TUTOS & ASTUCES
ÉTAPE PAR ÉTAPE

LE GUIDE *ANTI-SURVEILLANCE*

PC N°60

TRUCS & ASTUCES

FICHES PRATIQUES

ANONYMAT & VIE PRIVÉE

PC & WEB 100% PROTÉGÉS





TOUT FAIRE FACILEMENT

VIE PRIVÉE
> EFFACEZ vos TRACES sur PC

ANONYMAT
> Les MEILLEURES ASTUCES pour VPN

DONNÉES
> Attention à CHATGPT !

HISTORIQUE
> AMAZON : Arrêtez le suivi !

INTERNET
> Comment DOPER sa NAVIGATION PRIVÉE

RÉSEAU
> OBJETS CONNECTÉS : Repérez les traitres

PC & Fichiers

CHIFFREZ en **LOCAL** et dans le **CLOUD** !

Dossier

Le **GUIDE** pour un **WHATSAPP ANONYME & SÉCURISÉ**

Qui m'espionne ?

REPÉREZ ET COUPEZ LES **FUITES DE DONNÉES** À LA **SOURCE** !

SOMMAIRE

N°60 – JANV. / MARS 2026

DÉCRYPTAGE & REPÈRES



04 USURPATION D'IDENTITÉ : La fraude qui n'arrive pas qu'aux autres

INTERNET & RÉSEAUX

Naviguez et communiquez incognito.

10 Le MYTHE de la NAVIGATION PRIVÉE : Quelles traces subsistent vraiment ?



13 FINGERPRINTING : Vous êtes PROFILÉS à VOTRE INSU



16 Fuites WEBRTC : La FAILLE INVISIBLE qui SABOTE votre anonymat





20 CHATGPT : Gardez le CONTRÔLE sur vos DONNÉES !

23 **DOSSIER** Le GUIDE pour un WHATSAPP ANONYME et SÉCURISÉ



34 EFFACEZ L'HISTORIQUE de votre navigation sur AMAZON

100 % PRATIQUE – 100 % GRATUIT

35 Créez un ACCÈS WI-FI TEMPORAIRE pour PARTAGER votre connexion



38 TOP 3 > Pour surveiller vos OBJETS CONNECTÉS



40 TOP 3 > Outils pour CONTRÔLER ses DONNÉES



42 5 ASTUCES pour votre VPN



PC & FICHIERS

Votre ordi et son contenu à l'abri des regards.

48 TOP 3 > LOGICIELS de CHIFFREMENT

49 MASQUER un DOSSIER sur Windows



50 CHIFFREZ votre CLÉ USB avec ROHOS





52 CRYPTOMATOR : PROTÉGEZ vos DOSSIERS SENSIBLES sur PC et dans le CLOUD

58 EFFACEZ vos TRACES avec GLARY

60 Envoyez une NOTE CHIFFRÉE avec ENCLOSED

62 EMPREINTES DIGITALES : Vendre son âme à Google ?



Décryptage & Repères



USURPATION D'IDENTITÉ

LA FRAUDE QUI N'ARRIVE PAS QU'AUX AUTRES

L'usurpation d'identité est le fait de prendre, sans son accord, l'identité ou les données personnelles d'une autre personne et de les utiliser dans un but malveillant. Le plus souvent pour effectuer des opérations financières, pour nuire à votre réputation ou encore pour commettre des actes illégaux en votre nom. Une vague de fond qui grossit chaque année et qui pourrait se transformer en tsunami avec la généralisation des démarches en ligne et de l'ingénierie sociale dopée à l'intelligence artificielle.

200 000.

Ce serait, selon France Victimes, le nombre de personnes victimes d'une usurpation d'identité chaque année en France. Avec la généralisation des démarches dématérialisées, ce chiffre atteint des proportions industrielles. C'est presque autant que le nombre de cambriolages et bien plus que celui de vols de voitures.
Nous sommes tous susceptibles d'être, un jour ou l'autre, victimes d'une usurpation d'identité. Nos données personnelles nous sont demandées



PHISHING

pour opérer de très nombreuses démarches, y compris anodines. Nous envoyons régulièrement des copies de documents officiels (justificatifs de domicile, pièces d'identité, etc.) sans être toujours certains de la sécurisation des organismes destinataires. Des identifiants, des documents et des bases de données sont volés et collectés frauduleusement, chaque jour, sur le Web... ou à domicile (poubelle, boîte aux lettres). Et de nombreux escrocs vous appelleront directement ou viendront même à votre porte pour obtenir ces informations, en se faisant passer pour telle ou telle autorité.

Quelles conséquences possibles ?

Les cybercriminels, armés de ces données personnelles et éventuellement de documents officiels ou copies, peuvent orchestrer une variété de délits en leur nom, incluant l'ouverture de comptes bancaires, la souscription à des abonnements téléphoniques, l'obtention de prêts, la création de profils sur les réseaux sociaux,

QUELS SONT LES TYPES DE DONNÉES OU DE DOCUMENTS NÉCESSAIRES À UNE USURPATION D'IDENTITÉ ?

L'usurpation d'identité par des cybercriminels peut se faire de différentes manières et nécessiter divers types d'informations ou de documents. En général, voici les informations, types de données personnelles et documents les plus couramment recherchés par les cybercriminels pour réussir une usurpation d'identité :

1# DONNÉES PERSONNELLES

- **Nom complet :** Souvent le point de départ pour d'autres recherches.
- **Date de naissance :** Utilisée en combinaison avec d'autres données.
- **Adresse postale :** Peut être utilisée pour des fraudes par correspondance ou pour obtenir d'autres informations personnelles.
- **Numéro de Sécurité sociale**: Permet l'accès à une multitude de services et informations financières.
- **Numéros de téléphone :** Utilisés pour la récupération de compte ou la vérification d'identité.
- **Adresses email :** Peuvent être utilisées pour le phishing ou l'accès à d'autres comptes via la récupération de mot de passe.
- **Mots de passe et identifiants de connexion :** Donnent un accès direct à des comptes personnels et financiers.
- **Données bancaires et financières :** Numéros de compte, numéros de carte de crédit, PIN, etc.
- **Questions et réponses de sécurité :** Souvent utilisées pour réinitialiser les accès aux comptes.
- **Photographies et informations biométriques :** Utilisées pour créer de faux documents ou contourner certaines sécurités basées sur la reconnaissance faciale.

2# DOCUMENTS OU COPIES DE DOCUMENTS



- **Carte d'identité nationale ou passeport :** Permettent une usurpation d'identité complète.
- **Permis de conduire :** Peut être utilisé comme pièce d'identité dans de nombreux contextes.
- **Relevés bancaires ou factures :** Contiennent des informations financières précises.
- **Justificatifs de domicile :** Utilisés pour prouver une adresse lors de la création de comptes ou la souscription de services.
- **Cartes de sécurité sociale ou d'assurance santé :** Donnent accès à des services et prestations.
- **Documents officiels signés :** Contrats, actes notariés, etc., peuvent être falsifiés ou modifiés.
- **Correspondance officielle :** Lettres de l'administration, décisions judiciaires, peuvent être détournées pour obtenir d'autres documents ou informations.

Décryptage & Repères

À SAVOIR

L'usurpation d'identité est punissable par la loi, entraînant jusqu'à un an d'emprisonnement et 15 000 euros d'amende pour utilisation frauduleuse des données identifiant une personne dans l'intention de nuire.

Les arnaques deviennent de plus en plus sophistiquées et crédibles, notamment grâce à l'aide d'outils basés sur l'intelligence artificielle. Ici, la DGCCRF met en garde contre des escrocs se faisant passer cette année pour certains de ses agents et tentant d'obtenir des informations sensibles.


DGCCRF

Direction générale de la concurrence, de la consommation et de la répression des fraudes

Actualités | La DGCCRF | Concurrence | Consommation | Sécurité | Infos presse | Publications | Sanctions | FAQ

Usurpation d'identité de la DGCCRF : attention arnaque !

La DGCCRF fait régulièrement l'objet d'arnaque à l'usurpation d'identité.

PROUVER SON INNOCENCE RELÈVE DU PARCOURS DU COMBATTANT POUR LES VICTIMES.

RÉAGIR À UNE USURPATION D'IDENTITÉ : GUIDE D'ACTION

1) COLLECTE DE PREUVES

Amassez toutes les preuves attestant de l'usurpation (messages, URL, documents justificatifs, captures d'écran) et contactez immédiatement les plateformes impliquées pour signaler le délit et demander la suppression de vos informations personnelles.

2) DÉPÔT DE PLAINTE

Portez plainte auprès de la police, de la gendarmerie, ou par courrier adressé au procureur de la République. Conservez une copie de chaque plainte, qui vous sera utile dans vos démarches ultérieures.

3) ALERTEZ VOTRE BANQUE ET VOS ORGANISMES FINANCIERS

Informez sans délai vos institutions bancaires de la situation pour surveiller toute activité suspecte sur vos comptes et, en cas de vol de données bancaires, faites opposition.

4) RENOUVELLEMENT DES PIÈCES D'IDENTITÉ

C'est essentiel pour que d'autres documents en libre circulation soient considérés comme caducs. Faites annuler et renouveler vos documents d'identité volés.

5) ATTESTATION SUR L'HONNEUR

Pour les démarches auprès des différents organismes, fournissez une attestation sur l'honneur accompagnée d'une copie de votre plainte.

6) CONTACTEZ LA BANQUE DE FRANCE

Signalez l'usurpation à la Banque de France pour vérifier l'ouverture frauduleuse de comptes ou de crédits en votre nom, et pour vous assurer de ne pas être inscrit sur des fichiers d'incidents bancaires.

7) FAITES-VOUS AIDER

Pour toute assistance, contactez France Victime au 116 006 et la plateforme Info Escroquerie au 0 805 805 817, services gratuits offrant conseils et accompagnement. En cas de besoin, un avocat peut également vous aider à défendre vos droits.

la location de véhicules, le non-paiement d'amendes (infractions routières, transports, etc.), la publication d'annonces frauduleuses, l'arnaque de proches, etc.
Sous couvert d'une fausse identité, ils peuvent aussi se faire passer pour un autre dans des cas de harcèlement en ligne, de chantage, de diffamation ou d'extorsion. Ces agissements placent les victimes dans une position précaire, les forçant à prouver leur innocence face à des infractions, délits ou crimes qu'elles n'ont pas commis. Et cela est un véritable parcours du combattant.

Un business qui a de l'avenir

Aux États-Unis, des sociétés spécialisées offrent leurs services pour répondre aux besoins de victimes de plus en plus nombreuses ou pour prévenir les risques d'usurpation. Et oui, au pays de l'Oncle Sam, quand un nouveau marché se développe, il y a toujours une entreprise privée qui se crée immédiatement au coin de la rue ! Lifelock, IdentityForce et Experian IdentityWorks par exemple offrent une surveillance des données personnelles et financières, alertes en cas d'activité suspecte, et apportent leur assistance en cas d'usurpation. Lifelock se distingue par son service de compensation en cas de vol d'identité. IdentityForce offre une surveillance étendue incluant les médias sociaux. Experian IdentityWorks combine la surveillance de l'identité avec des rapports de crédit détaillés. Les prix varient selon le niveau de service, généralement de quelques euros à plusieurs dizaines d'euros par mois.

TROIS EXEMPLES D'USURPATION D'IDENTITÉ

> PRÊT DE 500 000 EUROS

Virginie, une Normande, a vécu un cauchemar financier après que sa carte d'identité a été volée, menant à son usurpation d'identité. Comme le raconte Capital, des escrocs ont acheté un immeuble en son nom, engendrant une dette de 500 000 euros. Elle s'est retrouvée contrainte de vivre dans sa voiture, même en étant employée. La situation est devenue si critique que la banque, face aux impayés, s'est retournée contre elle, la laissant avec la responsabilité de rembourser les frais liés à l'immeuble. Un procès est prévu en 2025 pour résoudre cette affaire.

> 7300 EUROS D'AMENDES À SON NOM



Charly Acosta, étudiant en odontologie à Montpellier, subit depuis trois ans les conséquences d'une usurpation d'identité. Comme le raconte Le Parisien, des fraudeurs voyageant sans billet ont utilisé son identité, accumulant plus de 7 300 euros d'amendes à la SNCF en son nom. Charly doit désormais prouver qu'il n'était pas sur les trajets incriminés, une procédure chronophage qui impacte ses études et finances. Malgré ses efforts, les courriers de recouvrement et les saisies directes sur son compte bancaire continuent, aggravant sa situation financière et psychologique.

> 25 ANS DE CAUCHEMAR

Présentée dans Envoyé Spécial fin 2023, l'histoire de José illustre la difficulté à faire réparer une usurpation d'identité. Il a vécu un véritable cauchemar après le vol de ses papiers, en 2000, empêchant des événements importants comme la reconnaissance de ses enfants. La plainte déposée n'a pas empêché l'escroc de s'accrocher à cette fausse identité, puisque José apprend qu'il est « marié », à Londres, avec une femme qu'il ne connaît pas. Sous son nom, l'usurpateur a un emploi, des enfants... et a maille à partir avec la justice. José se voit réclamer des impôts impayés, des remboursements de prêts, etc. L'usurpation de son identité lui a coûté cher, l'impliquant même dans des affaires de viol et séquestration dont il était innocent, et l'a privé de ses droits sociaux et professionnels. Même après la condamnation de l'escroc, José continue de subir les conséquences de cette longue période d'usurpation.



En France, c'est la société ID Protect qui fait figure de pionnière en la matière. Elle se propose d'enquêter et de vous accompagner dans vos démarches, sous la forme de forfaits allant de 79 à 489 euros. Côté prévention, un système de surveillance en continu et d'alertes est proposé sous forme d'abonnements mensuels.

LES DOSSIERS DU

Pirate

DES DOSSIERS THÉMATIQUES COMPLETS

À DÉCOUVRIR EN KIOSQUES

- PETIT FORMAT
- MINI PRIX
- CONCENTRÉ D'ASTUCES



100% Windows

Actuellement #Guide pratique

LE GUIDE 2026 DU HACKER

INTERNET & RÉSEAUX

Naviguez et communiquez incognito !

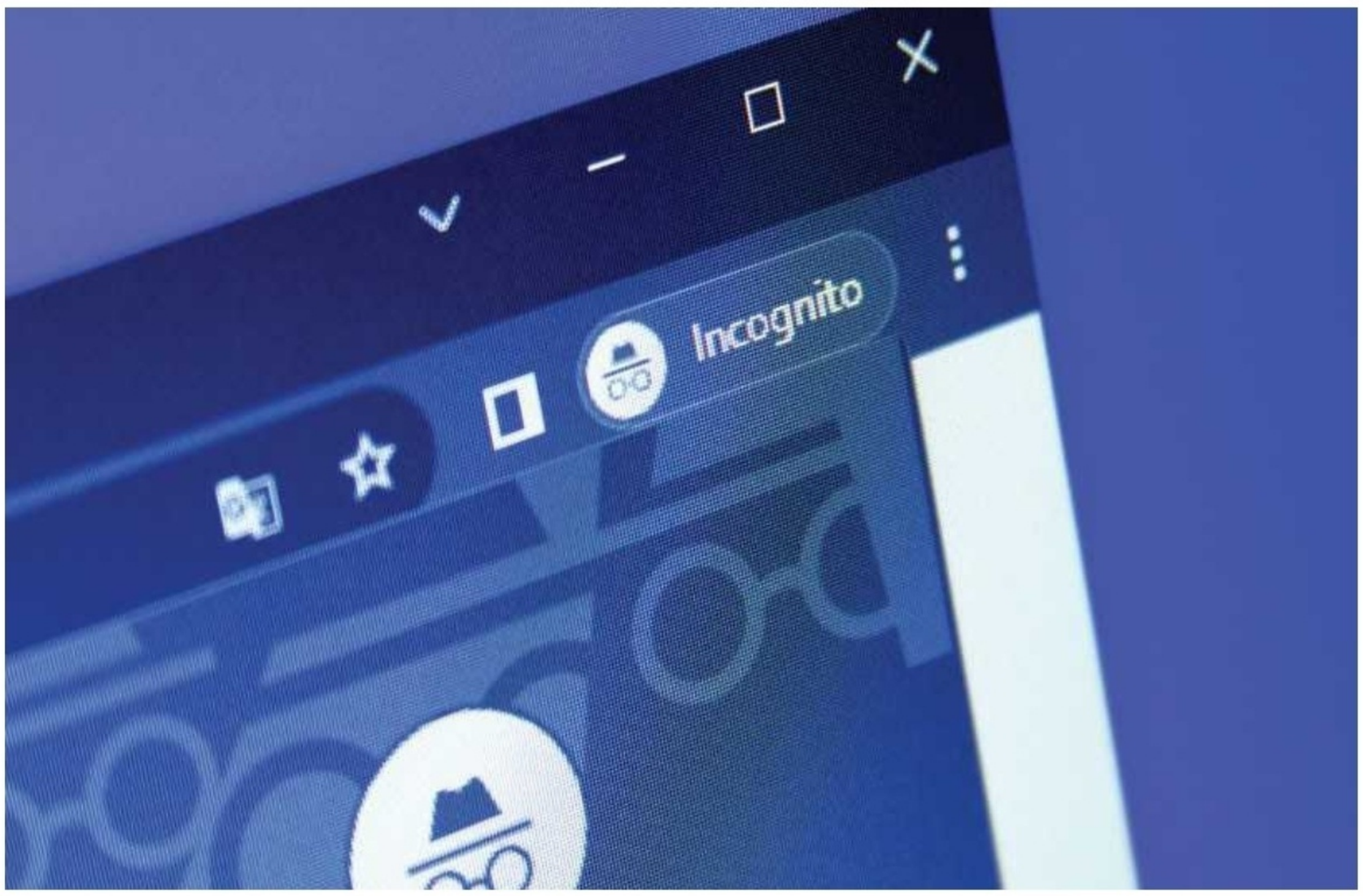


Internet & Réseaux

LE MYTHE DE LA NAVIGATION PRIVEE

Quelles traces subsistent vraiment ?

La navigation privée est un outil utile, mais limité. Un rideau fermé n'est pas une forteresse. Beaucoup d'informations continuent de fuiter et d'être interceptées par des tiers.



On l'active machinalement, comme un geste rassurant : clic droit, "Nouvelle fenêtre privée" ou le mode Incognito pour Chrome. En un instant, Chrome, Firefox ou Edge se parent d'un fond sombre, symbole commode d'une invisibilité supposée. Pour des millions d'utilisateurs, cette simple action suffirait à devenir introuvable : aucune trace, aucune fuite, aucune surveillance possible.

La réalité est pourtant bien différente. Si la navigation privée protège localement, elle laisse derrière elle une traîne de signaux visibles sur le réseau, chez les sites visités et auprès des fournisseurs d'accès. Autrement dit, elle n'est privée… que dans un périmètre très réduit.

Une protection efficace… mais simple

L'essor de ce mode, popularisé d'abord par Safari au milieu des années 2000, répondait à une demande simple : éviter que d'autres personnes utilisant le même ordinateur puissent lire votre historique, vos cookies, ou vos recherches. Et sur ce point, la promesse est tenue : la navigation privée n'enregistre ni historique, ni cookies persistants, ni formulaires sur l'appareil. Une fois la fenêtre fermée, tout disparaît. Mais il demeure beaucoup d'autres informations et données qui ne sont pas concernées par cette protection !

Pistage et profilage continuent

Car même en mode privé, le navigateur continue d'envoyer votre adresse IP, votre empreinte numérique (fingerprinting), votre résolution d'écran, vos polices installées, les informations de votre système d'exploitation, et même parfois des identifiants réseau



uniques générés par les services web. Les sites conservent également les pages consultées, et votre fournisseur d'accès sait toujours où vous êtes allé, à quelle heure, et pendant combien de temps.

CHROME INCOGNITO : QUAND "PRIVÉ" NE L'ÉTAIT MÊME PAS ASSEZ



La confiance dans le mode Incognito de Chrome a été secouée par l'une des affaires de vie privée les plus médiatisées de ces dernières années. Tout commence en 2020, lorsqu'une action collective est déposée aux États-Unis : des utilisateurs accusent Google de continuer à collecter leurs données — notamment via Google Analytics, Ad Manager et des cookie-less identifiers — même lorsqu'ils naviguaient en mode Incognito, supposé protéger de ces pratiques.Après plusieurs rebondissements judiciaires, Google accepte en avril 2024 un règlement historique : la firme annonce la suppression de plusieurs milliards de fichiers de données liés à la navigation privée et s'engage à rendre ses avertissements plus explicites sur ce que couvre réellement le mode Incognito. L'entreprise reconnaît ainsi — sans aveu de faute — que son interface prêtait à confusion.
En août 2024, une cour d'appel permet cependant à certains plaignants de continuer à réclamer des dommages individuels, estimant que la formulation initiale de Google pouvait objectivement induire en erreur.

BEAUCOUP ONT CONFONDU "DISCRÉTION LOCALE" ET "INVISIBILITÉ GLOBALE". OR C'EST PRÉCISÉMENT LÀ QUE LE MYTHE COMMENCE.

→ NAVIGATION PRIVÉE

Internet & Réseaux

Les entreprises publicitaires n'ont aucun mal à retrouver un utilisateur venant d'une fenêtre privée : la combinaison de ses paramètres forme une signature quasi unique, capable de le suivre d'un site à l'autre. Les fuites WebRTC, quant à elles, peuvent parfois exposer l'adresse IP réelle, même derrière un VPN mal configuré — preuve supplémentaire que "privé" n'est pas synonyme de "cloisonné".
Les utilisateurs le découvrent souvent à leurs dépens : billets d'avion qui changent mystérieusement de prix, publicités ciblées qui réapparaissent après une session "privée", ou formulaires préremplis malgré une apparente absence d'historique. En réalité, la navigation privée ne protège que de l'utilisateur suivant, pas d'Internet lui-même.

Incomplet mais utile

Alors faut-il abandonner ce mode ? Certainement pas : il reste extrêmement pratique pour éviter l'encombrement de cookies, tester un service sans personnalisation, se connecter à plusieurs comptes en parallèle ou limiter certaines formes de pistage basique. Mais l'utilisateur doit savoir ce qu'il obtient — et surtout ce qu'il n'obtient pas.
À l'heure où les menaces numériques, les trackers publicitaires et les systèmes d'identification se multiplient, le véritable outil de protection reste le chiffrement, le VPN, les bloqueurs de scripts, les navigateurs durcis contre le fingerprinting (comme Brave, Tor Browser ou Mullvad Browser) et une bonne dose de scepticisme.

Ce que la navigation privée PROTÈGE VRAIMENT	Ce qu'elle NE PROTÈGE PAS
- L'historique local n'est pas enregistré	- Votre adresse IP reste visible pour les sites
- Les cookies ne sont pas conservés après fermeture	- Votre FAI voit toujours vos connexions
- Les recherches ne sont pas ajoutées au navigateur	- Le fingerprinting fonctionne toujours
- Les sessions simultanées sont possibles (ex. deux comptes Gmail)	- Les trackers publicitaires continuent de vous profiler
	- Les fuites DNS, WebRTC ou scripts tiers restent actives

FIREFOX 145 : UN SAUT EN AVANT POUR LA NAVIGATION PRIVÉE

La version 145 de Firefox, publiée le 11 novembre 2025, introduit une nouvelle phase de protections anti-fingerprinting, dans les modes "Navigation privée" et "Protection renforcée contre le pistage (ETP Strict)". Selon les tests, le taux d'utilisateurs pouvant être identifiés de façon unique via des techniques de fingerprinting passe de plus de 60 % à environ 20 %.
Les protections incluent l'obfuscation de certaines caractéristiques : résolution d'écran, support tactile, nombre de cœurs CPU, polices système, ajout de « bruit » dans les rendus graphiques. Attention, ces protections s'appliquent dans les modes privés ou ETP Strict pour le moment — l'activation par défaut pour tous les utilisateurs est prévue mais pas encore généralisée. En pratique pour l'utilisateur grand public : activer la navigation privée et passer Protection renforcée contre le pistage en mode Strict dans les paramètres de confidentialité améliore sensiblement l'anonymat sans nécessiter d'extension externe.



FINGERPRINTING : VOUS ÊTES PROFILÉ À VOTRE INSU



Pas d'empreinte digitale à proprement parler ici. Dans le domaine de la navigation Web, le fingerprinting est une collecte de données qui s'affranchit des cookies et de vos habitudes de navigation pour se concentrer, en douce, sur toutes les petites infos techniques qui accompagnent votre navigateur.

