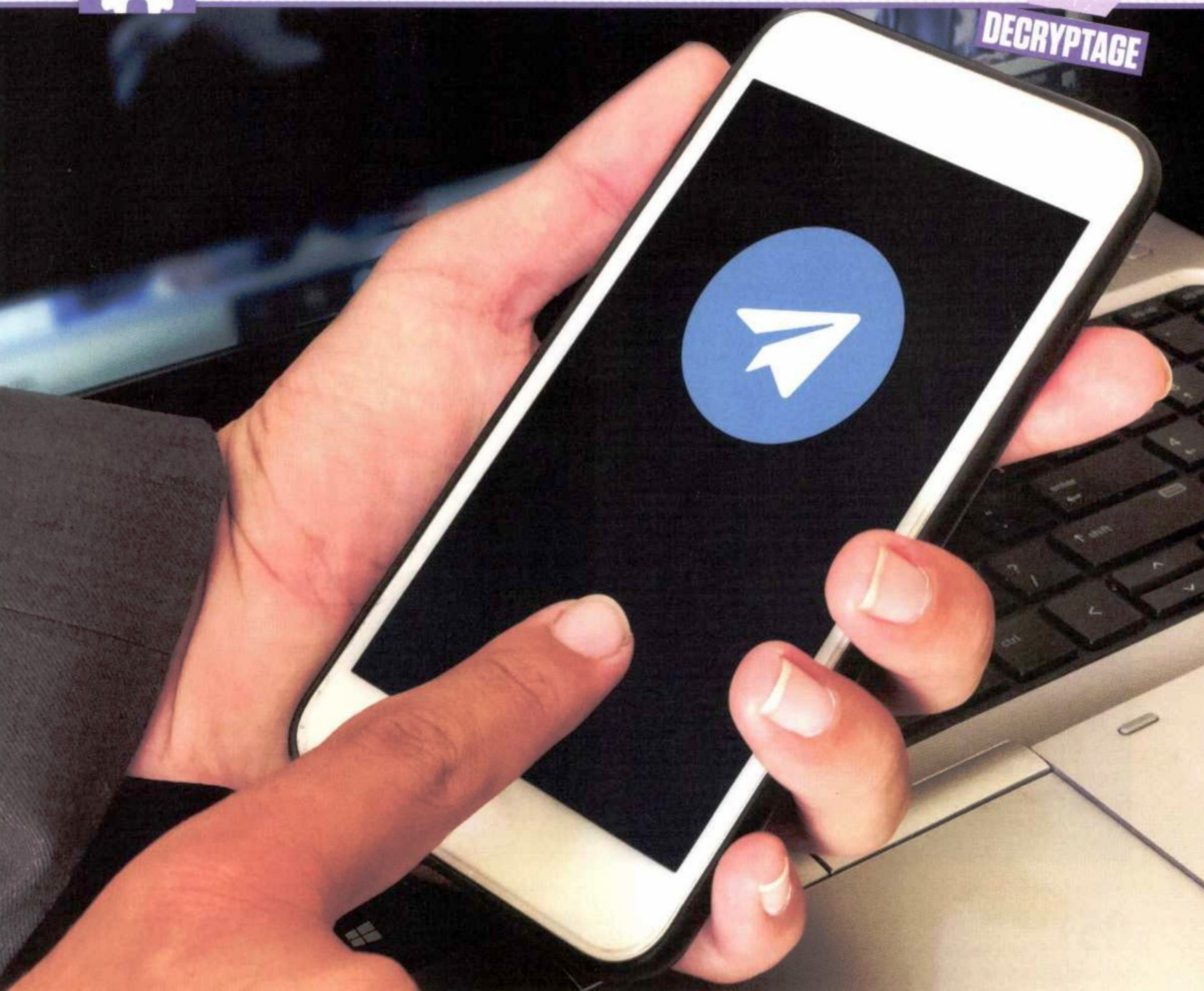
Une fois que votre clé est prête, il faudra juste penser à booter sur l'USB pour pouvoir s'en servir sur un ordinateur (ou botter sur le lecteur de DVD le cas échéant). Faites **Suppr**, **F1**, **F2** ou **F12** (en fonction de votre modèle de carte mère) juste après avoir allumé le PC et entrez dans le BIOS (**Setup**). Trouvez l'option **Boot Sequence** (qui peut aussi être sélectionnable avant même l'entrée dans les menus) et modifiez l'ordre en mettant en premier le port USB. Si vous avez des difficultés, consultez la notice de votre carte mère ou jetez un coup d'œil sur Google avec le nom de votre matériel.



05 > LE MENU MULTIBOOT

Si tout se passe bien, vous devriez voir le menu suivant. Boot from Hard Disk permet de revenir au système installé sur le disque dur (Windows ou un autre). Les autres lignes correspondent aux ISO que vous avez intégrés. Ils sont classés par catégorie (Linux, Antivirus, etc.) Dans notre cas, seul Hiren's BootCD n'est pas «rangé» car il n'a pas été reconnu nativement. Mais cela ne l'empêche pas de fonctionner ! Choisissez le Live CD que vous voulez et tapez sur Entrée. Bravo vous avez une clé USB multiboot avec plusieurs systèmes et des outils de diagnostic/réparation.





TELEGRAM, UNE MESSAGERIE SÉCURISÉE... OU À SÉCURISER ?

Telegram offre de nombreuses options de sécurité. Ce n'est pas pour rien que notre président l'utilise en priorité pour communiquer en privé. Mais a-t-il raison de le faire ?

Telegram est considérée, au choix, comme l'une des messageries les plus sécurisées existantes. Ou comme la pire. Et c'est ainsi que des groupes d'activistes, des terroristes ou des membres du gouvernement échangent régulièrement sur l'application. Et pas n'importe lesquels : Emmanuel Macron y partage une boucle privée avec Élisabeth Borne et Gérald Darmanin. Si eux le font, c'est parce qu'ils estiment que tous les messages échangés y restent privés. Sauf qu'il existe des doutes sur ce sujet. Et notamment liés à l'historique de Telegram.

POURQUOI TELEGRAM INQUIÈTE ?

Vous êtes prêt pour un petit voyage ? Telegram a été créée en 2013 par les frères Nikolai et Pavel Durov, fondateurs de VKontakte, le réseau social dominant en Russie. Opposants à Vladimir Poutine, ces frères voulaient un service qui permettrait de communiquer sans être repéré par les services secrets russes. Mais les Parov sont des mathématiciens, pas des spécialistes du chiffrement. Des failles de sécurité, permettant de récupérer les métadonnées des utilisateurs, ont été repérées. Les carnets d'adresses de chacun des usagers sont également téléversés sur les serveurs de Telegram. Le cryptographe

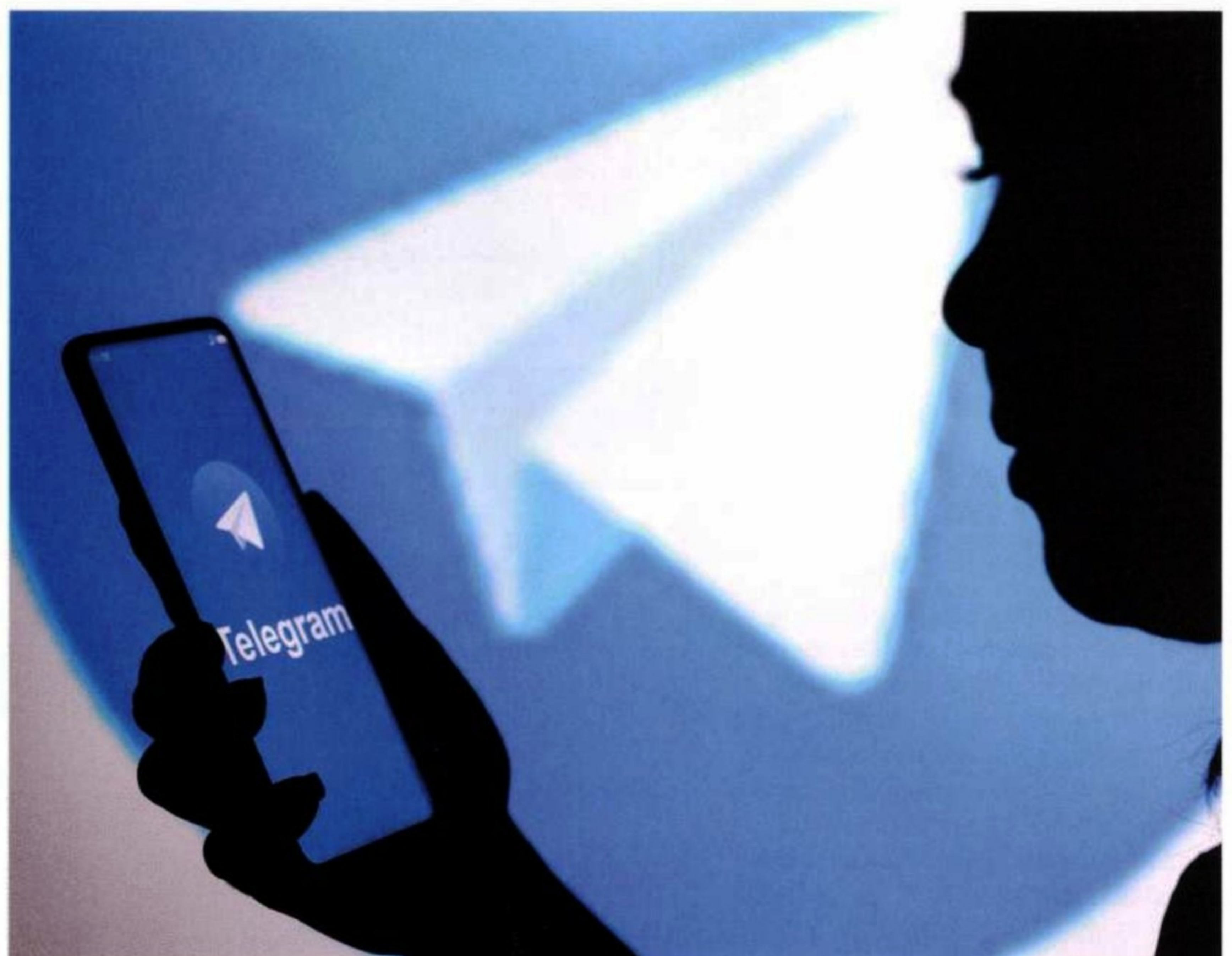
Moxie Marlinspike a, quant à lui, confirmé que le chiffrement de bout en bout n'y est pas présent dans les conversations de groupe.

Et c'est pourquoi l'entourage du chef d'État craint des possibilités d'espionnage par des services russes ou américains... Au point d'envisager de lui fournir, ainsi qu'à son entourage proche, des téléphones ultra-sécurisés et dont les données resteraient vraiment privées. Ceci dans le but de le décourager de continuer à utiliser Telegram. Parfois, il faut prendre des décisions à la place des décisionnaires.

ET NOUS, ON L'UTILISE OU PAS ?

Si vous devez échanger sur des secrets d'État, Telegram n'est peut-être pas la meilleure option. Mais il sera difficile de trouver un outil totalement protecteur pour vos données. Par contre, il reste intéressant si vous ne vous contentez pas d'y envoyer des messages, mais que vous en prenez les rênes. Vous pouvez sécuriser un grand nombre d'éléments, comme vous le verrez dans les pages suivantes. Et, si vous rejoignez un groupe, restez attentif à ce qui s'y passe : ce n'est pas nécessairement là que vos conversations seront le plus privées.

»»»
TELEGRAM N'EST PAS SANS RISQUE MAIS EST POURTANT PLÉBISCITÉE POUR SA PRATICITÉ ET SES OUTILS SOCIAUX. VOUS POUVEZ RENDRE LA MESSAGIERIE PLUS CONFIDENTIELLE ET GARDER LE CONTRÔLE.





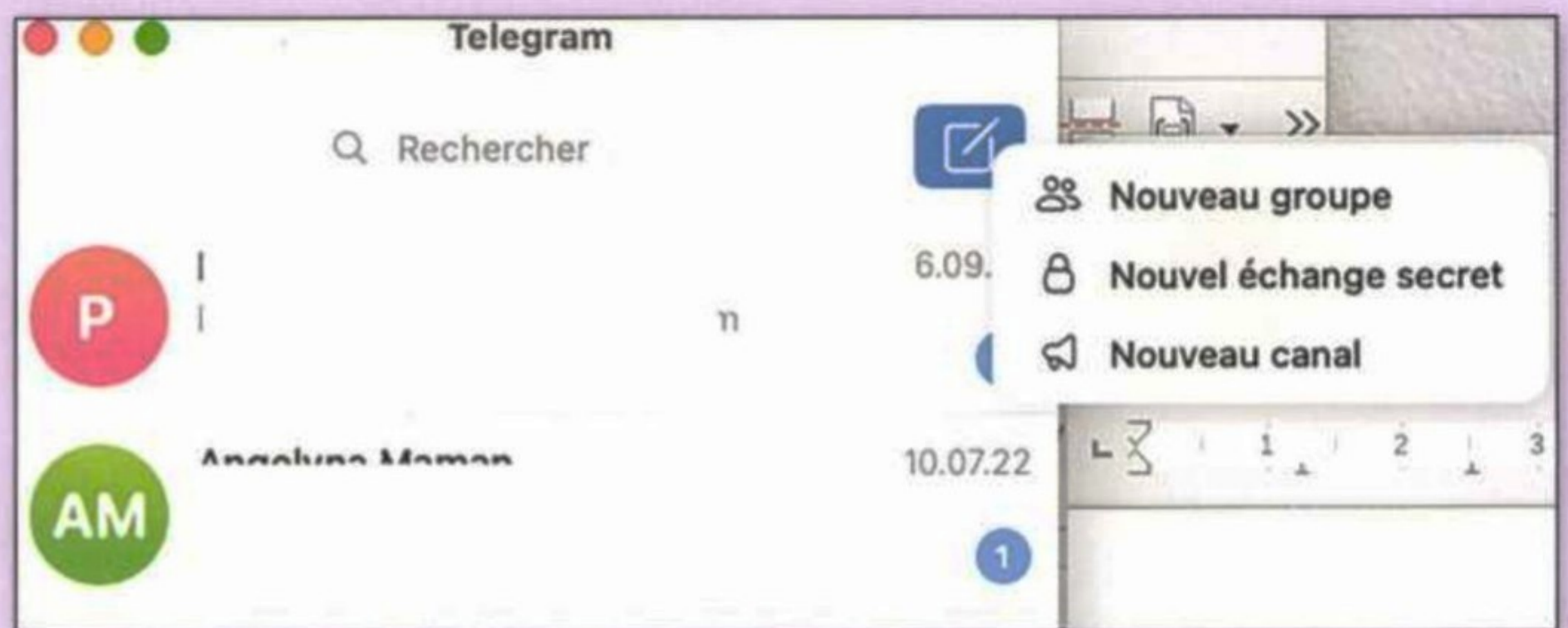
7 ASTUCES MÉCONNUES POUR TELEGRAM



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

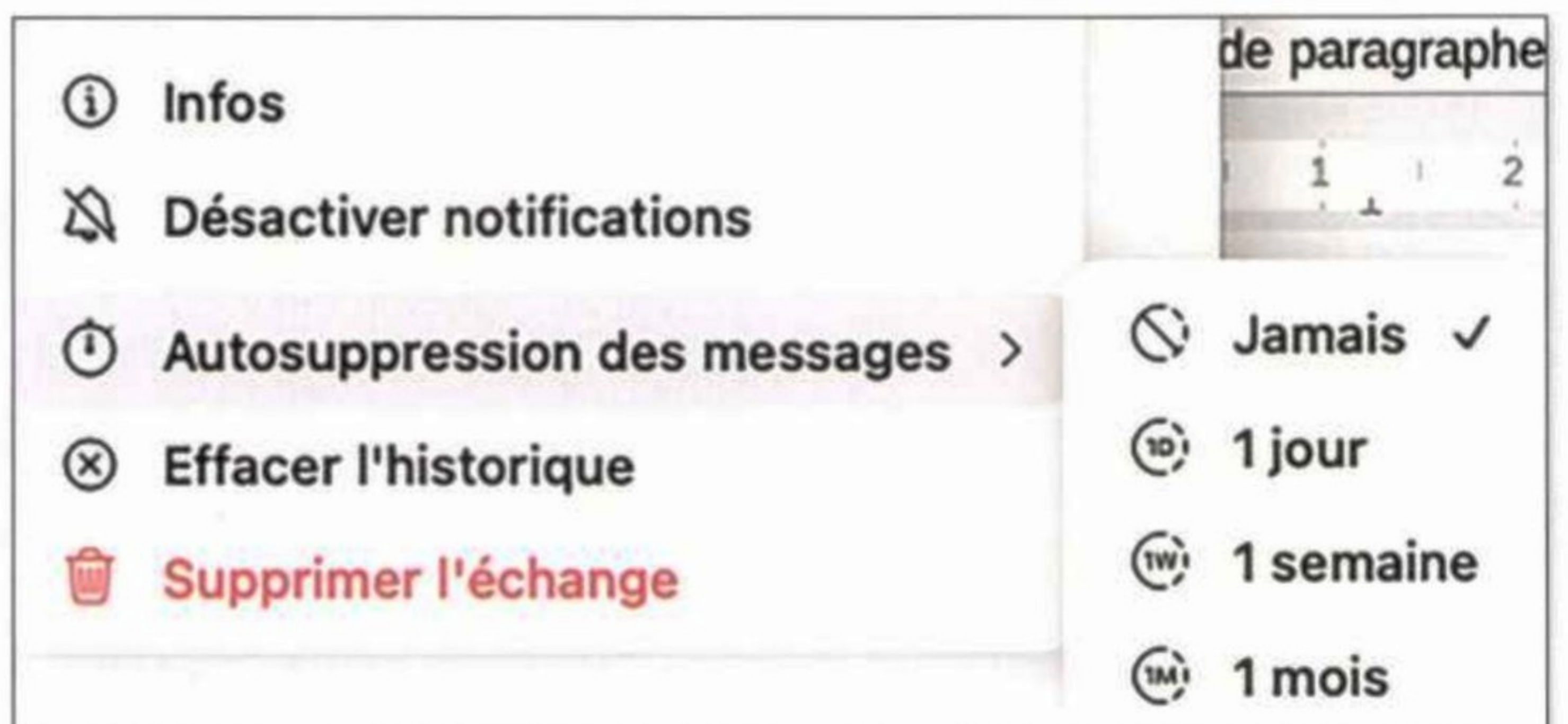
» CRÉER UNE CONVERSATION SECRÈTE (ET CRYPTÉE)

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



» AUTODÉTRUIRE VOS MESSAGES

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



» DÉCIDER QUI PEUT VOUS AJOUTER À DES GROUPES

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



MASQUER VOS INFORMATIONS

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



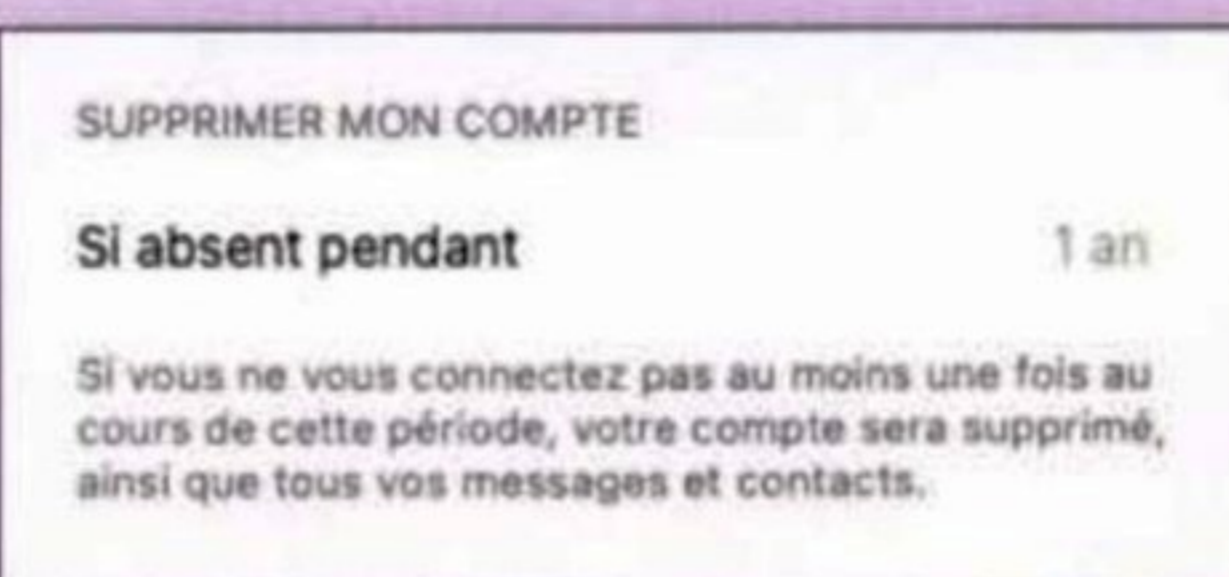
» UTILISER UN PROXY

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



» PRÉPARER VOTRE DISPARITION

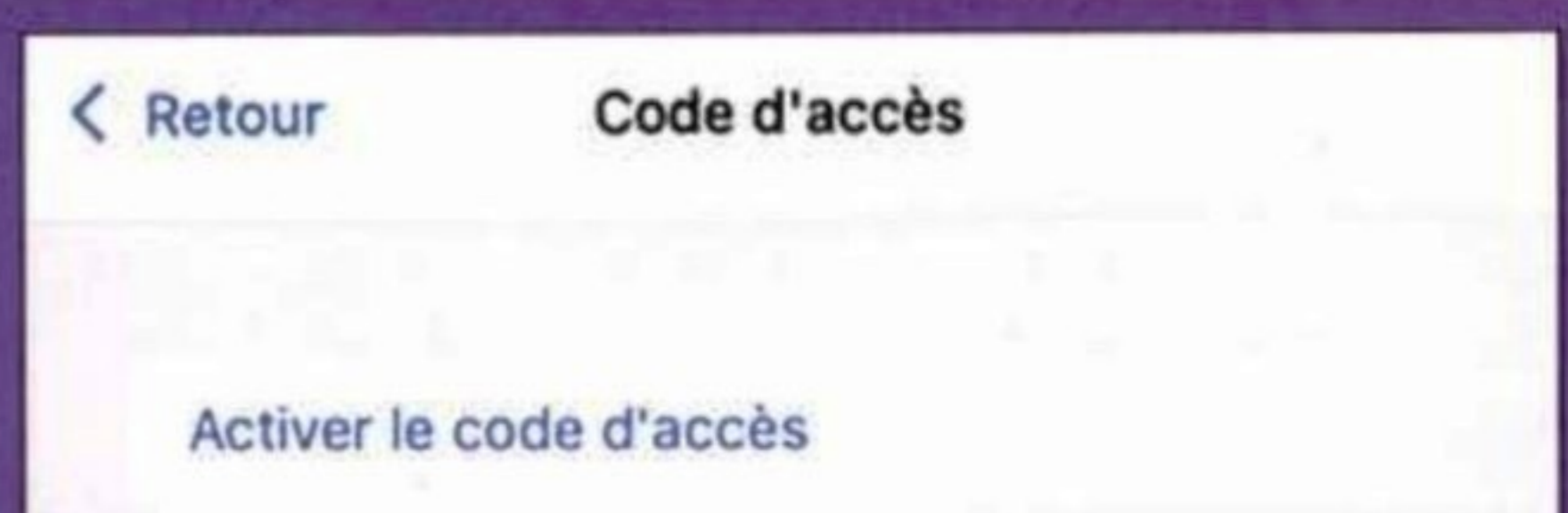
Vous pouvez programmer la suppression de votre compte si jamais vous en perdez l'accès pendant un certain temps. Allez dans la section **Paramètres**, puis dans **Confidentialité et sécurité**. Faites défiler jusqu'à la



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

» VERROUILLER L'ACCÈS À VOS CONVERSATIONS

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





... ET 9 ASTUCES POUR LES GROUPES TELEGRAM

Telegram est de plus en plus utilisé pour des conversations de groupe. Parfait pour faire circuler une information rapidement... À condition de savoir bien les utiliser.

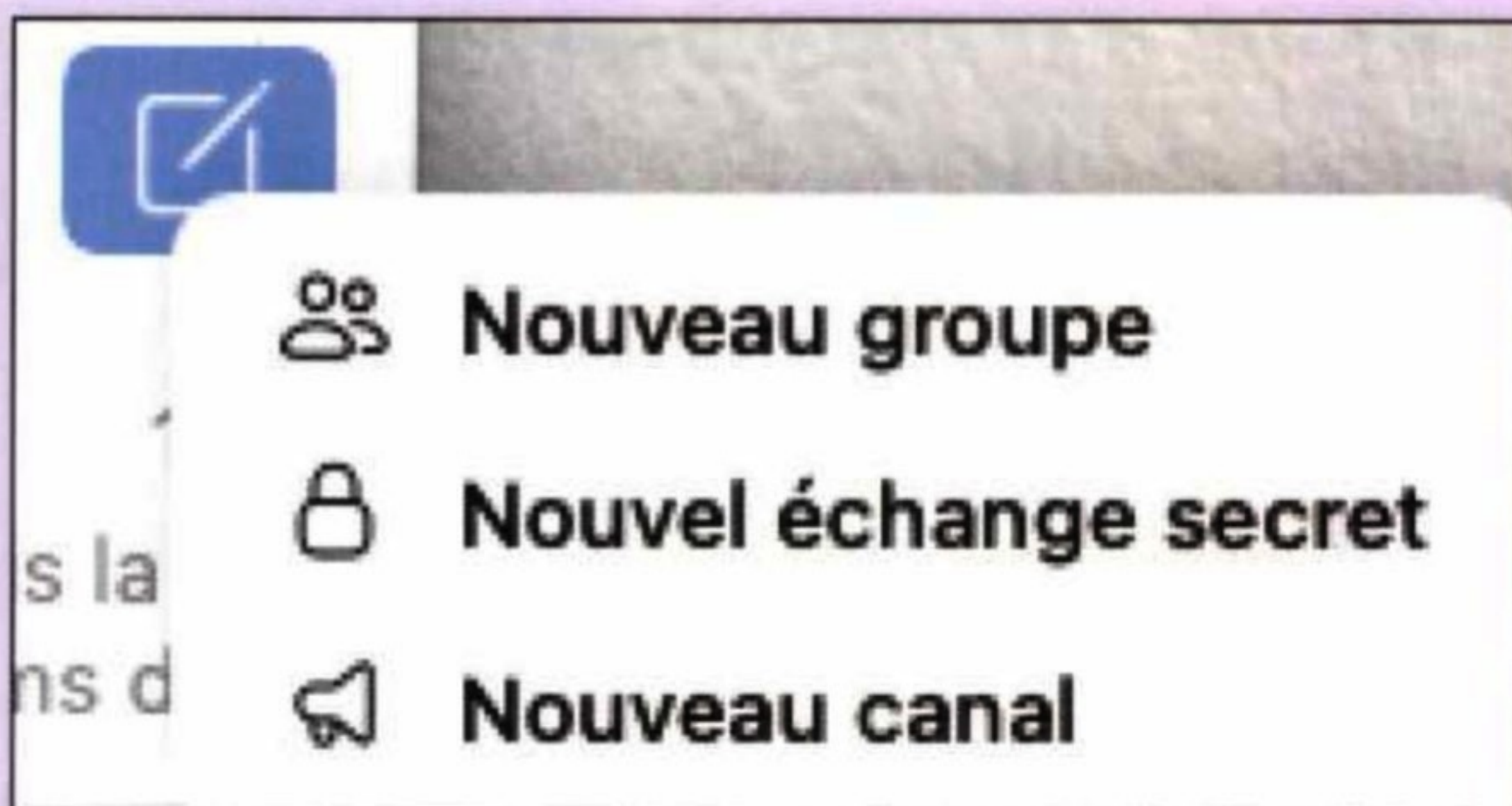
MAIS AU FAIT, C'EST QUOI UN GROUPE ?

Les groupes sont à distinguer des canaux, qui ont pour but de partager des messages publics à une large audience. Dans un groupe, tout le monde peut participer et envoyer des messages, pas seulement l'administrateur. Il est possible d'y échanger textes, mais aussi visuels et autres éléments multimédias. Les appels vidéo ou vocaux restent disponibles. Et chaque membre du groupe peut inviter d'autres personnes parmi ses contacts, ce qui peut les faire grandir très vite. D'ailleurs, il faut les convertir en supergroupe dès lors qu'il dépasse 200 000 membres.



» CRÉER UN GROUPE

Pour créer un groupe, cliquez sur l'icône en forme de crayon et sélectionnez **Nouveau groupe**. Ajoutez ensuite les personnes parmi vos contacts que vous souhaitez associer à ce groupe. Cliquez sur **Suivant** (vous pourrez toujours ajouter des utilisateurs par la suite). Donnez un nom à ce groupe et ajoutez-y un visuel pour le repérer plus facilement, puis cliquez sur **Créer**.



» LAISSER APPARAÎTRE LES ANCIENNES CONVERSATIONS

Si vous ne voulez pas que les nouveaux venus se sentent perdus en arrivant sur votre groupe, laissez-leur la possibilité de lire les anciennes conversations. Cliquez sur le nom du groupe, puis sur **Infos**, puis sur **Modifier**. Allez sur **Historique pour les nouveaux membres**, et cliquez sur **Visible**, puis sur **Valider**.



» AJOUTER DE NOUVEAUX MEMBRES

Un groupe peut avoir jusqu'à 200 000 membres. Pour en ajouter à celui existant, ouvrez le groupe puis cliquez sur son nom. Cliquez ensuite sur **Ajouter** pour intégrer d'autres contacts à ce groupe. Cliquez sur leurs noms puis sur **Ajouter**. Il est aussi possible au même endroit de créer un lien d'invitation en appuyant sur **Inviter avec un lien**.



» NOMMER D'AUTRES ADMINISTRATEURS

Gérer un groupe peut demander beaucoup de temps. Surtout s'il grandit. C'est là qu'il peut devenir intéressant de nommer d'autres administrateurs. Cliquez sur le nom du groupe, puis sur **Infos**, puis sur **Modifier**. Descendez jusqu'à **Administrateurs**, cliquez dessus puis sur **Ajouter un administrateur** et enfin sur **Valider** une fois ses droits décidés. Vous pourrez alors nommer le membre du groupe de votre choix. Si vous décidez ensuite de le renvoyer, il vous suffira de retourner sur cet espace, de cliquer sur son nom puis sur **Renvoyer l'administrateur**.



QUE PEUVENT FAIRE LES MEMBRES DE CE GROUPE ?

- Envoyer des messages
- Envoyer des médias
- Envoyer des autocollants et GIF
- Afficher les aperçus de liens
- Envoyer des sondages
- Ajouter des membres
- Épingler des messages
- Modifier les infos du groupe

MODE RALENTI

Aucun 10s 30s 1mn 5mn 15mn 1h

» LIMITER LES ACTIONS DES MEMBRES

Rappelez-vous que vous gérez le groupe. Et vous n'avez peut-être pas envie que tout le monde y fasse n'importe quoi. Vous pouvez décider de ce que vous tolérez ou non. Cliquez sur le nom du groupe, puis sur **Infos**, puis sur **Modifier**. Cliquez alors sur **Permissions**. Vous pouvez ainsi décider si tout le monde a le droit ou non d'ajouter de nouveaux membres ou de modifier les infos du groupe.



ANONYMAT

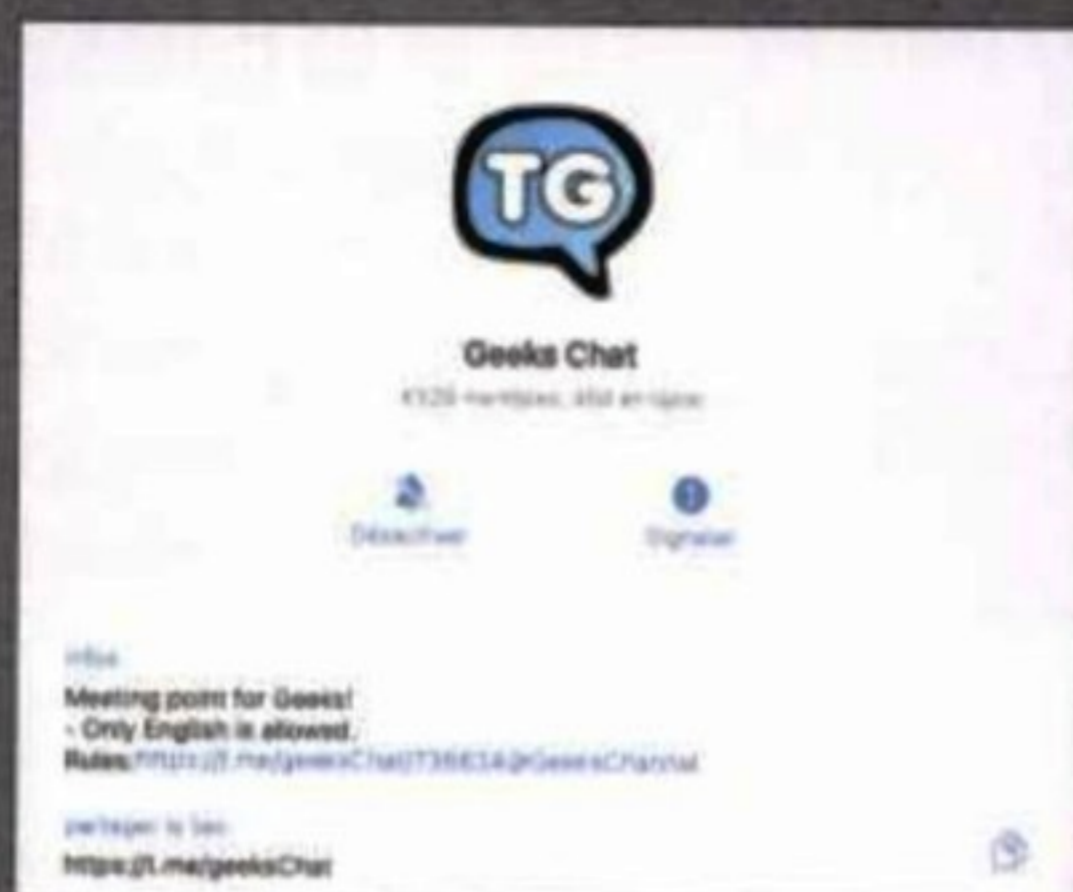
QUELQUES GROUPES GEEK À SUIVRE



» GEEKS CHAT

Un groupe anglophone qui évoque de nombreux sujets Tech et geeks. Les questions sont nombreuses et le ton est assez libre.

t.me/geeksChat



» TECHNOBUZZ

Un groupe issu d'une communauté indienne sur les technologies Android. Les sujets évoqués concernent maintenant aussi les PC.

t.me/technobuzznet



» CYBER SECURITY

Un groupe dédié à la cyber sécurité avec de nombreux intervenants. Les discussions partent parfois dans tous les sens, mais il y a de véritables informations à y trouver.

t.me/cybersecurityexperts



» ETHICAL HACKERS CHAT

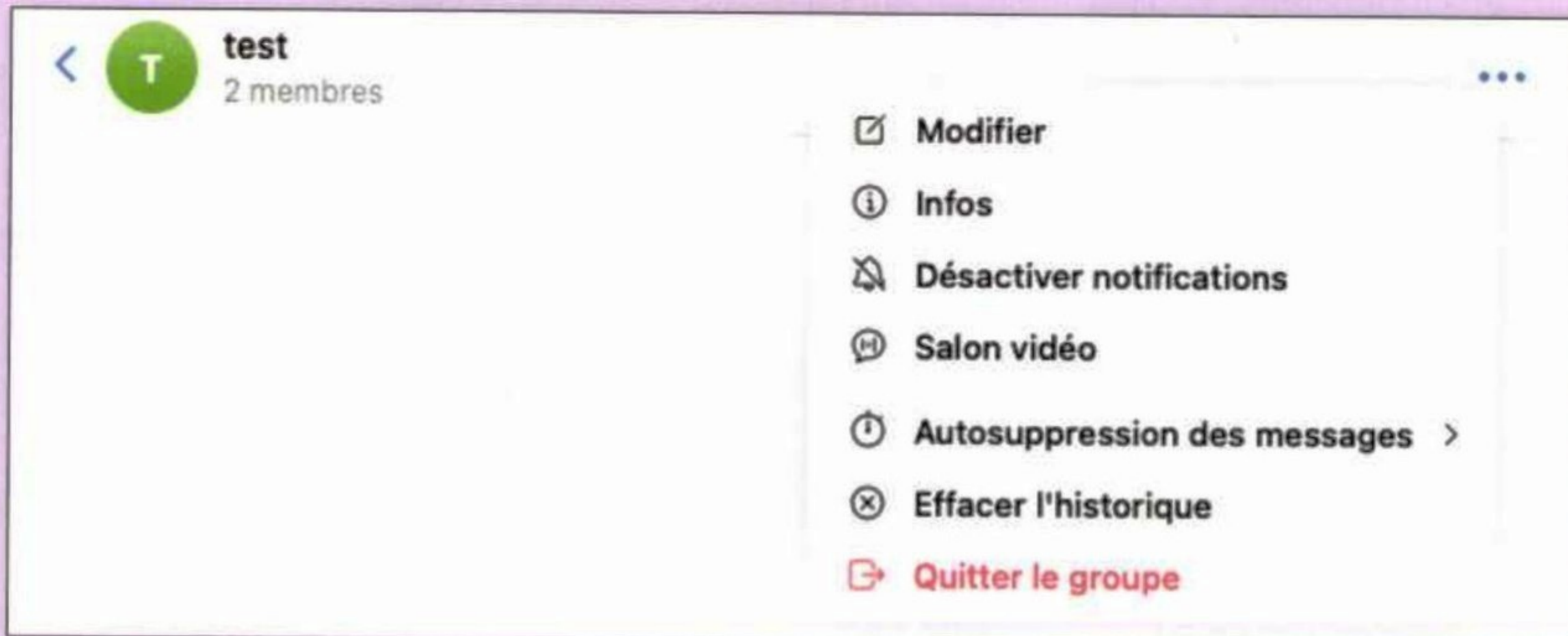
Ce groupe est issu d'un canal mais, contrairement à ce dernier, il est ouvert à la discussion. La modération essaie d'y être active pour éviter les indésirables.

t.me/ethicalhackersc



» QUITTER UN GROUPE

Si vous avez été ajouté à un groupe sans que l'on vous demande votre avis, ou juste si vous ne le trouvez plus intéressant, il est très facile d'en partir. Ouvrez-le, cliquez sur les trois points dans le coin supérieur droit puis sur **Quitter le groupe**. Et vous quitterez les lieux aussi facilement que cela.



» UTILISER DES BOTS DANS UN GROUPE

Les bots vous aident à gérer le groupe ou à y ajouter plus de convivialité. Le plus simple est d'utiliser des robots intégrés, qui sont directement ajoutés à votre groupe. Pour cela, vous devez d'abord les trouver en tapant le nom du bot dans la barre Recherche de Telegram. Cliquez ensuite sur son nom puis sur les trois petits points et sur **Ajouter à un groupe**.



» CRÉER UN SONDAGE

Cliquez sur l'attache trombone, en bas à gauche, puis sur **Sondage**. Vous ne pouvez poser qu'une question, mais ajouter jusqu'à huit options de réponse. Décidez si vous permettez les votes anonymes ou les multiréponses, ou optez pour un quizz puis appuyez sur **Envoyer**.

Question

Posez une question

OPTIONS DU SONDAGE

Option

Option

+ Ajouter une option

Vous pouvez encore ajouter 8 options.



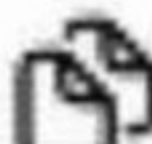







Vote anonyme

Réponses multiples

Mode quiz

Les quiz n'ont qu'une seule bonne réponse. Les utilisateurs ne peuvent pas révoquer leurs réponses.

Envoyer

-  Répondre
-  Traduire
-  Copier le texte
-  Copier le lien du message
-  Modifier
-  **Épingler**
-  Transférer >
-  Sélectionner
-  Personne n'a vu
-  **Supprimer**

» ÉPINGLER UN MESSAGE

Épingler un message permet qu'il soit toujours visible. Utile pour les informations importantes, d'autant que vous pouvez envoyer une notification à tous les membres du groupe pour le signaler. Allez sur le message et faites un clic droit dessus. Cliquez ensuite sur **Épingler** (deux fois de suite).

DEUX BOTS UTILES POUR LES GROUPES

» COMBOT

Combot comporte des outils de modération et d'analyses. Il sera particulièrement pertinent pour les communautés importantes.



Combot

» DR.WEB

Ce bot analyse automatiquement les fichiers et liens partagés sur le groupe pour s'assurer qu'ils ne contiennent pas de virus.



Dr.Web
bot



ET SI VOUS TRICHIEZ AVEC LES DNS ?

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

VÉRIFIEZ LE CHIFFREMENT



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



Il existe de nombreuses techniques pour conserver un minimum de confidentialité sur internet. Quand on n'a pas envie de s'embêter avec des outils supplémentaires, on a parfois trop tendance à croire que l'inscription HTTPS à l'entrée d'un site sert de videur et empêche

les indésirables de vous coller aux basques. Sauf qu'on ne vous dit pas tout : les requêtes DNS, qui font correspondre les noms de domaines et adresses IP des serveurs, sont toujours envoyées en clair. C'est à vous qu'il revient d'agir pour que ces données ne soient pas interceptées !

Chiffrez vos DNS sur Firefox et Chrome

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

1# SUR FIREFOX

01 > CHERCHER LES PARAMÈTRES RÉSEAU DE FIREFOX

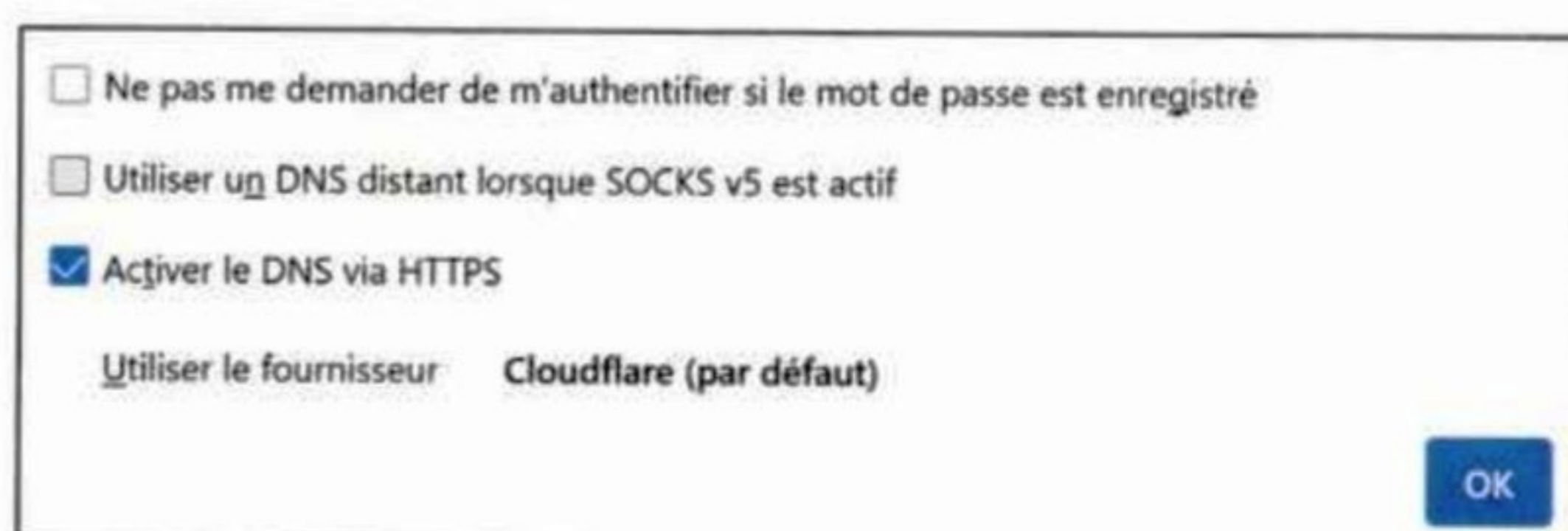
Firefox est capable d'utiliser des serveurs DNS DoH préconfiguré, sans vous demander de modifier vos réglages



réseau dans Windows. Dans Firefox, allez dans le **Menu**, puis dans **Paramètres**. Faites défiler jusqu'à atteindre la zone **Paramètres Réseau** et cliquez sur **Paramètres**.

02 > ACTIVER LE DNS

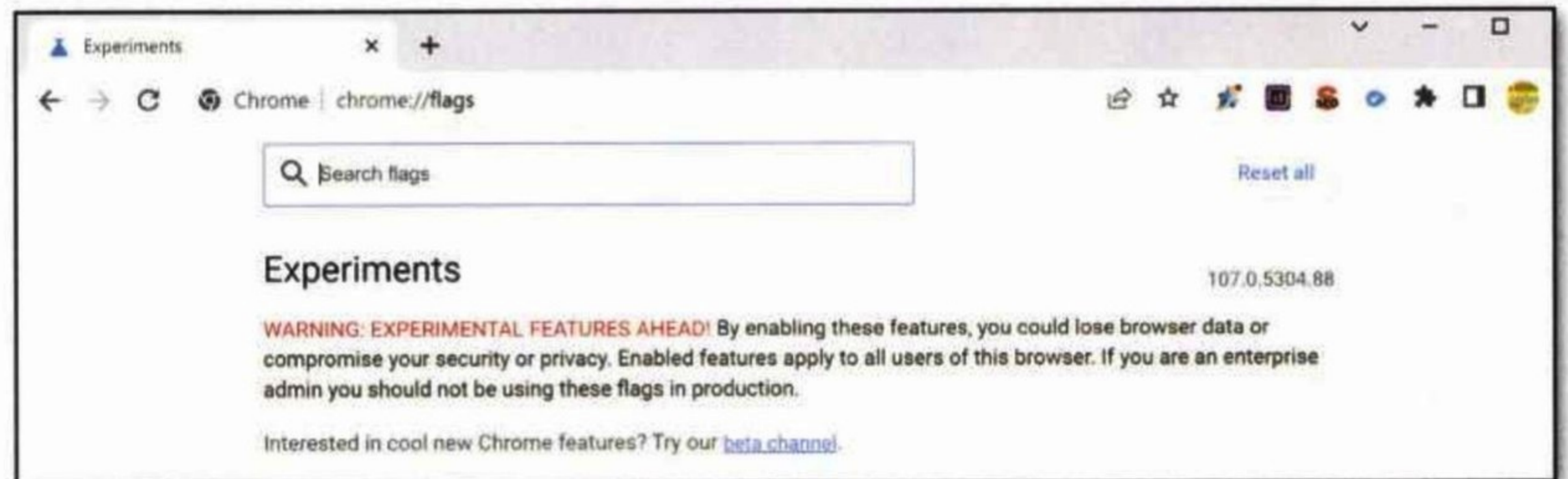
Tout en bas de la fenêtre, cochez la case **Activer le DNS via HTTPS**. Firefox va vous proposer plusieurs choix. Le plus simple est de laisser Cloudflare qui est proposé par défaut. Si vous le souhaitez, vous pourrez toujours opter pour un fournisseur DNS personnalisé.



2# SUR CHROME

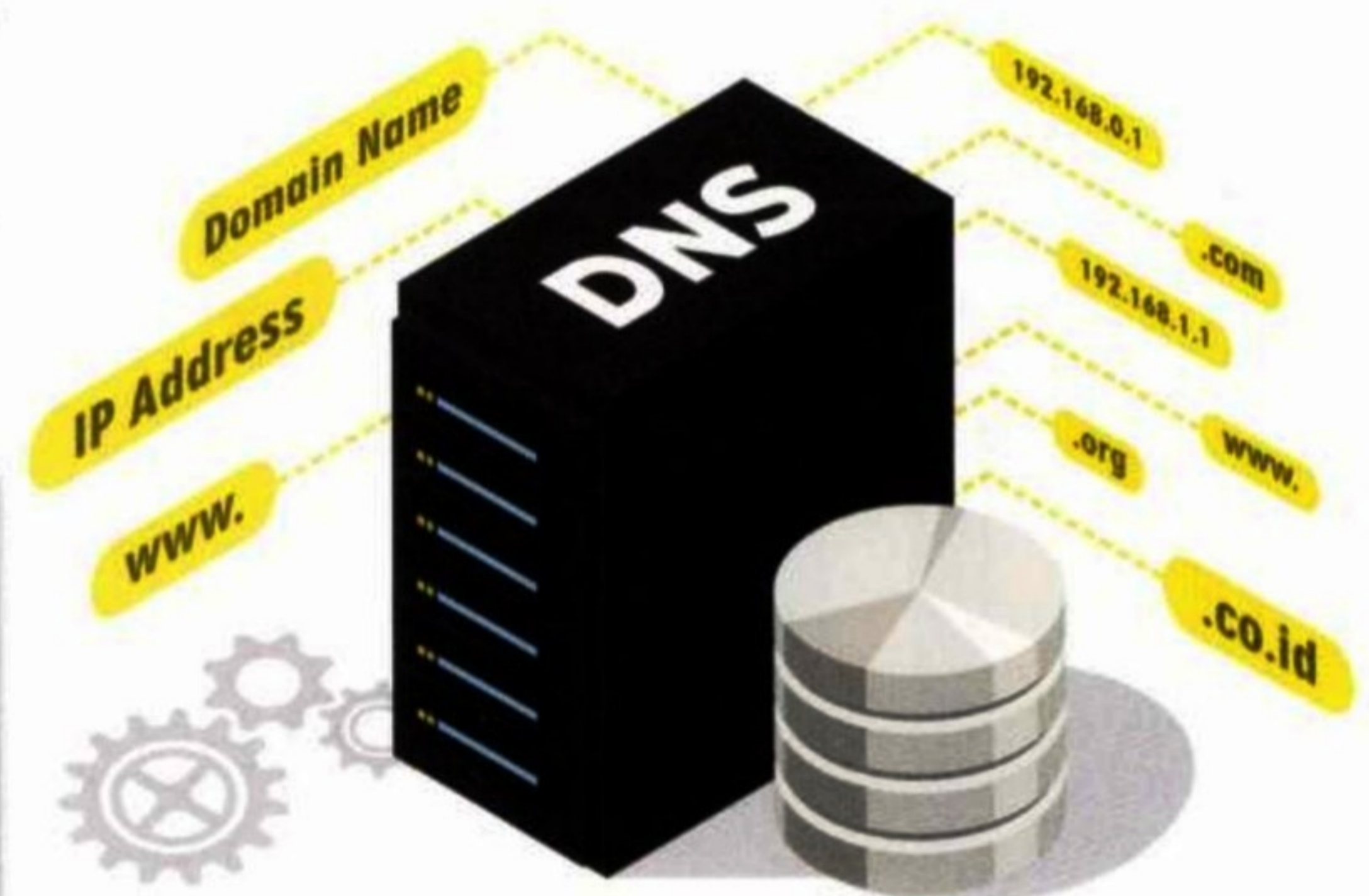
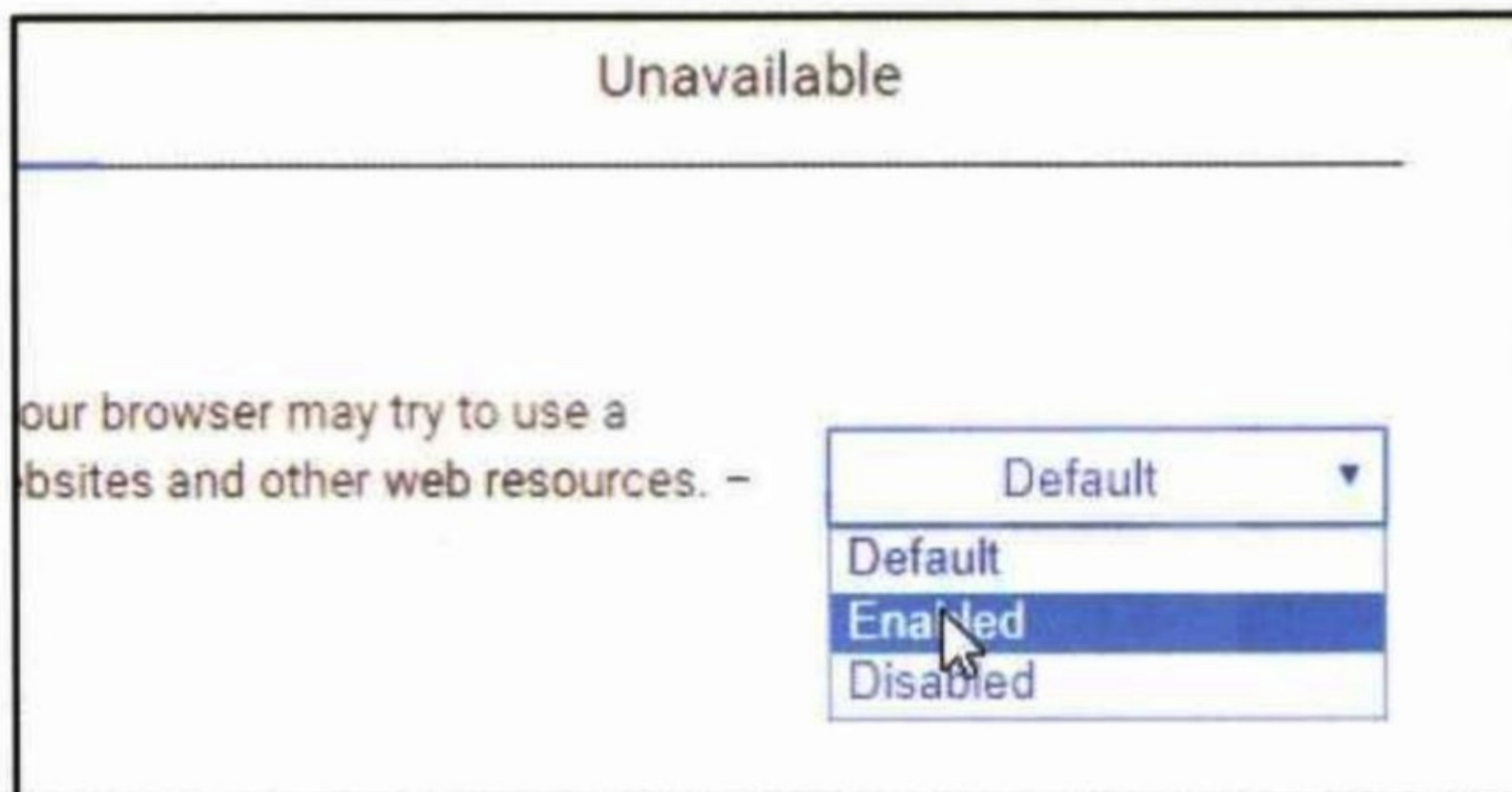
01 > ALLER AU BON ENDROIT

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



02 > MODIFIER VOS PARAMÈTRES

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



VÉRIFIEZ LE CHIFFREMENT



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

OpenDNS

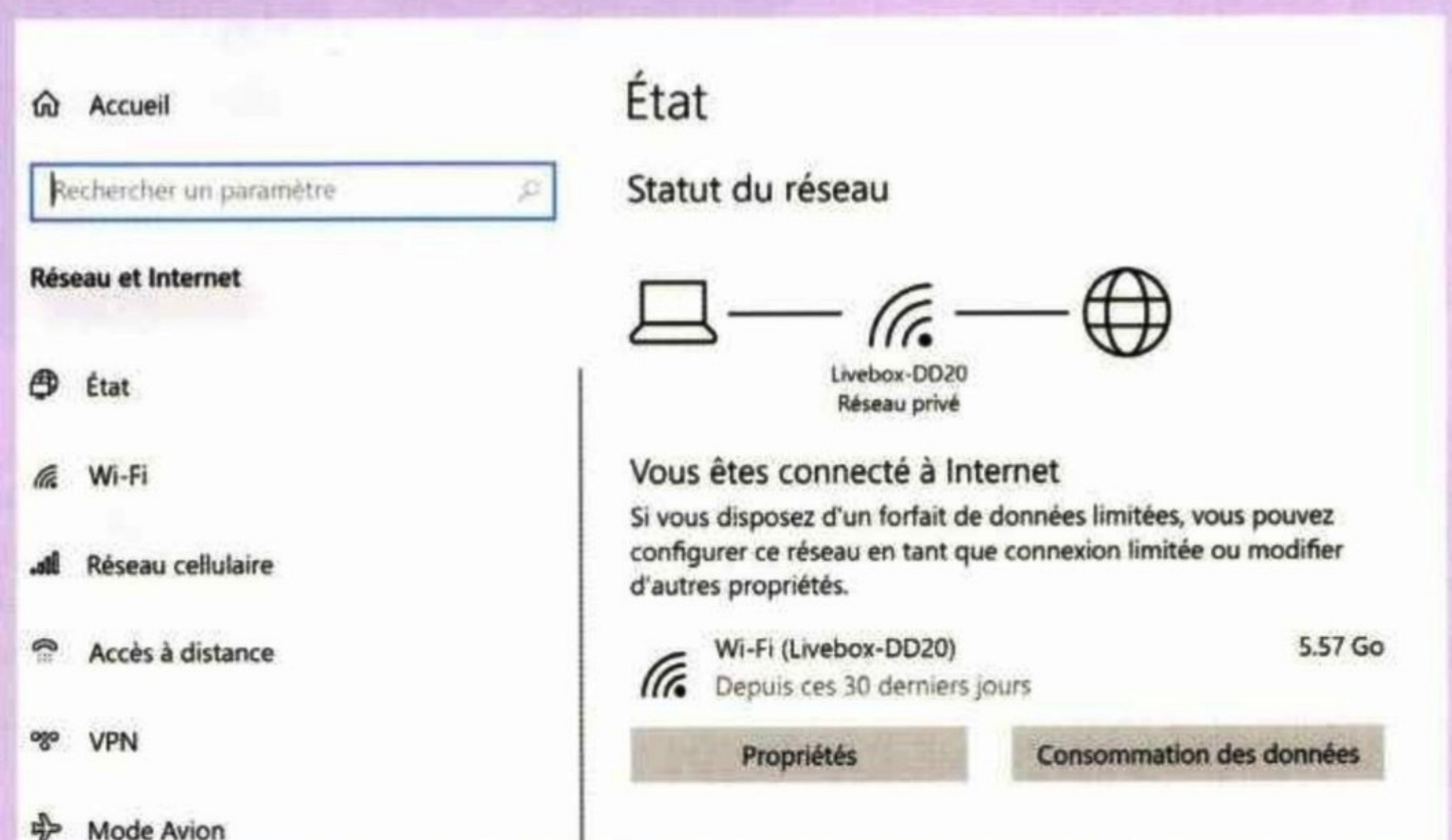
208.67.222.222
208.67.220.220

Google Public DNS

8.8.8.8
8.8.4.4

Cloudflare

1.1.1.1
1.0.0.1





LANTERN POUR VOIR PLUS LOIN



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

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

COMMENT FONCTIONNE LANTERN ?