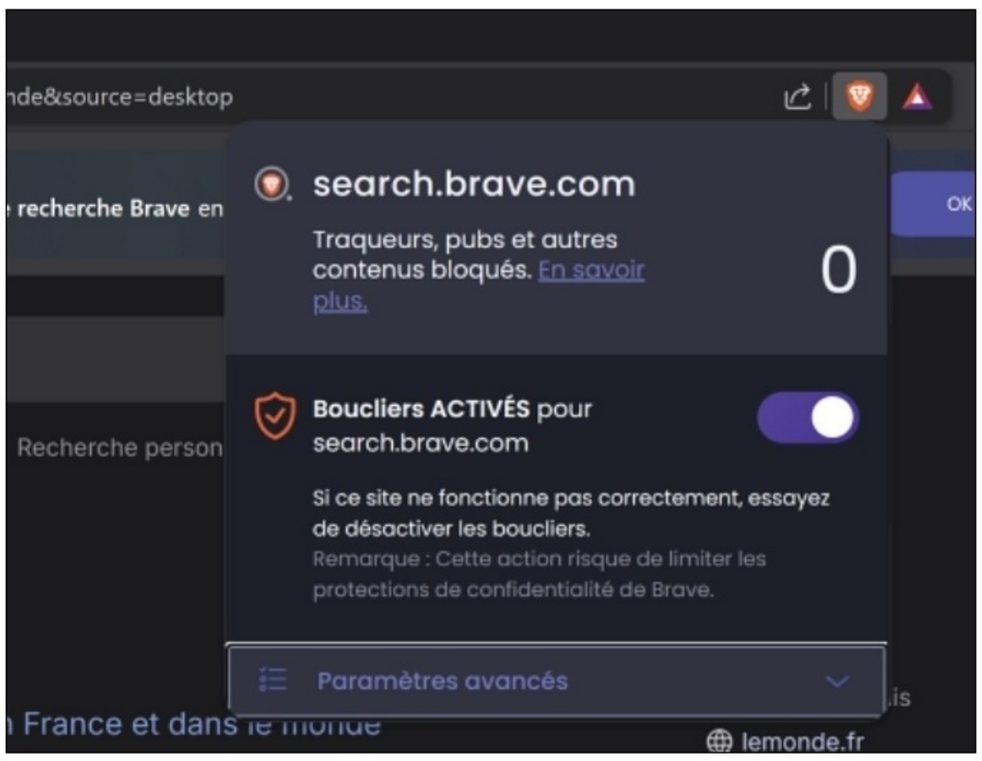
Imaginez : vous entrez dans un bar incognito, capuche baissée… mais le serveur annonce à voix haute : "Un espresso pour la personne mesurant 1 m 78, chaussant du 44, parlant français, équipée d'un Fairphone 5 sous Windows 11, réglé à 120 Hz !" Pas besoin de votre nom : ce cocktail de détails suffit à vous "re identifier". Sur le Web, c'est exactement ce que fait le « browser fingerprinting ».
À chaque fois que vous naviguez, le fingerprinting collecte, via JavaScript et les API du navigateur, des dizaines de micro caractéristiques : résolution d'écran, polices installées, fuseau horaire, version GPU, liste des capteurs, codec vidéo, empreinte Canvas/WebGL, comportement AudioContext, et même la façon dont votre CPU calcule ϖ (tout le monde n'arrive pas à la même décimale au même moment). Assemblées, ces valeurs créent un identifiant statistiquement unique – on parle "d'entropie" : plus il y a de bits d'entropie, plus l'empreinte est unique. Les chercheurs estiment qu'une quinzaine de paramètres suffisent souvent à isoler un internaute sur des millions. On parle parfois de "super cookies" : ces micro-caractéristiques ne se stockent pas dans votre navigateur, donc le bouton "Effacer les cookies" ne change rien.

Mais c'est quoi ce pistage ?!

À l'origine (fin 2000), c'était un outil… anti fraude bancaire : repérer un login louche parce qu'il arrive soudain d'un Mac OS Tigre avec une police coréenne alors que l'utilisateur se connecte d'habitude depuis un ThinkPad à Lille. Les publicitaires ont flairé le bon filon quand les cookies ont commencé à sentir le roussi. Résultat : depuis 2021, l'EFF mesure une hausse continue des empreintes "hautement uniques" dans son test Cover Your Tracks (**coveryourtracks.eff.org**).
Page suivante, nous vous montrons comment bloquer ce fingerprinting avec Brave et comment le limiter drastiquement sur Firefox. Mais, attention, certains services pourraient dysfonctionner voir vous refuser l'accès ! Certains pour des raisons de sécurité nécessaires (banques en ligne par exemple), techniques (sites de graphismes, de streaming audio ou vidéo) ou pour de basses raisons commerciales (« si moi pas pouvoir cibler pubs pour toi, moi pas marcher »).

Internet & Réseaux

BLOQUER LE FINGERPRINTING DANS

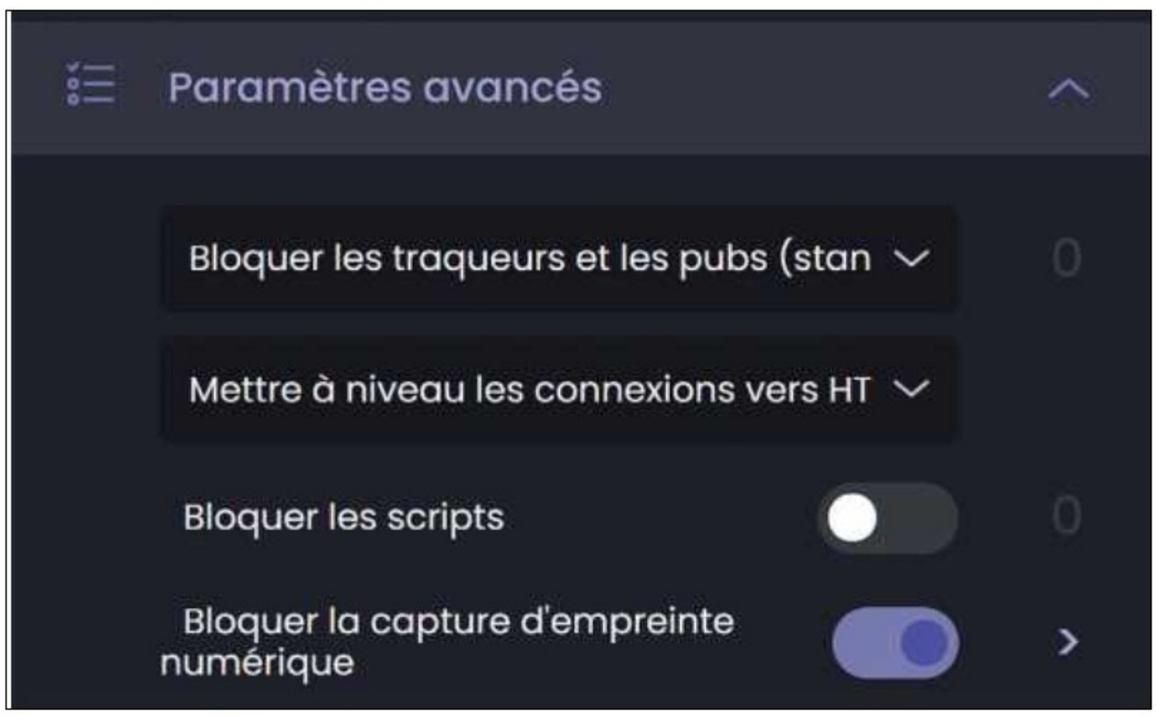


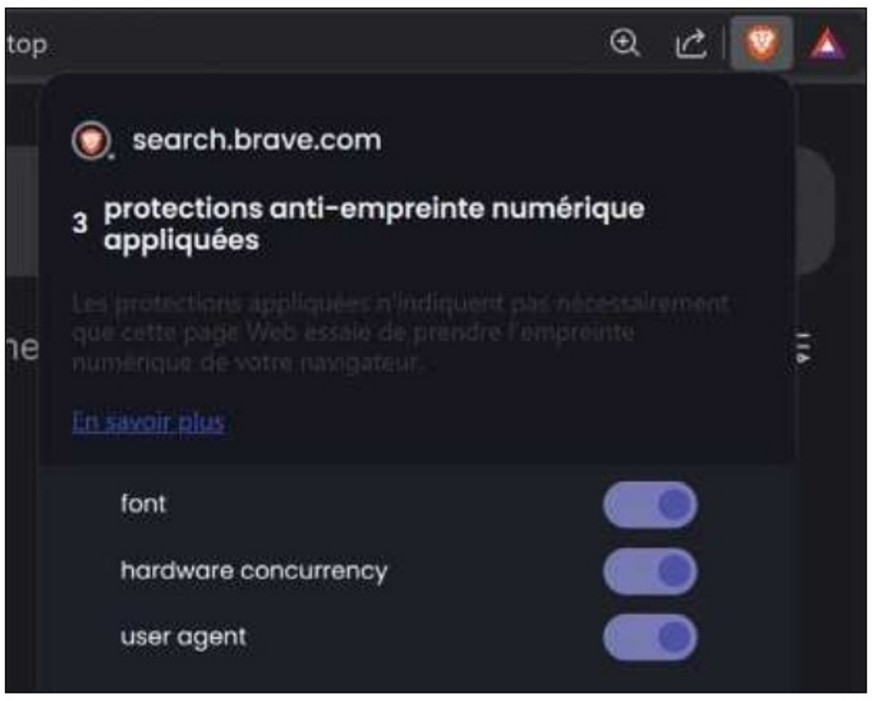
01 Brave Shields

Cliquez sur l'icône **Bouclier** (lion) en haut, à droite de la barre d'adresse pour ouvrir le le panneau Brave Shields. Allez dans **Paramètres avancés**.

02 Vérifier l'activation

Repérez la ligne **Bloquer la capture d'empreinte numérique**. Vérifiez qu'elle soit activée (c'est le réglage par défaut). Brave applique le farbling : les API JavaScript les plus bavardes renvoient des valeurs randomisées.





03 Réglages

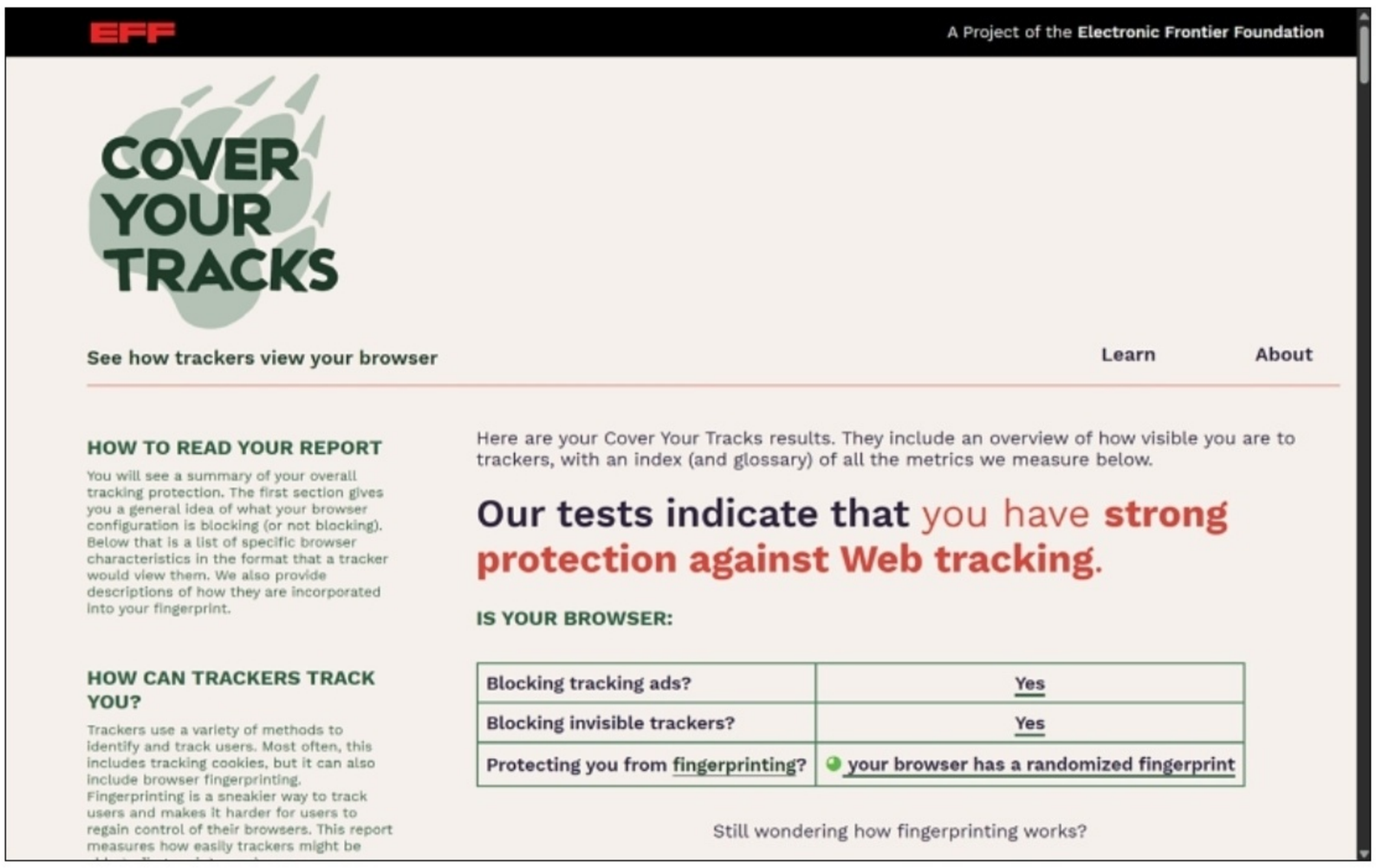
Si un service cartographique ou un éditeur audio refuse de fonctionner avec le farbling, désactivez temporairement la protection pour ce seul site via puis ré-activez-la en partant. Cliquez sur la petite flèche à droite : une liste s'affiche pour désactiver ponctuellement un ou plusieurs sous-composants.

BRAVE
https://brave.com/fr

2 min

Facile

BRAVE



Brave est aujourd'hui le seul "gros" navigateur à activer par défaut un brouillage baptisé farbling, qui modifie subtilement les paramètres afin de rendre votre empreinte aléatoire et donc inutilisable pour le pistage.

04 Tester son empreinte

Renez-vous sur **https://coveryourtracks.eff.org** pour vérifier si votre protection fonctionne et si votre empreinte numérique est bien reconstruite de façon aléatoire. Le résultat doit passer de **unique** à **randomized**.

ET SUR CHROME OU FIREFOX ?

En 2025, Brave reste la solution la plus simple pour "casser" son empreinte : protection active par défaut, désactivation granulaire site par site, et aucun plugin à installer.

Sur Firefox : Firefox offre une défense quasi équivalente mais demande de plonger dans les réglages avancés ; tapez **about:config** dans votre barre de recherche, recherchez **privacy.resistFingerprinting** à **true** pour activer le mode RFP (avec letterboxing). Attendez-vous à du "casse-site" (animations lentes, fuseaux horaires forcés en UTC, etc.).



Sur Chrome : Chrome, lui, avance prudemment via le **Privacy Sandbox** : réduction de l'User-Agent, partitionnement par site, futur IP Protection... mais aucun bouton unique pour bloquer le fingerprinting. L'utilisateur doit se contenter des réglages cookies ou d'extensions tiers (uBlock Origin, CanvasBlocker). Cette approche reste centrée sur l'équilibre publicité/vie privée plutôt que sur l'anonymat strict.

Internet & Réseaux

FUITES WEBRTC : LA FAILLE INVISIBLE QUI SABOTE VOTRE ANONYMAT



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

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

WebRTC (pour Web Real-Time Communication) est une technologie développée par Google en 2011, aujourd'hui intégrée nativement à la plupart des navigateurs (Chrome, Firefox, Edge, Brave, etc.). Elle permet les communications audio, vidéo ou de partage de fichiers en temps réel, sans passer par un serveur central.
En pratique, c'est ce qui permet à des services comme Google Meet, Discord, Jitsi ou même des services de transfert de fichiers peer-to-peer de fonctionner directement dans le navigateur, sans plugin externe.

LE PROBLÈME : WEBRTC PEUT EXPOSER VOTRE IP RÉELLE

Pour établir des connexions directes entre deux utilisateurs (connexion P2P), WebRTC utilise un mécanisme appelé STUN (Session Traversal Utilities for NAT). Ce processus oblige le navigateur à interroger les interfaces réseau de la machine, y compris votre adresse IP publique réelle… même si vous utilisez un VPN.
Résultat ? Un site malicieux peut insérer un simple script JavaScript dans sa page Web pour forcer votre navigateur à révéler :

- Votre adresse IP locale (LAN)

- Votre adresse IP publique réelle, non protégée par le VPN.

Cela se fait silencieusement, sans pop-up ni demande d'autorisation. Votre identité est donc traçable ainsi que le suivi marketing, la possibilité d'attaques ciblées, etc.

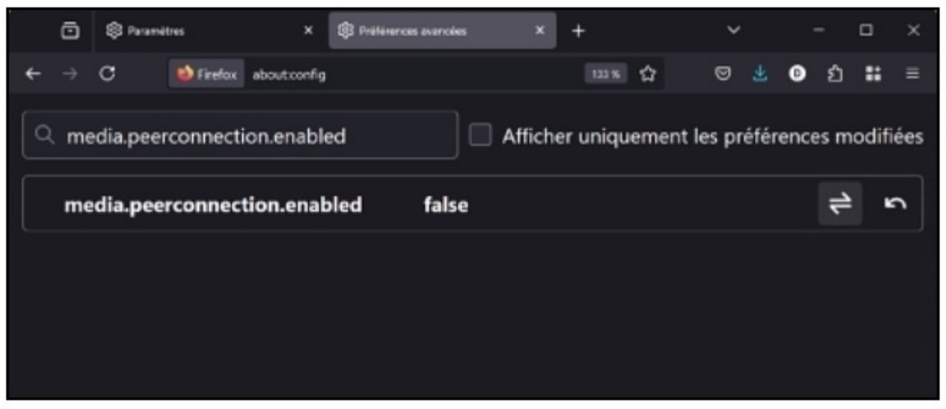
UNE TECHNOLOGIE À ENCADRER

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

MALGRÉ L'USAGE D'UN VPN, VOTRE ADRESSE IP ET DONC VOTRE IDENTITÉ NE SONT PAS À L'ABRI D'UNE FUITE. COMMENT VÉRIFIER ET S'EN PROTÉGER ?

COMMENT SE PROTÉGER ?

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



01 Désactiver WebRTC dans votre navigateur

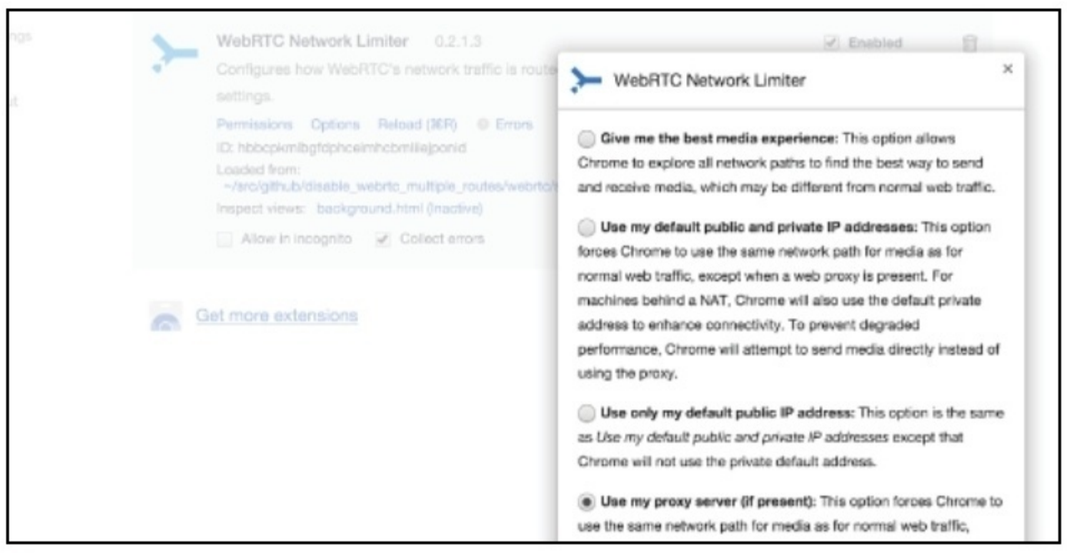
> Firefox : Tapez **about:config** dans la barre d'adresse. Cherchez **media.peerconnection.enabled**. Passez-le **à False**.