Lantern est développée par une équipe de petits malins qui n'aiment rien tant que contourner la censure et les

pare-feu. Quand une technique ne fonctionne pas, ils en cherchent une nouvelle. Et ils mettent régulièrement leur système à jour : la dernière version est sortie en décembre dernier et permet maintenant de partager des fichiers sur son réseau interne en prime. Votre trafic est quant à lui chiffré et il n'enregistre aucune de vos informations. Mieux, ils ont décidé de ne pas collaborer avec les organismes d'application de la loi. Ce qui est surtout intéressant dans les pays en



tension : en mars 2022, des internautes russes ont reconnu utiliser Lantern pour contourner les blocages d'internet dans leur pays.

LES LIMITES DE LANTERN

Avec Lantern, vous croyez voir la lumière au bout du chemin. Mais attention, il a surtout pour but de vous permettre un accès rapide et sans limites aux sites que vous souhaitez consulter. Ce n'est pas un outil d'anonymisation pour autant : si la protection de votre identité est votre préoccupation principale, vous auriez plus intérêt à utiliser Tor.

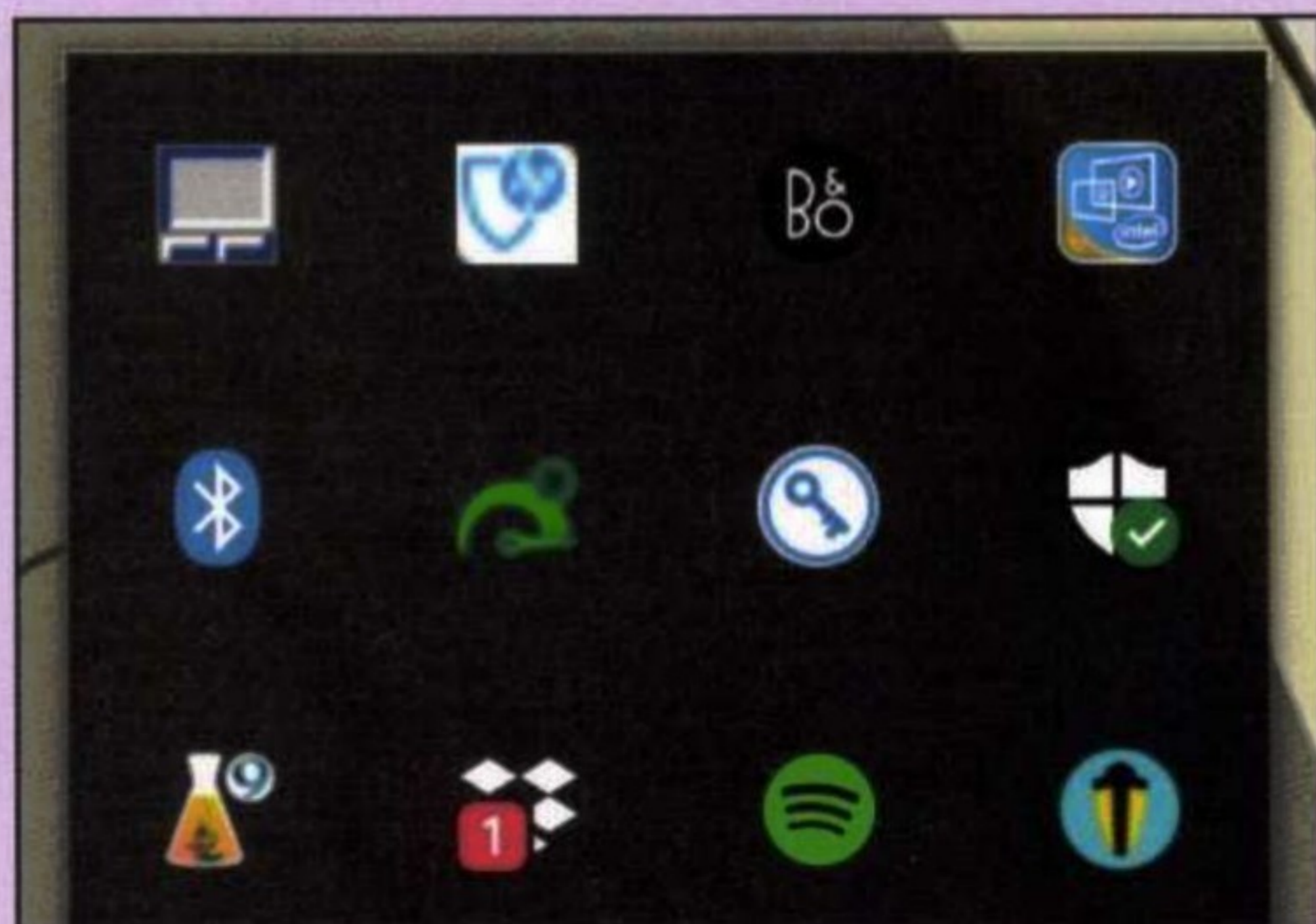
Par ailleurs, comme le nombre d'utilisateurs est en constante augmentation (étonnant, non, avec les lois de censure qui se durcissent partout dans le monde ?), ils ont été obligés de limiter la bande passante à 500 Mo/mois dans leur version gratuite. Au-delà, la connexion est ralentie et l'application vous suggère gentiment de vous renseigner sur sa version payante (à 32 \$ pour un an ou 48 \$ pour deux ans).

Ce n'est pas vous qui êtes anonyme, mais le contenu que vous recherchez, consultez et partagez. Les blocages anti-censure sont également contournés.

7 ASTUCES POUR BIEN COMMENCER AVEC LANTERN

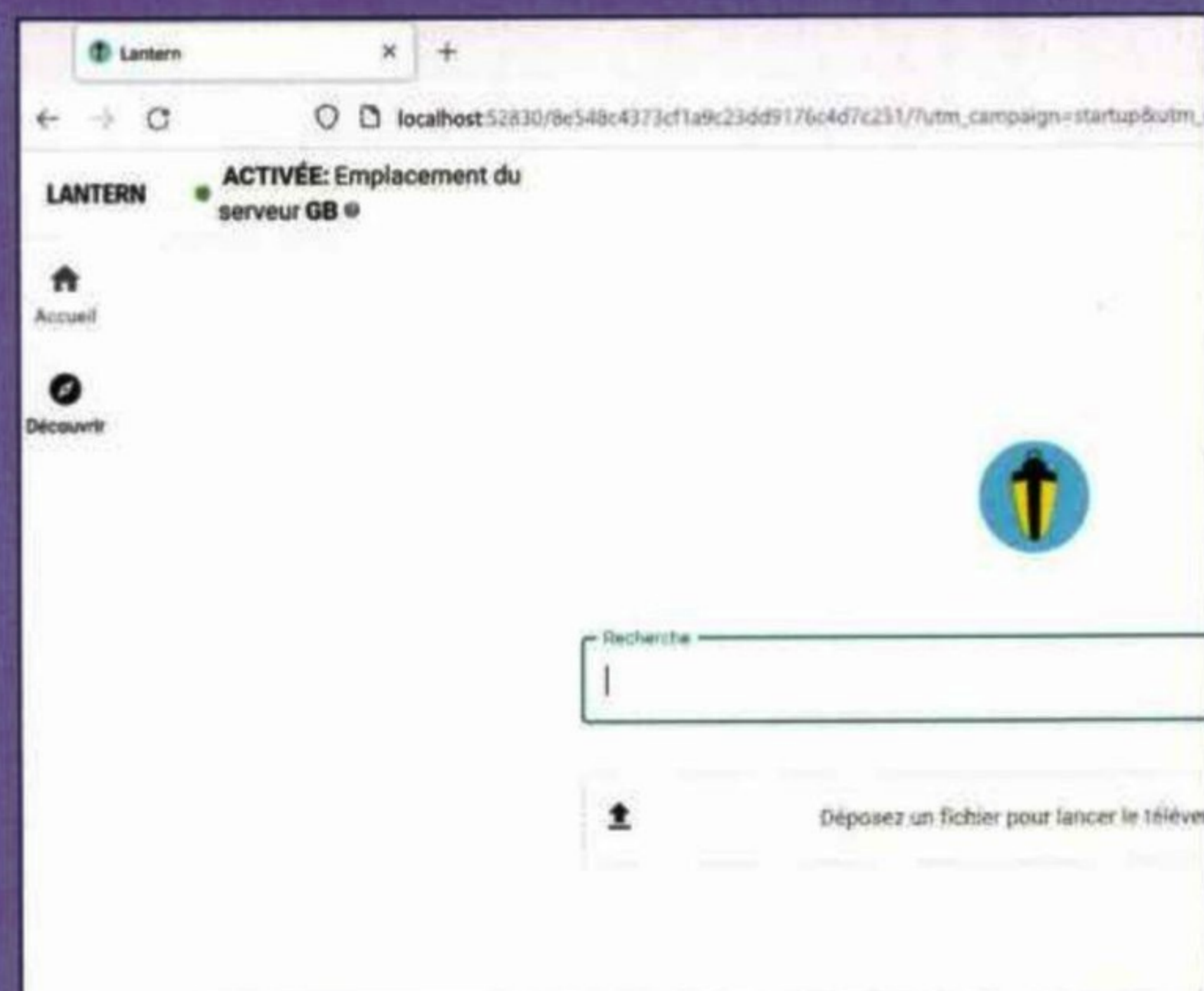
SAVOIR QUE LANTERN FONCTIONNE

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



SE DÉCONNECTER

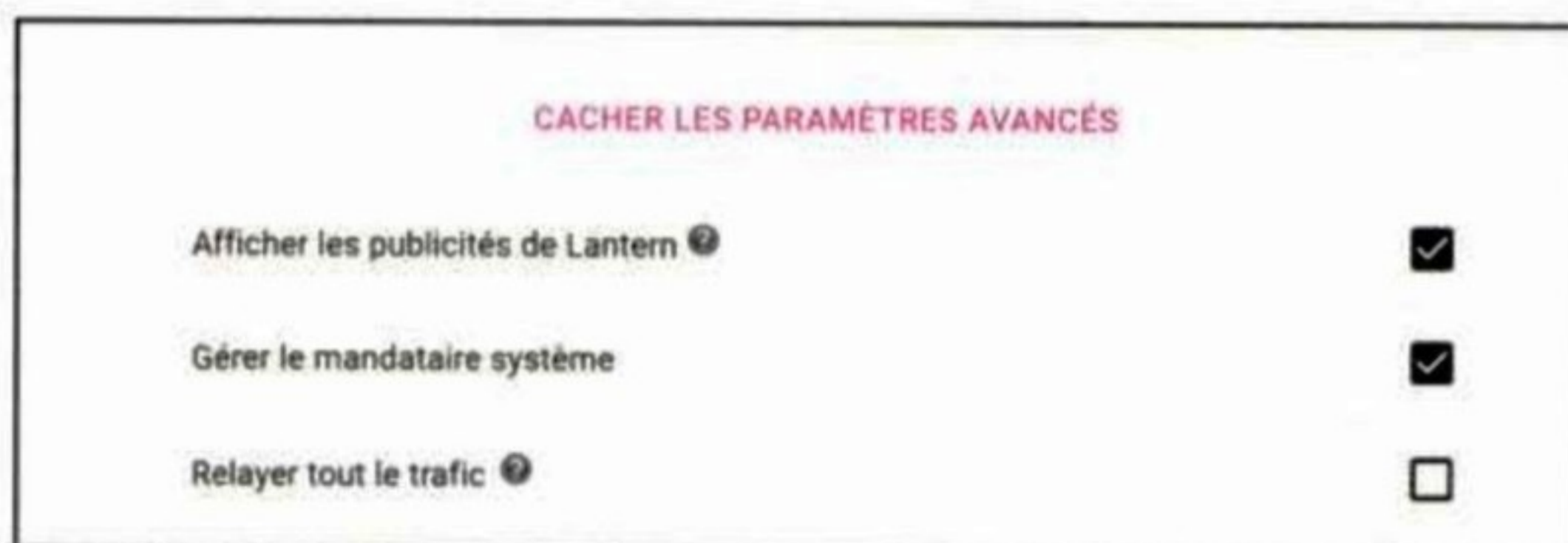
En allant sur Lantern, vous verrez apparaître l'emplacement du serveur utilisé pour votre connexion. Un rond vert avec « Activée » apparaît. Cliquez dessus pour que la connexion soit désactivée.





SÉLECTIONNER LE TRAFIC RELAYÉ

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



DÉCOUVRIR

Quand vous allez sur le menu de gauche et cliquez sur **Découvrir**, vous atterrissez dans une page qui ressemble à celle de n'importe quel moteur de



recherche. Sauf que les seuls résultats affichés du côté des vidéos, images et sons seront ceux des documents téléversés par les utilisateurs de Lantern.

CHOISIR LES PUBLICITÉS

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



TÉLÉVERSER UN FICHER

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



ACCÉDER À UN SITE BLOQUÉ

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



**LES JEUNES,
ON LEUR FABRIQUE
DES VÊTEMENTS
PAS CHERS ET
AU LIEU DE DIRE
MERCI, ILS LUTTENT
CONTRE LE TRAVAIL
DES ENFANTS.**



BIENVENUE AUX IDÉALISTES

**ON SE BAT ENSEMBLE,
ON GAGNE ENSEMBLE.**

**AMNESTY
INTERNATIONAL**





COMMENT DÉTECTER UNE CAMÉRA DE SURVEILLANCE ?

Aujourd'hui, les caméras de surveillance se cachent partout... et parfois de façon illégale. Et si vous appreniez à les repérer ? On va vous donner un coup de pouce pour y arriver.



Plus besoin d'être un espion ou d'aller dans un magasin spécialisé pour installer une caméra cachée chez soi. Grâce à la vente en ligne et aux caméras de plus en plus petites, tout le monde peut en dissimuler une dans les moindres recoins de son habitation. Une bonne chose si vous êtes celui qui filme. Un peu moins si vous êtes filmé sans le savoir...

Et c'est ce qui arrive à de plus en plus de personnes. Pas seulement des nounous ou des femmes de ménage surveillées pendant leur travail, mais aussi juste des personnes qui réservent un logement chez un particulier pour y passer la nuit. Dans ces circonstances, avouez qu'il est assez désagréable d'apprendre que vous êtes devenu la vedette d'un film amateur pour lequel vous n'avez

pas signé. Heureusement, vous pouvez vous en protéger !

UNE APPLI QUI REPÈRE LES CAMÉRAS

Fing est une application pour Android ou iOS qui détecte la présence d'appareils électroniques connectés. Comme cette petite caméra justement cachée dans l'alarme incendie, par exemple. L'application fait tout le travail pour vous et vous fournit même les détails techniques de ces appareils. C'est la solution la plus efficace dans cette situation, même si vous pouvez aussi chercher des lumières infrarouges via l'appareil photo de votre smartphone ou encore scanner les réseaux wifi existants pour vérifier que certains d'entre eux ne se présentent pas sous des noms de produits plutôt que sous celui d'une box.



ÉTUDIER SON ENVIRONNEMENT

01 > SCANNER LA PIÈCE

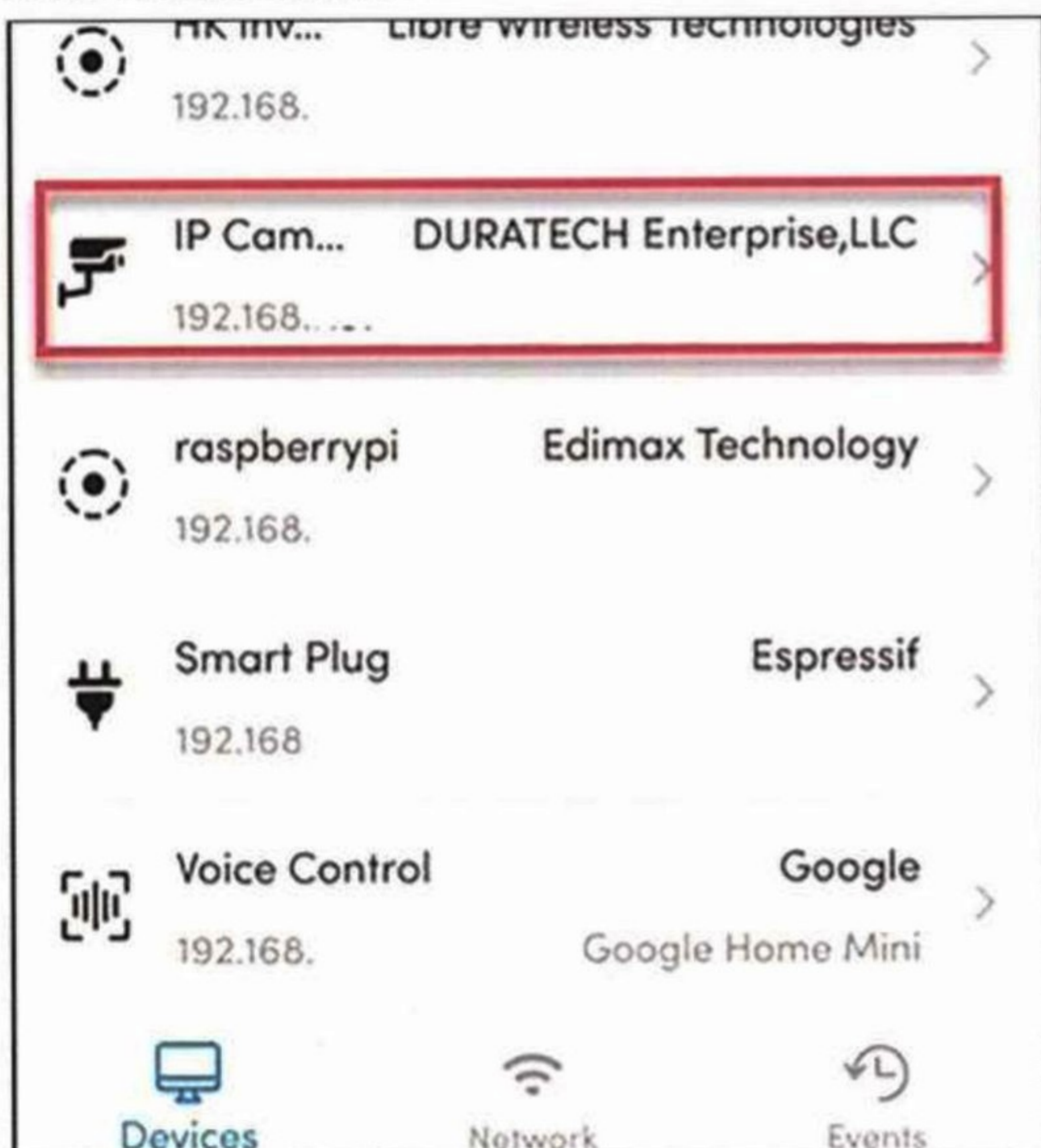
Sur l'application, allez sur **Aperçu** puis sur **Voir les appareils**. Après un petit scan de la pièce, vous verrez apparaître une liste d'appareils avec leurs fonctions. Vous devriez y repérer au minimum votre propre smartphone, avec un logo qui permet de le reconnaître.

**03** > CHERCHER LES PORTS OUVERTS

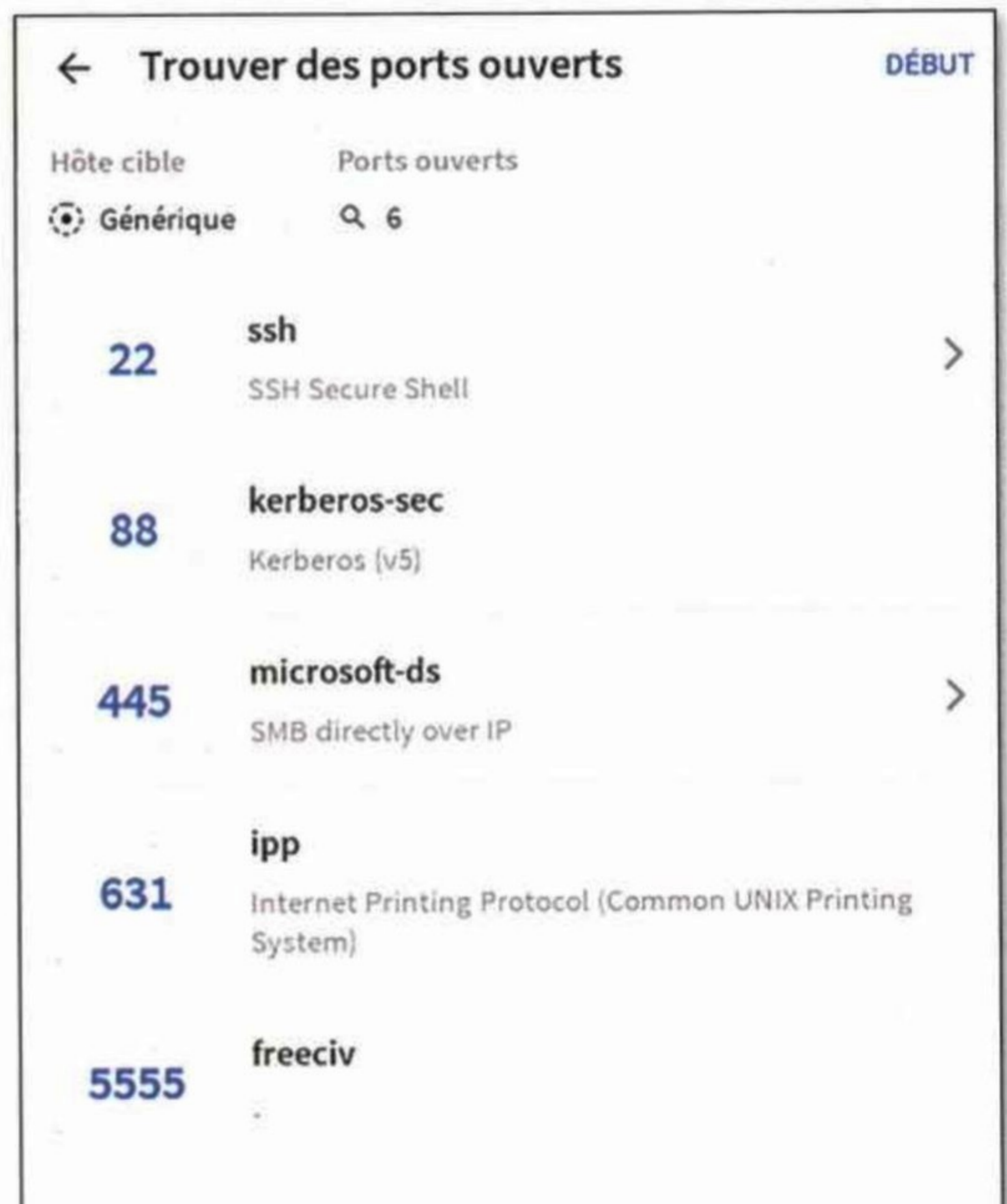
Dans la liste des appareils, notez l'adresse IP de ceux qui vous semblent suspects. Allez sur **Outils** puis sur **Trouver des ports ouverts**. Dans la fenêtre qui s'ouvre, entrez une adresse IP puis cliquez sur le bouton **Trouver des ports ouverts**.

**02** > CHERCHER LA CAMÉRA

Chaque appareil connecté au réseau apparaît avec son nom et un logo qui permet de l'identifier. Les caméras sont donc repérables très facilement. Il est cependant possible que certains d'entre eux vous semblent suspects sans que vous ne compreniez ce que c'est. Passez alors à l'étape suivante.

**04** > ÉTUDIER LA LISTE

Dans la liste des ports ouverts, cherchez si vous obtenez un résultat en RTSP ou RTMP, qui sont couramment utilisés pour les flux de vidéo en direct. Vérifiez aussi les liens qui commencent par HTTP, qui pourraient signaler une diffusion (à vérifier alors directement dans votre navigateur).





LISEZ vos MAILS DANS UNE APPLICATION OPEN SOURCE

Toujours plus de sécurité pour vos mails ? C'est la promesse de FairEmail. L'application centralise toutes vos boîtes mail en laissant de côté ce qui pourrait vous nuire.

Un peu de justice dans ce monde numérique. Voilà comment se positionne FairEmail, une application open source qui prend soin de tous vos petits messages. La configuration de base est rapide dans une interface entièrement traduite en français. Pour les experts, il est toujours possible de jouer avec les règles : tout est modifiable.

POURQUOI ÇA PEUT VOUS INTÉRESSER ?

Le positionnement de FairEmail est clair : aucune de vos données n'est sauvegardée. Vous constaterez d'ailleurs lors de votre inscription que vous ne rentrerez pas vos mots de passe directement dans l'application.

Par ailleurs, les emails sont reformatés pour vous éviter le tracking lié aux publicités. Les messages apparaissent sans images, et avec une mise en page simplifiée, mais c'est pour mieux vous protéger. Et vous devrez toujours confirmer avant de cliquer sur un lien. Sécurité, on vous dit !

DES PETITS PLUS

L'appli est conçue pour vous aider à économiser de la batterie, comme de la consommation de données. Sans publicité, rapide et efficace, sa version gratuite est



déjà très complète. Vous pourrez même décider de ne pas recevoir de messages certains jours de la semaine (vive la déconnexion numérique) ou tester les options de traduction.

Quant à la version pro, vous pourriez apprécier sa synchronisation avec votre agenda, des techniques supplémentaires pour trier vos messages, des envois différés (pour un prix annuel de 6,99 €).



PRÉPAREZ VOTRE NOUVELLE BOÎTE MAIL

Un assistant vous guide tout au long des étapes pour configurer FairEmail. En quelques clics, tout sera prêt à fonctionner.

01 > TÉLÉCHARGER

Après avoir téléchargé et installé l'application sur votre smartphone, vous arriverez sur un écran d'accueil. Ce dernier vous présente les spécificités de FairEmail, via un contrat de licence réduit, qu'il vous faut accepter.

FairEmail est une application de messagerie open source centrée sur la confidentialité et la sécurité. C'est pourquoi certaines fonctionnalités peuvent être différentes de ce à quoi vous êtes habitué.

Par exemple, les messages sont reformatés par défaut pour supprimer tout élément dangereux ainsi qu'améliorer la lisibilité et l'ouverture des liens doit être confirmée pour des raisons de sécurité. Les deux options peuvent être désactivées si souhaité.

[Contrat de licence d'utilisateur final](#)

02 > LANCER L'ASSISTANT

La configuration s'effectue en trois étapes. Cliquez sur **Assistant** sur l'écran principal pour rentrer les informations de la boîte mail que vous voulez créer. Vous aurez ensuite à indiquer votre nom et votre adresse mail. Le mot de passe se rentrera directement dans la page du serveur mail correspondant.

Bienvenue

La configuration d'un compte se fait en trois étapes seulement et après cela, vous pouvez envoyer et recevoir des e-mails

Il n'est pas nécessaire de modifier d'autres options

FairEmail a été développé pour vous aider à protéger votre vie privée et représente littéralement des milliers d'heures de travail. Si vous avez des problèmes, veuillez me contacter d'abord pour obtenir de l'aide avant de laisser une mauvaise évaluation. Je serai heureux de vous aider !

FairEmail n'affiche pas de publicités et ne piste pas ou n'analyse pas votre comportement. Bugsnag est utilisé pour les rapports d'erreurs et est désactivé par défaut.

[Politique de confidentialité](#) [Assistance](#)

1 Ajouter ou modifier des comptes

Assistant ?

L'assistant peut être utilisé plusieurs fois pour configurer plusieurs comptes

03 > OPTIMISER L'APPLICATION

Les deux étapes suivantes pour l'installation consistent à cliquer sur **Autoriser** dans le cadre 2 pour accepter que l'application accède aux informations de contact. Et par changer la manière dont l'application utilise la batterie (cadre 3).

FairEmail Paramètres

PRINCIPAL RÉCEPTION ENVOI

2 Accorder les autorisations

Pour accéder aux informations des contacts (facultatif)

✓ Effectué [Autoriser](#)

[Quelles autorisations sont nécessaires et pourquoi ?](#)

[Comment puis-je importer des contacts ?](#)

3 Désactiver les optimisations de la batterie

Pour envoyer et recevoir des e-mails de manière fiable en arrière-plan

✓ Effectué [Gérer](#)

Bien que cela puisse sembler contradictoire, désactiver les optimisations de batterie pour cette

04 > ACCÉDER À VOS DOSSIERS

Pour atteindre les différents dossiers de votre boîte mail, cliquez simplement sur son nom. Ils s'ouvriront alors dans la fenêtre suivante. Sinon, vous verrez simplement apparaître les dossiers principaux, ainsi que différentes options à utiliser en fonction de vos besoins.

Conversations

...ook/dcmelanie (1)

Outlook/dcmelanie

Boîte de réception (1)

Boîte d'envoi

Brouillons (14)

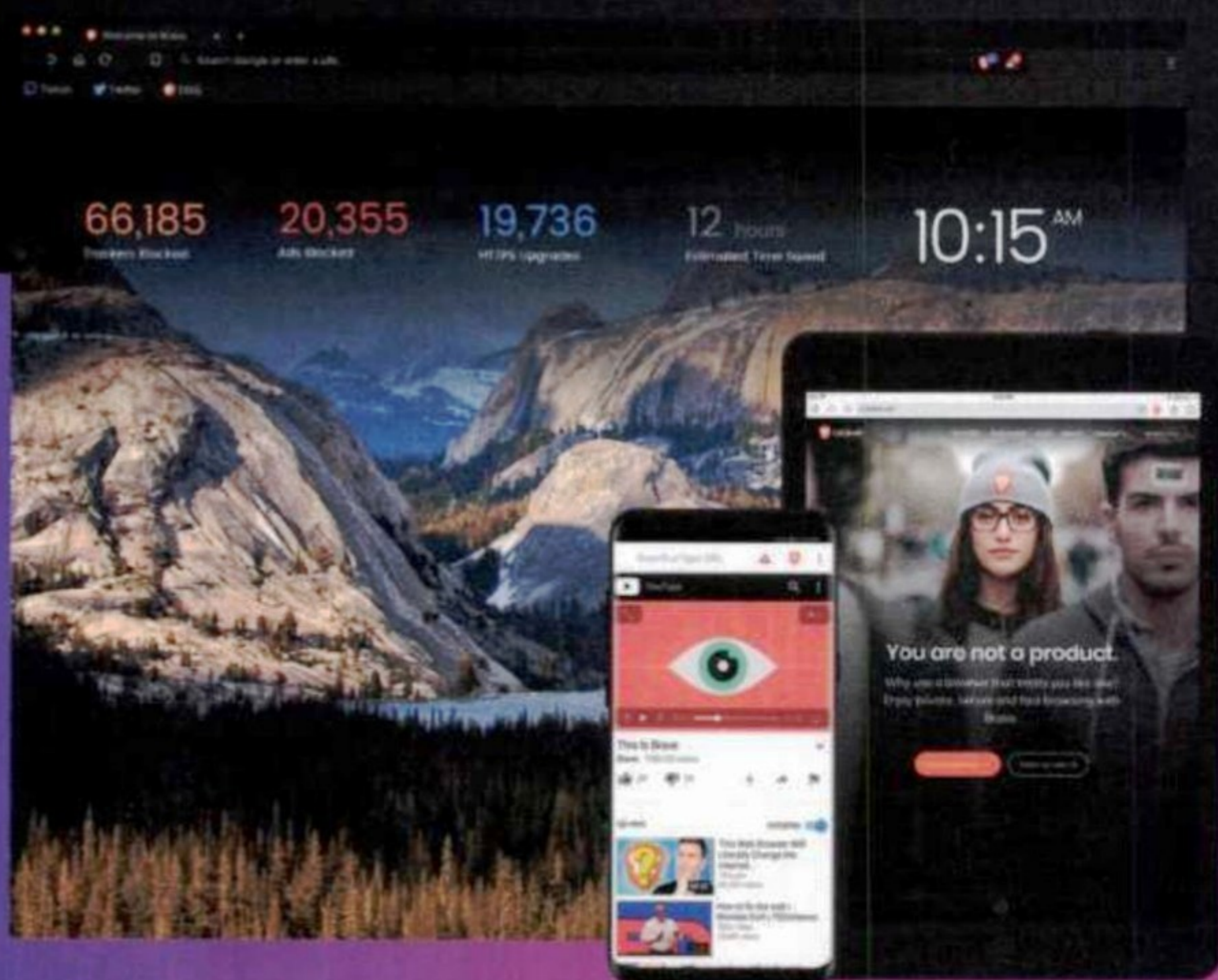
Envoyés

Corbeille (507)

Indésirables (4)



SOYEZ BRAVE : QUITTEZ GOOGLE CHROME !



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

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

EN QUOI EST-IL DIFFÉRENT ?

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

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

BIEN PLUS QU'UN NAVIGATEUR

Par défaut, Brave propose son propre moteur de recherche (toujours dans l'optique du respect de la vie

Même Larry Sanger, cofondateur de Wikipedia, a annoncé abandonner Chrome pour Brave.

ET EN PLUS, IL OFFRE DES CADEAUX !

Brave a décidé de récompenser aussi votre attention (et les créateurs de contenus). Si vous le désirez, et uniquement dans ce cas, vous pouvez regarder des publicités sélectionnées (et respectueuses de votre vie privée), vous obtenez avec Brave des BAT (Basic Attention Token). Quand vous en avez obtenu suffisamment, vous pouvez les échanger contre des cartes-cadeaux, les envoyer à des sites web ou à des créateurs de contenus ou les utiliser comme n'importe quelle autre e-monnaie. Cependant, les sites web ou créateurs de contenus qui veulent recevoir ces récompenses doivent se faire connaître de Brave afin d'obtenir le statut « vérifié ». Et comme Brave n'est pas encore le plus célèbre des navigateurs, tous n'en profitent pas encore.

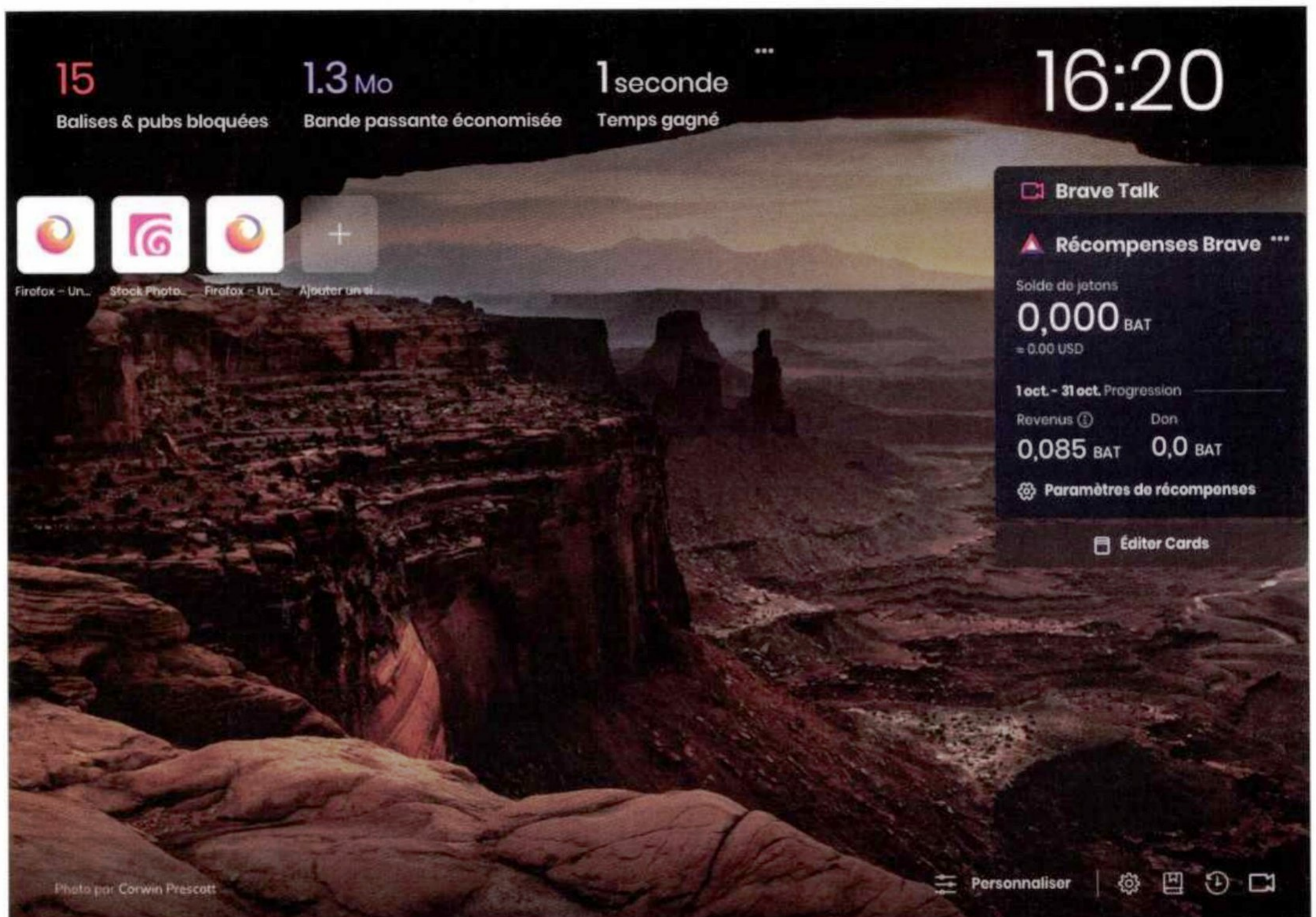


privée de ses utilisateurs). Mais comme la liberté de chacun ne lui fait pas peur, vous pourrez aussi revenir vers Google ou une de ses alternatives.

Brave comporte des outils intéressants, comme Brave Talk, qui permet de passer des vidéos privées illimitées directement depuis le navigateur (parfait pour des visioconférences sans les limites de Zoom. Mais en petits groupes seulement : il faudra payer pour parler à plus de quatre participants). Vous trouverez aussi un fil d'actualité personnalisable, et les listes de lecture (uniquement sur iOS pour le moment) pour pouvoir accéder à vos contenus audio et vidéo depuis n'importe où (et même hors ligne).

D'OÙ VIENT BRAVE ?

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





4 ASTUCES POUR PERSONNALISER VOTRE PAGE D'ACCUEIL

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

Cacher les statistiques

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



Importer vos favoris au lancement

Dès son premier lancement, Brave se propose d'aller récupérer les favoris du navigateur que vous utilisez habituellement. Il vous suffit de choisir le nom du navigateur dans le menu déroulant, puis de cliquer sur **Importer**.



Vous n'aurez aucune autre action à effectuer. Même leur présentation sera préservée.

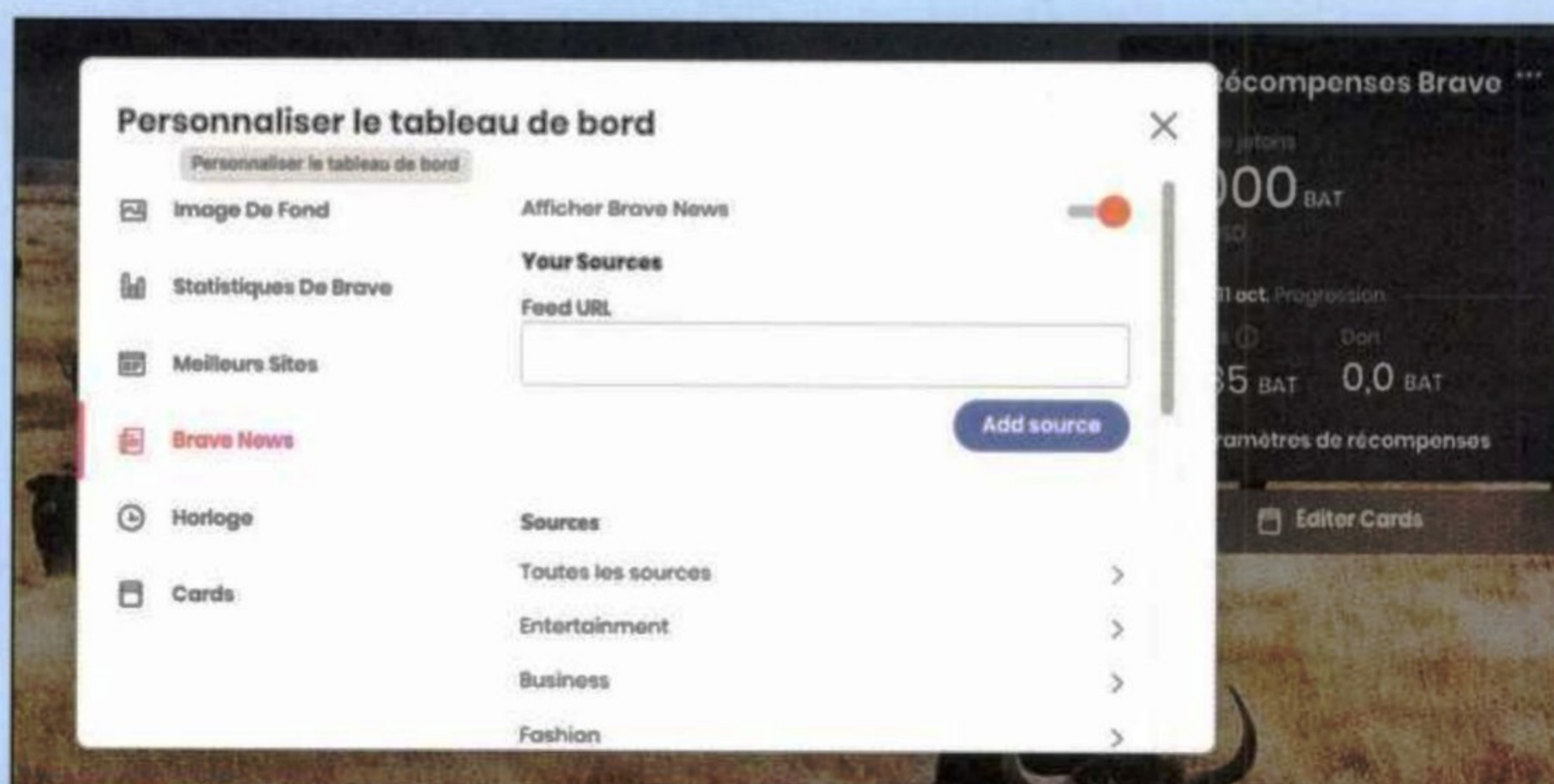
Libérer la fenêtre

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



Suivre l'actualité

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



8 FONCTIONS À ACTIVER

Gérer votre portefeuille

Comme une des grandes différences de Brave repose aussi sur ses jetons de récompense, créer un porte-feuille



à tokens peut être utile si vous n'en possédez pas un. Allez dans **Paramètres**, puis dans **Portefeuille** pour vous laisser guider dans sa création.

Prévoir des listes de lecture

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



Ne plus suivre un média

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

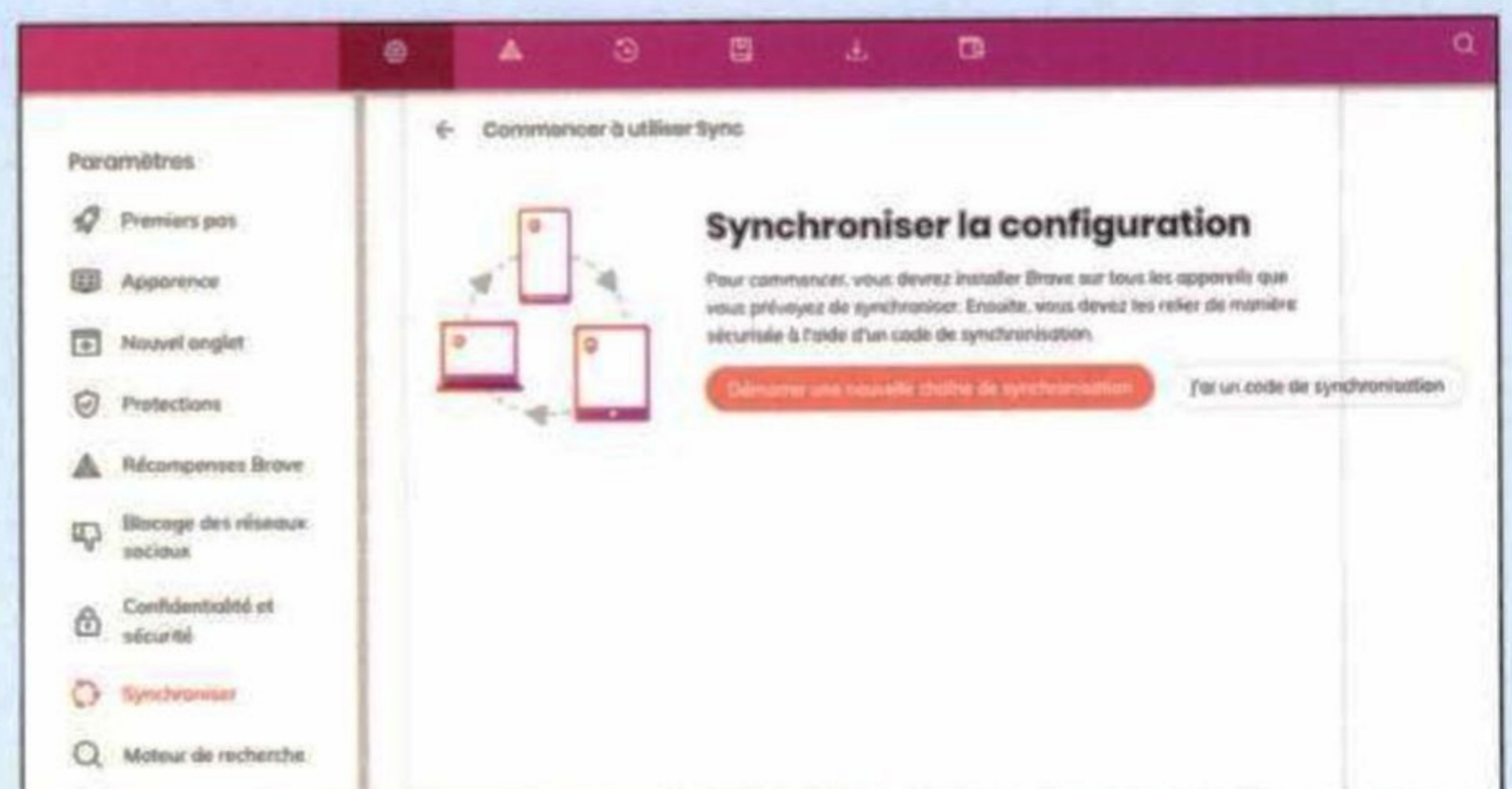


Synchroniser vos appareils

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

Synchroniser le code QR de la chaîne

Sur votre appareil mobile, accédez à Brave Synchronisation dans le panneau Paramètres et cliquez sur le bouton "Numériser le code de synchronisation". Utilisez votre appareil photo pour scanner le code QR ci-dessous. **Considérez ce code comme un mot de passe. Si jamais quelqu'un le découvre, il pourra lire et modifier vos données synchronisées.**

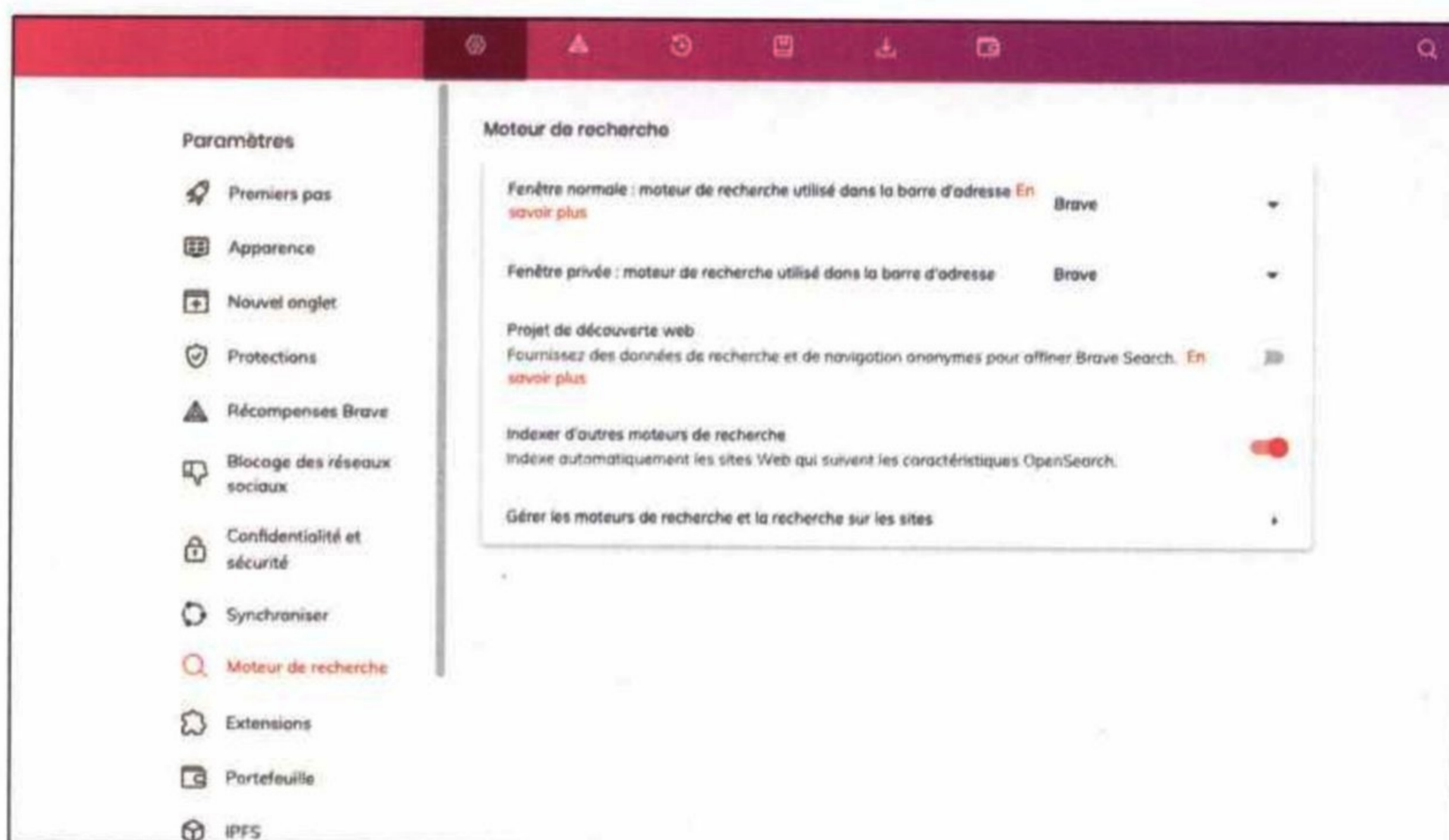




PROTECTION

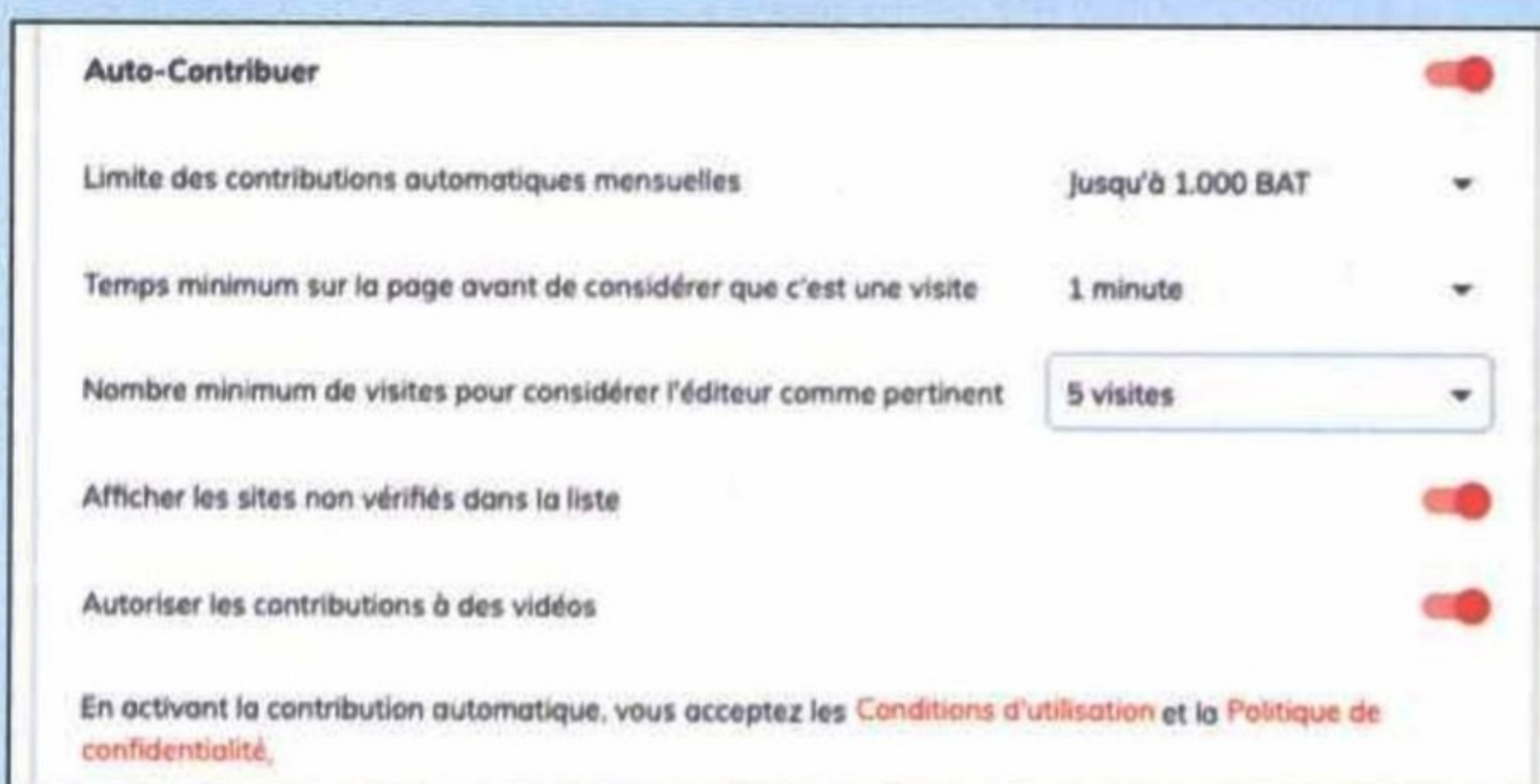
Choisir votre moteur de recherche

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



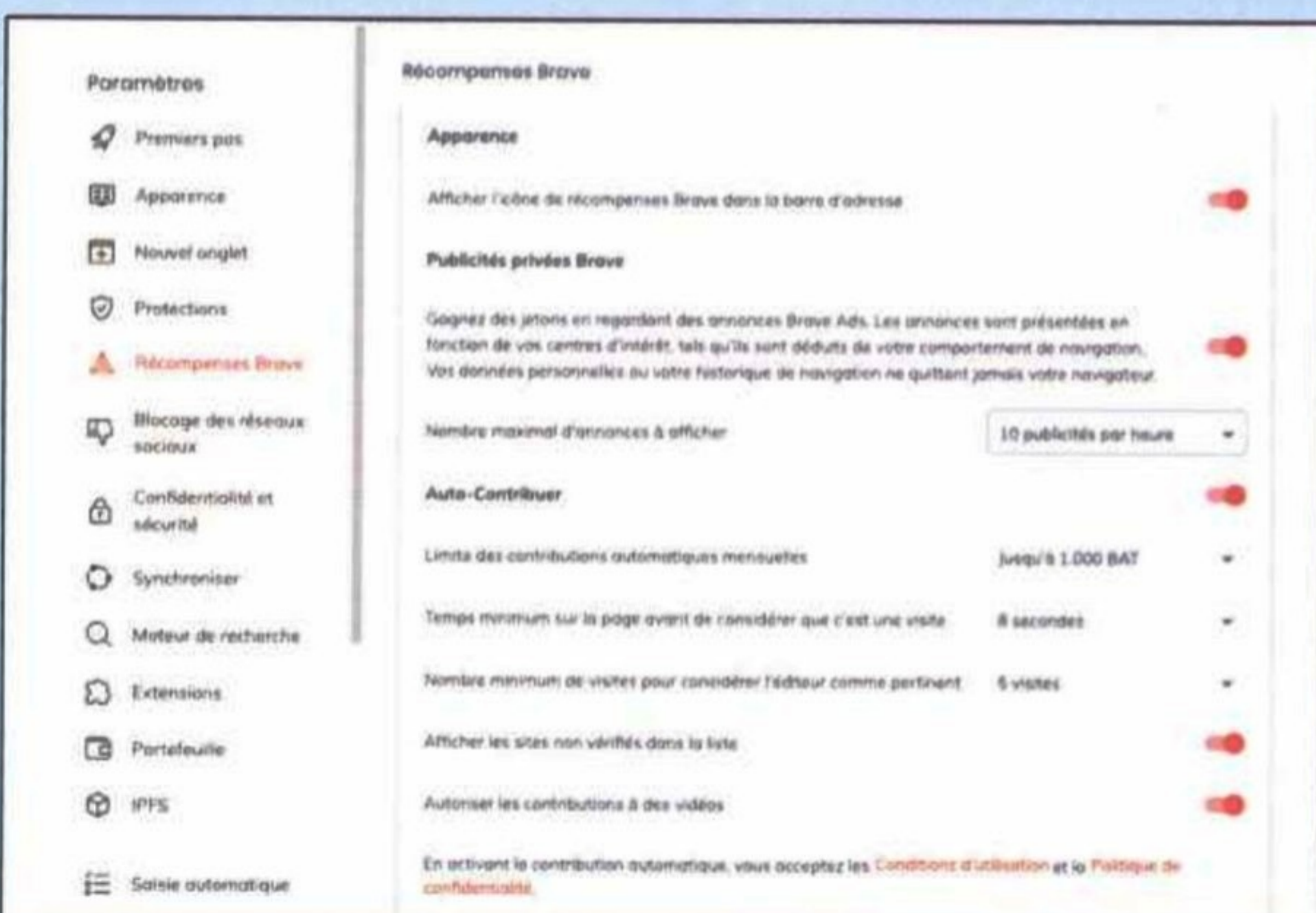
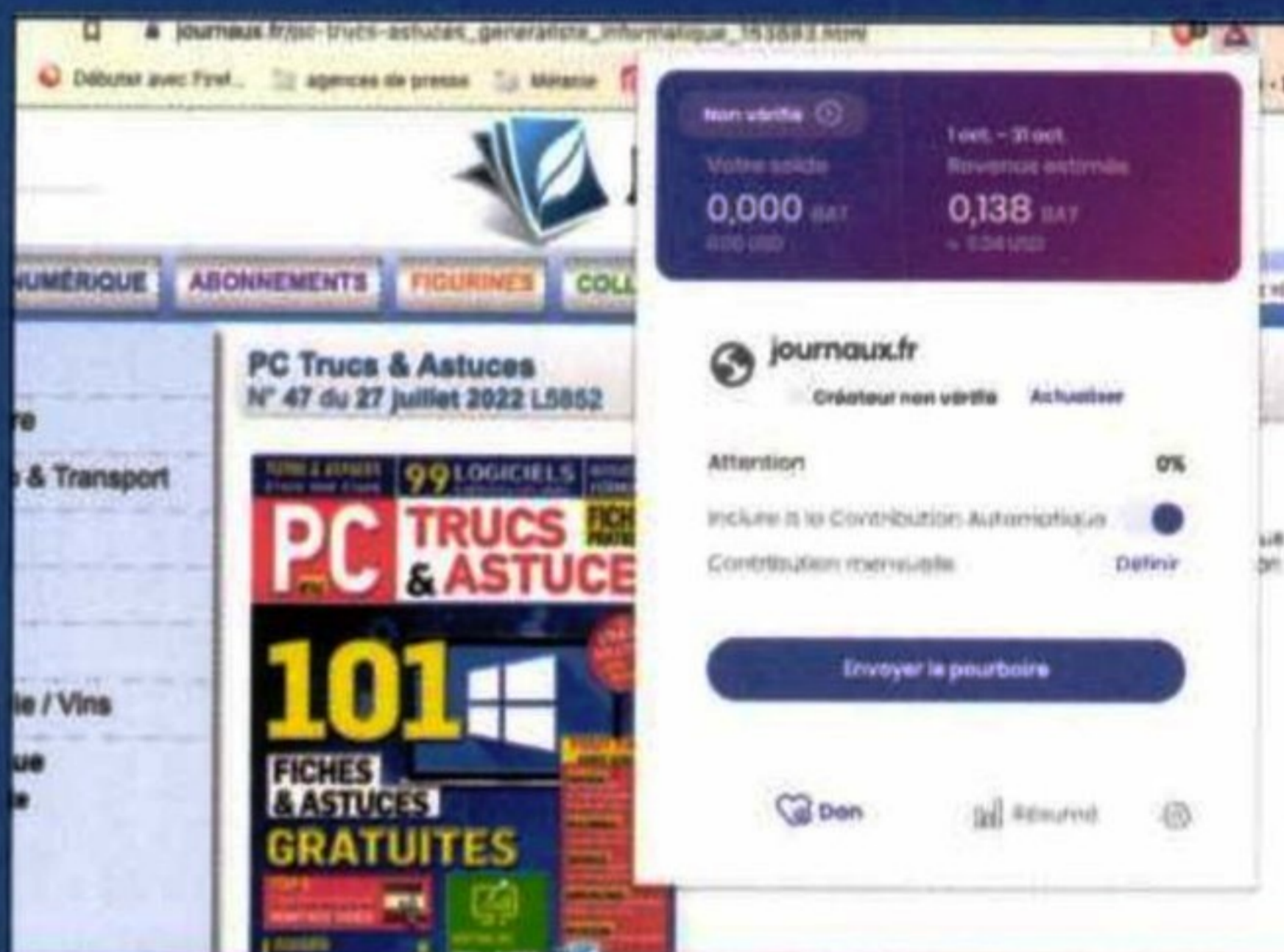
Garder ou partager vos récompenses