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

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

02 Utiliser un navigateur orienté vie privée

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



03 Extensions sélectives

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

04 Tester votre exposition

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





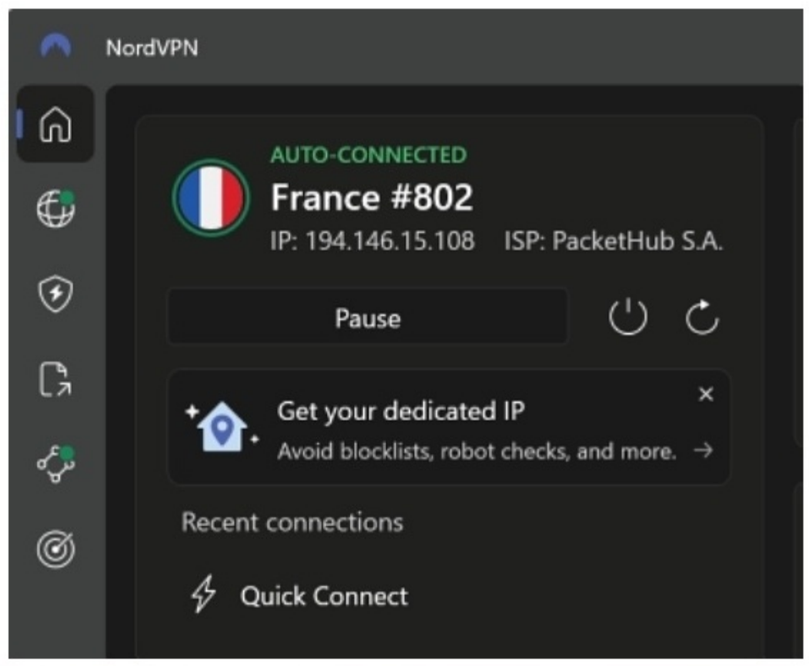
Internet & Réseaux

IPLEAKS : VÉRIFIEZ LES FUITES DE VOTRE IP

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

01 Préparer votre environnement

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





02 Accéder au site

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

03 Bloc IP Adress

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



IPLEAKS
https://ipleak.net

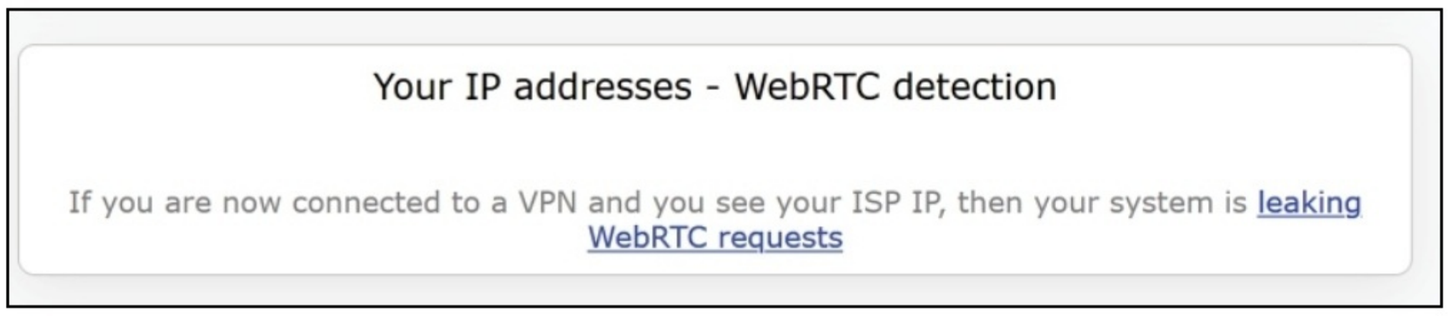
20 min

Moyen

MÊME AVEC UN VPN

04 Bloc WebRTC detection

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





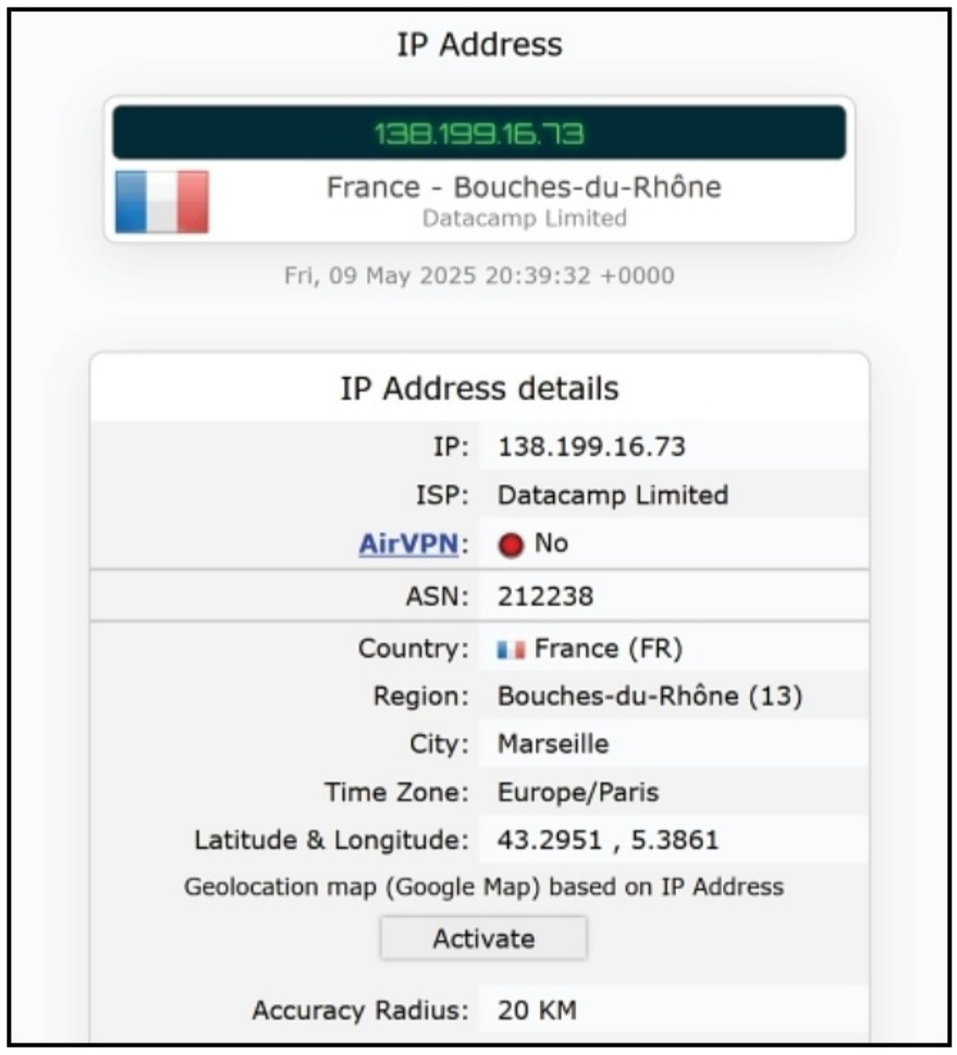
05 Bloc DNS Adresses

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

06 Vérifier un serveur suspicieux

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





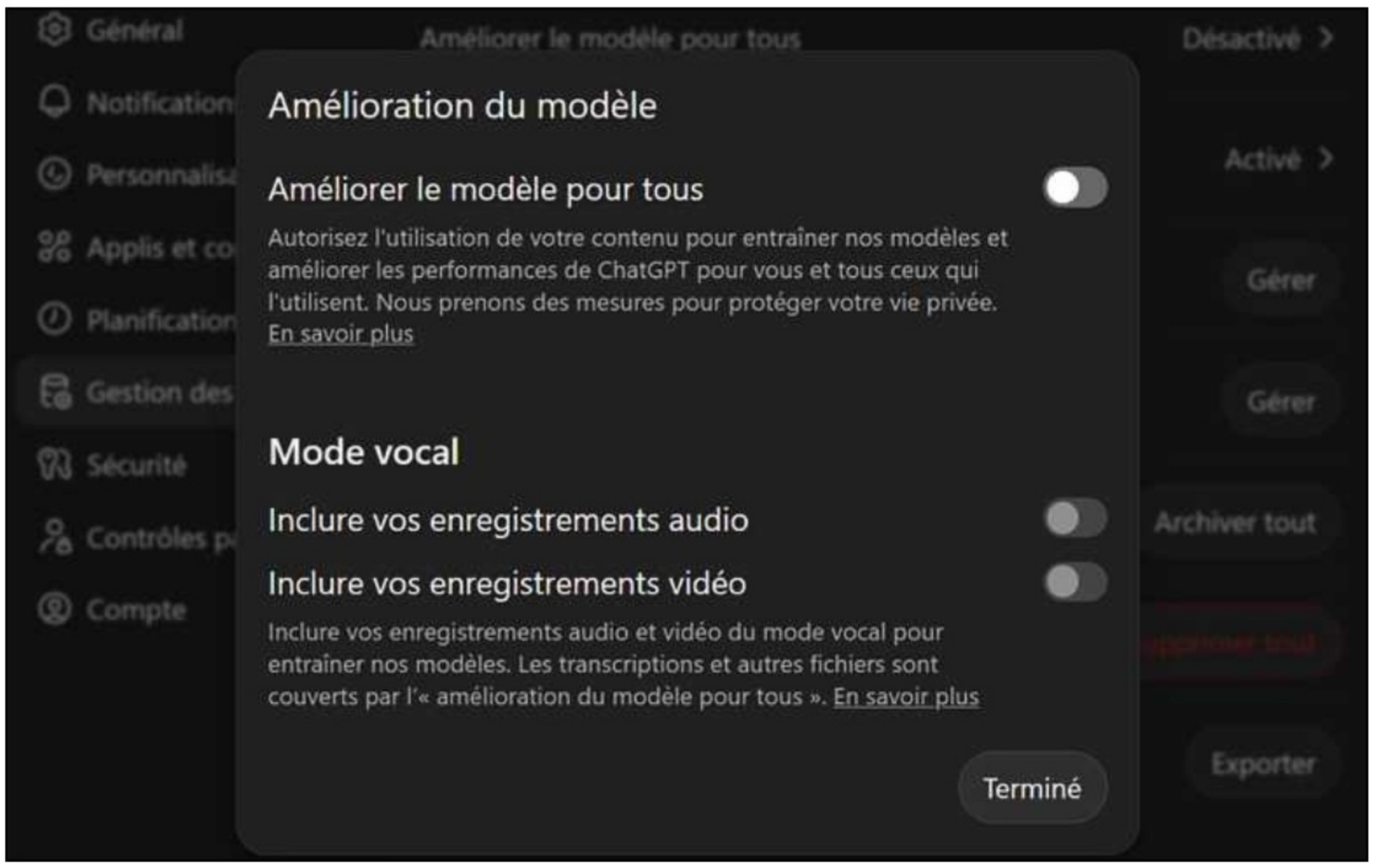
Internet & Réseaux

CHATGPT : GARDEZ LE CONTRÔLE SUR VOS DONNÉES !

Quelques réglages essentiels vous permettent de ne pas être la victime de ce merveilleux outil qu'est ChatGPT.

01 Désactiver l'entraînement sur vos conversations

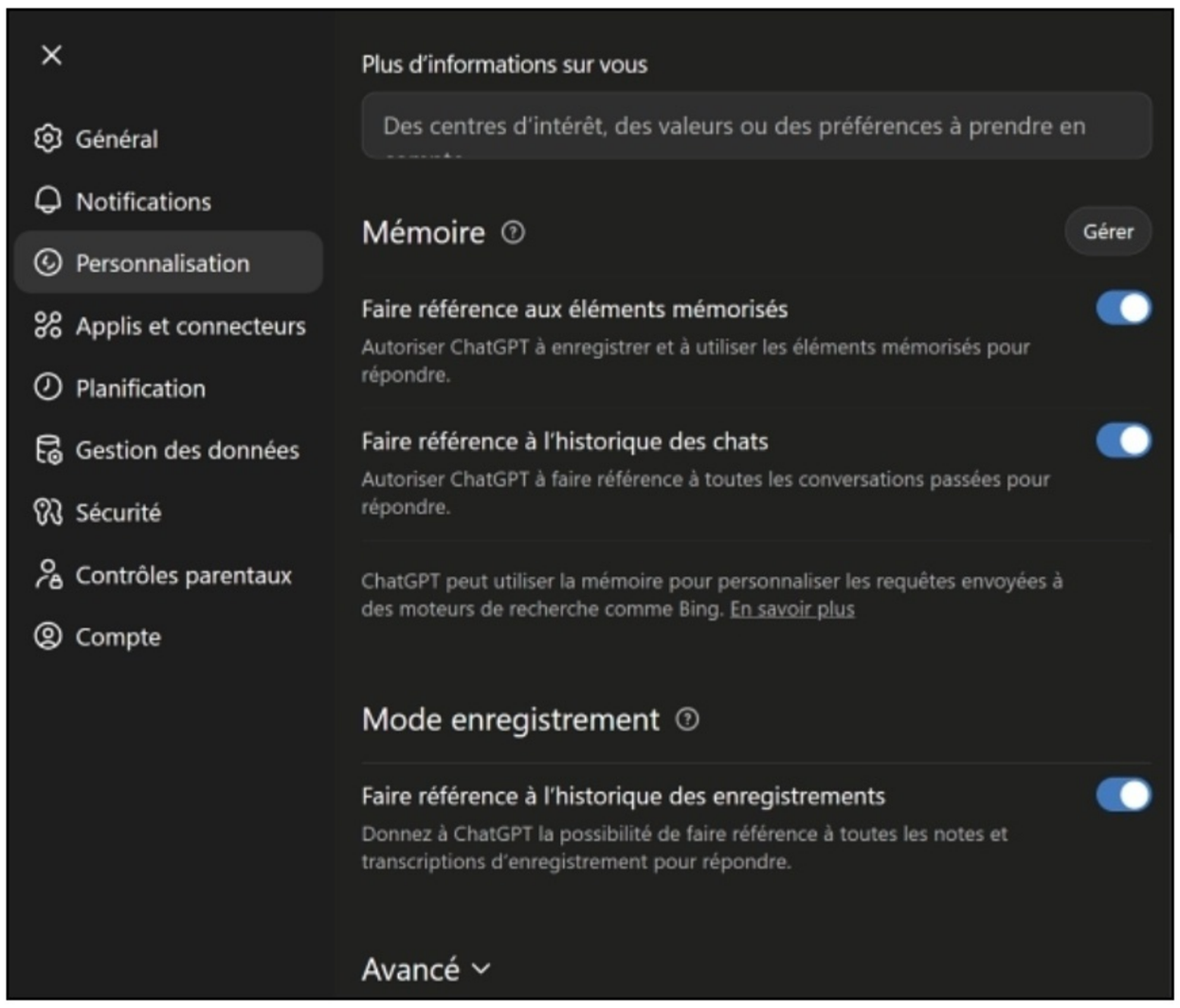
Passez par **Paramètres > Gestion des données > Améliorer le modèle pour tous**. Et désactiver. Vous noterez que ce réglage inclut aussi les enregistrements audio et vidéo. Vous empêchez ainsi OpenAI d'utiliser vos nouveaux échanges pour améliorer ses modèles : un bon réflexe pour des contenus sensibles (travail, données clients, documents internes). Vos chats restent dans l'historique et le service fonctionne normalement ; ils ne servent simplement plus à l'entraînement.





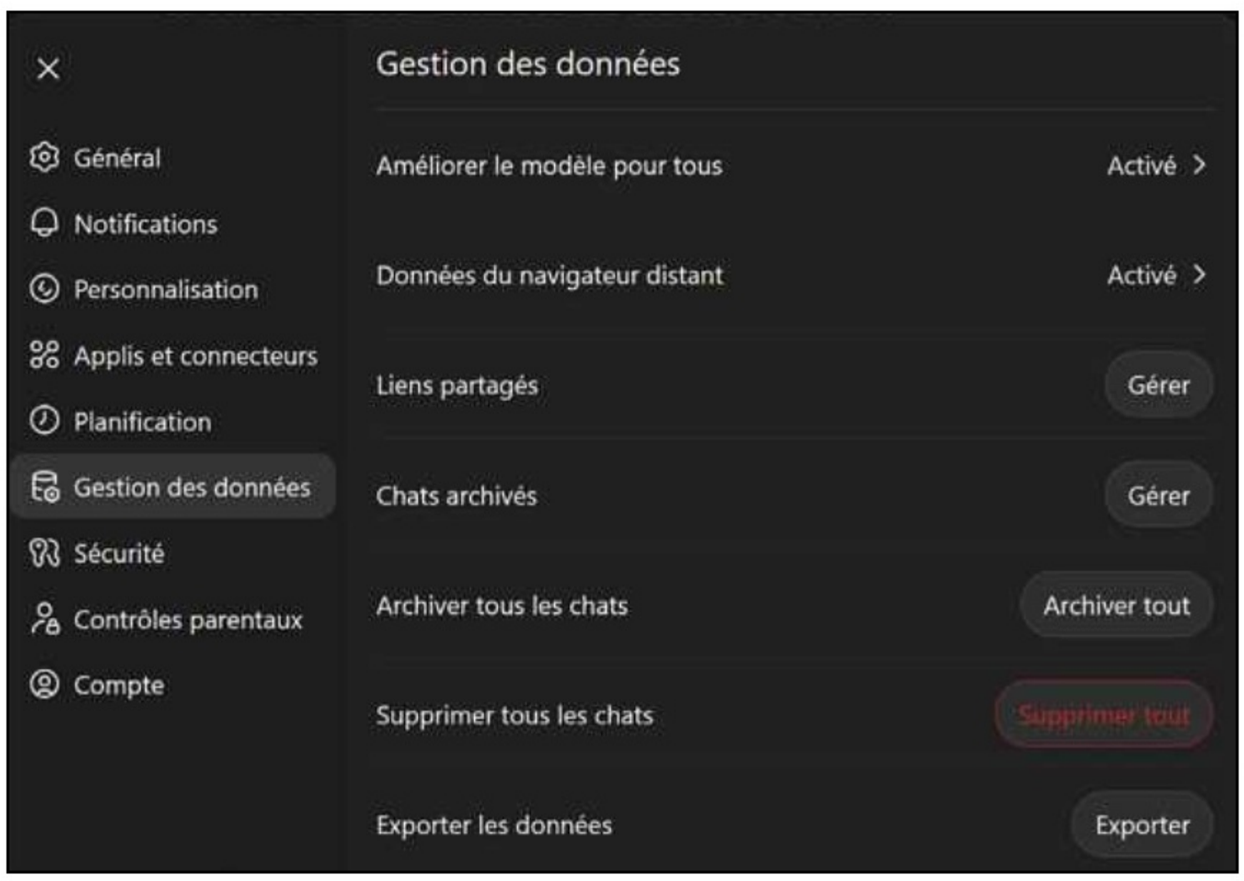
02 Utiliser le Chat temporaire pour les sujets sensibles

En haut à droite de ChatGPT, cliquez sur la petite bulle en pointillé pour activer le chat temporaire. Vous démarrez une conversation en "ardoise blanche" : pas de mémoire, pas d'entraînement, et la conversation n'apparaît pas dans l'historique. Idéal pour un one-shot. Limite : ces chats ne peuvent pas être ajoutés à des "Projets".



03 Désactiver/Nettoyer la Mémoire de ChatGPT

Passez par **Paramètres > Personnalisation** et descendez jusqu'à **Mémoire**. Vous pourrez désactiver la possibilité pour ChatGPT d'utiliser les éléments échangés précédemment et aussi supprimer certains souvenirs précis en passant par le bouton **Gérer**. Ces réglages évitent que ChatGPT retienne des faits persistants sur vous (préférences, habitudes).

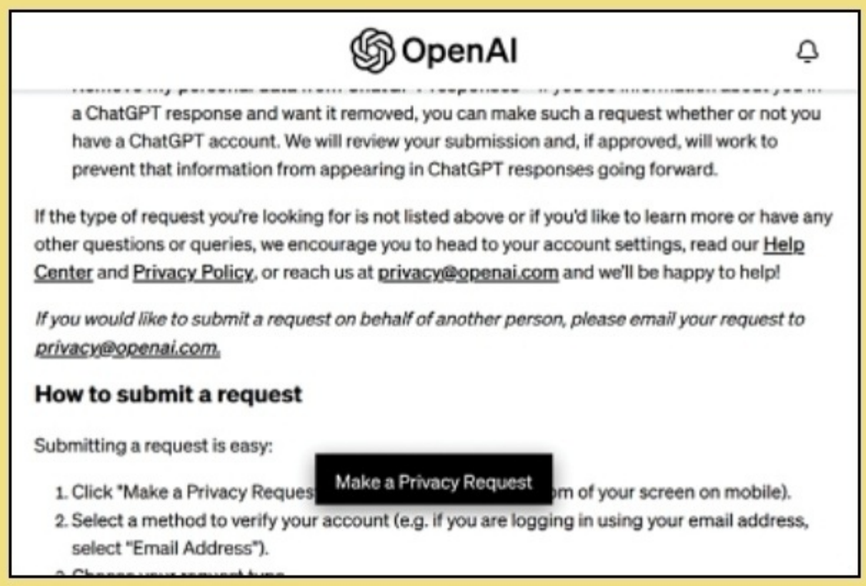


04 Exporter ses données

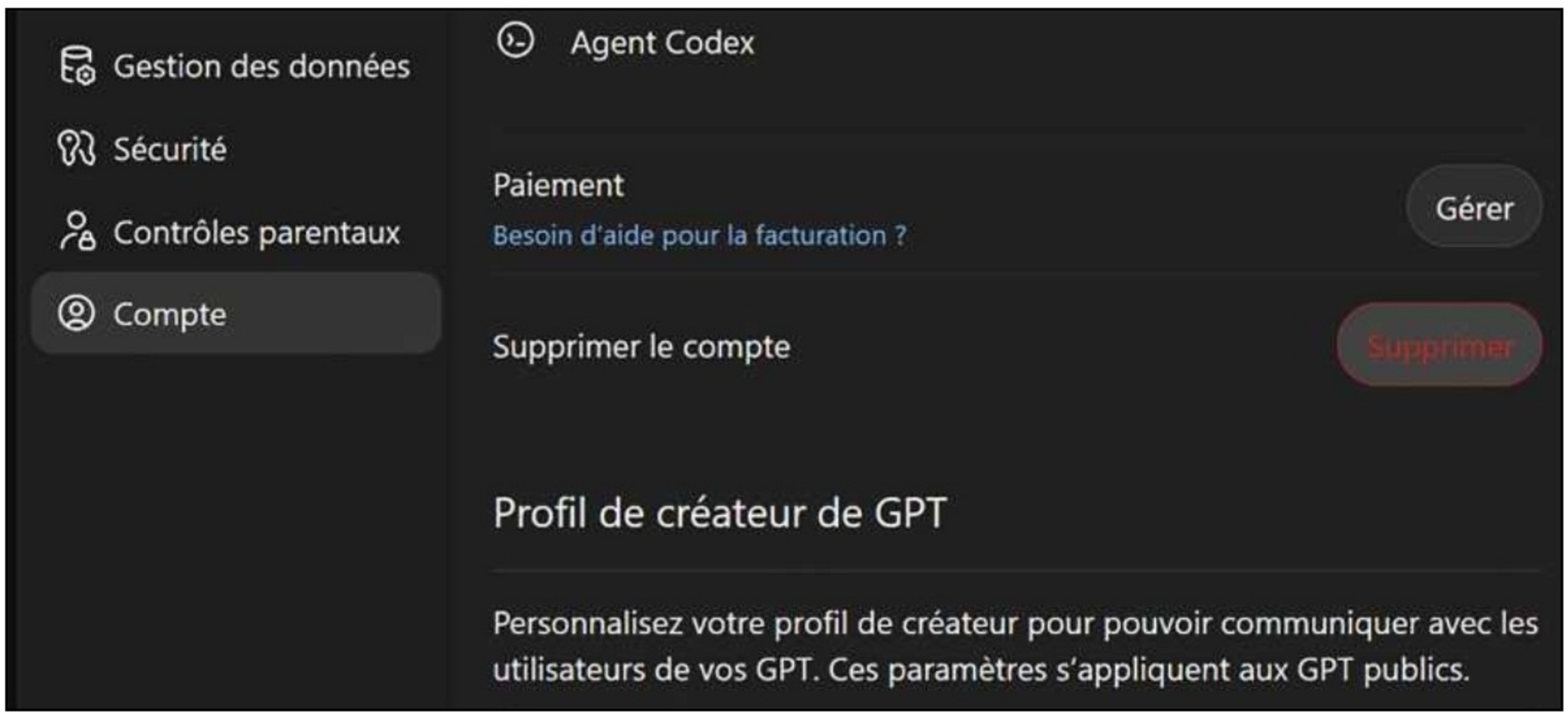
Toujours dans **Paramètres**, allez dans **Gestion des données** puis **Exporter les données > Exporter**. Vous recevrez une notification par email avec un lien de téléchargement (valable 24h) pour récupérer vos archives.

LE PRIVACY PORTAL D'OPENAI, QU'EST-CE QUE C'EST ?

Le Privacy Portal (**privacy.openai.com**) est la porte d'entrée méconnue pour exercer vos droits "vie privée" chez OpenAI. Sous la pression réglementaire (UE, États-Unis), OpenAI a centralisé les demandes via un portail dédié pour standardiser les "DSAR" (Data Subject Access Requests) et répondre aux obligations d'accès/effacement/transparence. La politique de confidentialité (mise à jour le 27 juin 2025) renvoie désormais explicitement au portail pour exercer ses droits.
Via ce guichet unique, vous pouvez lancer des actions déjà disponibles via l'application ChatGPT (Supprimer un compte, Exporter des données). Mais vous pouvez aussi faire des demandes fines qui concernent des données ou documents spécifiques (modification, suppression).
Rendez-vous sur **privacy.openai.com > Make a Privacy Request**. Vérifiez votre identité (adresse e-mail ou n° de téléphone lié au compte) et choisissez ensuite l'action : **Download my data, Delete my ChatGPT account, Correct/Remove data**, etc.



Internet & Réseaux

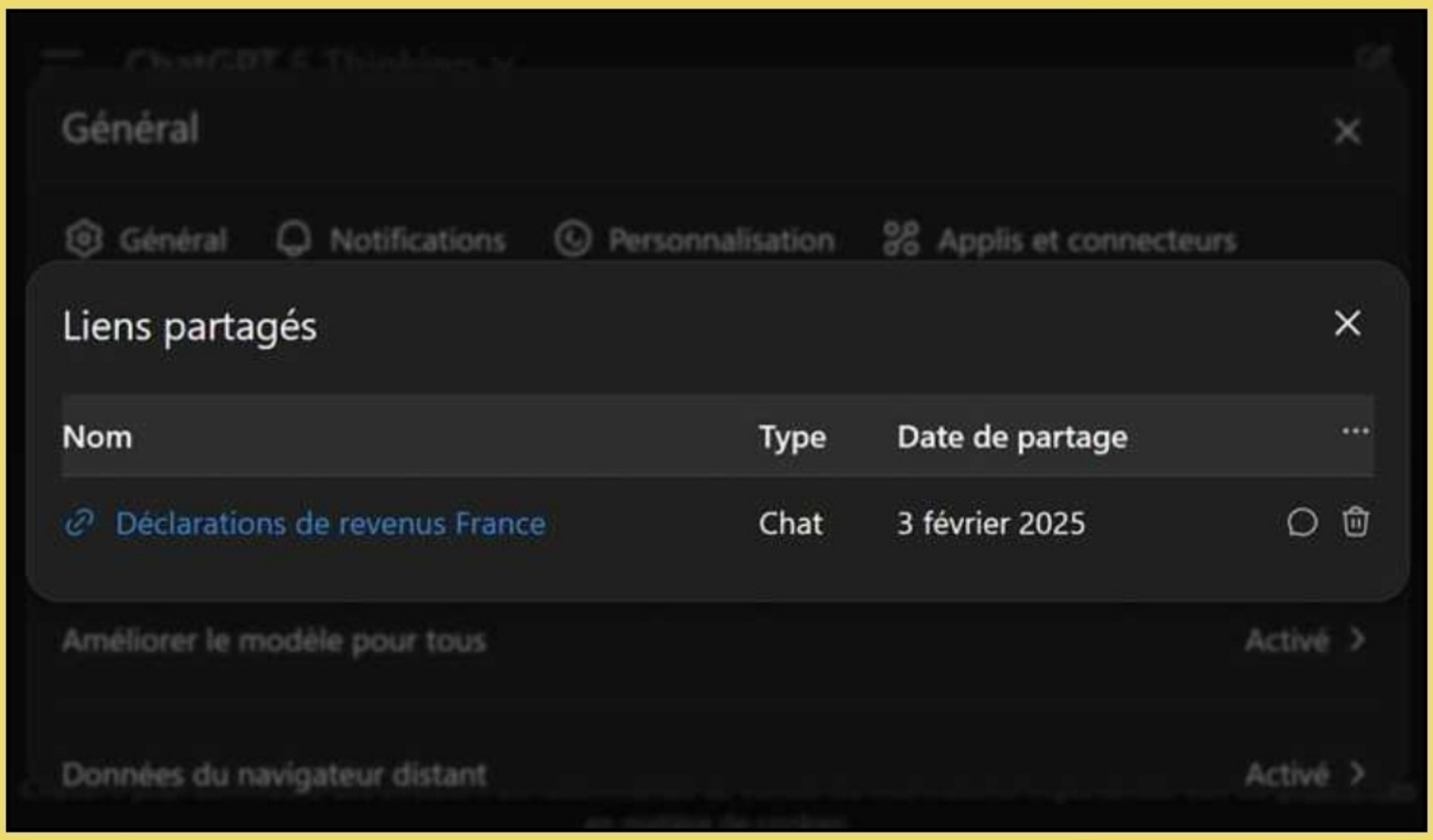


05 Supprimer son compte

Via **Paramètres**, allez cette fois-ci **Compte > Supprimer le compte > Supprimer**. Attention, la suppression d'un compte est définitive et ne peut être annulée et vous ne pourrez pas créer un nouveau compte en utilisant la même adresse e-mail. Vos données seront supprimées dans un délai de 30 jours, délai majoré pour certaines (raisons légales).