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



Envoyer des pourboires

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



Regarder (ou pas) des publicités

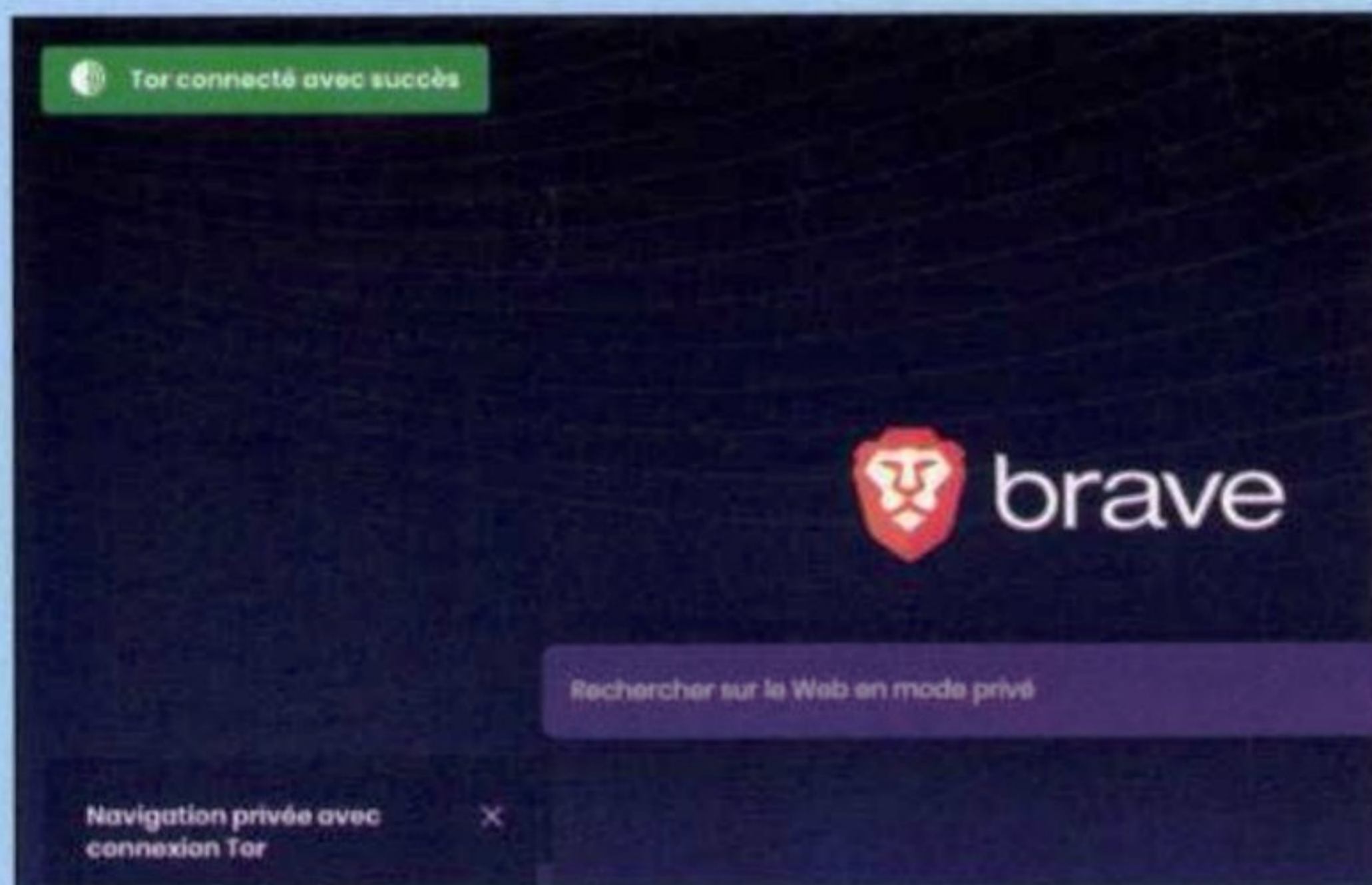
Depuis la page d'accueil ou les **Paramètres**, accédez aux **Récompenses Brave**. Décochez les publicités privées si vous ne voulez plus en voir ou choisissez combien vous êtes prêt à en regarder par heure (jusqu'à 10 maximum).

4 OPTIONS POUR PROTÉGER SA VIE PRIVÉE

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

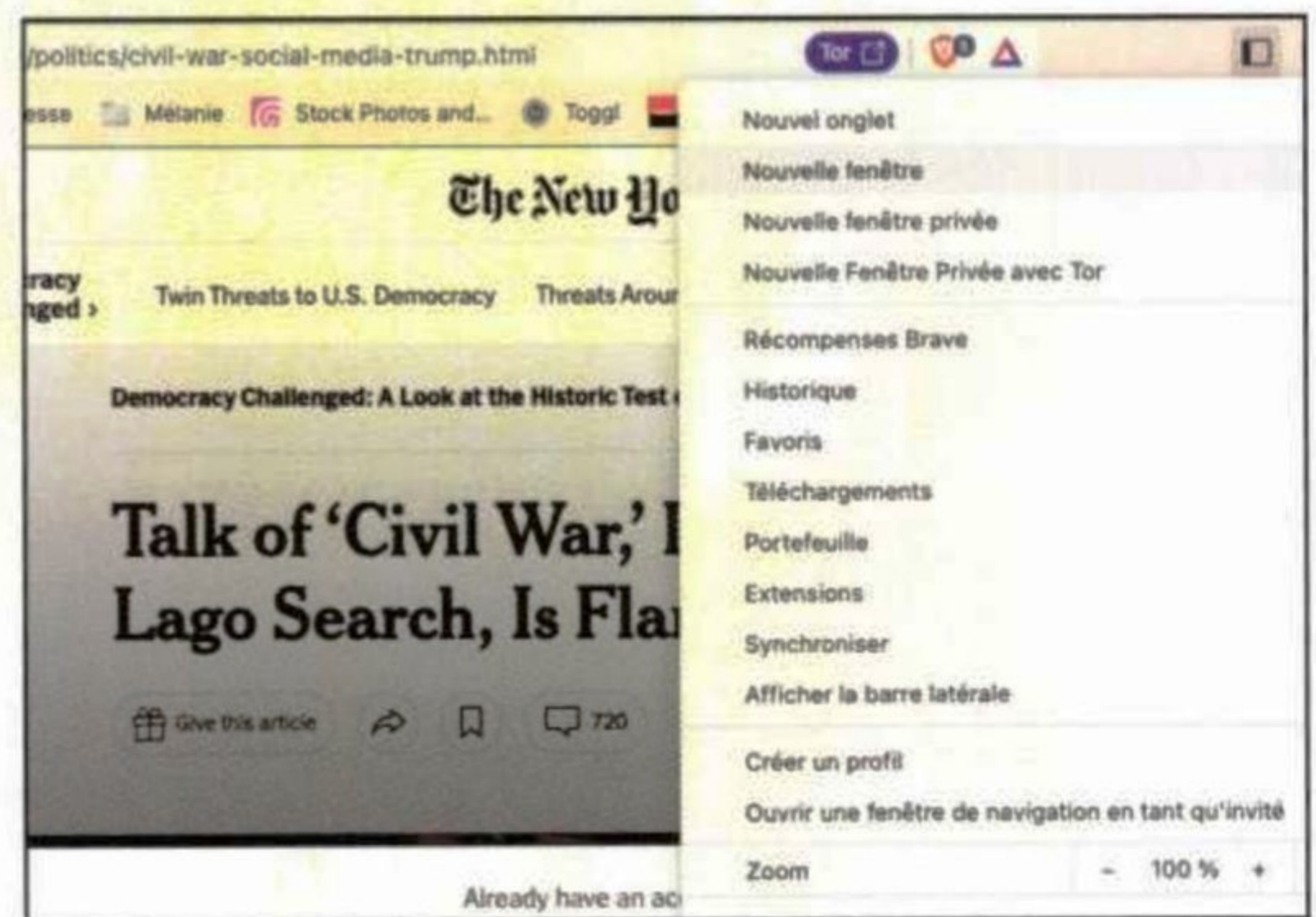
Utiliser Tor

Dans le menu déroulant (à droite de la barre d'adresse), allez sur **Nouvelle fenêtre privée avec Tor**. Votre adresse IP sera alors masquée pour les sites que vous consultez. Certains sites seront peut-être ralentis, mais il sera beaucoup plus difficile pour votre FAI (fournisseur d'accès à Internet) de savoir ce que vous faites.



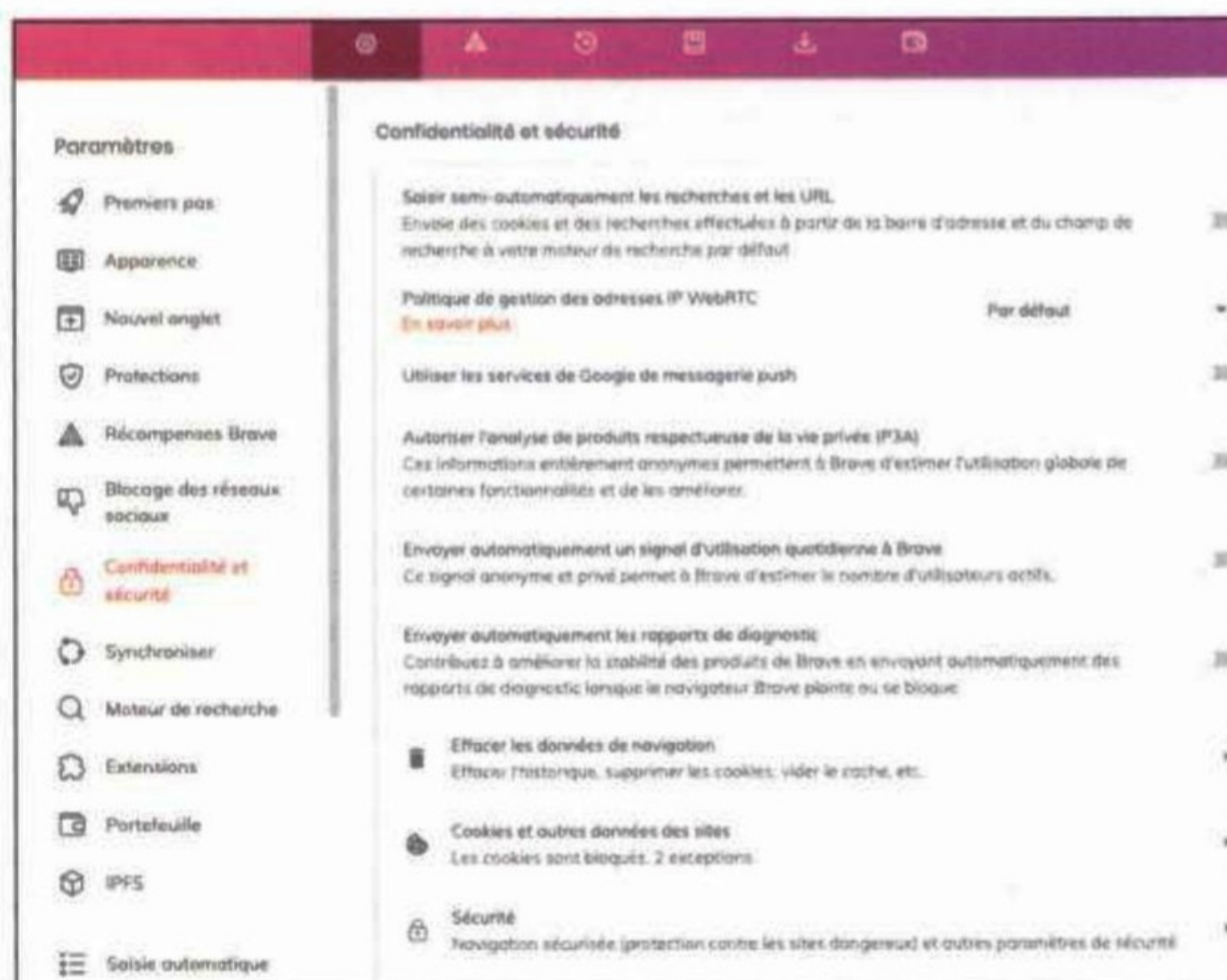
Naviguer en mode privé

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



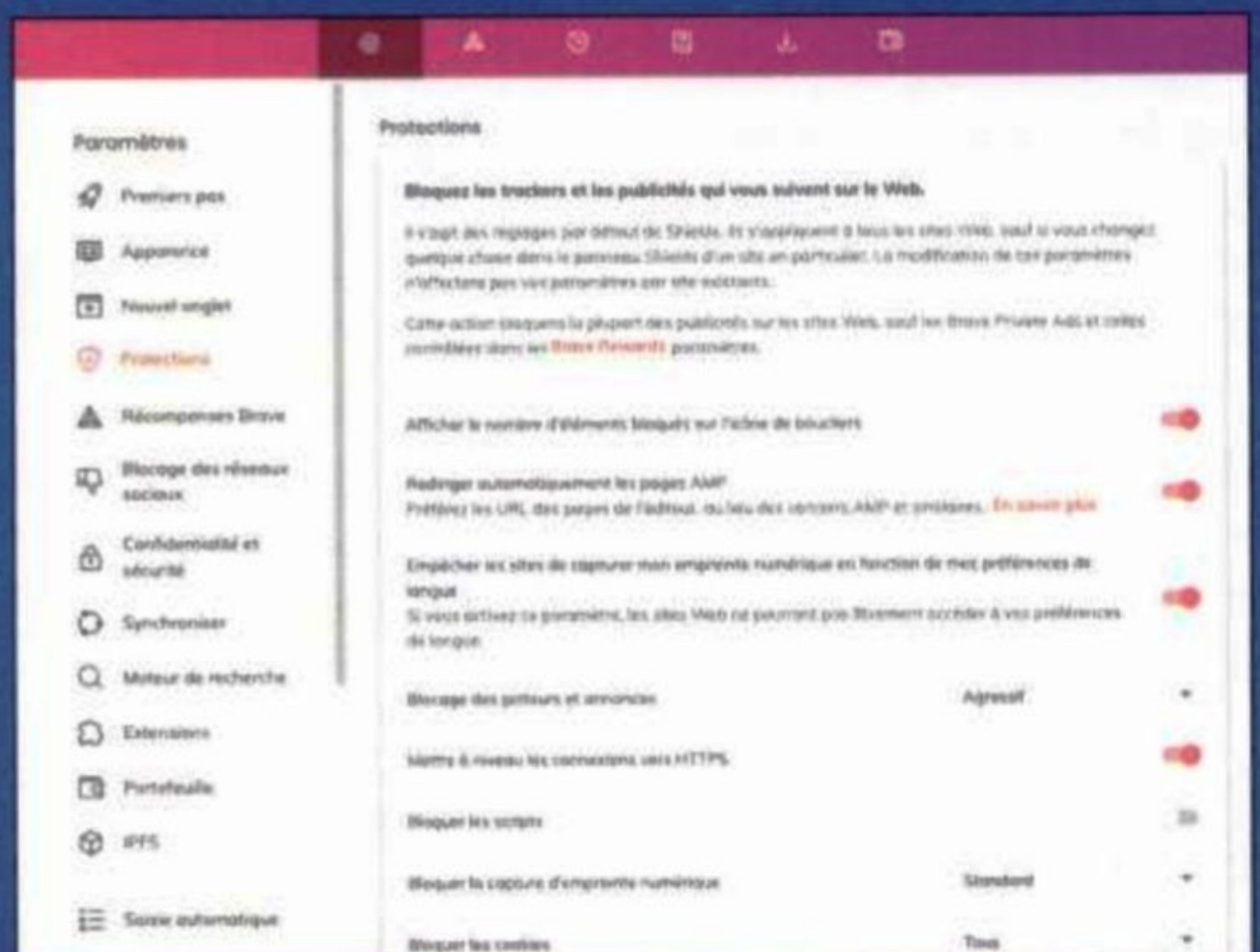
Rester discret

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



Opter pour un maximum de sécurité

Dans les **Paramètres**, allez sur **Protections**. Dans **Blocage des pisteurs et annonces**, choisissez l'option



Agressif. Dans **Bloquer les cookies**, retenez **Tous**. Il est largement conseillé d'activer aussi **Mettre à niveau les connexions vers HTTPS** et **Rediriger automatiquement les pages AMP**.



POUR QUI ?

Pour ceux qui utilisent avidement leur espace cloud

POUR QUOI FAIRE ?

Protéger ses fichiers les plus sensibles

CHIFFREZ VOTRE ESPACE CLOUD AVEC BOXCRYPTOR

Si vous sauvegardez des documents confidentiels dans le cloud, verrouillez-les avec l'outil gratuit BoxCryptor.



On stocke un peu tout et n'importe quoi dans le cloud. Des photos, des documents sans grand intérêt comme des factures, des fichiers texte, etc. Et l'on accorde notre confiance aux géants du cloud comme Microsoft, Google ou encore Dropbox pour garder un œil dessus. Mais qu'advierait-il s'ils se faisaient pirater ? Apple se souvient encore avec amertume des photos volées de stars sur iCloud en 2014. Pour éviter ce genre de désagrément, la solution consiste à chiffrer ses données. Ainsi, personne d'autre que vous, ou celui à qui vous aurez donné les droits d'accès, ne pourra ouvrir votre fichier. Et sur ce terrain, vous pouvez vous en remettre à BoxCryptor.

UN SEUL SERVICE DE CLOUD DANS SA VERSION GRATUITE

Ce logiciel, gratuit dans sa version de base, prend l'apparence d'un lecteur virtuel dans Windows. Il est en lien direct avec un espace cloud à choisir parmi plus d'une trentaine de fournisseurs (il faudra s'offrir la version Personal à 36 € / an pour cumuler les services). Il chiffre à la volée ce que vous y déposez suivant un cryptage AES 256. Si bien que vos données se trouvent

verrouillées sur votre compte cloud (le nom des fichiers est même brouillé avec la version Personal) sans que vous n'ayez à vous en occuper.

Mais attention : si vous oubliez vos identifiants, c'est fichu. BoxCryptor ne saura pas déchiffrer vos fichiers. Avec la version gratuite utilisée dans ce pas à pas, vous disposez également d'un accès depuis un second appareil (le nombre devient illimité avec la version payante). Pratique pour accéder à tous ses fichiers sensibles même depuis un smartphone.

Attention, si vous perdez vos identifiants BoxCryptor, vous ne pourrez plus retrouver vos fichiers en clair sur votre cloud préféré!



CHIFFRER GOOGLE DRIVE AVEC BOXCRYPTOR

PRATIQUE



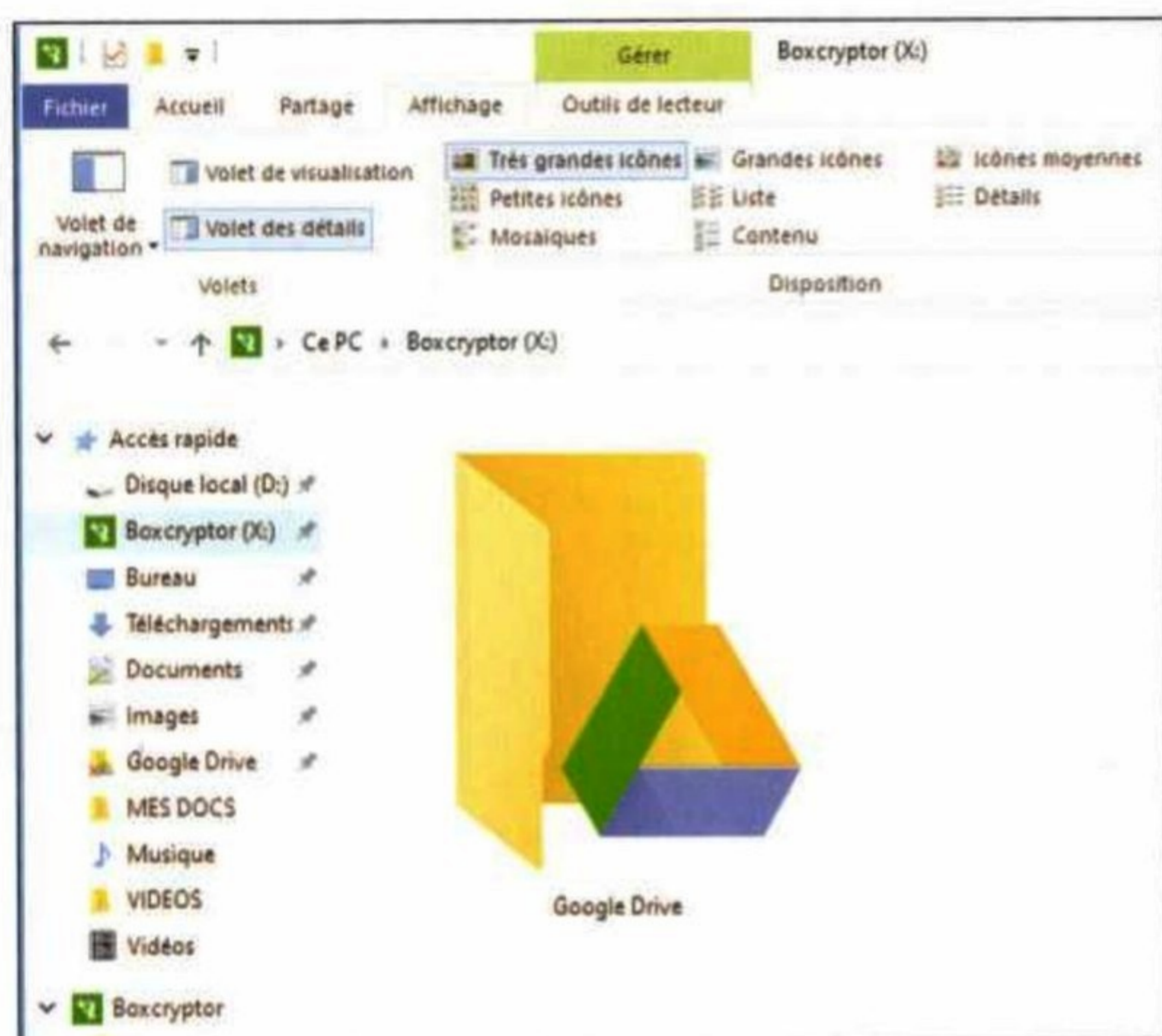
01 > INSTALLER BOXCRYPTOR

Créez un compte (gratuit) sur le site de Boxcryptor et cliquez sur le lien **Je souhaite conserver l'offre gratuite** pour accéder au téléchargement (n'oubliez pas de valider votre inscription d'un clic sur le lien reçu par mail). Lancez l'installation puis saisissez vos identifiants.



02 > ACCÉDER À GOOGLE DRIVE

Fermez la fenêtre d'aide de Boxcryptor. Puis ouvrez l'**Explorateur de fichiers** : un nouveau lecteur **Boxcryptor** y apparaît. Ouvrez-le depuis la colonne de gauche, puis allez dans le dossier **Google Drive** qu'il contient (s'il n'apparaît pas, voyez l'encadré ci-contre). Tous les fichiers qui se trouvent sur votre espace en ligne s'affichent.



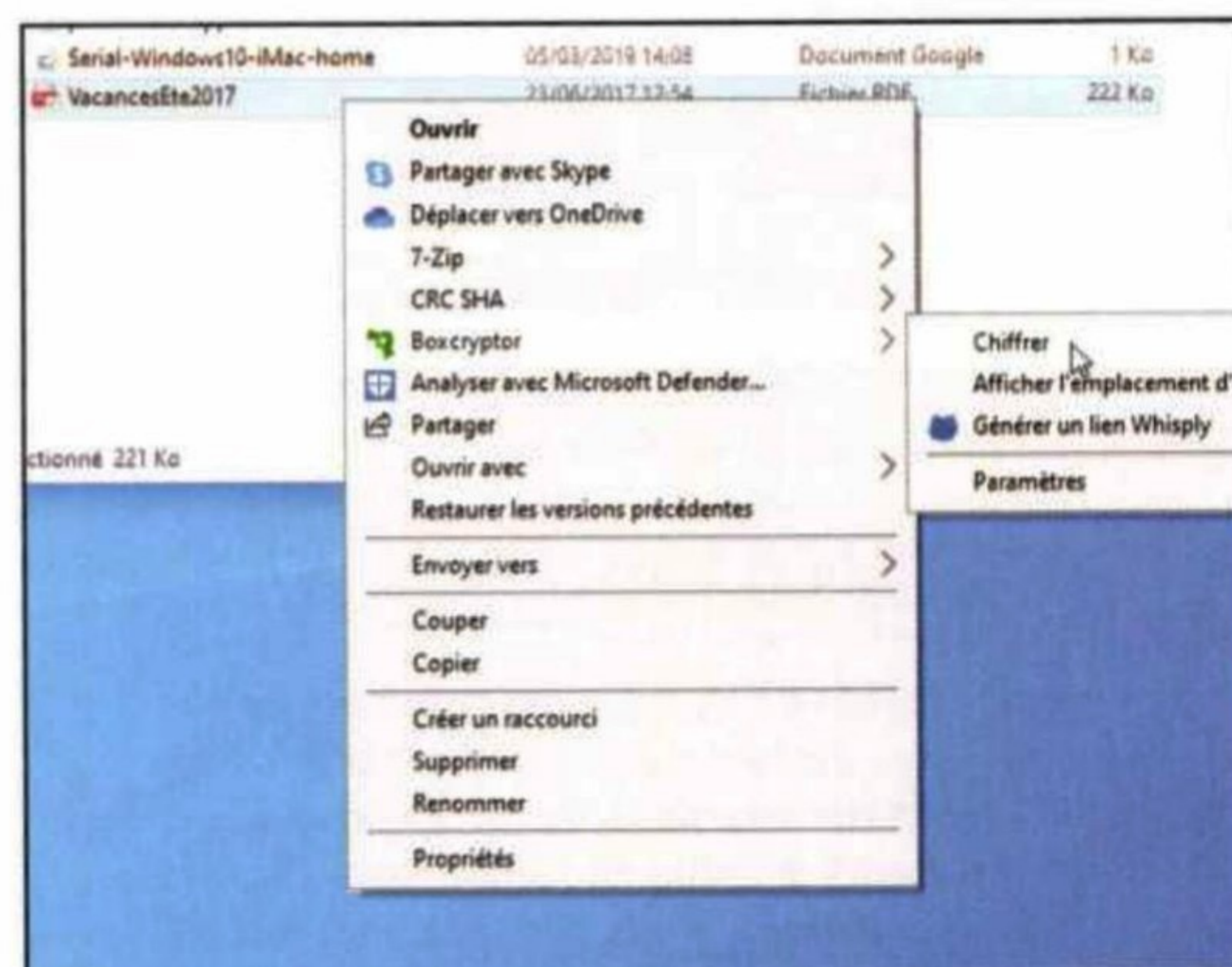
PLUSIEURS CLOUDS



Vous exploitez plusieurs services de Cloud ? En version gratuite, Boxcryptor ne peut en gérer qu'un. Si Google Drive n'apparaît pas (étape 2), faites un clic droit sur l'icône de Boxcryptor, à l'extrémité de la barre des tâches, choisissez **Paramètres**, et dans **Emplacements**, cochez **Google Drive**.