ATTENTION AUX LIENS PARTAGÉS

Les liens partagés donnent accès en lecture seule à une conversation ChatGPT. Toute personne qui possède le lien peut lire l'échange. Si quelqu'un importe votre conversation dans son historique, supprimer le lien n'efface pas la copie déjà importée chez cette personne. D'où l'intérêt d'éviter tout contenu sensible dans un partage public.



Durant l'été 2025, des conversations partagées sont apparues dans Google (et autres) lorsqu'une option de "découvrabilité" avait été activée ; OpenAI a retiré cette expérimentation suite aux signalements. Mais même sans "découvrabilité", un lien public peut être crawlé (copié/archivé) s'il circule sur le Web. La suppression du lien dans ChatGPT réduit l'exposition, mais n'efface pas instantanément les résultats déjà indexés ni les caches des moteurs.

Pour supprimer un lien partagé, dans les **Paramètres**, passez par **Gestion des données > Liens partagés > Gérer**. Vous pourrez revoir et supprimer chaque lien.

LE GUIDE POUR UN WHATSAPP ANONYME ET SÉCURISÉ

Connaissez-vous les techniques et fonctions Whatsapp qui vous donnent le contrôle total sur la messagerie instantanée ? Vie privée, protection et anonymat : avancez sur Whatsapp en utilisant les meilleures astuces pour discuter et échanger en maîtrisant l'art de savoir qui peut voir quoi, quand et pour combien de temps. Sans oublier de protéger votre identité et vos contenus des regards intrusifs ou malveillants.



Internet & Réseaux

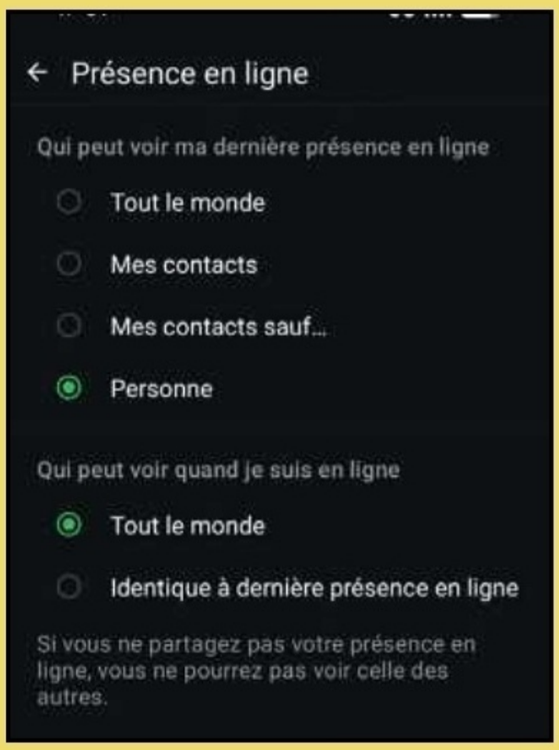
CONVERSATIONS ET CONTACTS

Masquer sa dernière connexion

Sur WhatsApp, l'indicateur “Dernière connexion” et le statut “En ligne” trahissent votre activité en temps réel. Un contact peut ainsi savoir à quelle heure vous consultez vos messages, voire en déduire vos habitudes de sommeil ou de travail. Heureusement, il est possible de garder la maîtrise de ces informations sans bloquer la réception des messages.

Ouvrez **Paramètres > Confidentialité > Présence en ligne**. Cette rubrique contrôle à la fois la trace horaire de vos connexions et votre visibilité en direct.

Sous **Qui peut voir ma présence en ligne**, sélectionnez **Personne** si vous souhaitez que personne ne voie plus vos heures de présence. Si vous préférez limiter la visibilité à vos proches, optez pour **Mes contacts sauf...** et excluez les curieux.

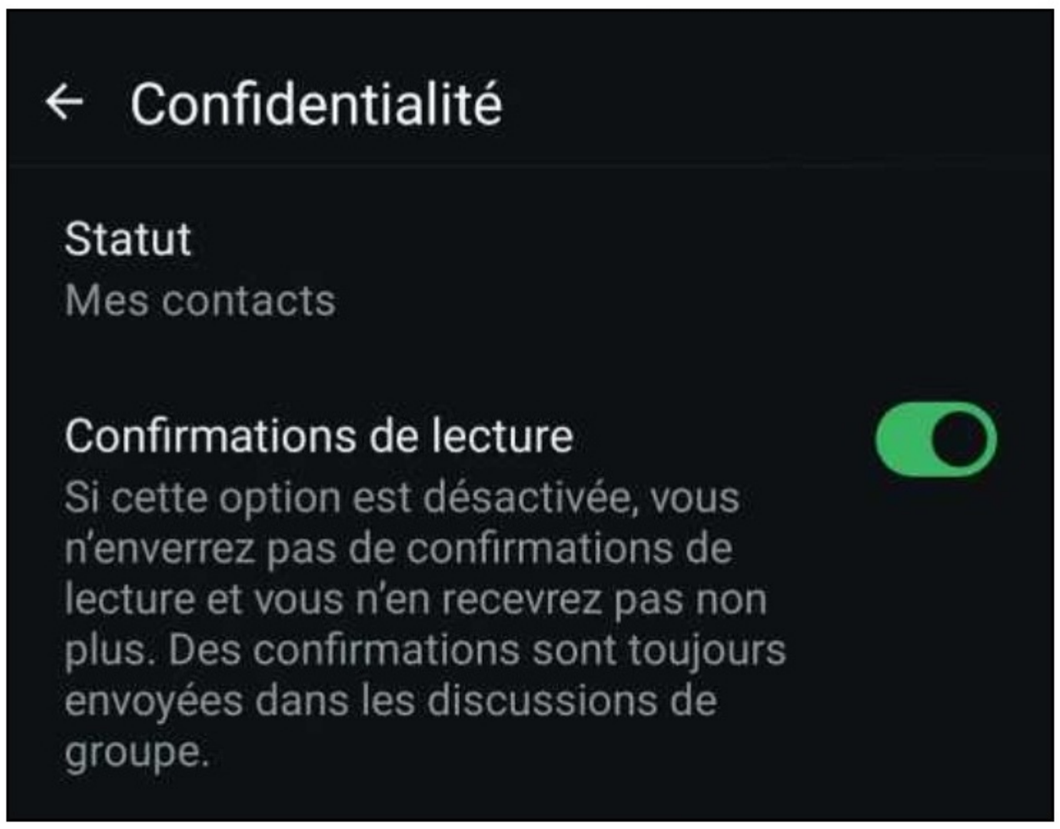


Pour le champ En ligne, choisissez **Identique à la dernière présence en ligne** afin d'unifier le réglage : ceux qui ne peuvent pas voir votre dernière connexion ne verront plus non plus quand vous êtes actif.

Désactiver les confirmations de lecture (les deux coches bleues)

Les fameuses coches bleues, signes de lecture, peuvent vite devenir envahissantes : elles exposent vos temps de réponse, créent des malentendus et brisent la frontière entre vie privée et disponibilité. Les désactiver rend vos échanges plus sereins.

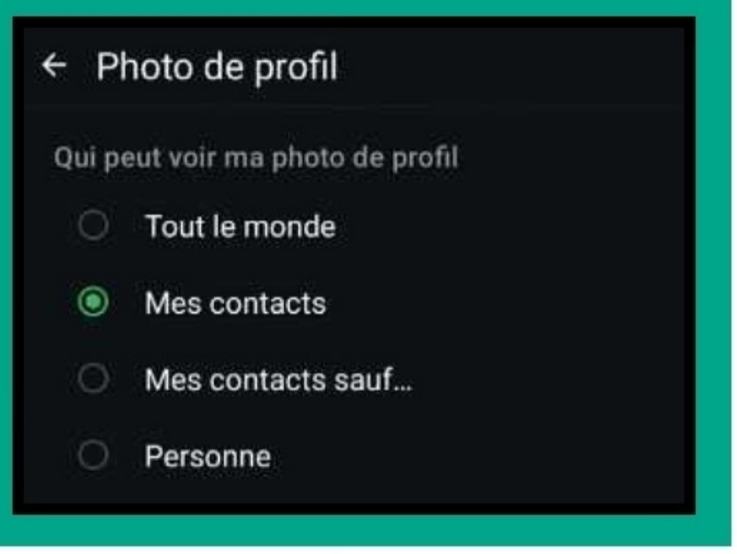
Ouvrez **Paramètres > Confidentialité > Confirmations de lecture**. Décochez l'option. Dès lors, vos contacts ne sauront plus si vous avez lu leurs messages. Vous ne verrez pas non plus les leurs, afin de préserver la réciprocité. Attention : dans les groupes, cette désactivation ne s'applique pas. WhatsApp continue d'afficher qui a vu un message collectif pour des raisons de transparence d'échanges.



Choisir qui peut voir sa photo de profil

Votre photo de profil peut sembler anodine, mais elle constitue une véritable porte d'entrée vers votre identité numérique : reconnaissance faciale, recoupements sur d'autres réseaux, voire usurpation. Mieux vaut décider précisément qui y a accès.

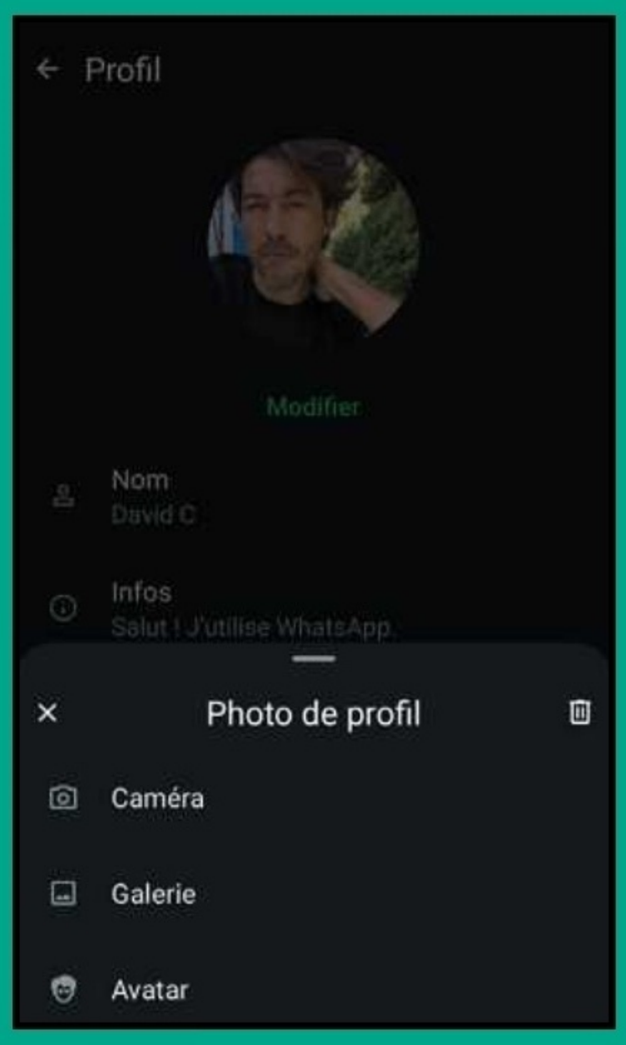
Rendez-vous dans **Paramètres > Confidentialité > Photo de profil**. Vous verrez ici trois options de visibilité. Choisissez **Mes contacts** pour restreindre l'affichage à vos seuls interlocuteurs enregistrés, ou **Mes contacts sauf...** pour exclure certains profils sensibles. Si vous souhaitez un anonymat total, sélectionnez **Personne** : votre profil affichera simplement une icône générique.



Créer un faux nom et une photo neutre

Votre nom réel n'est pas nécessaire pour dialoguer sur WhatsApp. En utilisant un pseudonyme, vous protégez votre identité dans les groupes publics, les forums de petites annonces ou les contacts éphémères.

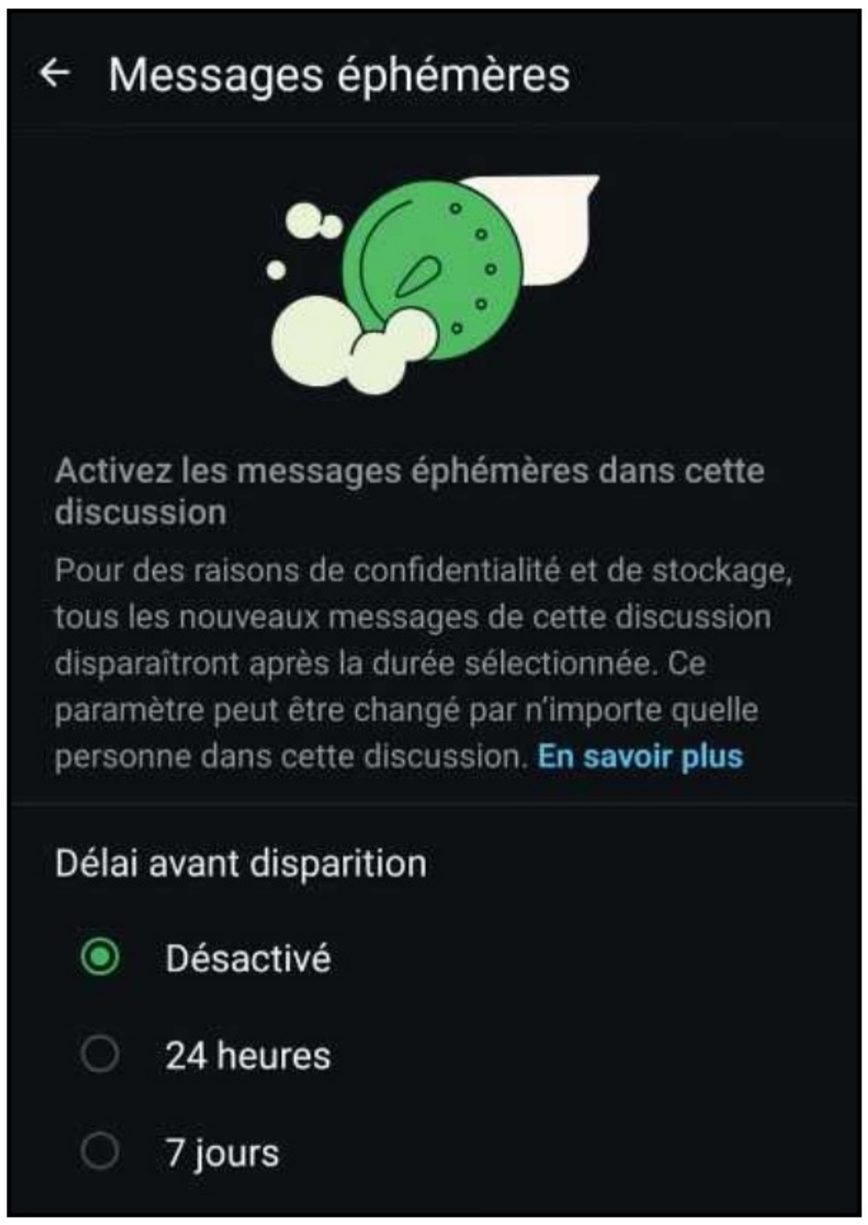
Ouvrez **Paramètres > Profil**. Remplacez votre nom par un pseudonyme sobre ou humoristique, selon le contexte. Pour la photo, optez pour une image neutre, un avatar généré ou un simple fond de couleur. Vérifiez ensuite la cohérence de vos autres informations (nom, infos), qui peuvent aussi révéler votre identité et que vous pouvez modifier. Un pseudonyme ne suffit pas à garantir l'anonymat total : votre numéro de téléphone reste visible.



Des messages qui s'autodétruisent par défaut

Vous avez possibilité que l'ensemble des échanges avec un ou plusieurs de vos contacts s'effacent automatiquement sans avoir à les supprimer manuellement au cas par cas. Vos messages disparaitront de l'appareil de l'expéditeur et du destinataire après un délai défini.

Ouvrez une discussion, puis appuyez sur le nom du contact et accédez à **Messages éphémères**. Choisissez une durée : **24 heures**, **7 jours** ou **90 jours**. Tous les nouveaux messages de ce chat seront supprimés automatiquement à l'expiration du délai. Cette option s'applique aux nouveaux messages, pas à ceux déjà envoyés.



Protéger des discussions sensibles par un mot de passe

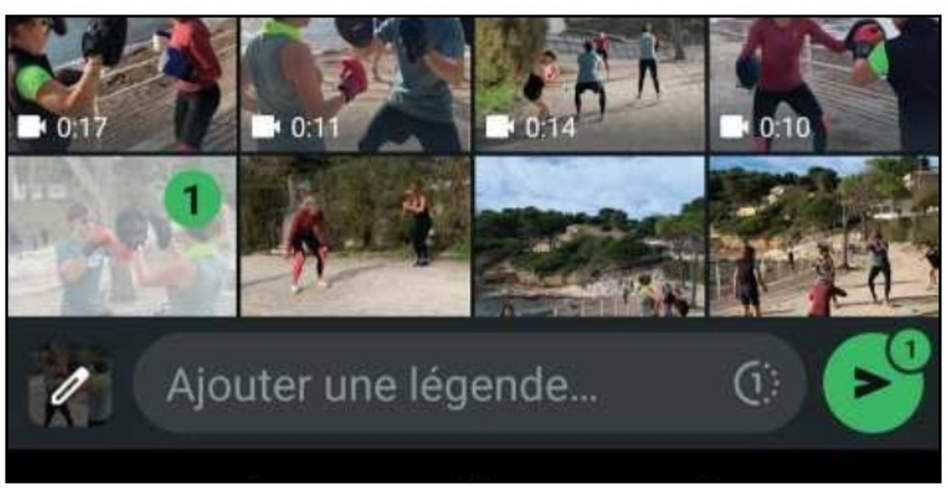
Certaines conversations ne regardent que vous. Depuis 2024, WhatsApp permet de verrouiller une discussion spécifique dans un dossier caché, accessible uniquement par empreinte ou code.

Ouvrez la discussion à protéger. Touchez le nom du contact, choisissez **Verrouillage de la discussion** puis **Activer**. Choisissez votre méthode d'authentification (code, empreinte ou Face ID). La conversation disparaît de la liste principale et se déplace dans un dossier spécial : **Discussions verrouillées**. L'accès se fait par glissement vers le bas sur l'écran d'accueil de WhatsApp, puis validation biométrique. Aucun aperçu ni notification ne s'affiche pour ces chats.



Internet & Réseaux

Envoyer des vocaux, photos et vidéos à “vue unique”

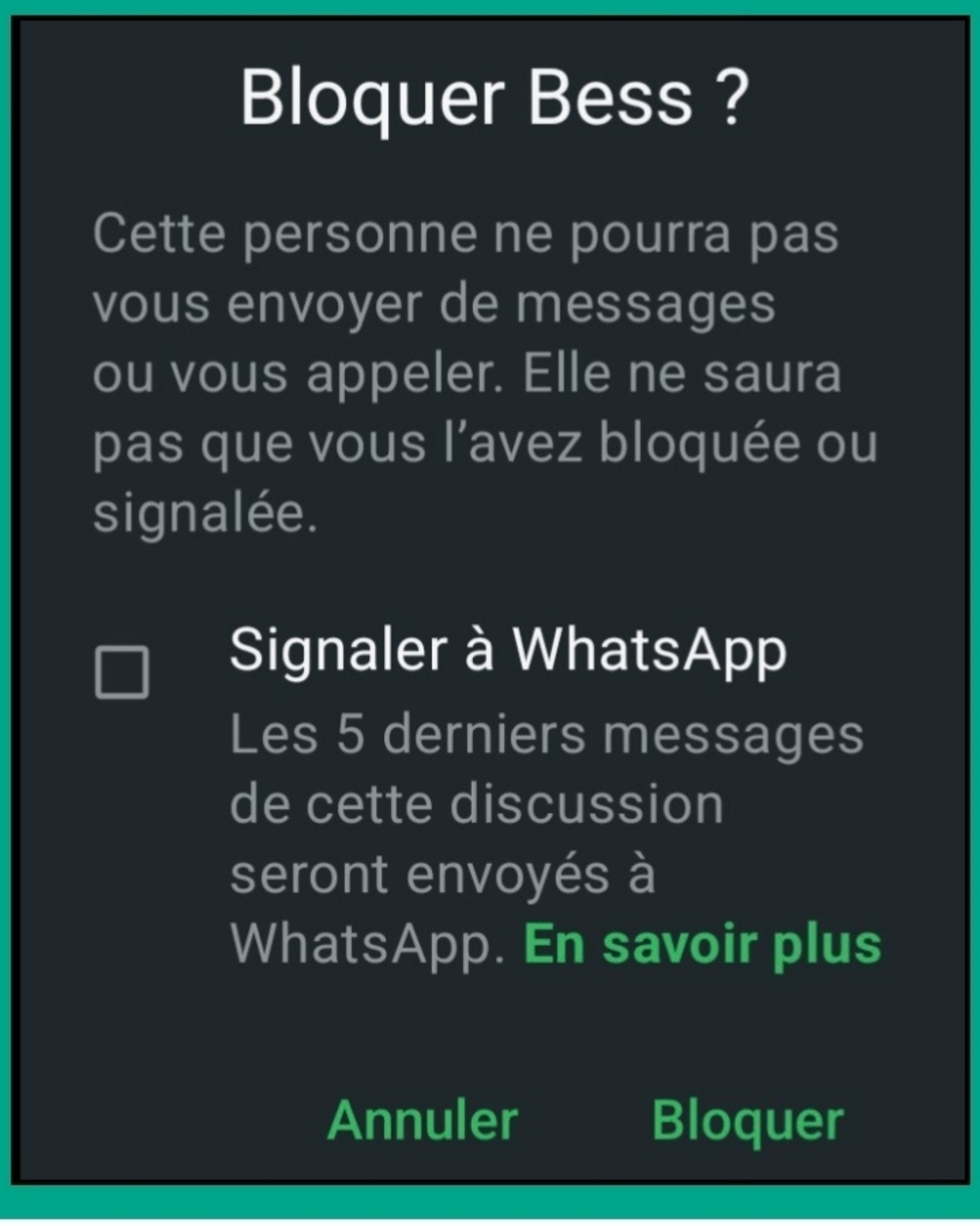


Cette option garantit qu'un média ne pourra être vu qu'une seule fois. Une fois ouvert, il s'autodétruit automatiquement sans rester en mémoire ni dans la galerie. Lors d'un envoi d'un vocal, photo ou vidéo, touchez l'icône “**1**” à droite de la zone de légende. Vous verrez apparaître la mention **Photo/Vidéo à vue unique**. Envoyez le fichier : le destinataire devra l'ouvrir immédiatement, et ne pourra plus le consulter ensuite. WhatsApp bloque aussi les captures d'écran pour ce type de média, renforçant la confidentialité de l'échange.

Bloquer et signaler un contact malveillant

Spam, harcèlement, usurpation : bloquer un contact est la première défense. Cela coupe tout canal de communication, tout en signalant le comportement à WhatsApp.

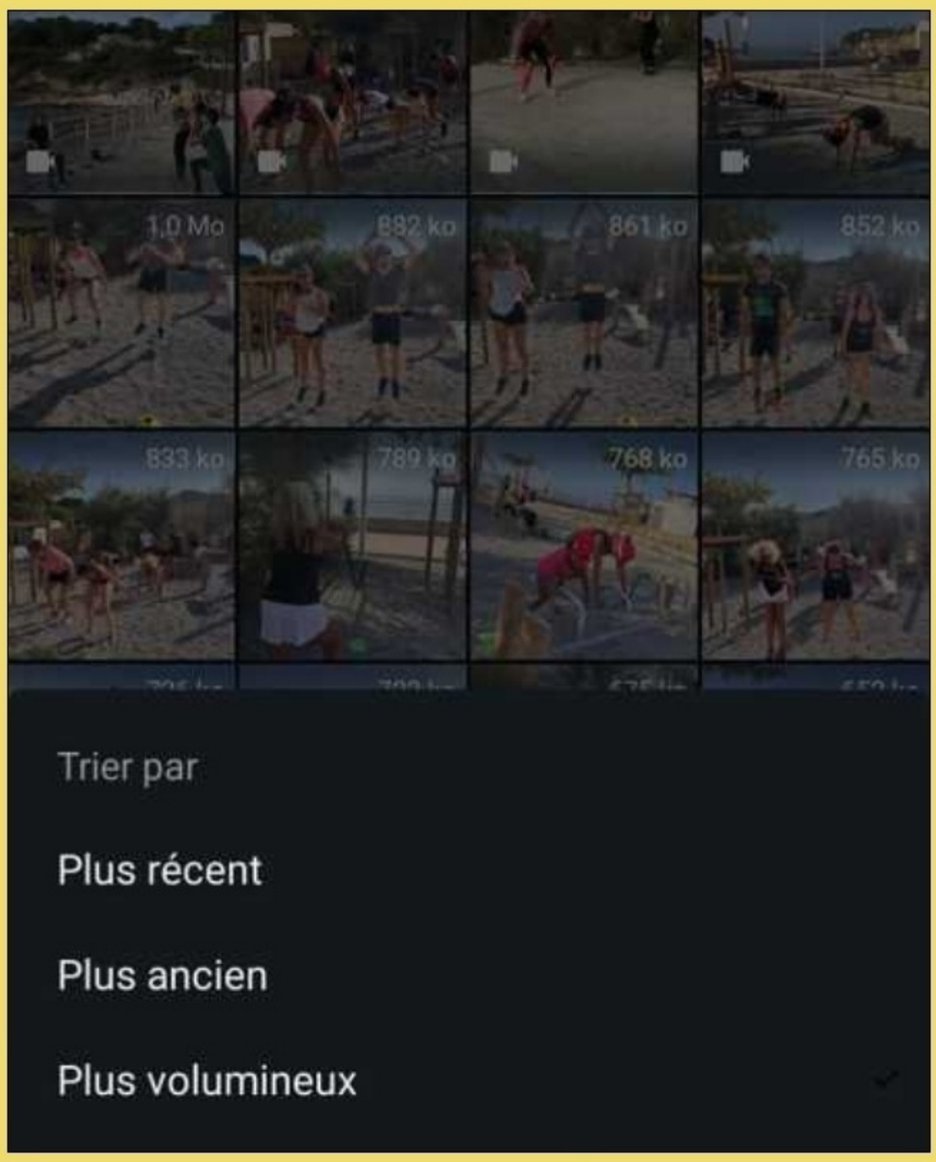
Ouvrez la conversation avec la personne concernée. Touchez le nom du contact puis choisissez **Bloquer > Bloquer et signaler**. Le contact ne pourra plus vous envoyer de messages ni voir vos informations de profil. Le signalement contribue à la détection globale des comptes abusifs ; il reste anonyme.



Supprimer le contenu d'anciens messages

Les discussions volumineuses s'accumulent et conservent des traces d'informations personnelles (photos, vidéos, documents). Le nettoyage des anciens messages limite les risques en cas de perte ou d'accès non autorisé. Outre la confidentialité, cela améliore les performances de l'application et libère de l'espace sur votre téléphone.

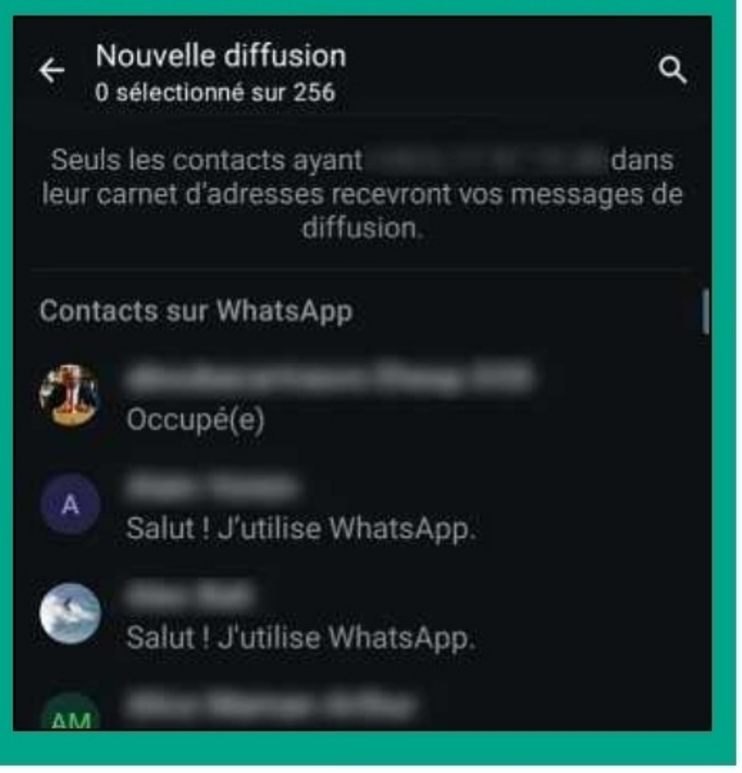
Ouvrez **Paramètres > Stockage et données > Gérer le stockage**. Sélectionnez une discussion, puis effacer les médias obsolètes. Vous pouvez trier par date ou par volume.



Créer une liste de diffusion sans révéler les destinataires

Vous voulez envoyer le même message à plusieurs contacts sans créer un groupe ? Les listes de diffusion permettent un envoi multiple invisible. Utile pour les annonces professionnelles, les invitations ou les alertes sans exposer votre carnet d'adresses.

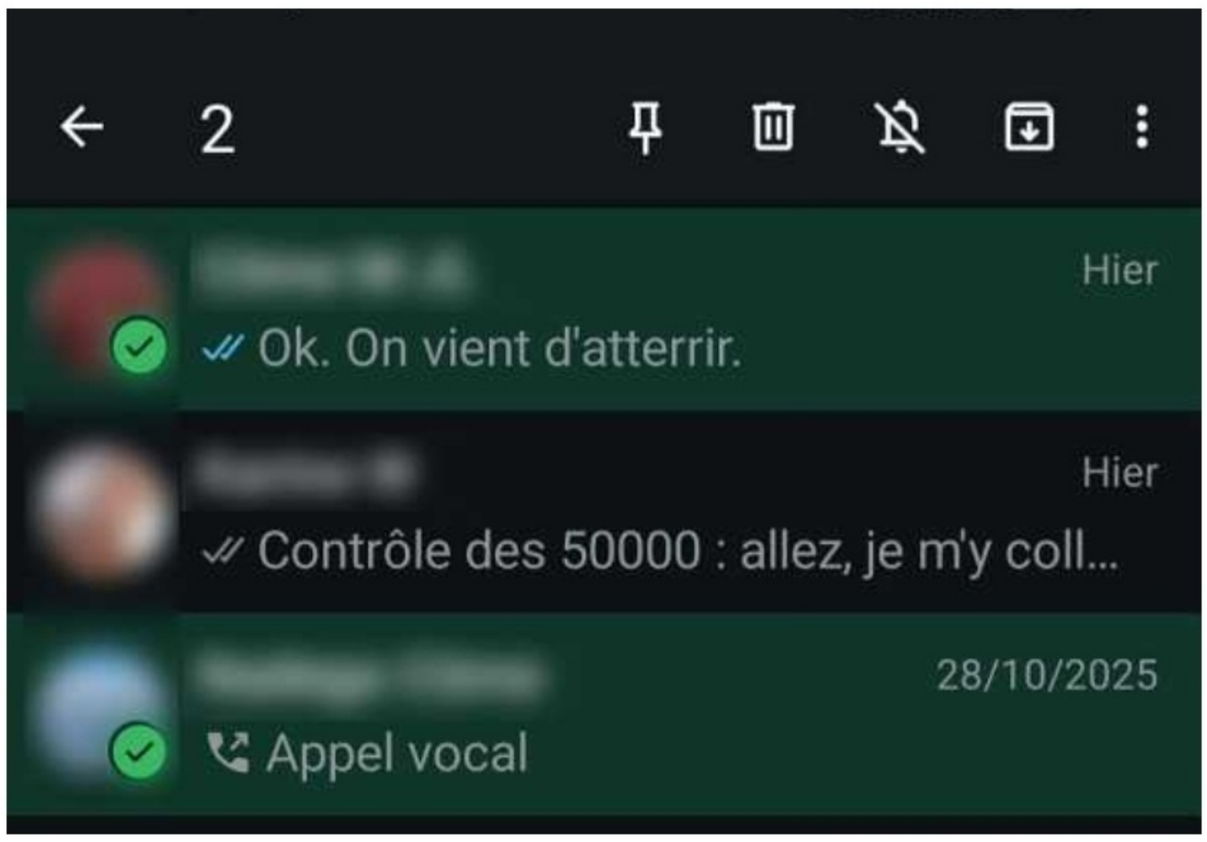
Sur l'écran principal, appuyez sur les trois points en haut à droite puis sur **Nouvelle diffusion**. Sélectionnez les contacts concernés (jusqu'à 256). Envoyez votre message : chacun le reçoit individuellement, comme un message privé.



Épingler plusieurs discussions en haut de l'écran

Vous pouvez désormais garder vos conversations importantes toujours visibles, même si vous recevez d'autres messages. Les conversations épinglées restent toujours en haut, mais ne contournent pas le chiffrement ni les notifications classiques.Pratique pour vos proches, votre travail ou vos groupes prioritaires.

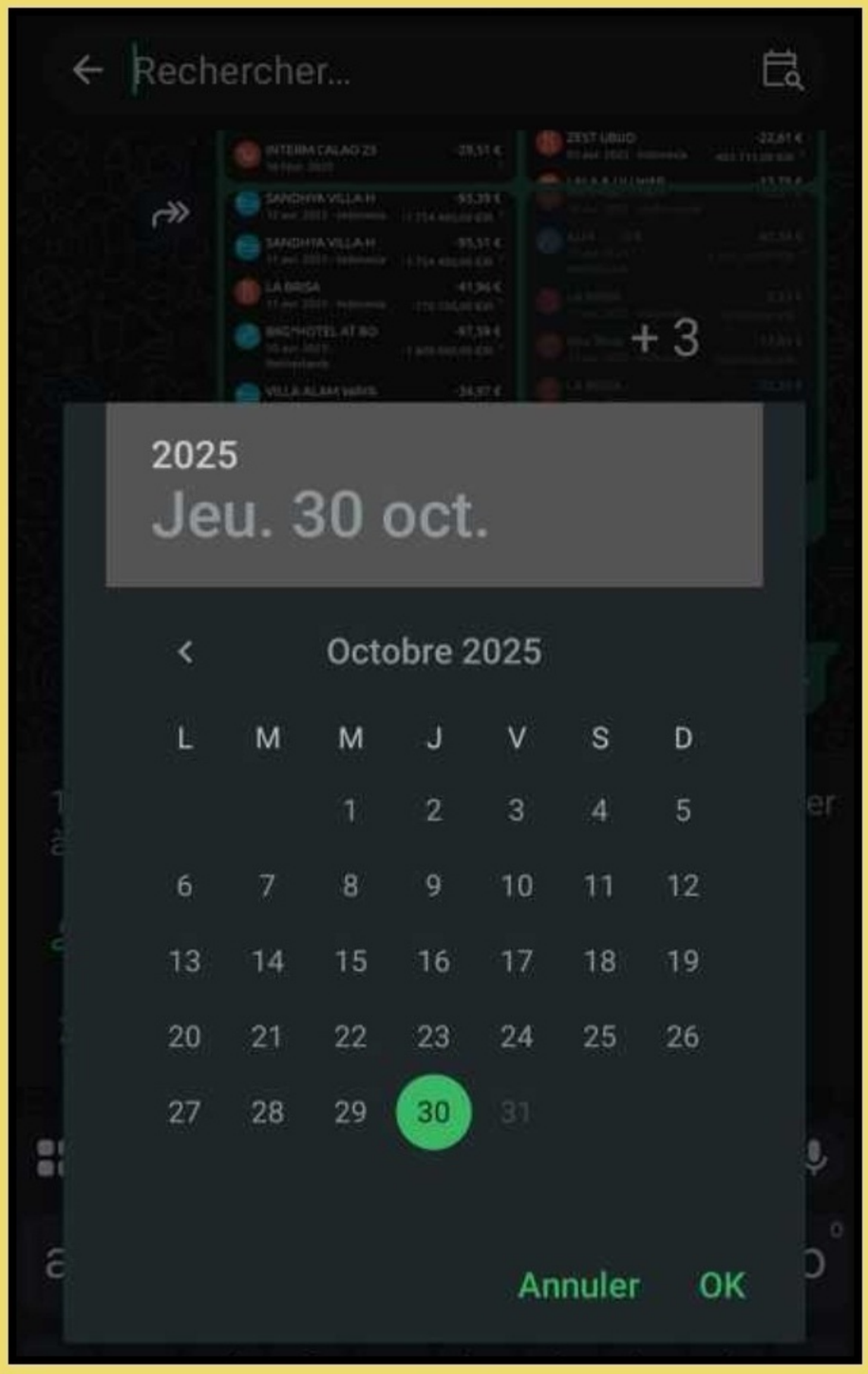
Depuis l'écran principal, effectuez un appui long sur la ou les discussions à épingler. Touchez l'icône épingler en haut de l'appli (en forme de punaise). Vous pouvez en épingler jusqu'à cinq (au lieu de trois auparavant).



Rechercher des messages par date ou mot-clé

Retrouver un message ancien peut être fastidieux. WhatsApp a ajouté une recherche chronologique qui facilite grandement la navigation dans l'historique.

Ouvrez une discussion. Appuyez sur les trois points puis sur **Rechercher**. Utilisez la nouvelle icône calendrier en haut à droite pour choisir une date précise, ou tapez un mot-clé.





Internet & Réseaux

Modifier un message déjà envoyé

Combien de fois avez-vous repéré une faute ou un mot mal choisi juste après avoir envoyé un message ? WhatsApp vous permet désormais de le corriger sans le supprimer. Vous pouvez utiliser cette fonction jusqu'à 15 minutes après l'envoi initial du message.



Maintenez le doigt sur le message que vous avez envoyé. Appuyez sur **Modifier** à partir des trois petits points en haut à droite. Corrigez votre texte, puis validez. La mention “Modifié” apparaît discrètement à côté du message, mais sans afficher la version d'origine.

À SAVOIR

Il existe aussi d'autres techniques qui ne sont pas prévues nativement par Whatsapp, mais que les utilisateurs les plus malins (ou pathologiques) emploient pour masquer la lecture de messages, effacer sans avoir consulté un contenu, etc., etc. Le plus souvent, il s'agit de passer par bloquer et débloquer un contact dans le bon timing ou d'agir via les notifications reçues.



Activer la fonction Confidentialité avancée pour vos discussions sensibles

Bien que WhatsApp assure depuis longtemps le chiffrement de bout en bout des messages, certaines publications peuvent encore être exportées, partagées à l'extérieur, ou engagées dans des processus externes (IA, captures d'écran, extraction de médias). C'est particulièrement vrai dans les discussions professionnelles, associatives ou confidentielles. C'est pourquoi WhatsApp a lancé début 2025 la fonction « Advanced Chat Privacy » : un réglage par discussion qui limite ce que les participants peuvent faire de vos échanges (export, téléchargement, IA). Ouvrez WhatsApp et naviguez dans la discussion à protéger (privée ou groupe). Touchez le nom du contact ou du groupe en haut de l'écran pour ouvrir les informations de chat. Sélectionnez **Confidentialité avancée de la discussion** (ou « Advanced Chat Privacy », situé en bas. Activez cette fonctionnalité. Dès à présent, ce chat bénéficiera d'une couche supplémentaire de protection : même si quelqu'un tente de faire une capture d'écran ou de transférer un fichier, certaines fonctions sont neutralisées.



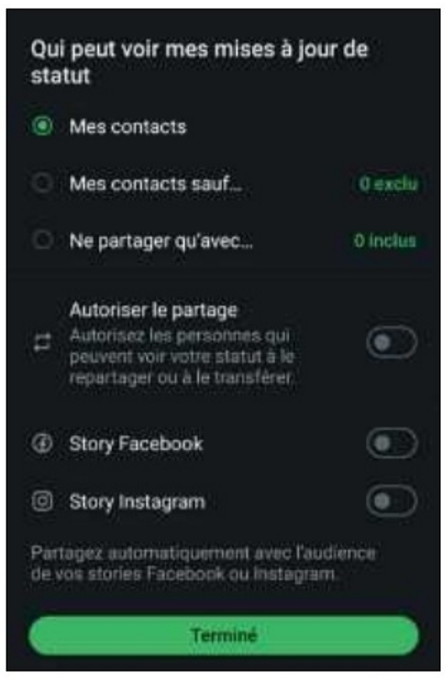
LE CAS DES « STATUTS »

Apparus en 2017 pour concurrencer les “stories” d’Instagram et Snapchat, les statuts WhatsApp permettent de publier des contenus temporaires visibles pendant 24 heures : textes, photos, vidéos, GIFs ou même messages vocaux. Ces publications apparaissent dans l’onglet Statut et s’effacent automatiquement au bout d’un jour, sauf si vous les supprimez plus tôt.

En pratique, cette fonction sert à partager des moments du quotidien, des annonces professionnelles, des citations, ou des messages personnels adressés à vos proches. Mais contrairement à Instagram, les statuts WhatsApp ne sont pas publics : ils ne sont visibles que par vos contacts — ou par certains d’entre eux, selon vos réglages de confidentialité.

Seulement, par défaut, tout contact enregistré dans votre répertoire peut voir vos statuts, et WhatsApp affiche à chaque utilisateur la liste complète des personnes ayant consulté sa publication. Autrement dit : si vous postez un statut, tout votre carnet d’adresses y a accès, et si vous regardez celui d’un ami, il le saura immédiatement.

C’est un comportement pratique pour un usage familial ou amical, mais il pose un vrai problème de confidentialité dès qu’on utilise WhatsApp dans un cadre professionnel, associatif ou anonyme. Peu d’utilisateurs savent que ces réglages peuvent être modifiés pour limiter la visibilité, masquer son activité, voire publier “en fantôme”.



01 Choisir qui peut voir ses statuts

Par défaut, vos statuts WhatsApp sont visibles par tous vos contacts. Cela inclut parfois des collègues, d’anciens proches ou des numéros oubliés dans votre répertoire. Définir précisément votre audience évite les regards indiscrets.

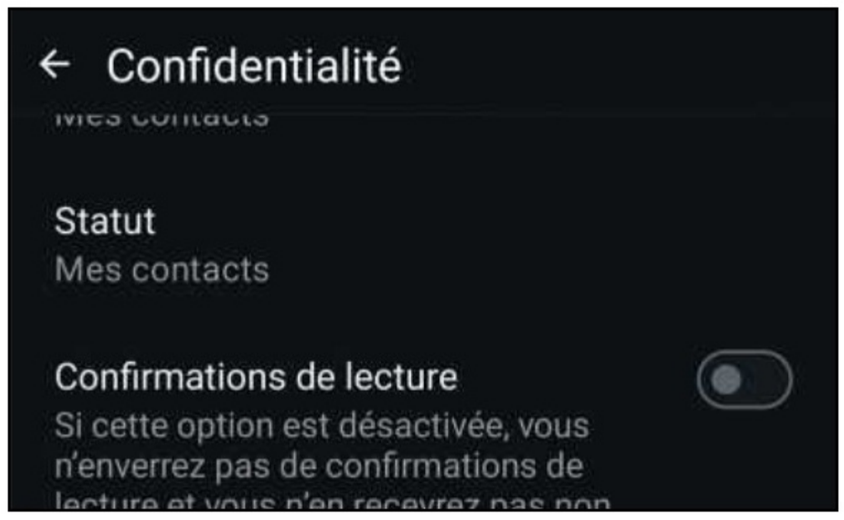
Ouvrez WhatsApp, allez dans **Actus** puis créez votre statut. Avant de publier, allez dans l’onglet **Statut** en bas à gauche. Trois options s’affichent : Mes contacts (par défaut) ; **Mes contacts sauf…** (pour exclure certaines personnes) ; **Ne partager qu’avec…** (pour créer une audience restreinte). Sélectionnez votre préférence avant chaque nouvelle publication. Attention, votre dernier réglage reste mémorisé pour vos prochains statuts, pensez donc à le réinitialiser si vous voulez revenir à une visibilité normale.

Les réglages de confidentialité s’appliquent uniquement aux nouveaux statuts : les anciens restent visibles selon l’ancienne configuration.

02 Masquer votre lecture d’un statut

WhatsApp affiche à chaque utilisateur qui a vu son statut. Vous pouvez désactiver cette fonction pour ne plus apparaître dans la liste des spectateurs. Mais la méthode est drastique, car ce réglage agit globalement : il masque aussi les accusés de lecture dans les discussions.

Allez dans **Paramètres > Confidentialité > Confirmations de lecture**. Désactivez l’option. Vous ne verrez plus non plus qui consulte vos propres statuts, mais c’est le prix de la discrétion.





03 Télécharger un statut sans notification

Il est possible de sauvegarder une photo ou vidéo de statut d’un contact sans utiliser de capture d’écran ni le prévenir, à condition d’employer une méthode discrète.

Sur Android, les statuts visionnés sont stockés temporairement dans le dossier caché : **/WhatsApp/Media/.Statuses**. Ouvrez un explorateur de fichiers (Files, Solid Explorer…) ou explorez votre mobile depuis un PC puis copiez le fichier souhaité avant qu’il ne soit supprimé. Sur iPhone, utilisez une appli tierce comme ReShare Story for WhatsApp (respectant les règles d’Apple).