03 > CHIFFRER DES ÉLÉMENTS

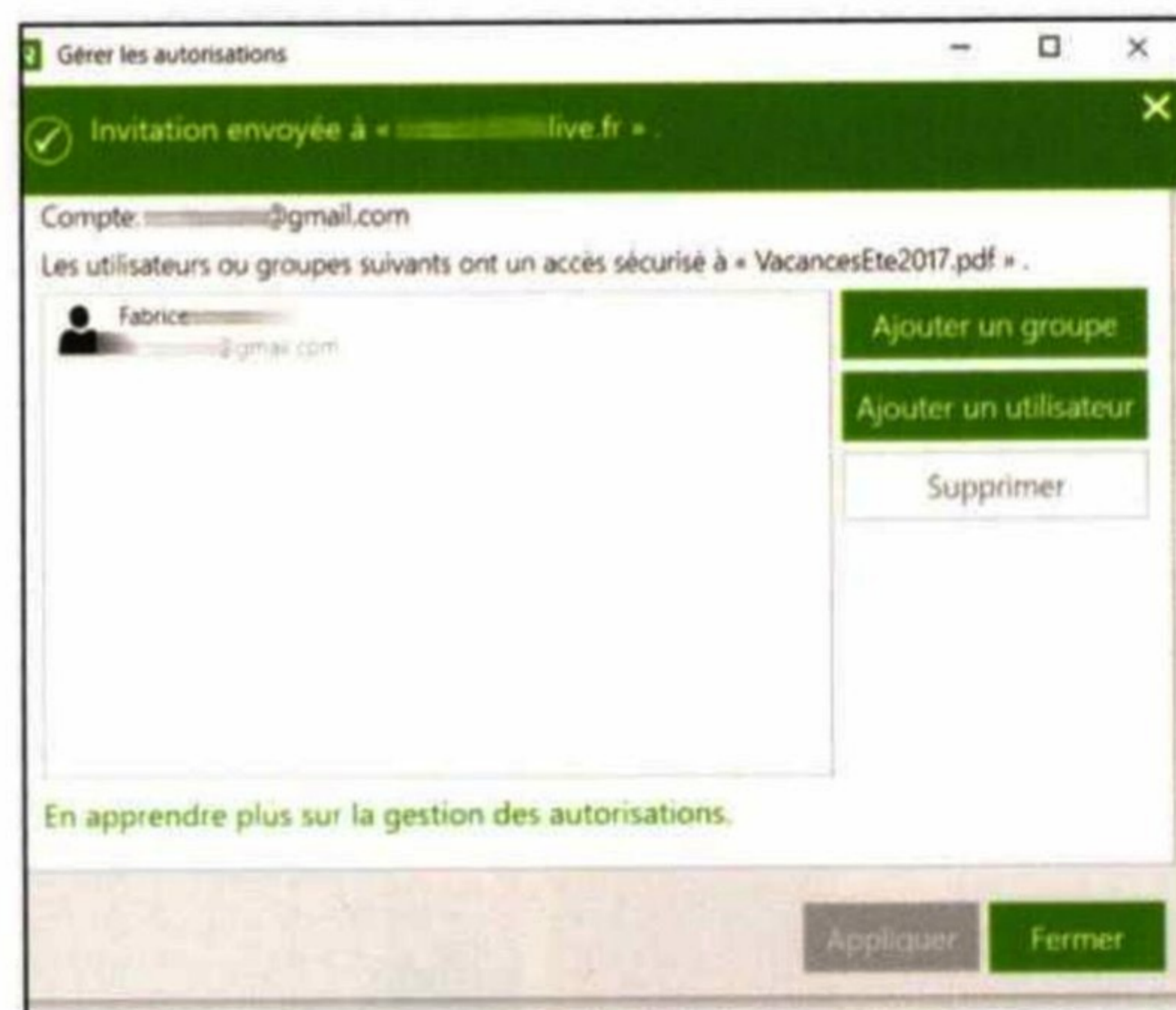
Ouvrez l'un des dossiers synchronisés avec votre PC. Sélectionnez le dossier ou le fichier que vous souhaitez chiffrer. Effectuez un clic droit et dans le menu contextuel,



choisissez **Boxcryptor > Chiffrer**. Au bout de quelques secondes, l'élément est verrouillé. Un petit symbole vert représentant un cadenas a d'ailleurs pris place en bas à gauche de l'icône.

04 > PARTAGER

Pour partager des éléments chiffrés avec d'autres utilisateurs, effectuez un clic droit sur un fichier ou un dossier verrouillé. Choisissez **Boxcryptor > Gérer les autorisations**. Dans la fenêtre qui s'affiche, cliquez sur **Ajouter un utilisateur**. Saisissez son adresse mail. S'il ne possède pas Boxcryptor, il recevra une invitation à l'installer afin de pouvoir ouvrir l'élément protégé.





FAITES DES CAPTURES D'ÉCRAN RAPIDES VIA CHROME

Un outil intégré dans Chrome vous permet de prendre des captures d'écran des pages web sans passer par un outil externe.

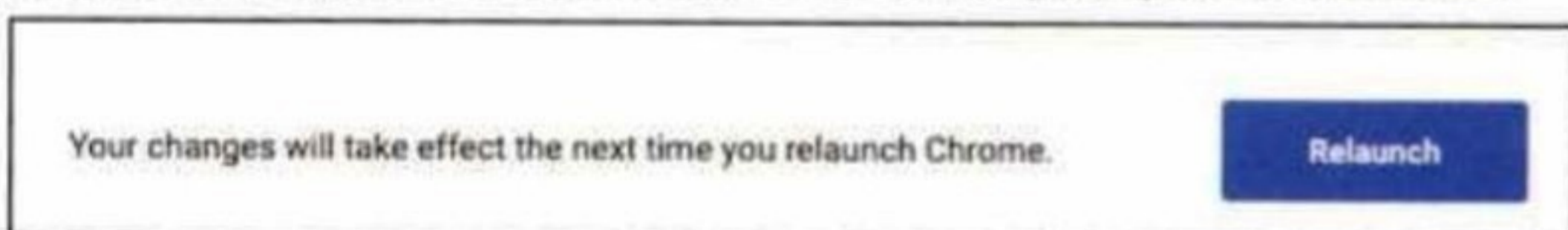
01 > ACTIVER L'OUTIL DE CAPTURE

Dans Chrome, accédez à la page des caractéristiques expérimentales en entrant dans la barre d'adresses **chrome://flags/#sharing-desktop-screenshots**. Sélectionnez ensuite le menu déroulant sur la droite de **Desktops Screenshots** pour choisir l'option **Enabled**.



02 > REDÉMARRER CHROME

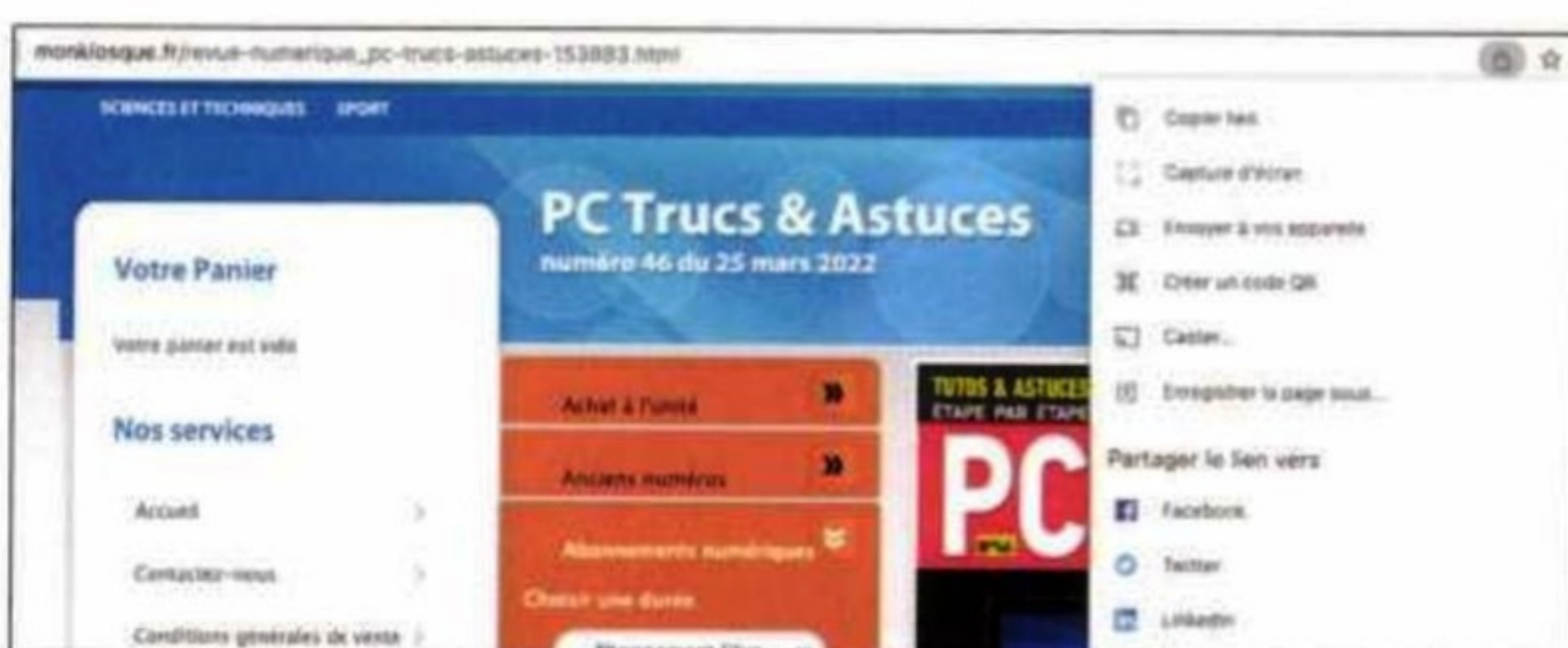
À peine l'option choisie, la fenêtre de navigation vous prévient que le changement sera effectif dès le redémarrage de Chrome. Cliquez sur **Relaunch** pour le faire immédiatement. L'opération ne prend quelques secondes



et l'option est immédiatement disponible directement via la barre d'adresses du navigateur.

03 > PRENDRE UNE CAPTURE D'ÉCRAN

Pour faire une capture d'écran, il vous suffit de cliquer sur l'icône **Partager cette page**, à droite de l'URL. Puis de sélectionner **Capture d'écran** dans le menu qui apparaît.



INFOS | Chrome |

Où le trouver ?

[www.google.com/chrome]

Difficulté :



Différentes options de partage sont d'ailleurs proposées, ce qui vous permet d'envisager de nombreux usages.

04 > ENREGISTRER L'IMAGE

À ce stade, il ne vous reste plus qu'à délimiter la zone à capturer. Elle est directement enregistrée



dans le presse-papiers et il vous suffit de cliquer sur **Télécharger** pour qu'elle s'enregistre dans votre dossier de téléchargements. L'opération est extrêmement rapide et intuitive. Comme si vous appuyiez sur un bouton pour prendre une photo.

BIEN UTILISER LE STOCKAGE DE ONEDRIVE

Gérez au mieux le partage de vos dossiers entre votre stockage dans le cloud et celui sur votre ordinateur.



On a tous besoin d'espaces de stockage supplémentaire. En plus, quand ils sont dans le cloud, cela facilite grandement la synchronisation et l'accès à distance (télétravail, bonjour !). Grâce à OneDrive, vous pouvez ainsi modifier un document d'où que vous soyez, grâce à votre compte Microsoft sur Windows (10 ou 11). Sauf que cet espace reste quand même limité (seulement 5 Go dans sa version gratuite, un peu plus si vous l'associez à un compte Microsoft Office). Tout comme la place disponible sur votre ordinateur. Et il faut donc les organiser au mieux. Ce n'est pas un jeu de Tetris® pour tout ranger dans les cases les plus appropriées, mais des

simples fonctions à choisir pour décider quels dossiers resteront uniquement en ligne ou seront aussi téléchargés sur votre ordinateur. Vous n'avez pas toujours besoin en effet de doubles copies, qui prennent de la place à deux endroits différents (oui, informatiquement, le clonage existe, mais il nécessite deux fois plus de ressources). Petite remarque : si votre connexion internet n'est pas des plus fiables, ou si vous vous déplacez régulièrement, il pourra être plus intéressant pour vous que tous vos fichiers OneDrive soient aussi présents sur votre ordinateur. La synchronisation se fera lors de votre prochaine connexion et vous aurez ainsi toujours accès à la dernière version.

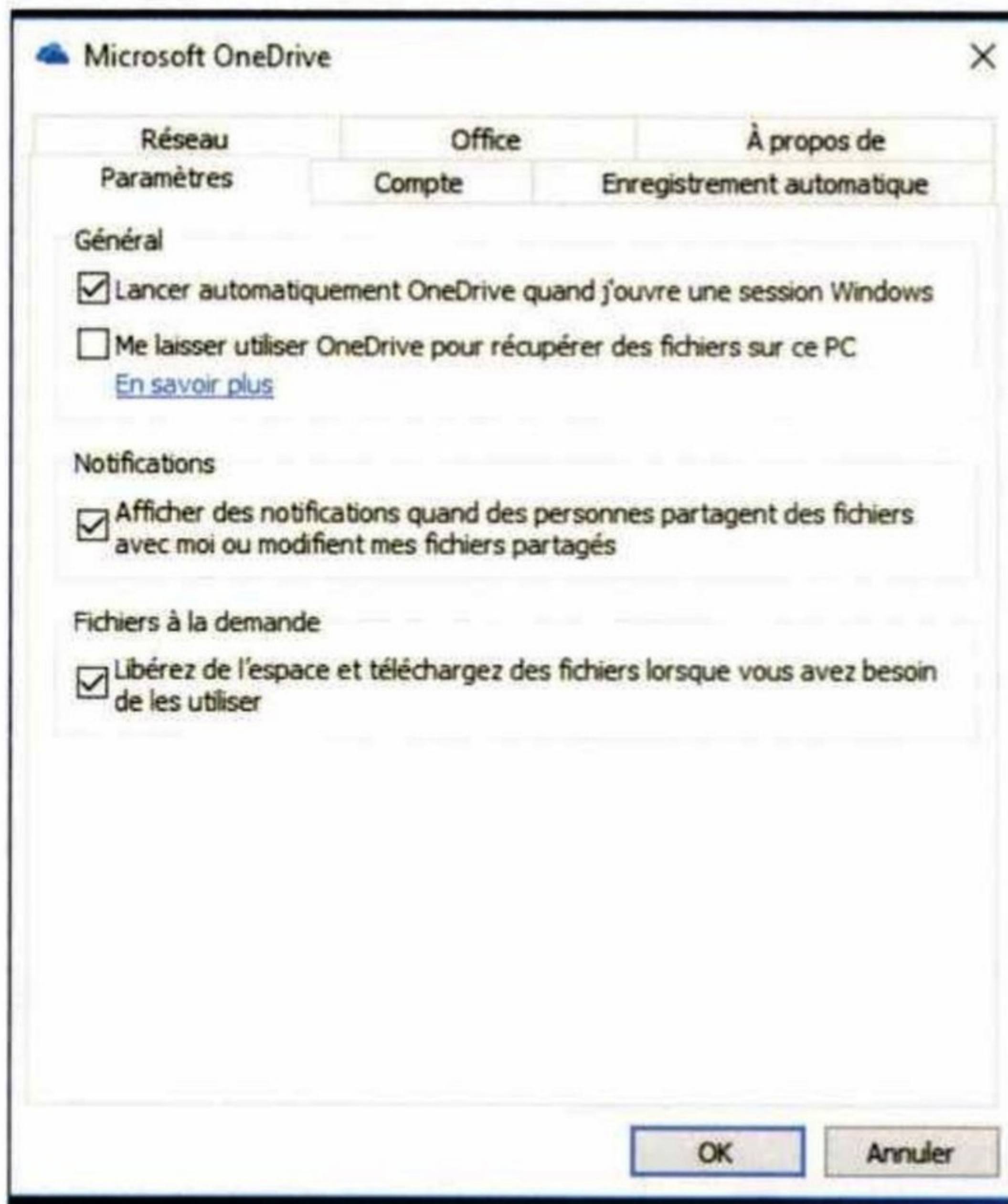


TÉLÉCHARGER UNIQUEMENT LES FICHIERS À LA DEMANDE

PRATIQUE

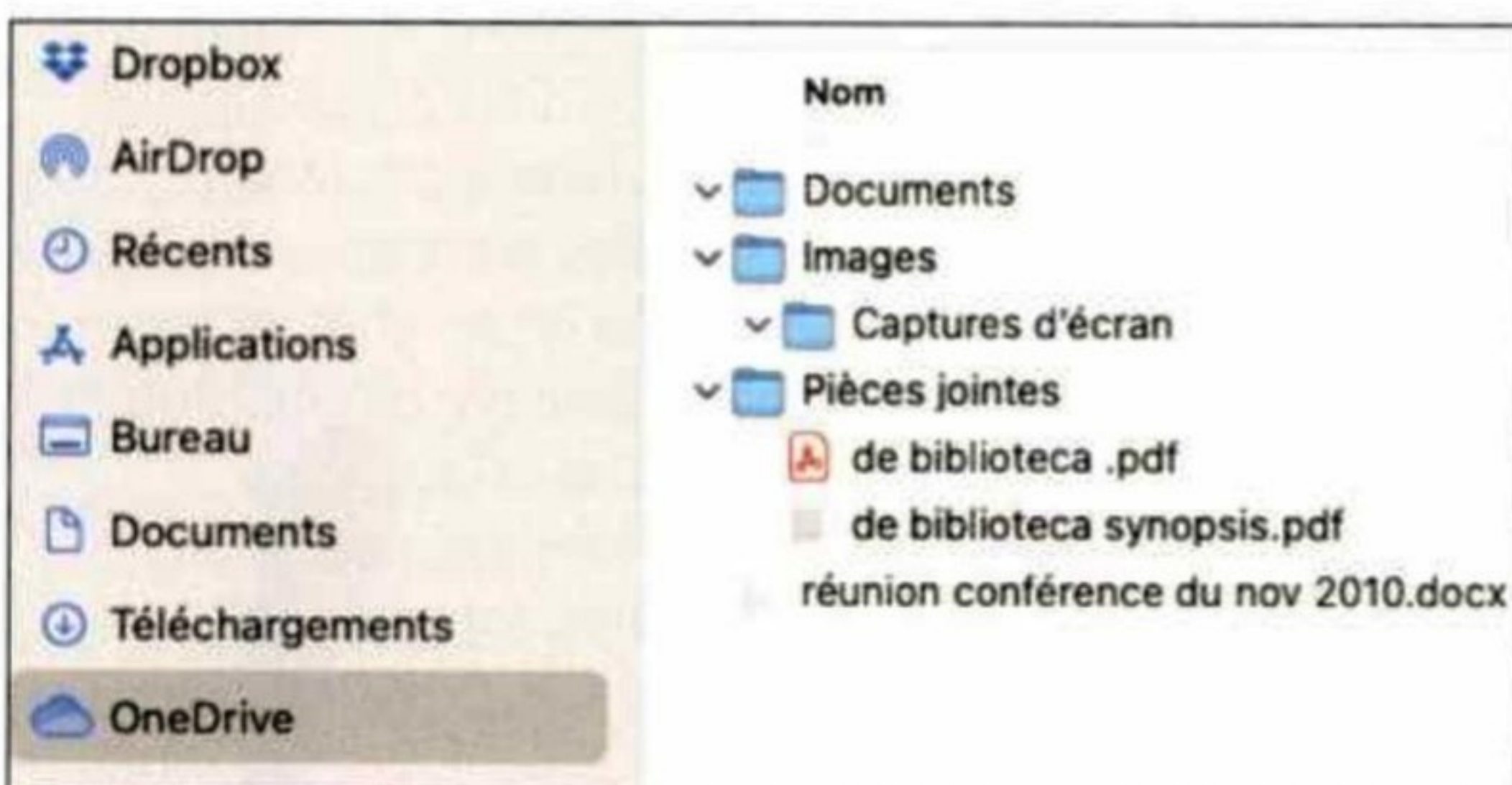
01 > DÉFINIR LES PARAMÈTRES ONEDRIVE

Dans la barre des tâches, cliquez sur l'**icône OneDrive** (le double nuage). Cliquez sur **Plus**, puis sur **Paramètres** et allez dans la zone **Fichiers à la demande**. Cochez la case **Libérez de l'espace et téléchargez des fichiers lorsque vous avez besoin de les utiliser**. Validez en appuyant sur **OK**.



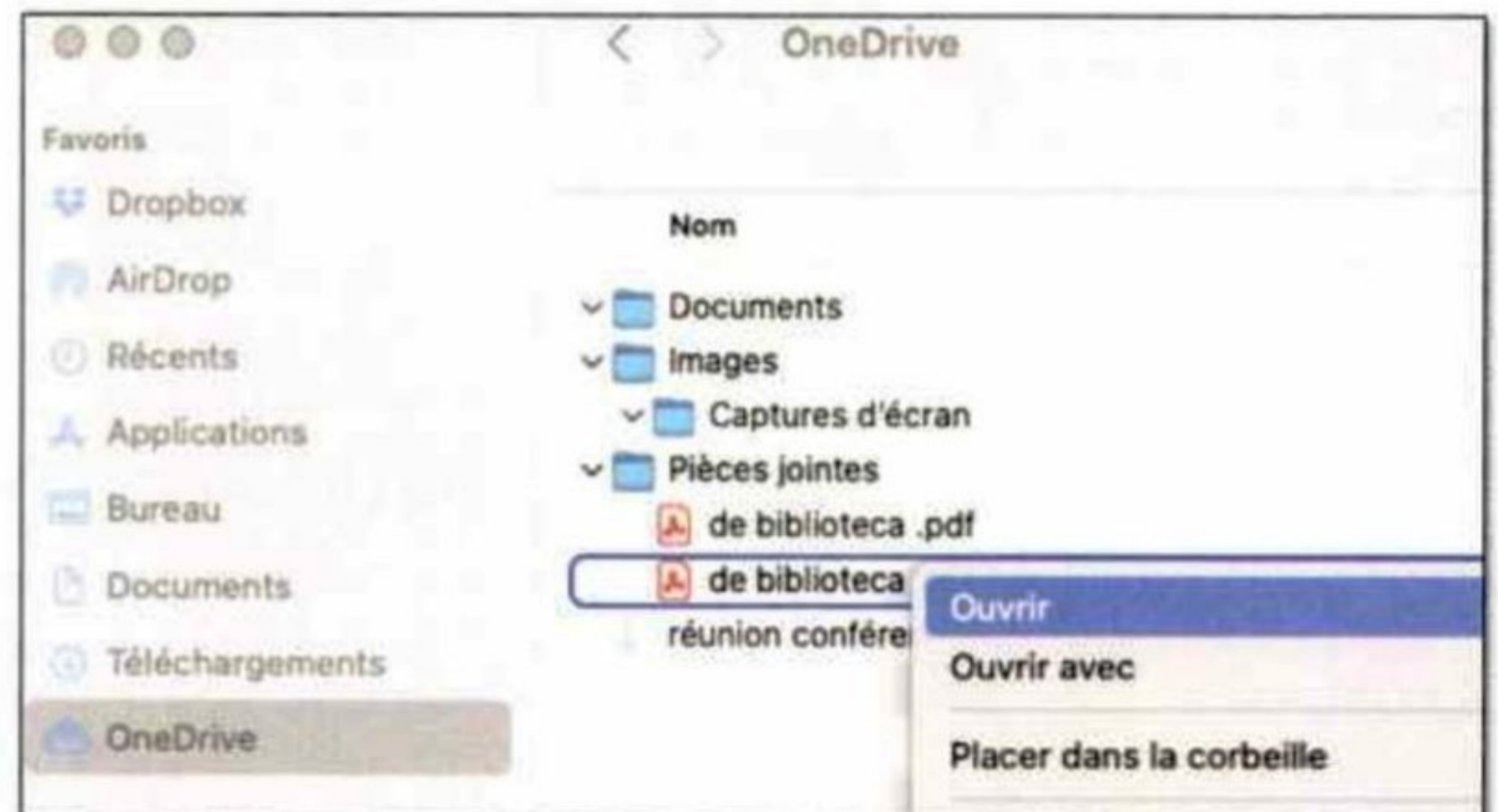
02 > VÉRIFIER LE STATUT DES FICHIERS

Depuis l'Explorateur, allez sur votre dossier **OneDrive**. À droite de chaque fichier ou dossier, une colonne **Statut** est maintenant affichée. Un nuage bleu indique que ces derniers sont uniquement disponibles en ligne, un cercle vert validé signifie qu'ils sont présents sur votre ordinateur. Les flèches bleues signalent une synchronisation en cours.



03 > TÉLÉCHARGER UN FICHIER

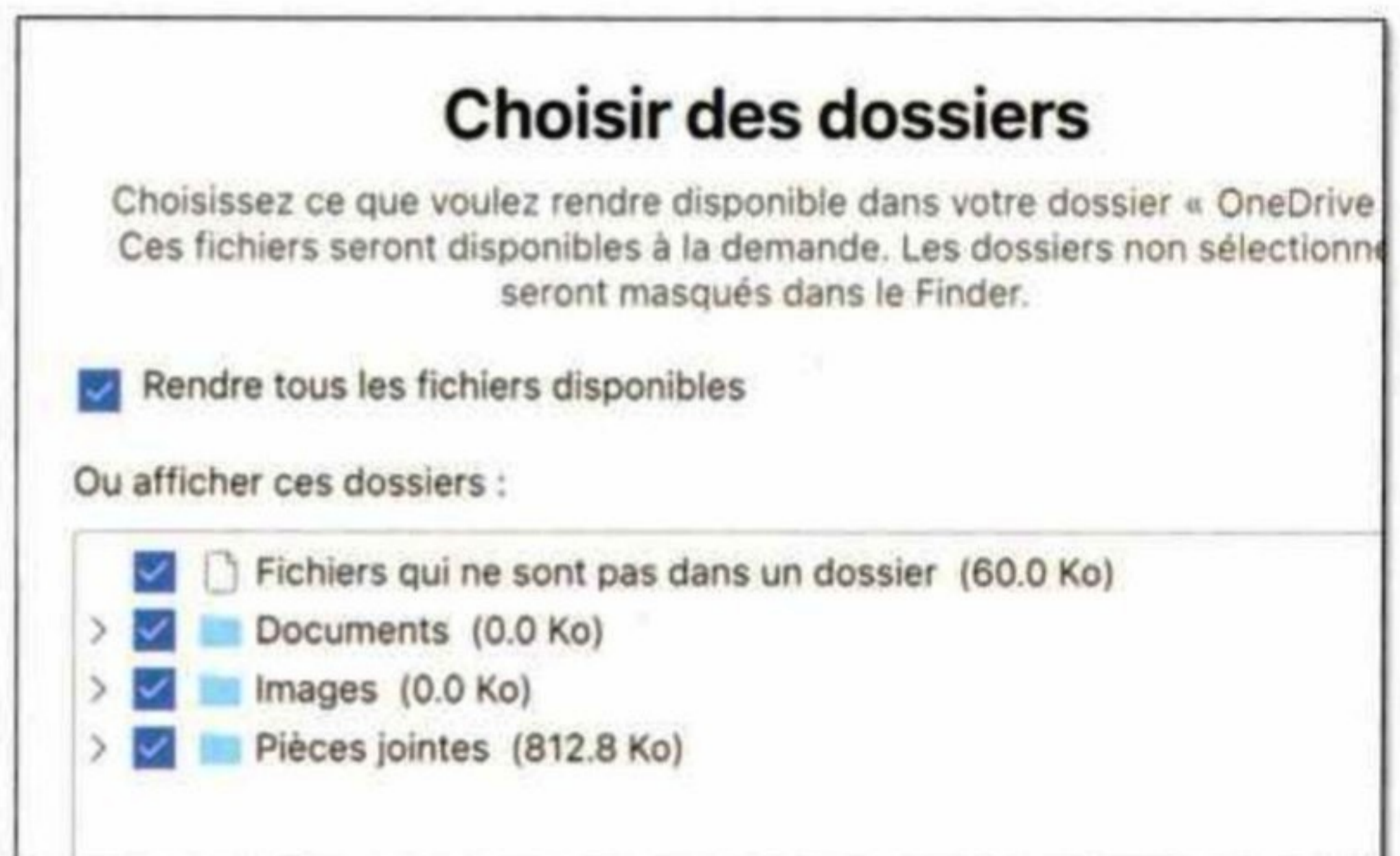
Si vous avez besoin de travailler sur un fichier, il est temps de le télécharger. Un double-clic sur son nom suffira. S'il était uniquement disponible en ligne auparavant, il sera automatiquement téléchargé, ce qui



peut prendre un certain temps s'il est volumineux. Il occupera maintenant aussi de la place dans la mémoire de votre ordinateur.