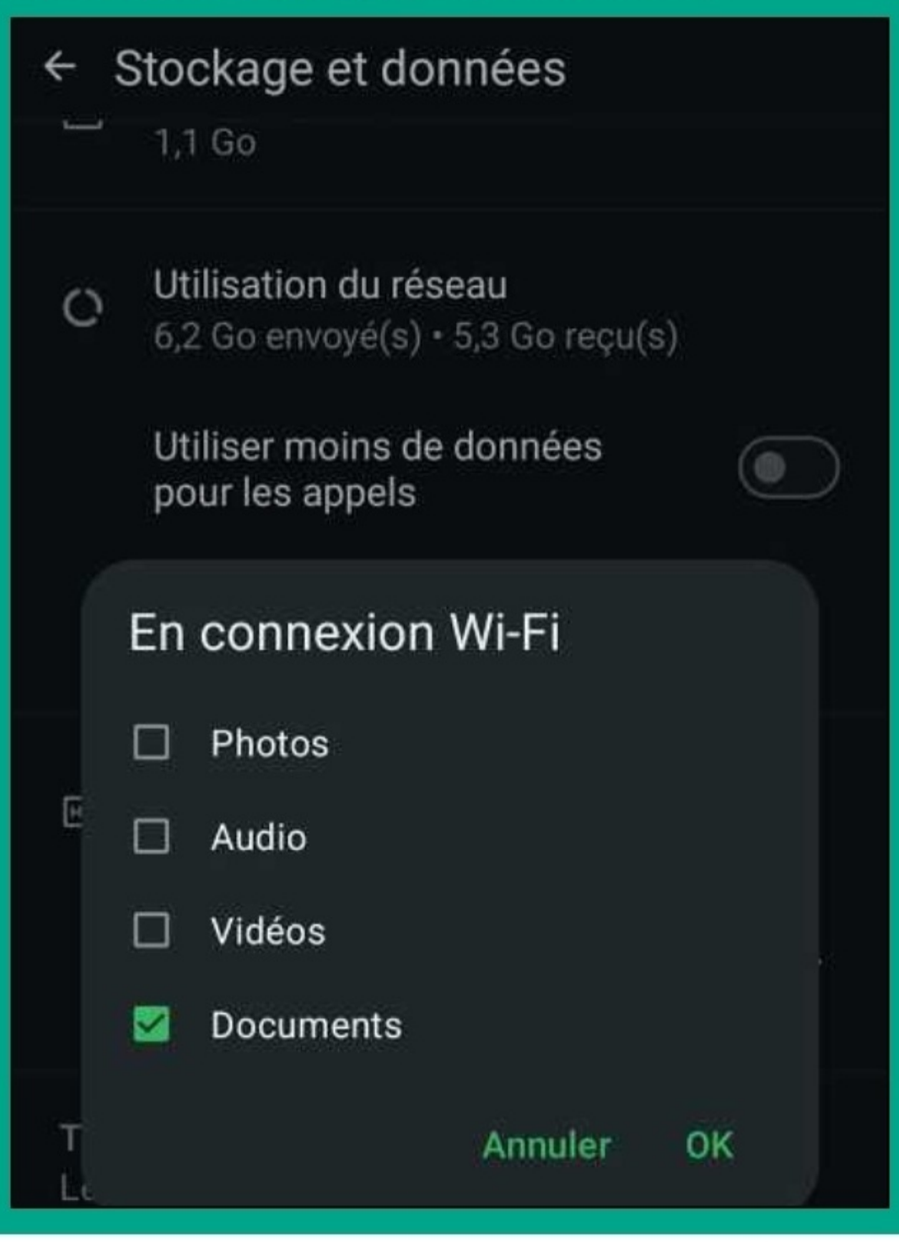
Internet & Réseaux

SÉCURISER COMPTE ET CONTENUS

Empêcher WhatsApp d'enregistrer les médias dans la galerie – Option 1

Les photos et vidéos reçues sur WhatsApp s'enregistrent par défaut automatiquement dans la galerie de votre téléphone. Résultat : un contenu privé peut se retrouver affiché dans un diaporama familial ou dans le cloud de synchronisation. Et ces téléchargements automatiques finissent par encombrer la mémoire de stockage de votre appareil.

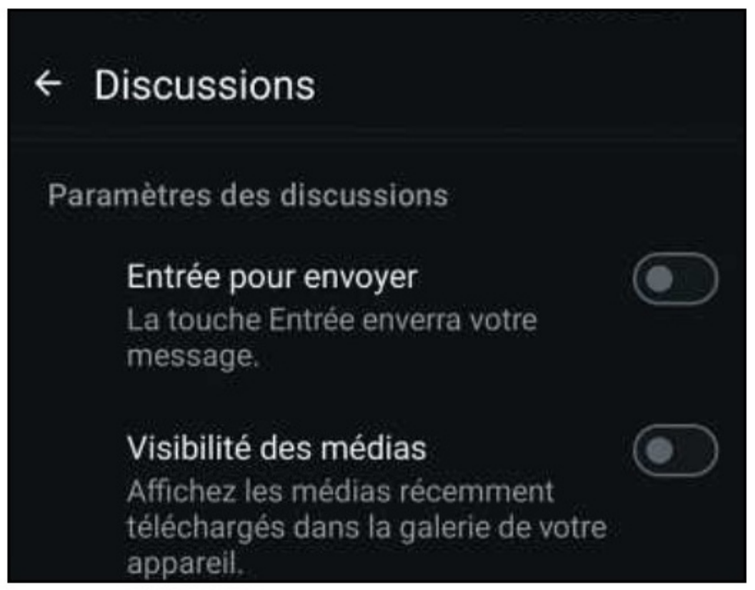
Allez dans **Paramètres > Stockage et données.** Sous **Téléch. Auto. des médias**, vous allez pouvoir piloter exactement ce qui ne peut être sauvegardé sans votre accord (vous devrez lancer le chargement manuellement – ou pas ! - à chaque nouvelle réception. Par exemple, ici, **Aucun média** en données mobiles ou en itinérance et seulement les **Documents** en connexion WiFi.



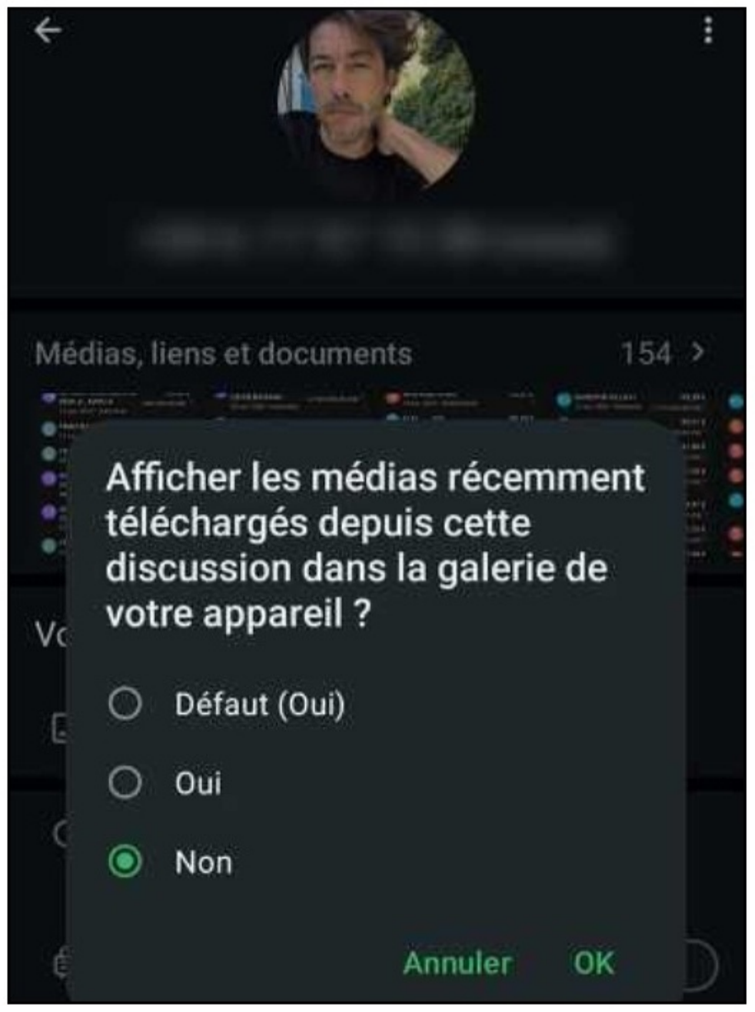
Empêcher WhatsApp d'enregistrer les médias dans la galerie – Option 2

Par commodité, vous pouvez aussi choisir de laisser Whatsapp charger automatiquement ces contenus multimédias sans votre intervention… tout en les bannissant par défaut de votre galerie. En fait, Whatsapp a bien besoin de les télécharger sur votre téléphone pour pouvoir vous les afficher, mais grâce à la fonction « Visibilité des médias », il va créer en coulisse un fichier caché nommé .nomedia dans le dossier du contact ou du groupe pour empêcher l'indexation par la galerie.

Allez dans les **Paramètres** puis **Discussions**. Désactivez l'option **Visibilité des médias**. Dès lors, les nouvelles photos et vidéos reçues resteront visibles uniquement dans WhatsApp, sans être indexées par la galerie Android.



Pour affiner par contact ou par groupe, ouvrez la discussion concernée. Appuyez sur le nom du contact ou du groupe. Sélectionnez **Visibilité des médias > Non**. Les fichiers de ce fil en particulier ne s'afficheront plus dans la galerie, même si l'option globale est activée.



Désactiver la sauvegarde automatique sur Google Drive ou iCloud

Les sauvegardes de conversations sont très pratiques, mais lorsqu'elles partent sur le cloud, elles perdent le bénéfice du chiffrement de bout en bout. En cas de piratage ou de demande judiciaire, vos discussions et contenus multimédias peuvent être accessibles en clair.

Allez dans **Paramètres > Discussions** puis sur **Sauvegarde des discussions** en bas. Sous le menu "Sauvegarde sur Google Drive" (Android) ou "Sauvegarde sur iCloud" (iPhone), allez dans **Sauvegarde automatique** pour choisir **Seulement lorsque j'appuie sur Sauvegarder** ou même désactiver par défaut cette possibilité.



Mais activer la sauvegarde Whatsapp chiffrée

Si vous souhaitez tout de même conserver vos échanges, activez la sauvegarde chiffrée proposée par Whatsapp : la messagerie enregistrera alors une copie sécurisée sur ses propres serveurs dédiés, sous protection cryptographique. Pour les utilisateurs avertis, il est possible de copier manuellement ce fichier chiffré sur un support externe (clé USB, disque dur sécurisé).

Allez dans les **Paramètres > Discussions** et descendez jusqu'à **Sauvegarde des discussions**. Dans la nouvelle fenêtre, descendez également jusqu'à **Sauvegarde chiffrée de bout en bout**. Vous pourrez activer cette sauvegarde via la **Clé d'Accès** crée lors de votre création de compte ou passer par **Autres options** et choisir un mot de passe ou une nouvelle clé de 64 caractères que vous créerez vous-même !
Attention, si vous perdez ce mot de passe ou cette nouvelle clé, la restauration sur un nouvel appareil sera impossible.



Vérifier les permissions Android / iOS accordées à WhatsApp

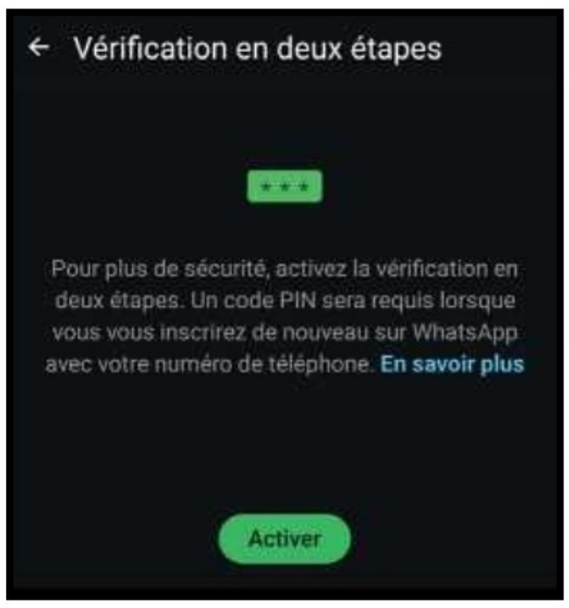
WhatsApp demande souvent l'accès à la caméra, au micro, aux fichiers ou à la géolocalisation. Ces permissions, bien qu'utiles pour certaines fonctions, constituent autant de portes d'entrée potentielles pour la collecte de données. La désactivation permanente de la géolocalisation est par exemple vivement conseillée : elle évite de révéler vos déplacements via les métadonnées des partages.

Sur Android, ouvrez **Paramètres > Applications > WhatsApp > Permissions**. Examinez chaque autorisation et désactivez celles que vous n'utilisez pas (micro, position, fichiers, contacts). Sur iPhone, rendez-vous dans **Réglages > WhatsApp** et retirez les accès inutiles en basculant les interrupteurs.



Internet & Réseaux

Activer la vérification en deux étapes



Le vol de compte WhatsApp est devenu l'une des escroqueries les plus recherchées. Un pirate peut usurper votre identité en récupérant le code SMS de vérification. Activer la vérification en deux étapes ajoute un second mot de passe secret : sans lui, personne ne peut consulter ou transférer votre compte sur un autre appareil.

Ouvrez **Paramètres > Compte > Vérification en deux étapes**. Appuyez sur **Activer** et définissez un code PIN à six chiffres. WhatsApp demandera ce code pour confirmer que vous êtes bien le propriétaire du compte en cas de déconnexion ou d'utilisation de votre numéro de compte sur un autre terminal. Ajoutez une adresse e-mail de secours pour récupérer l'accès en cas d'oubli du code PIN (**Paramètres > Comptes > Adresse e-mail**).

Verrouiller WhatsApp avec empreinte digitale ou reconnaissance faciale

Si votre téléphone est déverrouillé, vos conversations WhatsApp peuvent être ouvertes par quiconque y accède. Le verrouillage biométrique de l'application ajoute une barrière supplémentaire.

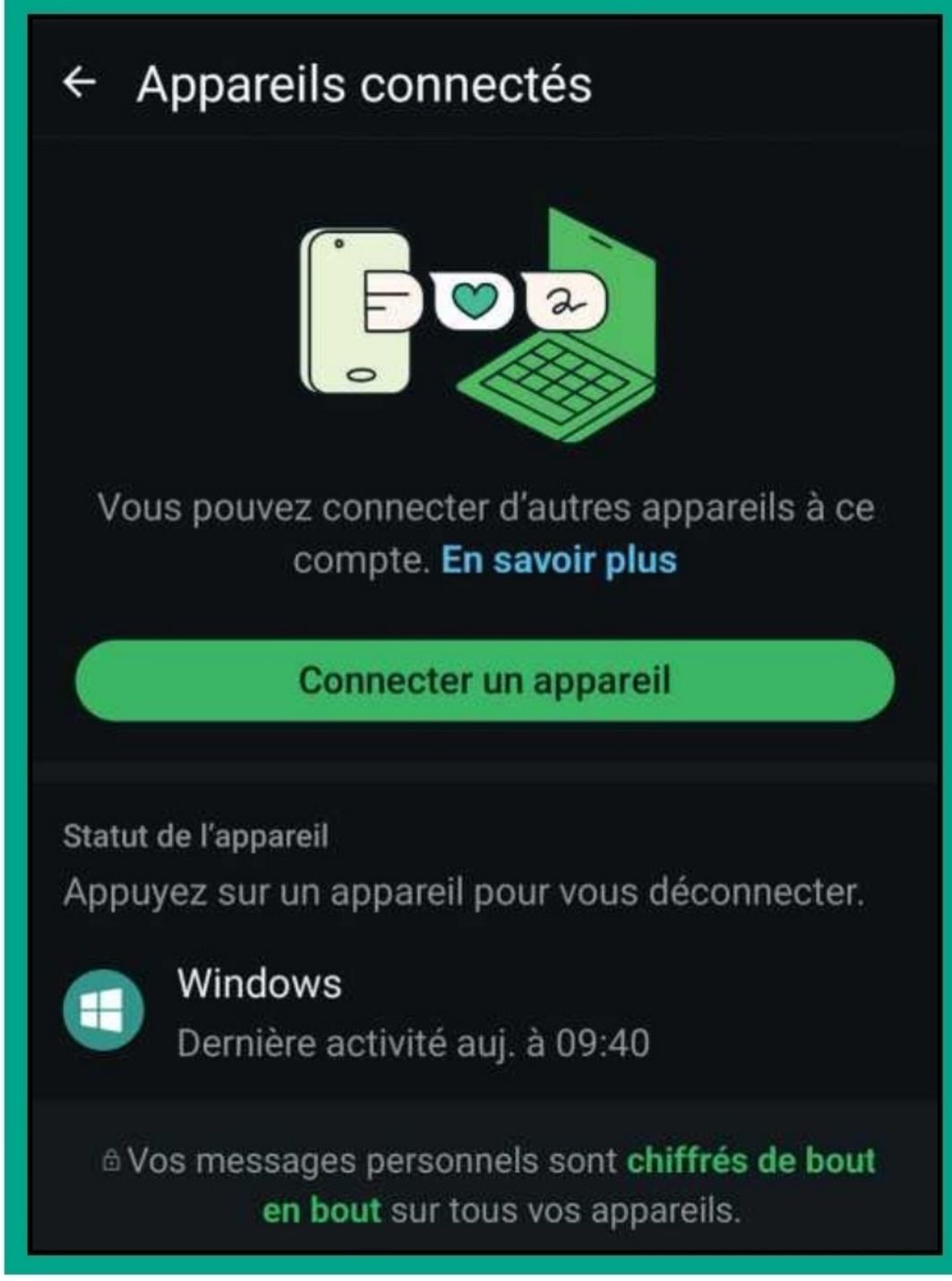
Allez dans **Paramètres > Confidentialité > Verrouillage de l'application**. Activez **Déverrouillage biométrique** (Android) ou **Face ID / Touch ID** (iPhone). Choisissez le délai d'activation automatique : immédiatement, après 1 ou 15 minutes. Cette fonction bloque l'accès complet à l'application, mais les appels entrants et les notifications restent visibles selon vos réglages.



Utiliser le mode "compagnon" sur plusieurs appareils

Vous pouvez désormais utiliser le même compte Whatsapp sur quatre appareils, avec une synchronisation de l'ensemble de vos discussions. Vous pouvez ainsi synchroniser un second téléphone, un PC, une tablette, un Mac, etc.

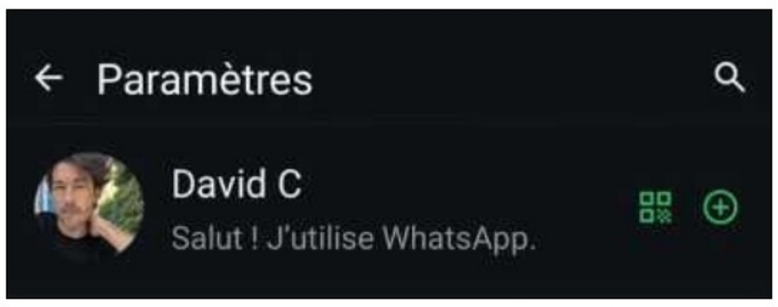
Sur votre téléphone principal, sur la page d'accueil, appuyez sur les trois petits points du menu en haut à droite et sélectionnez **Appareils connectés**. Sur l'autre appareil, installez WhatsApp et choisissez **Se connecter à un compte existant**. Avec ce nouveau terminal, scannez le QR code affiché avec votre téléphone principal.
Mais cette fonctionnalité simple à mettre en place est aussi une faille de sécurité possible. Si quelqu'un a eu accès temporairement à votre téléphone, il a pu synchroniser votre compte Whatsapp sur un appareil tiers lui appartenant et pourra donc suivre toutes vos discussions voire se faire passer pour vous ! Pour vérifier, retournez dans **Appareils connectés** et regardez la liste des appareils qui donnent accès à votre compte Whatsapp. Si vous avez un doute, vous pourrez les déconnecter depuis votre téléphone maître.

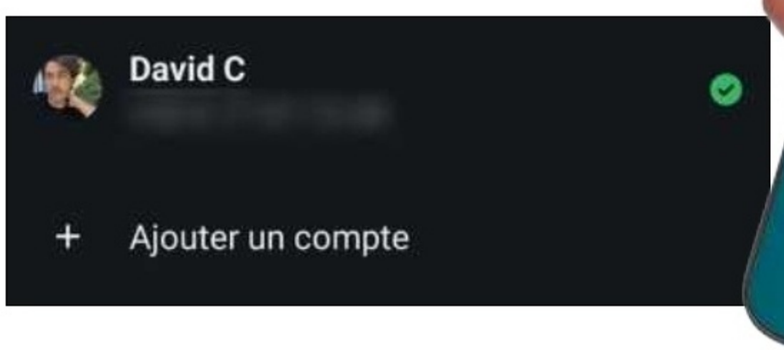


UTILISER UN SECOND NUMÉRO SUR LE MÊME MOBILE POUR UN COMPTE ANONYME

WhatsApp repose sur un numéro de téléphone, mais rien n'oblige d'utiliser le même numéro pour tous vos contacts. Sur un même téléphone et via la même appli Whatsapp, vous pouvez enregistrer un second compte qui reposera sur un autre numéro mobile !
Pour ce faire, vous pouvez bien sûr avoir une double carte SIM, mais vous pouvez aussi utiliser un numéro virtuel ou temporaire. Téléchargez par exemple une application de numéro virtuel fiable, comme TextNow, OnOff, Hushed ou Silent Phone. Ces services fournissent des lignes jetables ou secondaires.
Quelle que soit la solution choisie, ce second numéro vous permettra de séparer vie privée, vie pro ou échanges plus sensibles sur Whatsapp.







01 Compte principal

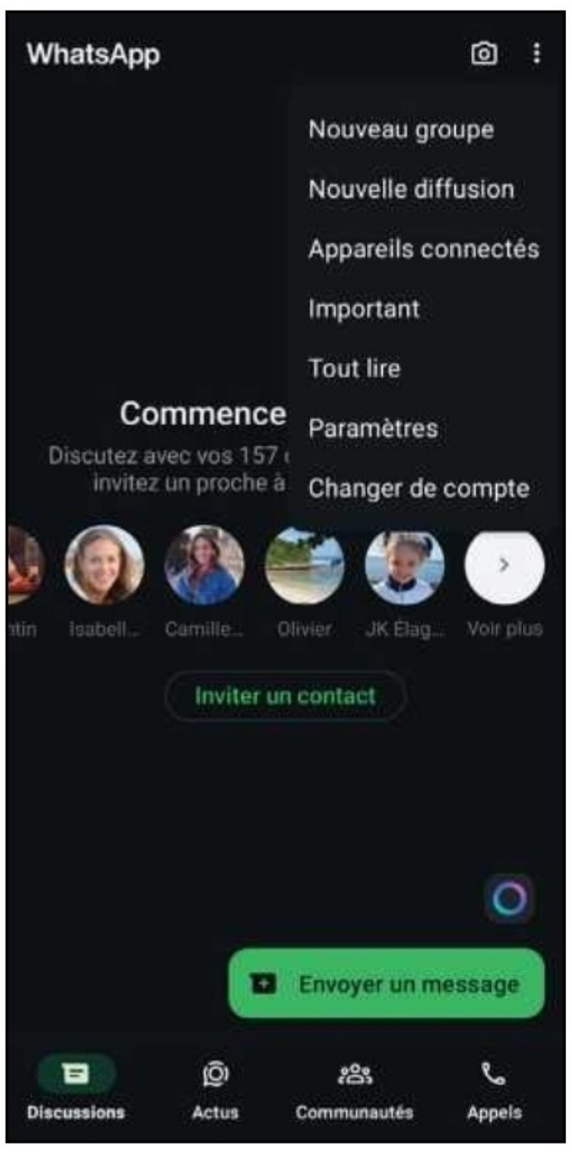
Ouvrez votre Whatsapp habituel puis passez par les trois points du menu en haut à droite de votre fenêtre d'accueil. À côté de votre profil, à droite, appuyez sur le petit « **+** ». L'option **Ajouter un compte** apparait. Poursuivez, acceptez les conditions Whatsapp et continuez.





02 Second compte

Saisissez votre second numéro puis **Suivant**. Une vérification par SMS vous sera envoyée pour valider ce numéro par Whatsapp. Puis renseignez le nom de votre profil tel qu'il apparaîtra pour vos futurs contacts. Appuyez à nouveau sur **Suivant**.



03 Passer de l'un à l'autre

Votre second compte Whatsapp est désormais créé. Pour basculer d'un compte à l'autre, il vous suffira de passer par les trois points du menu en haut à droite de votre fenêtre d'accueil et de choisir **Changer de compte**. Le basculement se fait en deux secondes. Attention de toujours vérifier sur quel compte vous êtes avant tout échange !

Internet & Réseaux

EFFACEZ L'HISTORIQUE DE NAVIGATION SUR amazon

Au-delà du pistage, Amazon conserve et donne accès à toutes vos recherches de produits sur son site. Ce qui est problématique lorsque vous préparez l'achat d'un cadeau ou que vous recherchez une tenue sexy pour madame ou monsieur sur le PC familial. Vous pouvez supprimer de cet historique un ou plusieurs articles (ou la totalité), voire bloquer définitivement cette fonctionnalité.





01 Trouver l'Historique

Une fois loggué, ce n'est pas forcément le plus intuitif selon votre terminal (PC ou mobile). Amazon n'a pas très envie que vous lui enleviez cet historique qui en dit tellement sur vous. Les deux accès les plus simples sont, soit via le lien en bas du bloc **Continuez vos achats** sur la page d'accueil, soit via le menu **Historique de navigation** en haut à droite quand Amazon daigne vous l'afficher !

02 Supprimer un ou plusieurs articles

Amazon vous affiche alors tous les produits que vous avez recherchés et affichés. Un simple bouton **Supprimer** vous permet de les effacer, l'un après l'autre, selon vos besoins.



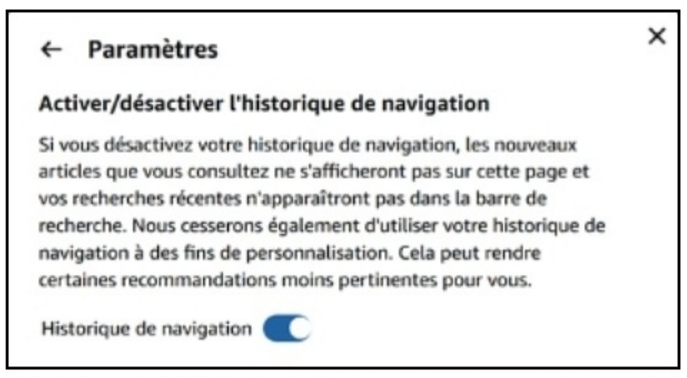


03 Supprimer ou bloquer temporairement

Toujours sur cette page d'historique, en haut à droite, cliquez sur l'icône Paramètres. Vous aurez alors plusieurs options : Retirer tous les articles affichés via le bouton **Retirer des articles** (l'ensemble de votre historique sera supprimé) et bloquer l'historique pour une durée déterminée afin de mener les recherches que vous souhaitez sans qu'elles soient enregistrées.

04 Désactiver l'historique

Si vous souhaitez désactiver par défaut cette fonction et ne plus avoir à y penser, rien de plus simple : à partir de la fenêtre précédente (**Paramètres**), cliquez sur **Plus de paramètres**. Vous n'avez plus qu'à désactiver l'**Historique de navigation**.



AMAZON
Amazon.fr

5 min

Facile

Internet & Réseaux

CRÉEZ UN ACCÈS WI-FI TEMPORAIRE POUR PARTAGER VOTRE CONNEXION

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

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

COMMENT ÇA FONCTIONNE ?

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

ATTENTION

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



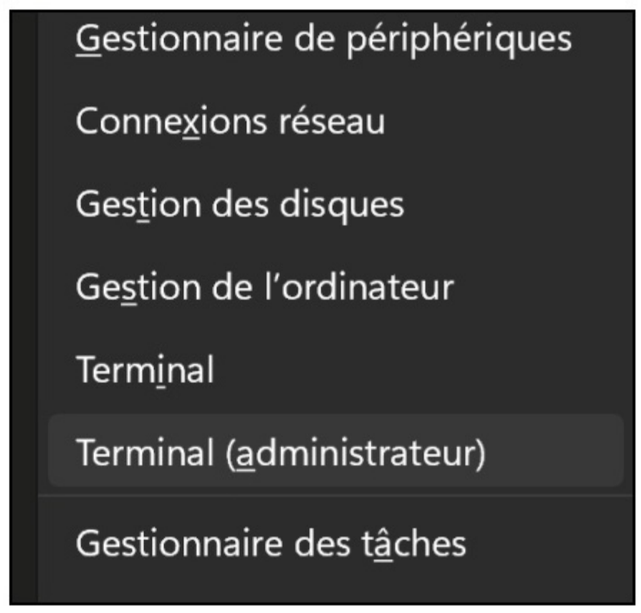
Internet & Réseaux

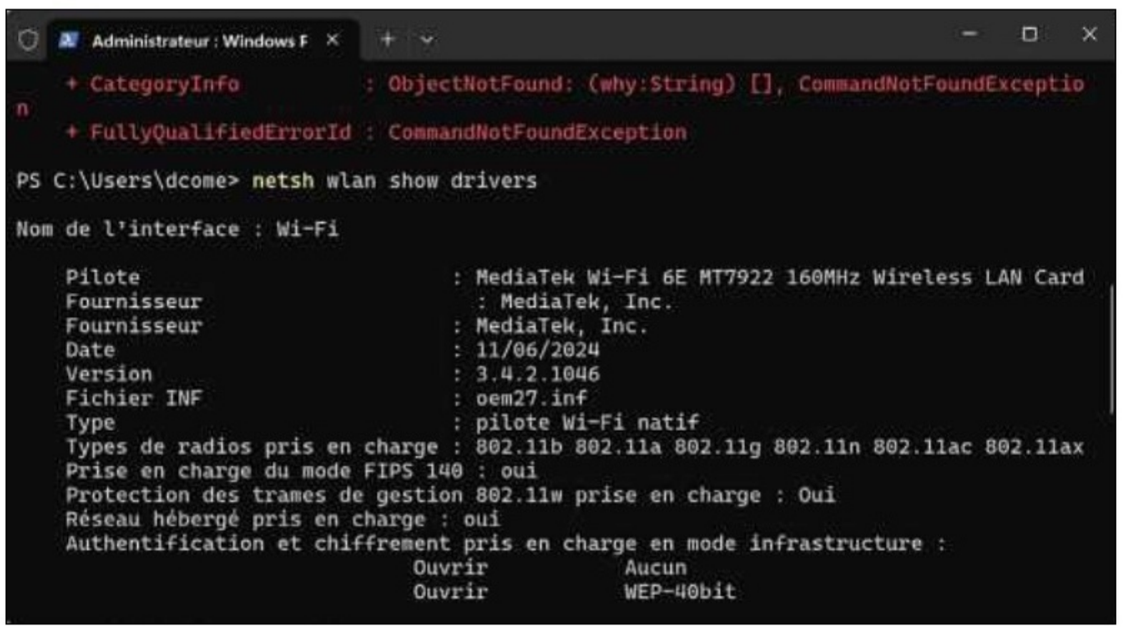
NOUVEAU HOTSPOT TEMPORAIRE AVEC

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

01 Carte réseau compatible 1/2

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



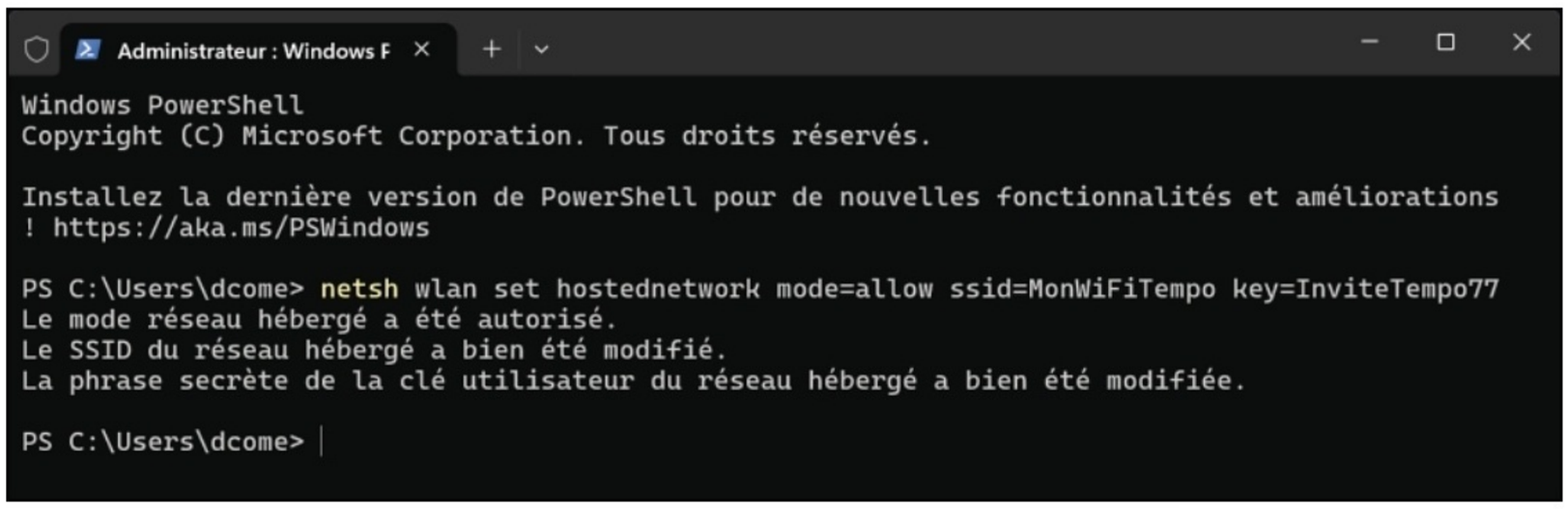


02 Carte réseau compatible 2/2

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

03 Création de l'accès temporaire

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

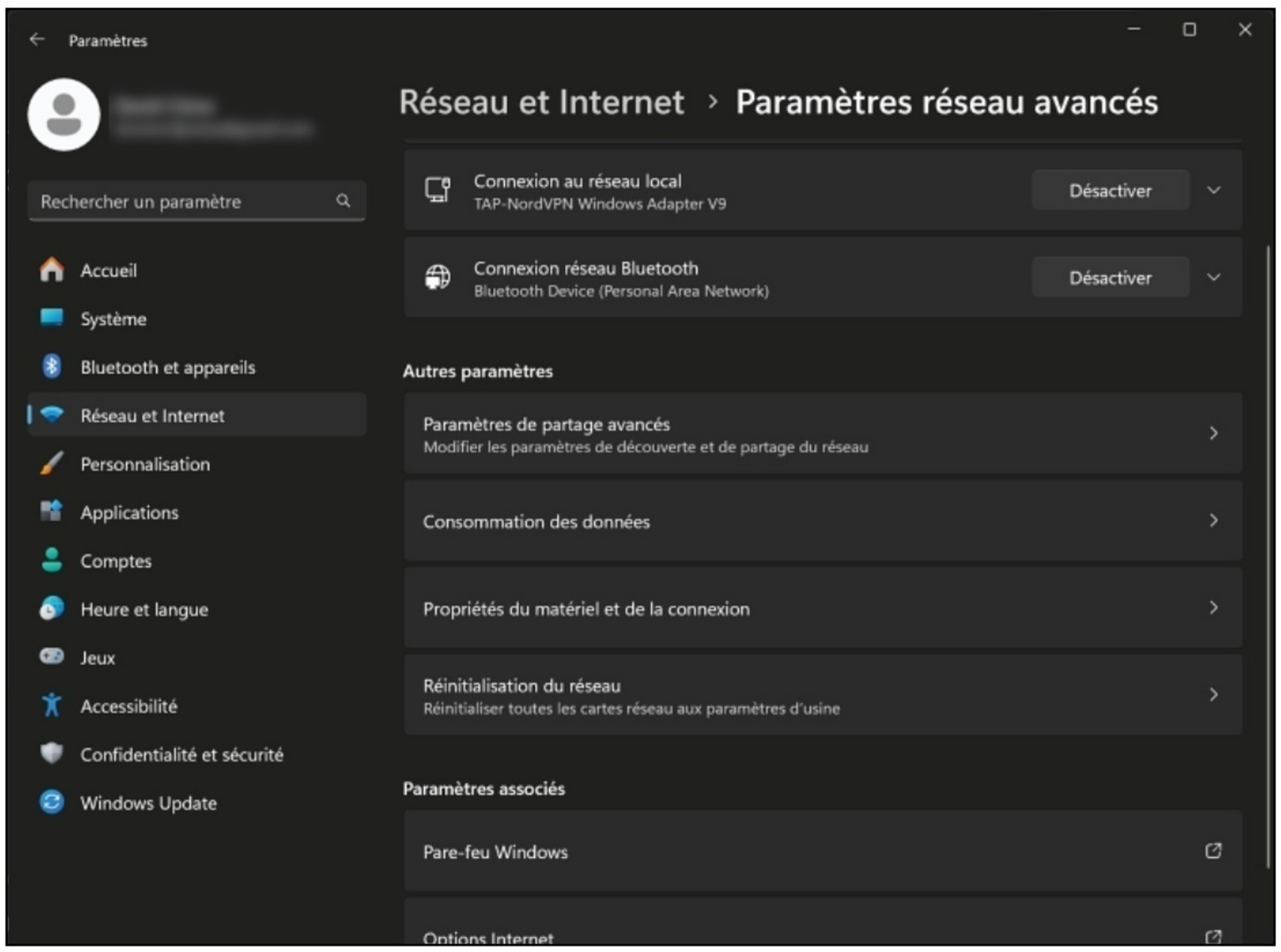


WINDOWS

10 min

Moyen

WINDOWS

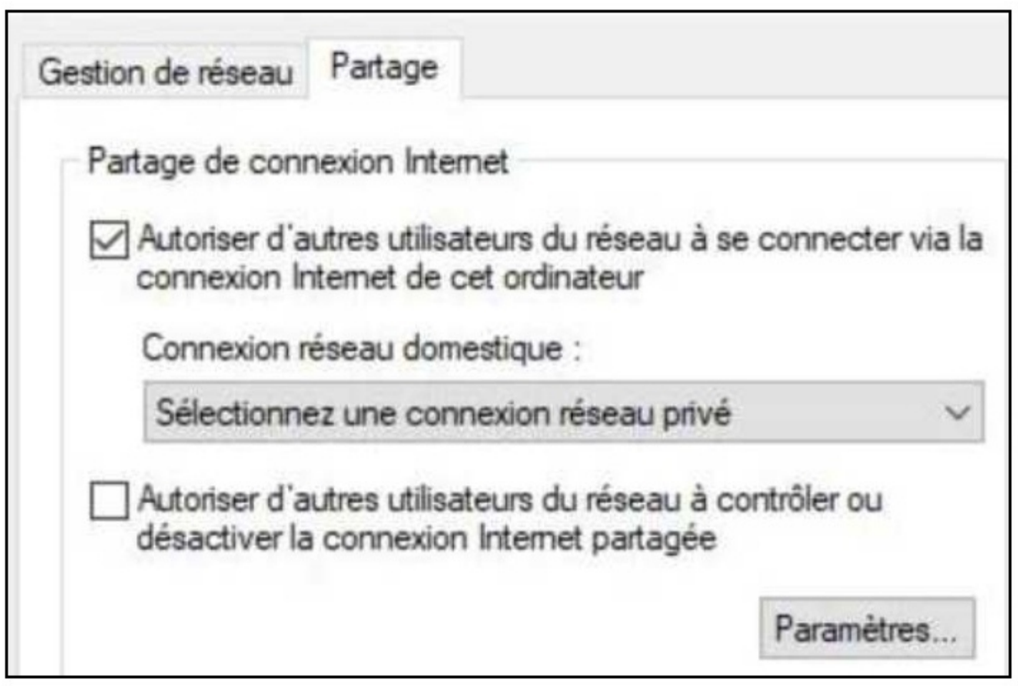


04 Donner l'accès 1/2

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

05 Donner l'accès 2/2

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



UN ACCÈS TEMPORAIRE PERMANENT ?

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

Internet & Réseaux

TOP 3 POUR SURVEILLER VOS OBJETS CONNECTÉS

Alexa, la TV connectée, la caméra de la sonnette, l'ampoule "intelligente" du salon… On ne compte plus les objets qui dialoguent en silence avec Internet. Pratiques, mais parfois indiscrets, ces appareils forment un réseau parallèle dans nos maisons, souvent mal protégé, rarement surveillé. Voici trois solutions pour un audit de votre "foyer connecté".



Fing Desktop > La carte d'identité de votre réseau domestique

Découvrir qui est connecté à votre réseau est la première étape de tout diagnostic IoT. Fing Desktop, outil gratuit et multiplateforme, y excelle. Une fois installé sur PC ou Mac, il scanne votre réseau local et dresse la liste de tous les appareils : smartphones, télévisions, caméras, imprimantes, ampoules, hubs domotiques… Fing identifie la marque, l'adresse MAC, la nature de l'appareil et son comportement réseau.
L'intérêt grand public est immédiat : l'outil signale les appareils inconnus, les ports ouverts, les services actifs et les adresses IP internes. On visualise la structure réelle de son réseau comme on découvrirait le plan électrique de sa maison. De nombreux utilisateurs s'étonnent d'y trouver des objets oubliés depuis longtemps… ou même des équipements que l'on n'a jamais installés soi-même.



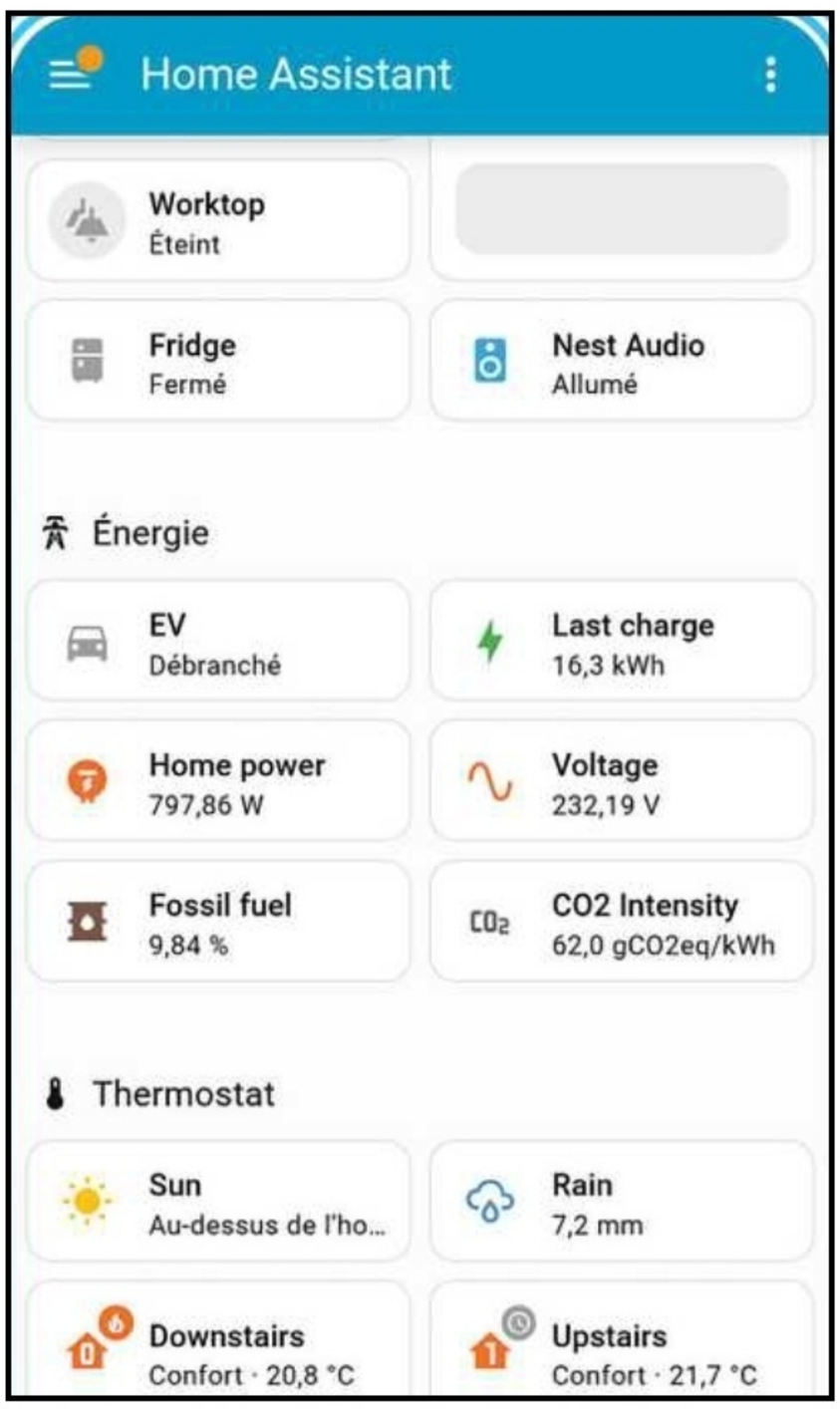
Fing Desktop peut également envoyer des alertes lorsque de nouveaux appareils se connectent, et propose des tests intégrés (latence, qualité Wi-Fi, disponibilité du réseau). Sa version gratuite suffit largement pour auditer un foyer numérique complet.

Lien : www.fing.com/products/fing-desktop

Home Assistant > Le tableau de bord de la maison connectée

Home Assistant centralise les objets connectés de dizaines de marques (Philips Hue, Xiaomi, Somfy, Shelly, TP-Link, Aqara...) dans une interface unique. Pour l'utilisateur, c'est l'équivalent d'une « tour de contrôle » : on voit quels appareils sont actifs, leur état réseau, leur dernière activité et, surtout, on peut automatiser des règles.
Contrairement aux plateformes cloud comme Alexa ou Google Home, Home Assistant est auto-hébergé : l'intégralité des données reste chez vous. Les modules de sécurité intégrés permettent aussi de surveiller les connexions inhabituelles, d'identifier les appareils en échec de mise à jour ou de forcer l'utilisation de protocoles locaux (Zigbee, Z-Wave, Matter) au lieu du cloud.
Home Assistant peut sembler technique mais les tutoriels officiels et la communauté rendent l'outil accessible, grâce aussi à l'interface “Wizards” guidée.

Lien : www.home-assistant.io

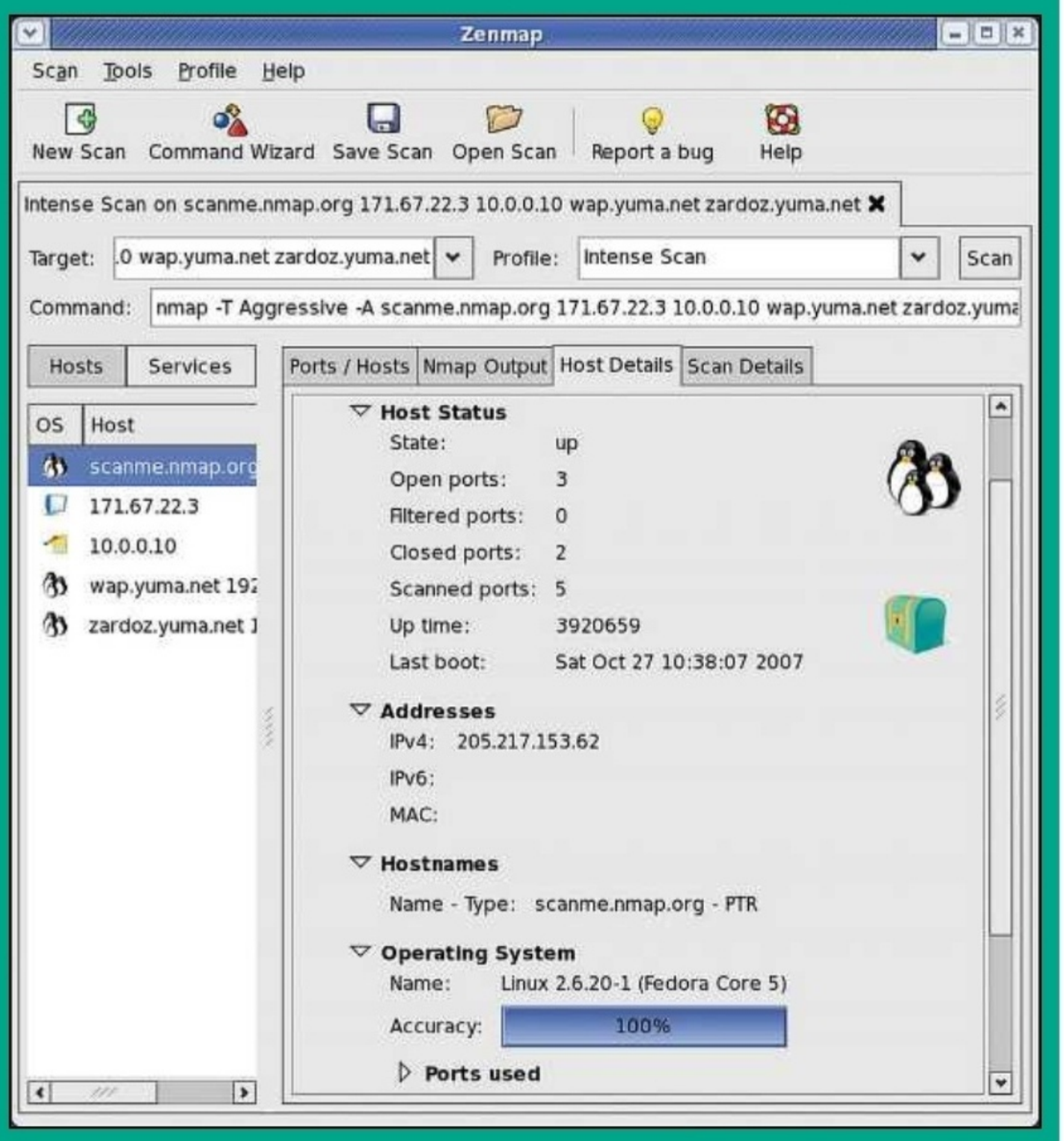


Nmap (mode simplifié)

> Le stéthoscope du réseau domestique



Nmap est un outil mythique du monde de la cybersécurité, souvent associé aux experts. Mais pour un usage domestique, son interface simplifiée Zenmap (toujours disponible en 2025 via des forks communautaires) permet d'exécuter des scans accessibles : découverte d'équipements, ports ouverts, services réseau exposés, protocoles actifs. Dans un foyer connecté,



Nmap met en lumière des informations cruciales : une caméra expose-t-elle un serveur web non protégé ? Votre frigo connecté ouvre-t-il des ports inutiles ? Un objet déploie-t-il un protocole obsolète comme Telnet ?
Le scan se fait en quelques secondes. L'utilisateur sélectionne simplement un “profil” prédéfini (“Quick Scan”, “Intense Scan”, “Ping Scan”), et l'outil cartographie tout le réseau local.