04 > INVISIBILISER CERTAINS FICHIERS

Vous pouvez choisir que certains fichiers ne s'affichent pas sur votre ordinateur. Dans la barre des tâches, cliquez sur l'**icône OneDrive** (le double nuage). Cliquez sur **Plus**, puis sur **Paramètres**. Allez dans l'onglet **Comptes** puis cliquez sur **Choisir des dossiers**. Décochez ceux à invisibiliser sur l'ordinateur, et validez par **OK**.



GÉRER LES FICHIERS STOCKÉS EN LOCAL

PRATIQUE

01 > CONSERVER SUR L'APPAREIL

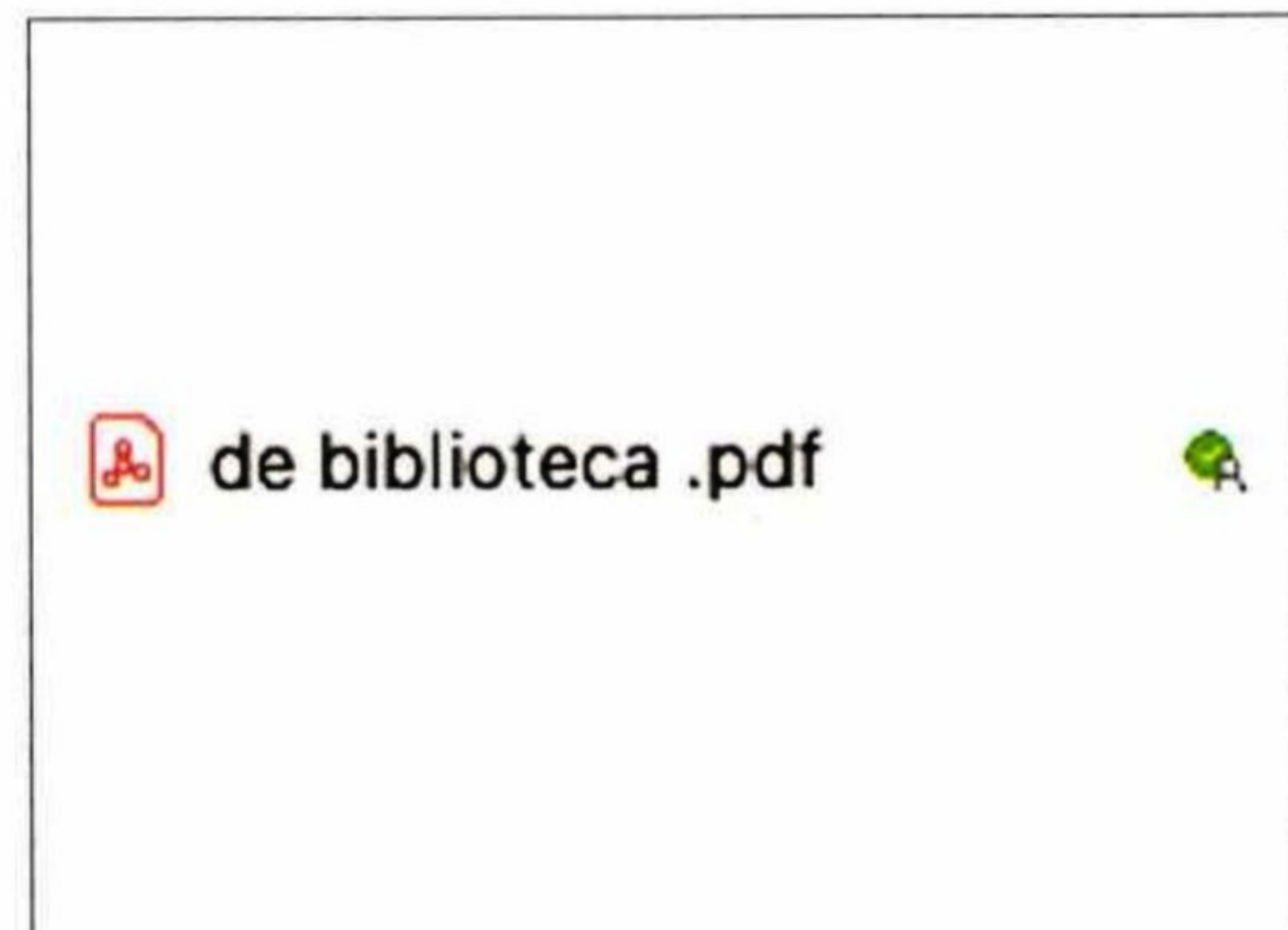
Pour pouvoir accéder en permanence à certains dossiers, même sans connexion internet, cliquez dessus avec le bouton droit de la souris. Dans le menu qui apparaît,



cliquez sur **Toujours conserver sur cet appareil**. Si ce n'est pas déjà fait, l'élément sera téléchargé sur votre ordinateur. Et, surtout, il sera accessible en permanence.

02 > VÉRIFIER SA PRÉSENCE

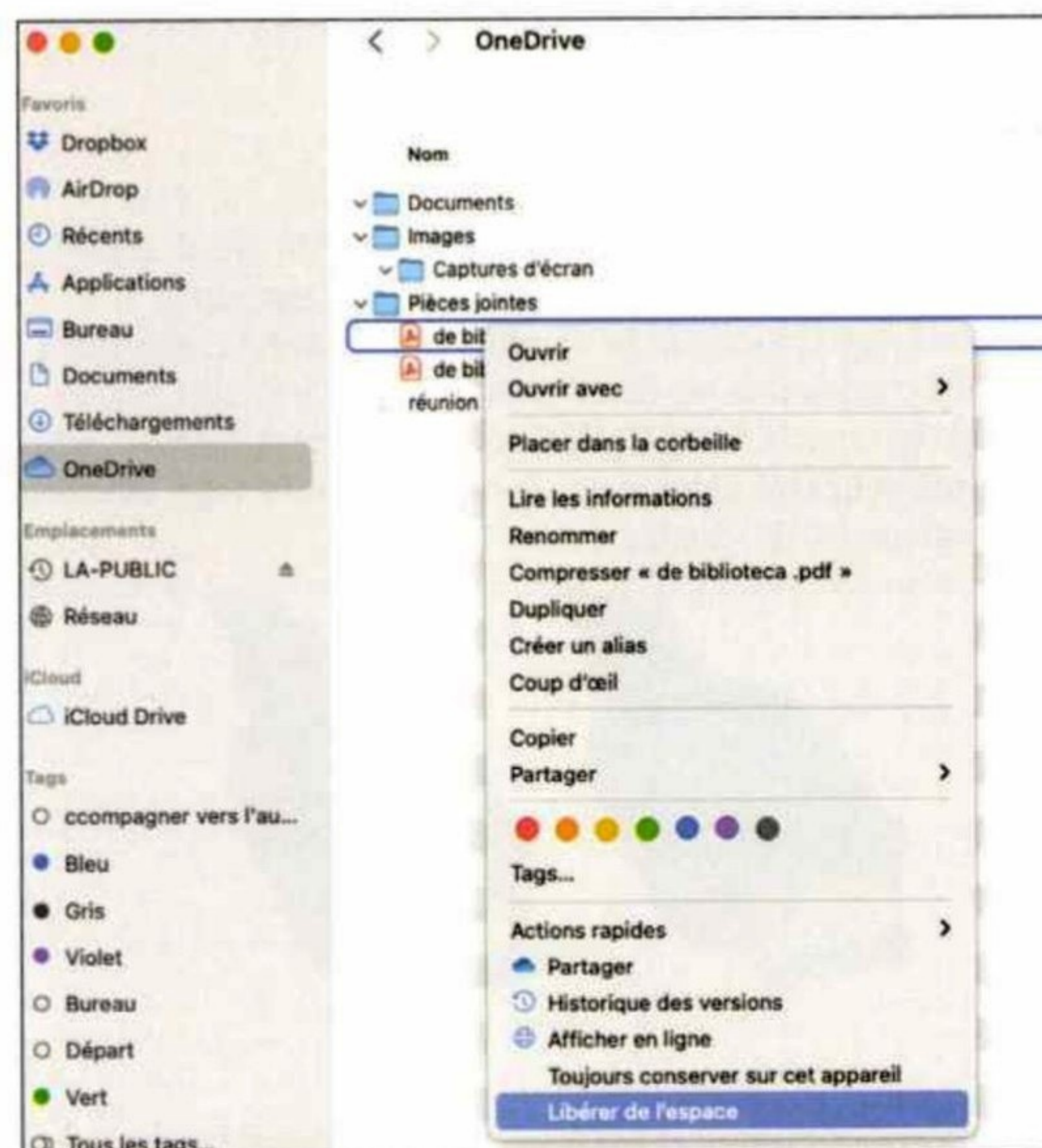
En accédant à OneDrive via l'Explorateur, vous devriez maintenant voir une coche verte à droite du nom du fichier (ou du dossier). Elle indique sa présence à la fois



sur le drive et sur votre ordinateur. Vous pourrez travailler dessus hors-ligne, et la synchronisation se fera lors de votre prochaine connexion.

03 > GAGNER DE L'ESPACE

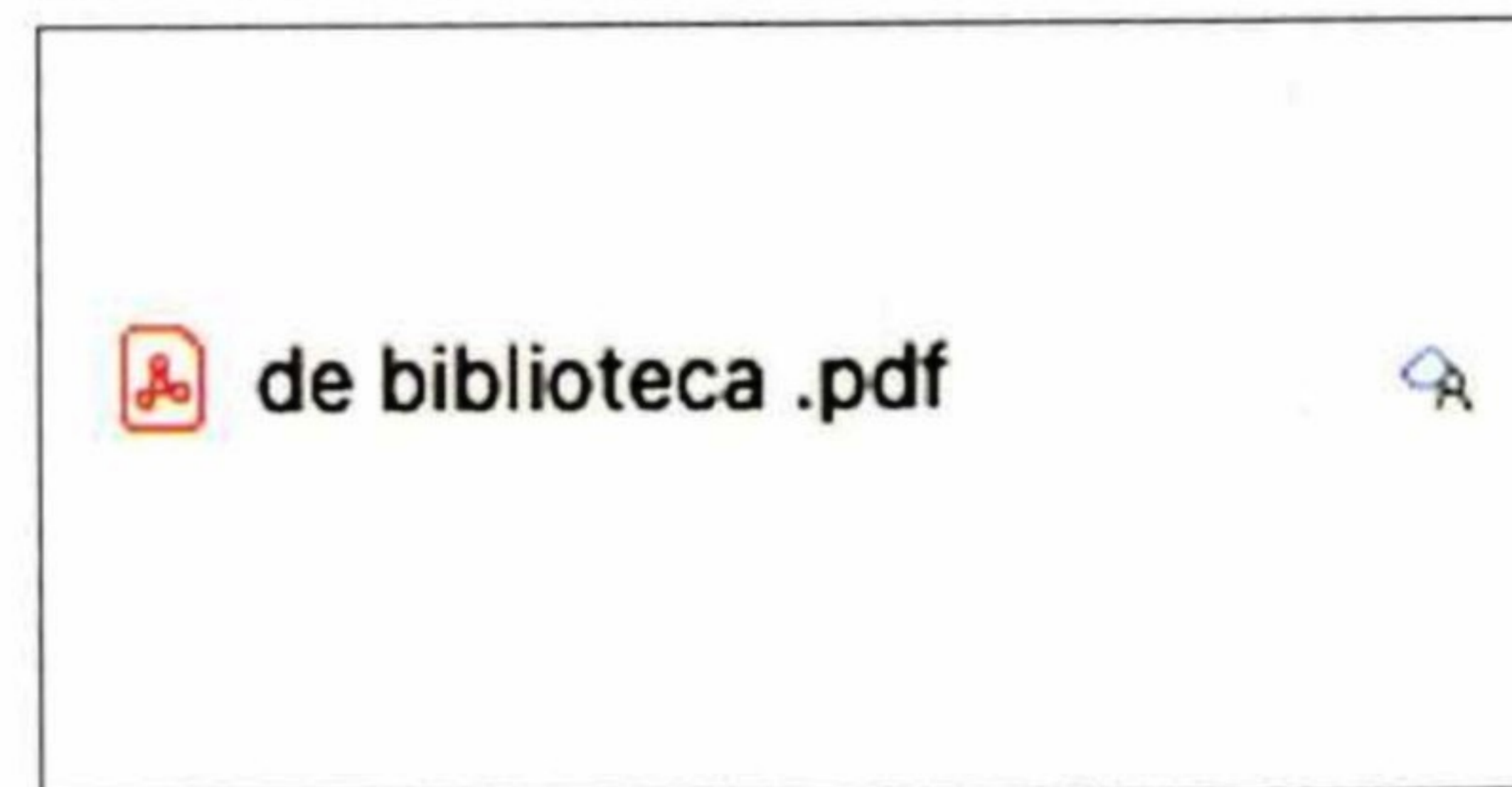
Votre ordinateur commence à saturer un peu tellement vous y entassez des documents ? Décidez de conserver certains d'entre eux uniquement sur le drive. Depuis OneDrive, cliquez sur le nom des documents dont



vous n'avez pas un besoin immédiat avec le bouton droit de la souris. Cliquez ensuite sur **Libérer de l'espace** dans le menu qui s'affiche.

04 > TRAVAILLER DESSUS

Le statut du dossier ou du fichier devrait maintenant être symbolisé par un nuage bleu. Vous pourrez toujours travailler dessus, le modifier, le partager... Mais il n'occupera plus de la place que dans le cloud, et pas sur



votre ordinateur. Une option pratique si votre stockage en ligne est suffisant ou si vous n'avez pas besoin d'accéder à cet élément régulièrement.



RELIEZ PC ET TÉLÉ

Vous avez envie de profiter de vos sources de streaming sur le téléviseur du salon ? Reliez l'ordinateur à ce dernier.

01 > BRANCHER EN HDMI

Toutes les télé produites depuis 20 ans disposent d'une prise HDMI transportant l'image et le son. On la retrouve également sur de nombreux ordinateurs, portables ou fixes. Connectez les deux appareils avec un câble HDMI, et sélectionnez la source HDMI sur le téléviseur. Celui-ci est automatiquement détecté par l'ordinateur et l'image affichée à l'écran du PC est dupliquée sur la TV.



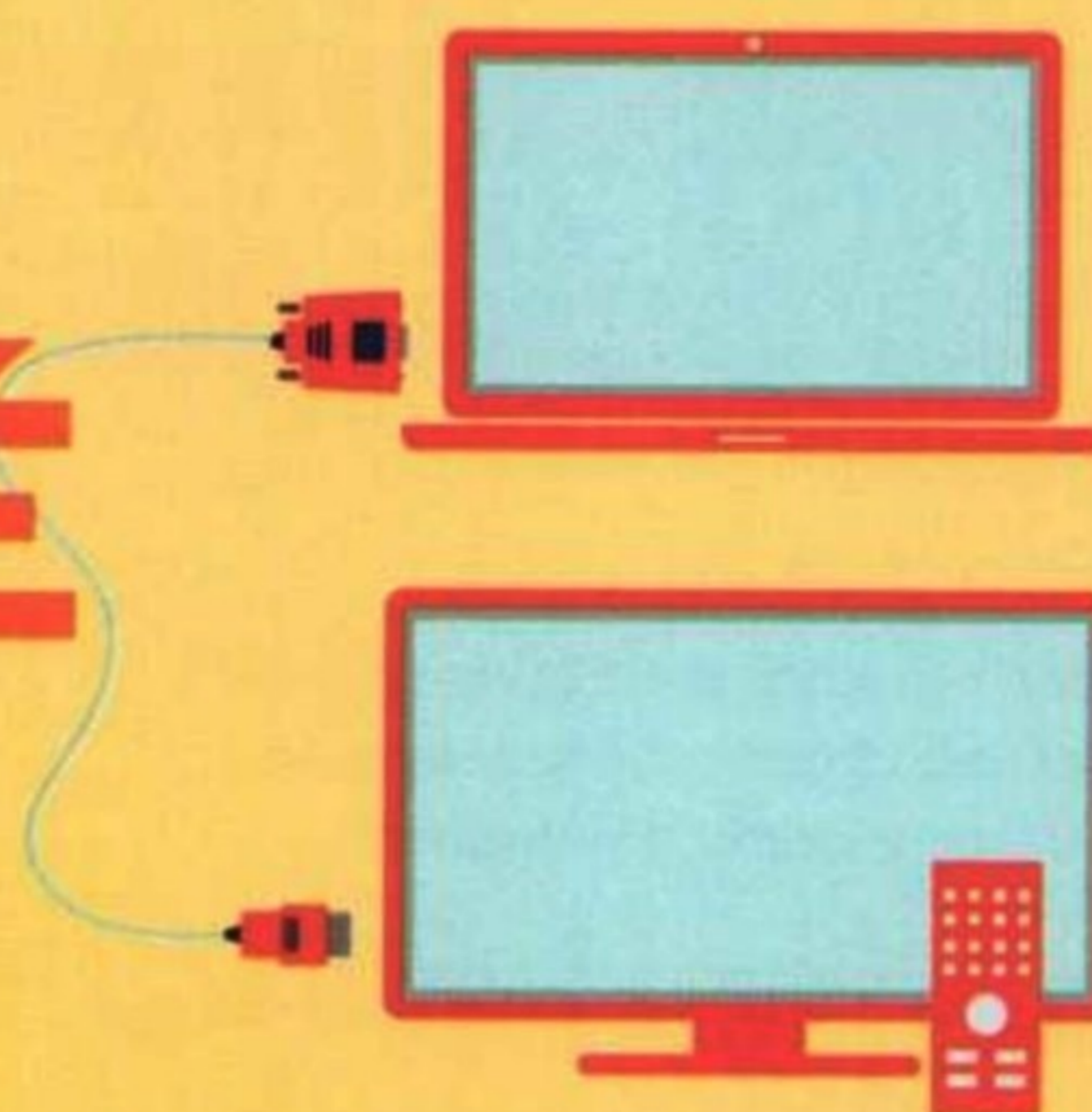
02 > UTILISER UN ADAPTATEUR

Si votre téléviseur ou votre PC ne dispose pas de prise HDMI, repérez le type de prise présent et commun aux deux appareils. S'il n'y en a aucune, vous pouvez pour quelques euros vous équiper d'un adaptateur adéquat dans une boutique spécialisée ou en ligne : DisplayPort/HDMI, VGA/HDMI, USB-C/HDMI, DVI/HDMI et même HDMI/Péritel pour les téléviseurs les plus anciens.



03 > CONNECTER EN WI-FI

Les TV connectées embarquent un module Wi-Fi, qui peut servir à afficher du contenu provenant d'un PC. Assurez-vous que les deux appareils sont connectés au



INFOS

[Windows]

Difficulté : 🧑🏻 🧑🏻 🧑🏻

CONNECTER

Recherche d'appareils audio et de dispositifs d'affichage sans fil

Où est mon appareil ?

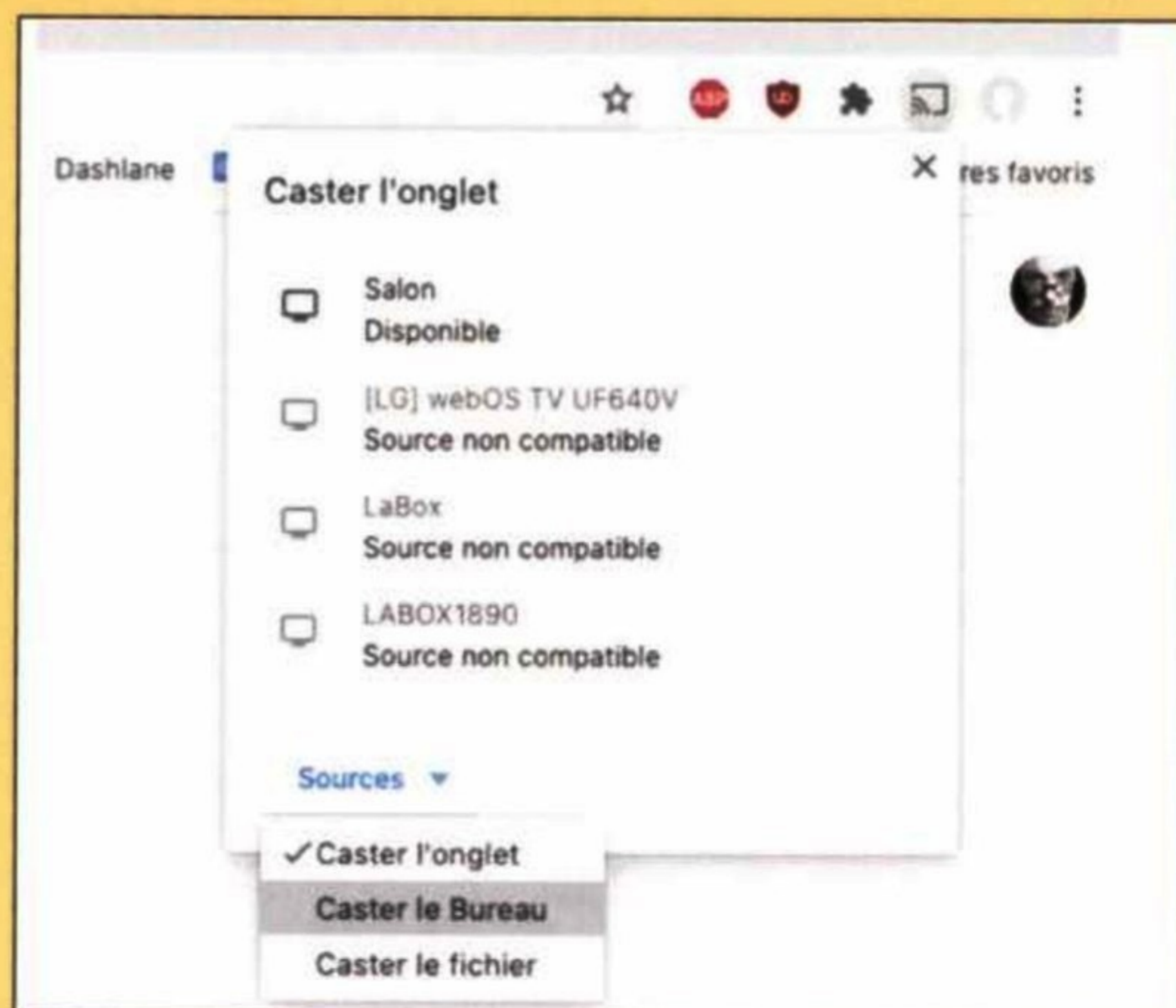
Rechercher un appareil par nom

[LG] webOS TV UF640V
Affichage

même réseau Wi-Fi. Sur le PC, pressez les touches **Windows + P**. Dans le volet qui se déploie, cliquez sur **Dupliquer** puis sur **Connecter à un dispositif d'affichage sans fil**. Cliquez sur le nom de votre téléviseur lorsqu'il s'affiche.

04 > UTILISER UN CHROMECAST

Vendu une quarantaine d'euros par Google, le boîtier Chromecast se branche sur une prise HDMI du téléviseur. Une fois installé et paramétré, vous pouvez streamer l'écran de votre PC sur la télé, par Wi-Fi, avec le navigateur Google Chrome via les **Paramètres** et la fonction **Caster**, ou encore avec le lecteur multimédia VLC depuis le menu **Lecture > Rendu**.



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.





IDEACENTRE MINI GEN8 : PETITE BOMBE EN APPROCHE

LE DERNIER-NÉ DE LA GAMME IDEACENTRE MINI SERA COMMERCIALISÉ À PARTIR DE JUILLET PROCHAIN. AUSSI ÉLÉGANT QUE PUISSANT, CE MINI PC A TOUT D'UN GRAND POUR UN PRIX COMPÉTITIF.

Les mini PC ont le vent en poupe et séduisent de plus en plus de particuliers. Réservés il y a une dizaine d'années aux geeks, aux entreprises voire aux industriels, les fabricants rivalisent aujourd'hui d'efforts pour proposer des petites bombes puissantes, mais aussi esthétiques pour trôner au milieu du salon ou du bureau.

DESIGN INSPIRÉ DU MAC MINI

La référence en matière de design étant pour beaucoup le Mac Mini, le groupe chinois Lenovo ne fait pas dans la dentelle et poursuit sa guerre des clones avec son nouveau IdeaCentre Mini Gen8. Mais que vaut-il en termes de performances et de modularité ? Si nous écrivons ces lignes, c'est que son ramage vaut bien son plumage !

Le dernier-né de la gamme mini PC de Lenovo coche toutes les (bonnes) cases.

Le fabricant a choisi d'équiper son nouvel ordinateur fixe de la dernière génération de processeurs Intel Core, ainsi que de la puce graphique Intel Iris Xe Graphics. Il est également doté de 8 ou 16 Go de mémoire en DDR4 au format SO-DIMM, qui peut être upgradée, offrant ainsi une durée de vie prolongée. Pour le stockage, le IdeaCentre Mini est équipé d'un SSD d'une capacité de 256, 512 ou 1 To.

Avec sa petite taille, qui tient dans une main, et son poids réduit de 1,81 kg, ce mini PC peut être installé n'importe où, même sur un coin de bureau. Il peut être placé à la verticale ou à l'horizontale, grâce au support métallique fourni.

La connectique est également à la pointe de la technologie, avec du Wi-Fi 6 pour des vitesses de débit optimales, et du Bluetooth 5.2. Il sera livré avec Windows 11 Pro sur certains marchés, ou Windows 11 Famille. Le nombre et la diversité des ports sont également impressionnants sur un si petit volume ! Il dispose ainsi d'un port Ethernet RJ45, de trois ports USB-A (deux USB 3.2 Gen 2 et un USB 2.0), d'un port USB-C Thunderbolt 4, d'un port HDMI 2.1 et d'un port DisplayPort, ainsi que d'un port USB 3.2 Gen 2, un port USB-C et une prise jack à l'avant.

Le Lenovo IdeaCentre Mini Gen8 sera disponible dès juillet 2023 à partir de 599 euros pour la configuration la plus basse.



CARACTÉRISTIQUES

- **Processeur** : Intel Core i5-13500H ou Core i7-13700H (45W)
- **Mémoire vive** : 8 ou 16 Go de RAM DDR4
- **Stockage** : entre 256 et 1 To d'espace
- **Connectique** : Thunderbolt 4 ; DisplayPort ; HDMI 2.1 ; Ethernet ; USB Type-C et Type-A ; audio 3.5 mm
- **Connectique sans fil** : Wi-Fi 6 et Bluetooth 5.2
- **Dimensions** : 19,55 x 19,05 x 3,81 cm
- **Poids** : 1,8 kg



CAMERA V3 POUR RASPBERRY PI

AVEC AUTOFOCUS ET HDR

ENFIN UN PEU DE NOUVEAUTÉS POUR LES AMATEURS DE RASPBERRY ! LA FONDATION ANNONCE LA SORTIE DE SA TROISIÈME GÉNÉRATION DE MODULES CAMÉRA, APPORTANT ENFIN L'AUTOFOCUS MOTORISÉ AUX UTILISATEURS (LA PREMIÈRE VERSION EN 2013 ÉTAIT À MISE AU POINT FIXE ET, EN 2016, LA SECONDE À FOCUS RÉGLABLE MANUELLEMENT.

Ce nouveau module caméra, appelé Camera Module 3, est doté d'un capteur d'image de 12 Mpix, hérité des smartphones, avec la possibilité de choisir entre différentes configurations... et proposant enfin le HDR. La fondation Raspberry explique s'être à nouveau « associée à Sony, cette fois en utilisant leur capteur IMX708 rétro-éclairé : celui-ci offre une résolution plus élevée ; une conception de pixels plus grande et plus sensible ; et prise en charge de l'imagerie à plage dynamique élevée. »

Ce capteur IMX708 est ainsi plus grand que celui de la version précédente (1/2.43 pouces contre 1/4 pouce) et utilise la technologie Exmor-R, ce qui permet de générer automatiquement des images en HDR (High Dynamic Range). La qualité d'image devrait être améliorée par rapport



à la version précédente, malgré une résolution moindre (12,3 Mpix contre 12 Mpix).

La grosse nouveauté de ce module est donc l'ajout de l'autofocus, grâce à un module AF de smartphone, appelé voice-coil actuator ou VCA. Cela permet un ajustement automatique de la distance de mise au point, de 5 cm à l'infini en grand-angle (10 cm à l'infini pour l'angle normal).

DEUX COMPOSANTS, QUATRE CHOIX POSSIBLES !

Le Camera Module 3 n'est pas un module unique, mais un choix entre deux composants offrant quatre options différentes. Si, si, c'est en fait assez simple à comprendre : la première option est la couverture angulaire, avec deux optiques disponibles : une optique grand-angle (66 degrés, équivalent à un 28 mm f/1.8) et une optique ultra grand-angle (102 degrés, équivalent à un 14,5 mm f/2.2). La seconde option est la présence ou non d'un filtre infrarouge. Il est donc possible de choisir entre un module normal à PCB vert pour l'imagerie classique ou un module sensible à l'infrarouge (NoIR) à PCB noir pour l'imagerie nocturne.

Le module de caméra 3 peut être utilisé pour prendre des vidéos Full HD et des photos jusqu'à 12MP sans HDR et jusqu'à 3MP avec HDR.

COMPATIBILITÉ

Les modules de caméra sont livrés avec un câble ruban de 20 cm pour la connexion avec un Raspberry Pi SBC. Le module de caméra 3 est ainsi compatible avec tous les ordinateurs Raspberry Pi dotés de connecteurs CSI, c'est-à-dire tous sauf le Raspberry Pi 400 et la version de lancement 2016 de Zero. Les dimensions de la carte et les positions des trous de montage sont identiques au module de caméra 2. En raison des changements de taille et de position du module de capteur, il n'est pas mécaniquement compatible avec le couvercle de la caméra pour le Raspberry Pi Zero Case.

La fondation Raspberry Pi a réussi à maintenir un prix abordable pour ce module grâce à l'utilisation de composants couramment utilisés dans les smartphones.



- LE CAMERA MODULE V3 À CAPTEUR COULEUR ET OPTIQUE NORMALE : 30 €



- LE CAMERA MODULE V3 À CAPTEUR NOIR ET OPTIQUE NORMALE : 30 €



- LE CAMERA MODULE V3 À CAPTEUR COULEUR ET OPTIQUE GRAND-ANGLE : 40 €



- LE CAMERA MODULE V3 À CAPTEUR NOIR ET OPTIQUE GRAND-ANGLE : 40 €



TOP 15

Logiciels & services GRATUITS

TOP 5 IMAGES LIBRES DE DROITS



PEXELS > PHOTOS ET VIDÉOS

Pexels propose une large sélection d'images et vidéos libres de droits,

avec des photos de haute qualité prises par des professionnels et des amateurs talentueux. Vous pouvez utiliser ces images gratuitement pour n'importe quel usage commercial ou personnel, sans avoir à demander la permission ou à créditer l'auteur.

Lien : www.pexels.com

PIXABAY > LA RÉFÉRENCE

Avec plus d'un million d'entrées, vous trouverez votre bonheur. Le site propose sept sections pour télécharger au choix des photos, illustrations, images vectorielles, vidéos, musiques, effets sonores ou gifs libres de droits, y compris pour une utilisation commerciale.

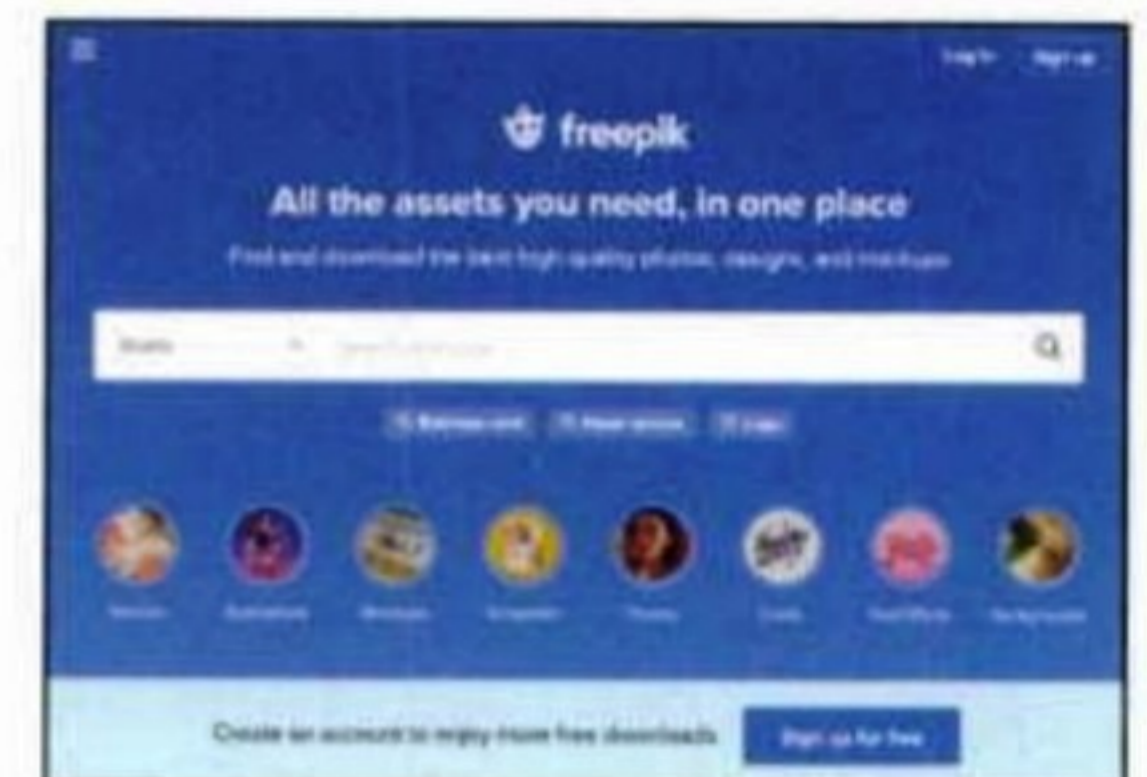
Lien : pixabay.com



FREEPIK > VECTORIEL

Freepik est une source populaire d'images et d'icônes libres de droits, avec une grande collection de vecteurs, de photos et de PSD (Photoshop). La plupart des images sont gratuites à utiliser, mais certaines exigent un abonnement premium.

Lien : www.freepik.com



BURST > POUR LES COMMERCE EN LIGNE



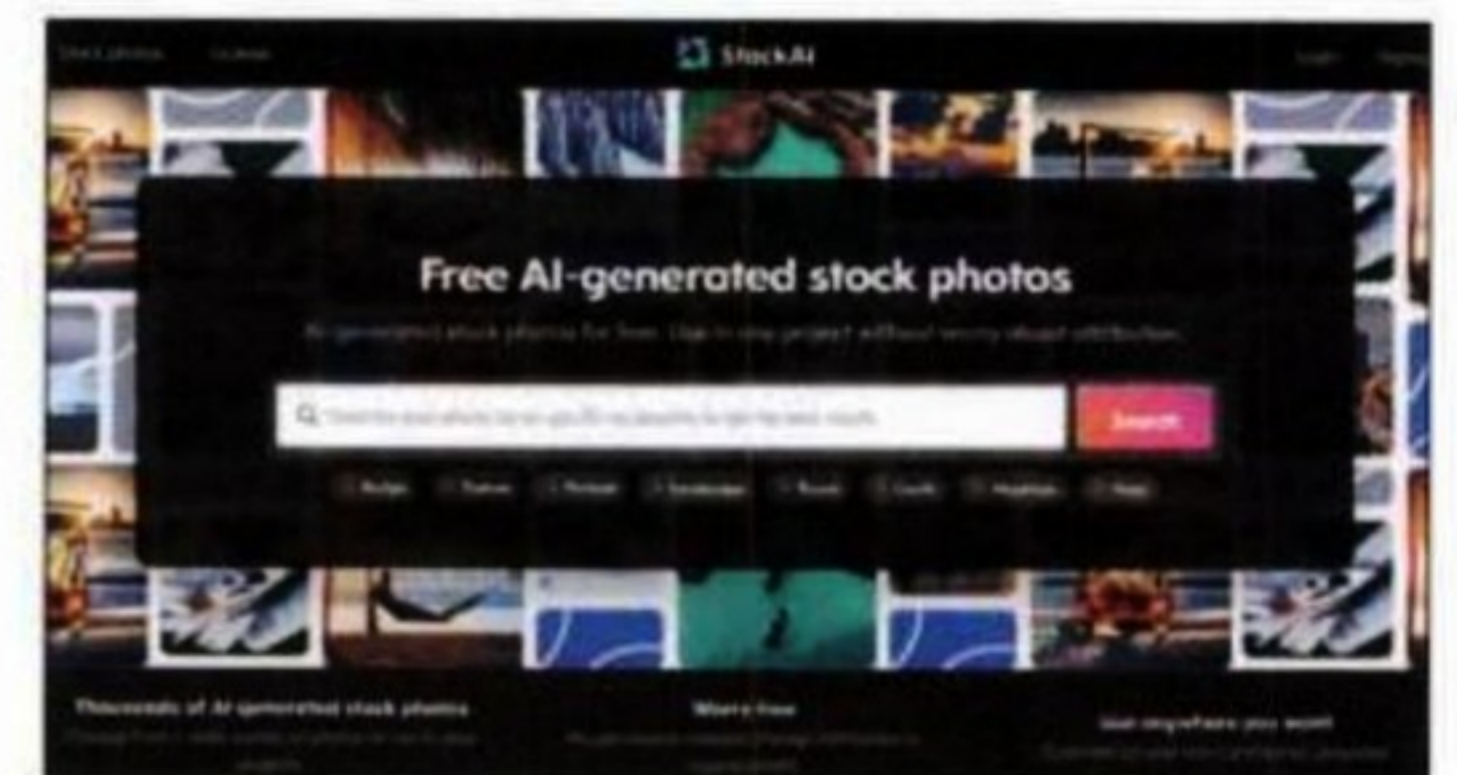
Burst est une source d'images gratuites pour les entreprises, avec une grande collection de photos de produits et de fonds d'écran pour le commerce électronique. Des kits de photos prêts à l'emploi par secteur sont aussi proposés.

Lien : burst.shopify.com

STOCKAI > INTELLIGENCE ARTIFICIELLE

Une plateforme qui surfe sur les nouveaux services permettant de générer automatiquement des images et illustrations grâce à l'intelligence artificielle. Un choix déjà impressionnant, mais le moteur de recherche devra être amélioré. À suivre !

Lien : www.stockai.com



TOP 5 POUR LANCEURS D'ALERTE

SOURCESURE > MÉDIAS FRANCOPHONES ASSOCIÉS

Source sûre permet l'envoi d'infos et de documents aux journalistes de quatre rédactions francophones : Le Monde, Le Soir, la RTBF et la RTS. « Seuls les messages précis et factuels concernant des informations d'intérêt public (...) seront pris en compte » indiquent d'emblée ces dernières. Un service qui s'appuie sur la solution sécurisée GlobalLeaks.

Lien : ensecurite.sourcesure.eu



LA MAISON DES LANCEURS D'ALERTE > COMME À LA MAISON

Un site ressources pour connaître vos droits, les outils existants, découvrir guides pratiques et actualités. La Maison des Lanceurs d'Alerte déclare avoir reçu 300 demandes de soutien et avoir accompagné plus de 150 lanceurs d'alerte depuis sa création.

Lien : mlalerte.org

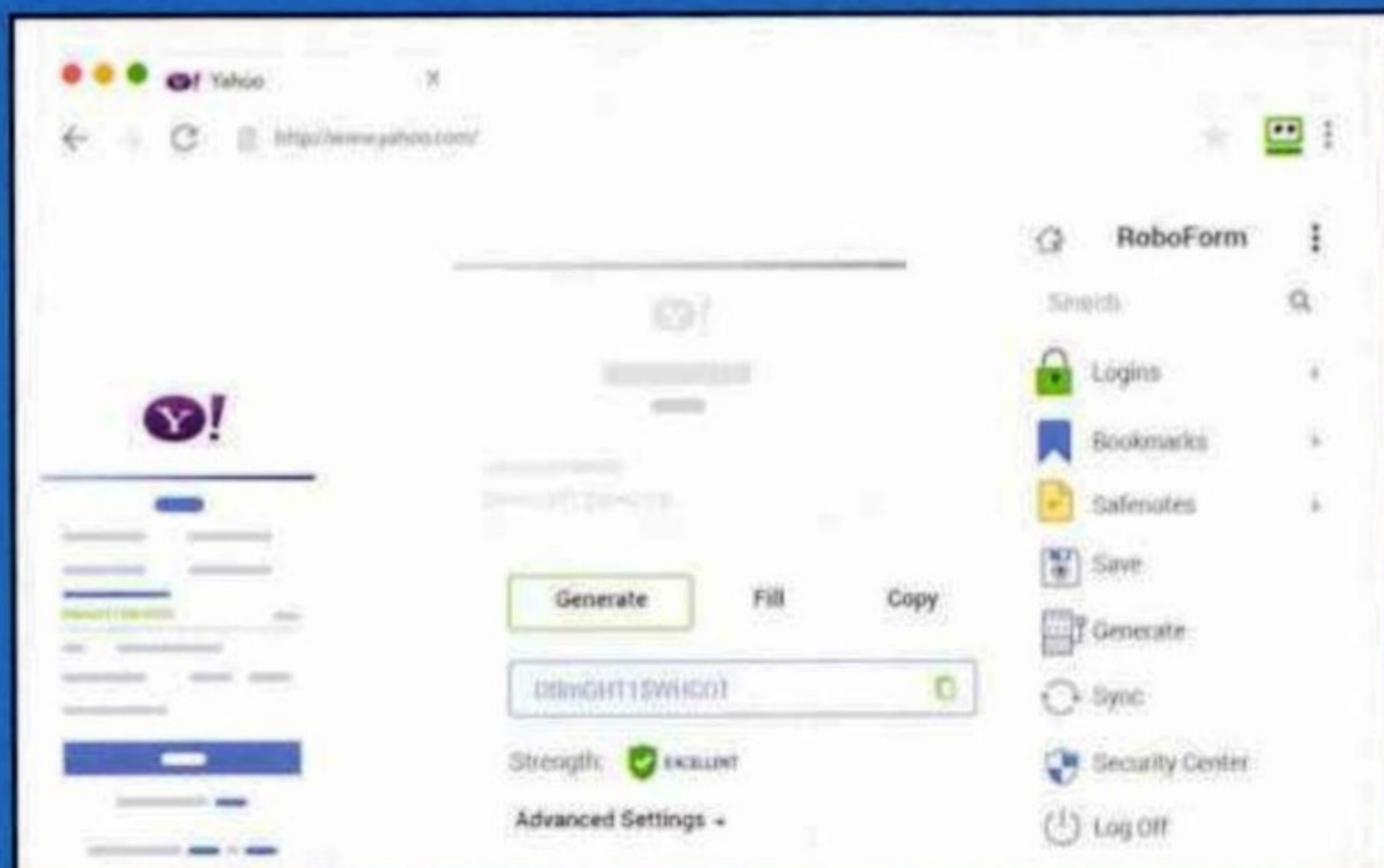


➤ TOP5 GESTIONNAIRE DE MOTS DE PASSE

ROBOFORM > LES ROBOTS SONT ÉTERNELS

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

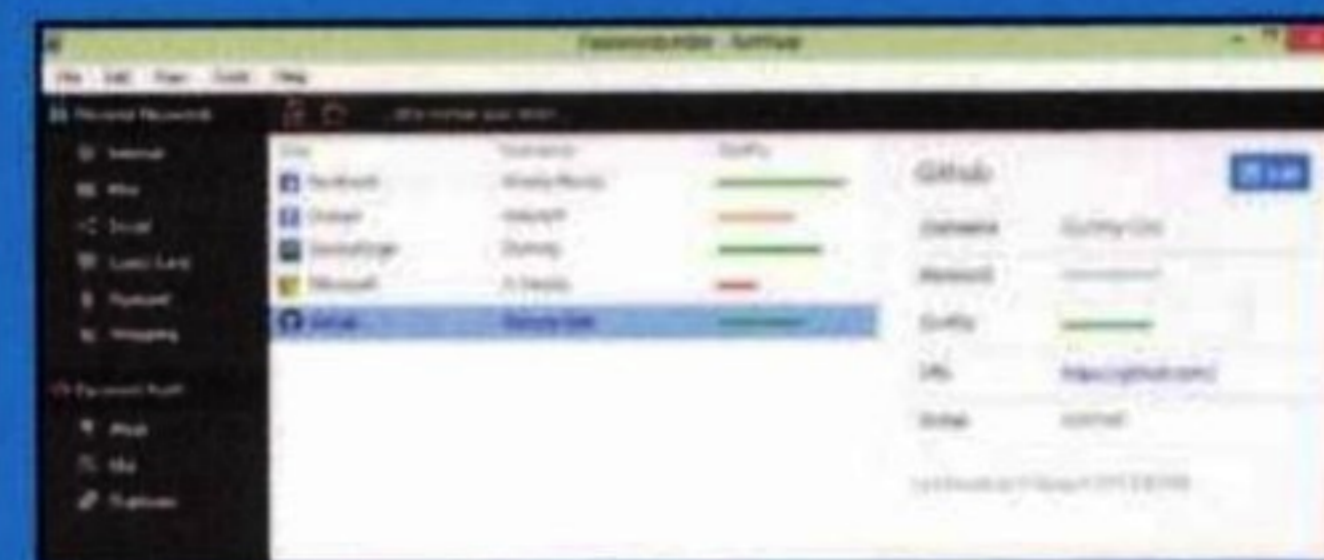
Lien : www.roboform.com



KEEPASS > L'USINE BLINDÉE

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

Lien : keepass.fr



STICKY PASSWORD > BIOMÉTRIE INTÉGRÉE

Basé sur un chiffrement AES-256, nous avons surtout remarqué la prise en charge par Sticky Password de la biométrie. Cela signifie que si vous verrouillez votre smartphone par empreinte digitale,

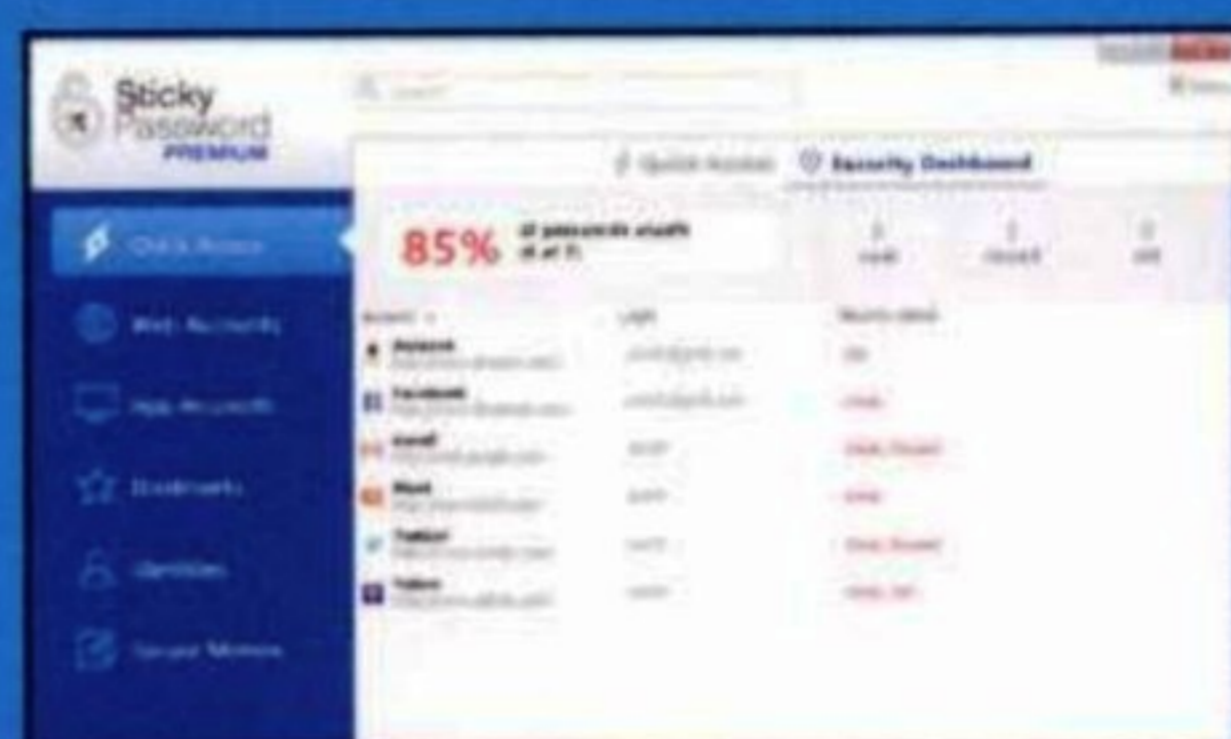
StickyPassword suivra le mouvement ! La version gratuite est complète, hormis une offre Cloud réservée aux membres Premium.

Lien : www.stickypassword.com

DASHLANE > LA TENTATION PC

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

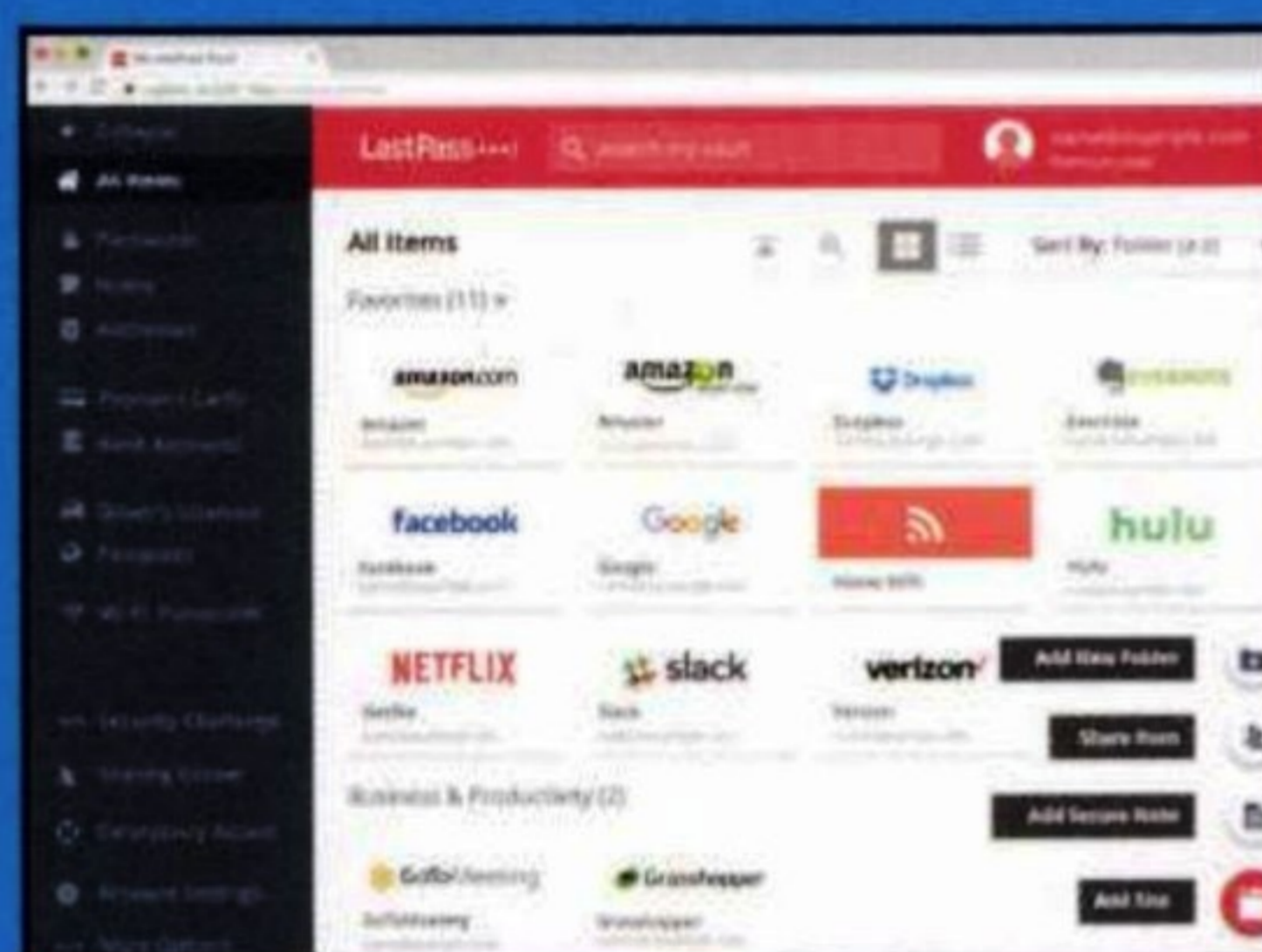
Lien : www.dashlane.com



LASTPASS > LE + POPULAIRE

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

Lien : www.lastpass.com/fr



MEDIAPART > SECUREDROP

Le média indépendant qui adore les révélations croustillantes utilise le service de transfert de fichiers SecureDrop, développé spécialement pour le navigateur Tor. Il permet aux internautes de partager des documents avec les journalistes du pôle enquête de façon sécurisée et anonyme.

Lien : www.mediapart.fr/contact/securedrop



RADIO FRANCE > BONNES ONDES

Le tout dernier service, lancé en décembre dernier, est celui de Radio France. Les auditeurs et les internautes peuvent transmettre des informations de manière anonyme et sécurisée. Les informations recueillies seront examinées par la Cellule Investigation du groupe. Le téléchargement de Tor est recommandé par le service.

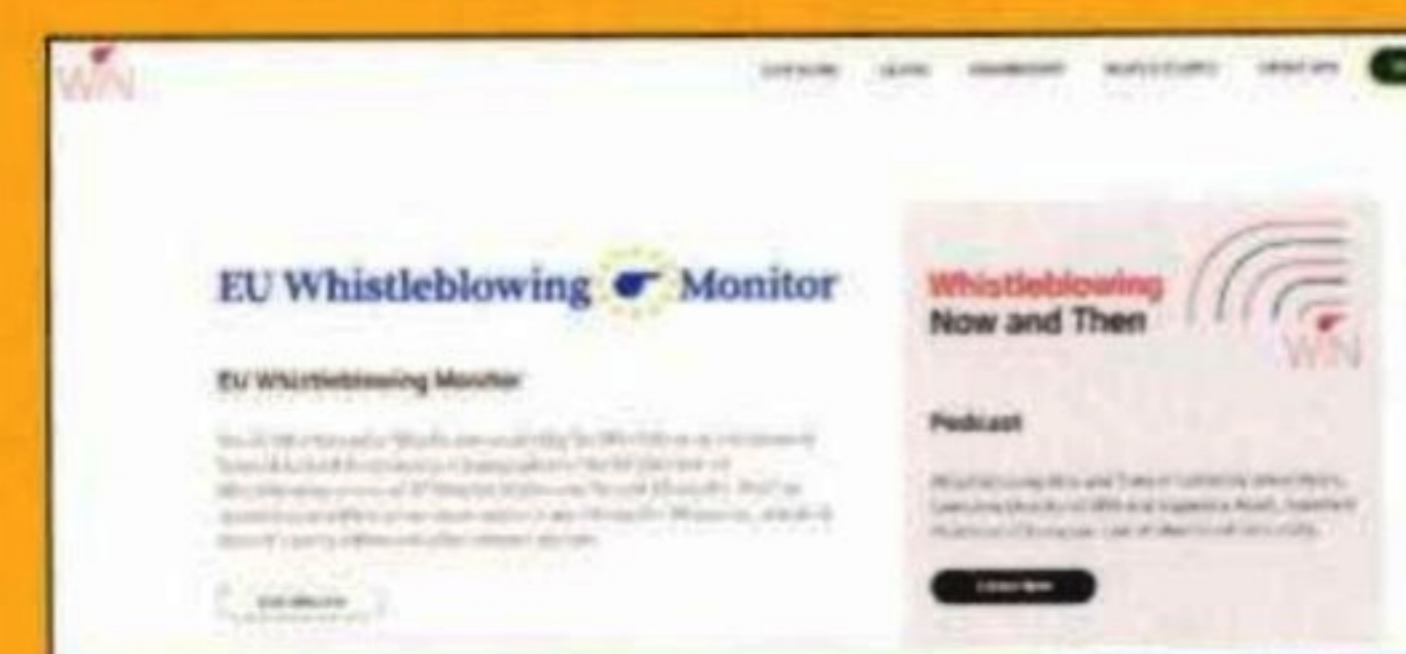
Lien : alerter.radiofrance.fr



WHISTLEBLOWING NETWORK > INTERNATIONAL

Une organisation à but non lucratif qui soutient les lanceurs d'alerte dans le monde entier, en leur offrant une plateforme pour partager leurs histoires et obtenir de l'aide juridique et psychologique. Seul (gros) bémol : le site est en anglais.

Lien : whistleblowingnetwork.org



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



*Offre valable jusqu'au 31 décembre 2023. 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

Signature obligatoire :

LES DOSSIERS DU Pirate

DES DOSSIERS
THÉMATIQUES
COMPLETS

À DÉCOUVRIR
EN KIOSQUES

PETIT FORMAT

MINI PRIX

CONCENTRÉ
D'ASTUCES



Actuellement

#Guide pratique

OBJECTIF :
ZÉRO TRACE !



CODE MESSAGERIES

ANONYMAT

CLOUD

ANTI-CENSURE

MOBILE

SURVEILLANCE

STREAMING



PIRATE
INFORMATIQUE



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