Lien : https://nmap.org

Internet & Réseaux

TOP 3 OUTILS POUR CONTRÔLER SES DONNÉES

Reprendre le contrôle, ce n'est pas disparaître du Web. Ces trois outils – de l'export de données à la configuration du système – constituent un kit d'autodéfense numérique grand public, gratuit et complémentaire.



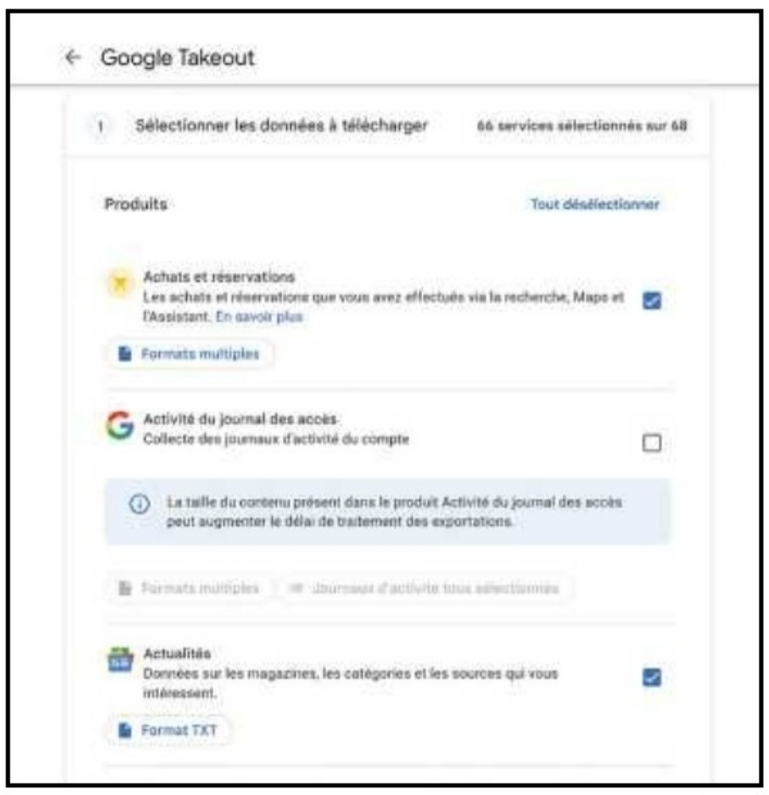
Google Takeout > Scannez votre vie numérique

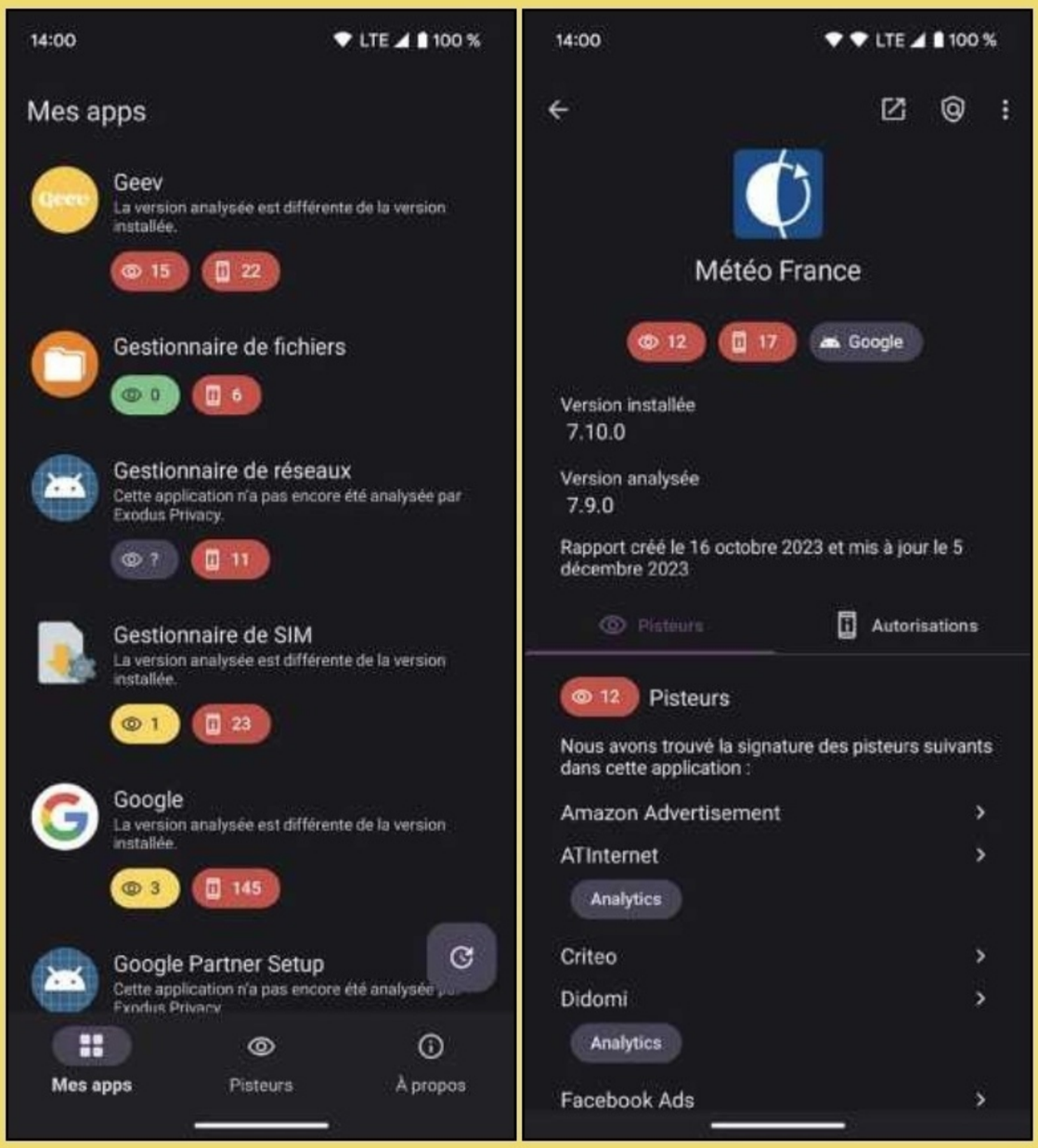
Google n'a pas volé sa réputation de glouton de données : historiques de recherche, géolocalisation, vidéos regardées, mails archivés… Chaque clic laisse une empreinte. Pourtant, le géant du Web offre lui-même un formidable outil d'audit : Google Takeout. Ce service, souvent méconnu, permet à tout utilisateur de récupérer une copie complète de ses données stockées dans les différents services Google (Gmail, YouTube, Drive, Maps, Photos, etc.).

En quelques clics, Takeout dresse une radiographie saisissante de votre vie numérique : un fichier ZIP ou TGZ contenant toutes vos activités, triées par application. L'outil n'a rien de technique : il suffit de se connecter, de sélectionner les services concernés, puis de demander l'export. Après quelques heures, Google envoie un lien pour télécharger l'archive.

L'expérience est souvent édifiante : on mesure l'ampleur des traces accumulées, parfois sur plus d'une décennie. Takeout est donc le premier geste de reconquête : comprendre avant d'agir.

Lien : https://takeout.google.com





Exodus Privacy

> Dévoile les coulisses de vos applis

Chaque application que nous installons dialogue en silence avec des régies publicitaires, des services d'analyse ou des trackers de comportement. On s'en doute vaguement, sans jamais pouvoir le vérifier. C'est précisément là qu'intervient Exodus Privacy, un projet open source français, qui a choisi de lever le voile sur ce qu'il appelle "l'écosystème invisible du pistage mobile".

Derrière une interface minimaliste, Exodus Privacy scanne les applications installées sur votre téléphone Android et affiche, noir sur blanc, la liste des traqueurs et des autorisations qu'elles contiennent. Pour chaque app, l'outil indique combien de bibliothèques de suivi publicitaire sont intégrées (Google Ads, Facebook Analytics, Firebase, etc.), et quelles permissions elles réclament : géolocalisation, accès micro, carnet d'adresses, stockage, etc. Le diagnostic est limpide : un code couleur classe les applis de la plus vertueuse à la plus curieuse. En quelques minutes, on découvre souvent que des jeux ou utilitaires anodins hébergent une dizaine de traqueurs — une prise de conscience souvent brutale, mais salutaire.

L'expérience est 100 % locale : aucune donnée personnelle n'est transmise à l'association ni à un serveur externe.

Lien : https://exodus-privacy.eu.org

MyPermissions

> Le détective des connexions cachées

Combien d'applications avez-vous autorisées à "se connecter via Facebook" ? Ou à accéder à votre compte Google ? Probablement plus que vous ne le pensez. Ces liens invisibles constituent un risque discret : chaque app garde parfois la permission de lire vos informations même si vous ne l'utilisez plus. MyPermissions traque précisément ces accès dormants.

L'outil scanne vos comptes et affiche une liste claire de toutes les applications tierces reliées. En un clic, vous pouvez révoquer les permissions inutiles et recevoir des alertes lorsqu'un nouveau service tente de se connecter. C'est une forme d'hygiène numérique simple et salvatrice : on découvre souvent des dizaines de connexions oubliées depuis des années.

Sa version gratuite suffit à faire un grand ménage ; les fonctions premium se limitent à des alertes automatiques et à la surveillance continue.

L'application ne demande pas de compétences particulières : son interface est lisible et intuitive.

Lien : https://mypermissions.com





Internet & Réseaux

5 ASTUCES POUR VOTRE VPN

Certaines fonctions de VPN, souvent méconnues ou inutilisées, méritent pourtant le détour. Les noms peuvent changer mais ces options sont un plus qu'il ne faut pas ignorer pour profiter de leur potentiel.

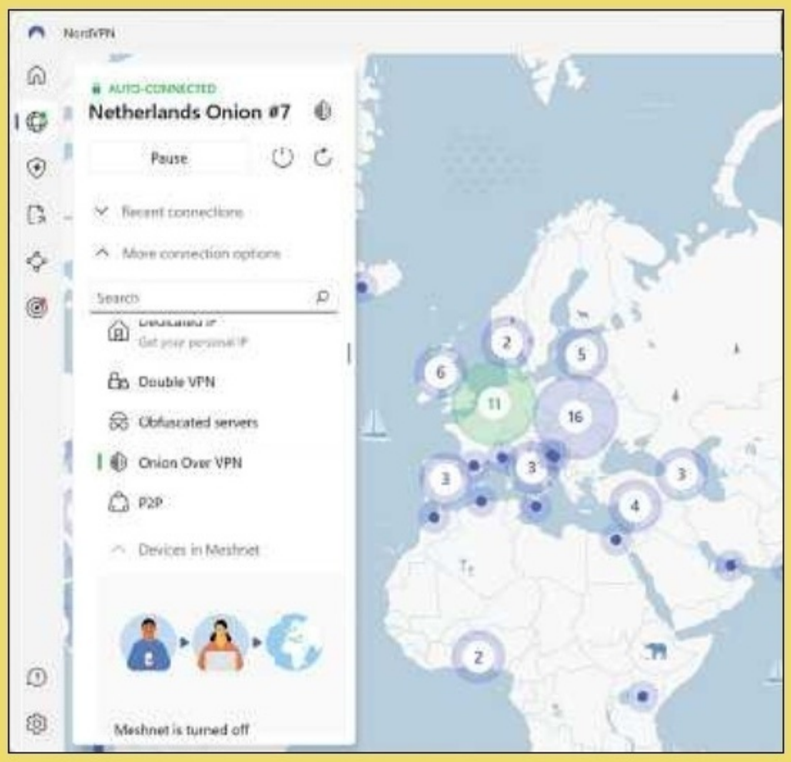


VPN + Tor : avec NordVPN

Onion Over VPN est une fonction de NordVPN qui permet aux utilisateurs d'accéder au réseau anonyme Tor via votre VPN et sans avoir besoin d'un navigateur Tor séparé.
En plus de votre VPN, vous pouvez ajouter une seconde couche de protection et d'anonymat en vous connectant au réseau Tor. Comme d'autres fournisseurs de VPN, NordVPN propose ce service qui masque votre IP d'origine autant que le protocole que vous utilisez.



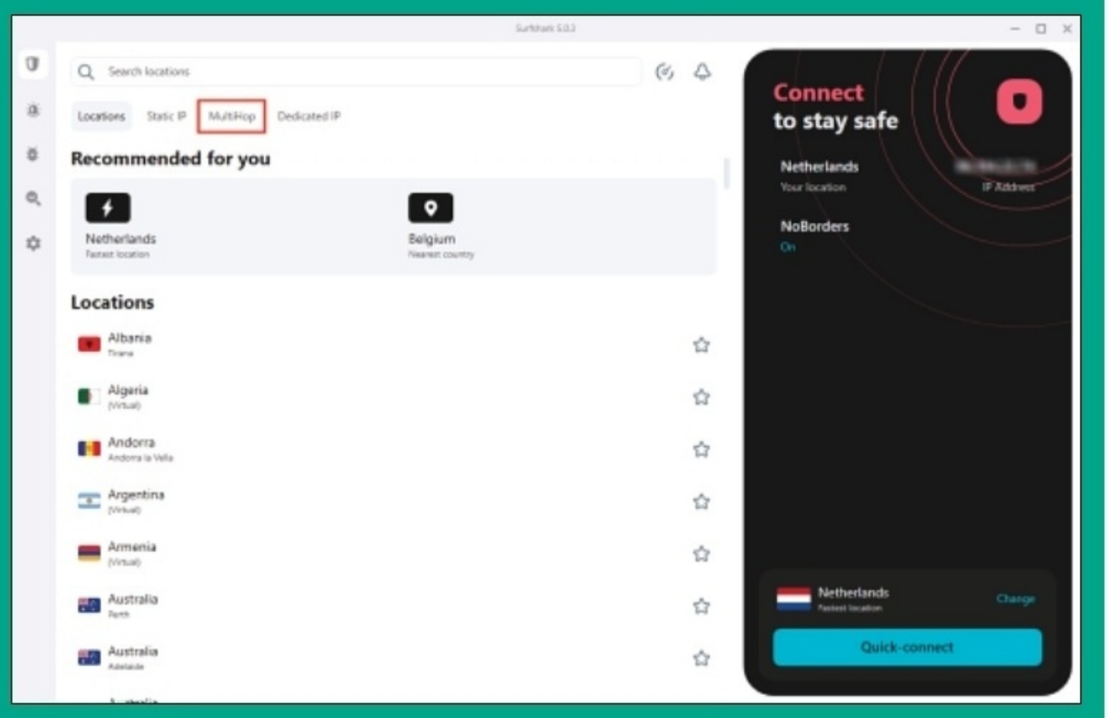
Dans **More connections options**, choisissez **Onion Over VPN**. Vous serez connectés au réseau Tor à partir des serveurs NordVPN dédiés (depuis la Suisse ou les Pays-Bas). Pour revenir à un mode VPN standard, cliquez sur **Quick Connect** dans **Recent connections**.



Passer au Camouflage et au Multihop > Avec Surfshark

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

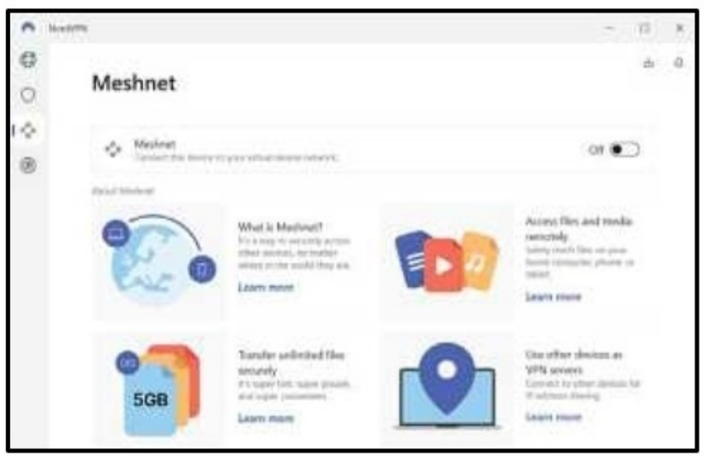
- Camouflage Mode : Cette fonction rend votre activité VPN indétectable même par votre fournisseur d'accès Internet (FAI). Il est utile dans les pays où l'utilisation des VPN est restreinte ou surveillée. Techniquement, il masque le fait que vous utilisez un protocole VPN en faisant paraître votre trafic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



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

Un petit peu de Mesh ? >

Avec NordVPN



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

Essayez le Split Tunneling

> Avec Cyberghost



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

Les possibilités de ProtonVPN Free

Changer de serveur > Vous pouvez demander à être basculé sur un autre serveur pour tester sa stabilité et rapidité. Attention, un temps de latence est nécessaire avant de changer à nouveau de serveur.

Profils > Enregistrez vos paramètres et serveurs préférés pour une utilisation future. Cette fonction n'est disponible que dans la version payante.



La version gratuite de ProtonVPN vous offre la puissance d'un VPN Pro malgré ses limitations en termes de géolocalisation et de vitesses de connexions.

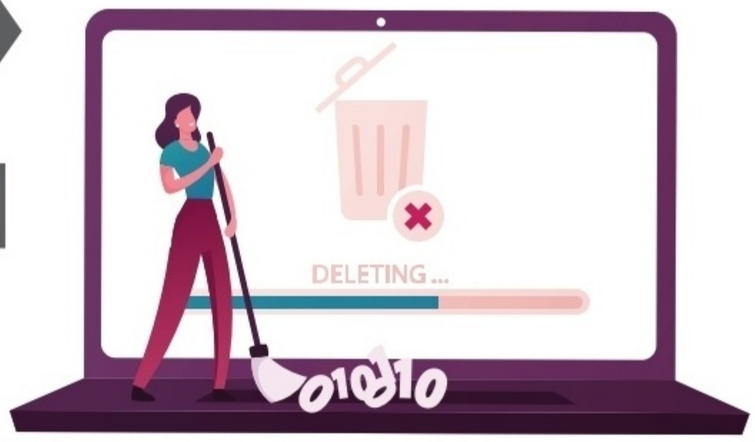
Kill switch > Disponible dans la version gratuite, cette fonction vous permet d'être déconnecté immédiatement d'Internet si le VPN se trouve malencontreusement désactivé.

Pays > La version gratuite ne vous permet pas de choisir librement mais vous connectera à l'un des quelques serveurs disponibles (États-Unis, Japon, Pays-Bas, Roumanie).

Le plus rapide > Se connecter automatiquement au serveur qui vous fournira la connexion la plus rapide

Internet & Réseaux

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



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

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

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

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

FAILLE DE SÉCURITÉ

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



Il est donc essentiel de privilégier des fournisseurs de VPN qui garantissent cette politique « No Log ». Mais, attention, certains l'affirment sans respecter cette exigence ! S'il est important de trouver des déclarations explicites affirmant que le fournisseur ne garde ni logs d'activité ni logs de session, seuls des audits indépendants réalisés par des tiers peuvent fournir une assurance supplémentaire quant à la véracité des déclarations d'un fournisseur. Heureusement, conscients de cette suspicion, la majorité des fournisseurs de VPN sérieux mettent en avant l'existence de ces audits et les références des sociétés spécialisées les ayant réalisées.

PC TRUCS & ASTUCES
FICHES PRATIQUES



JE SOUTIENS
LE COMMERCE DE PROXIMITÉ,

JE VAIS CHEZ MON
MARCHAND DE JOURNAUX

Direct éditeurs

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

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

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

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

ecofolio

PC & FICHIERS

Votre ordi et son contenu à l'abri des regards

PC & Fichiers

TOP 3 LOGICIELS DE CHIFFREMENT

AxCrypt

> Limité mais intuitif

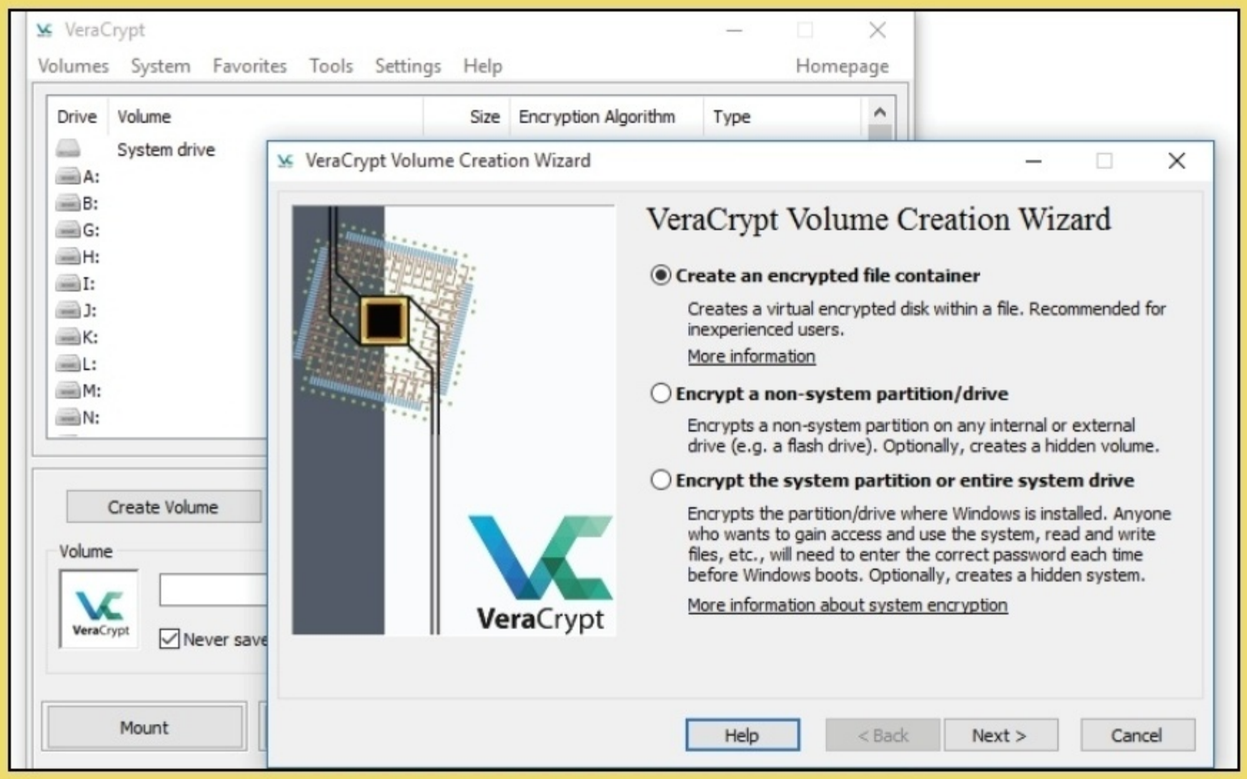
Programme open source disponible pour Windows, macOS, Android et iOS. Chiffre, déchiffre et supprime des fichiers et dossiers. La version payante est compatible avec Google Drive et Dropbox. Multilingue avec un gestionnaire



de mots de passe. La version gratuite a des fonctionnalités restreintes et un chiffrement 128 bits. Certains réglages par défaut nécessitent une activation manuelle.

Lien : axcrypt.net

VeraCrypt > Le numéro 1



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

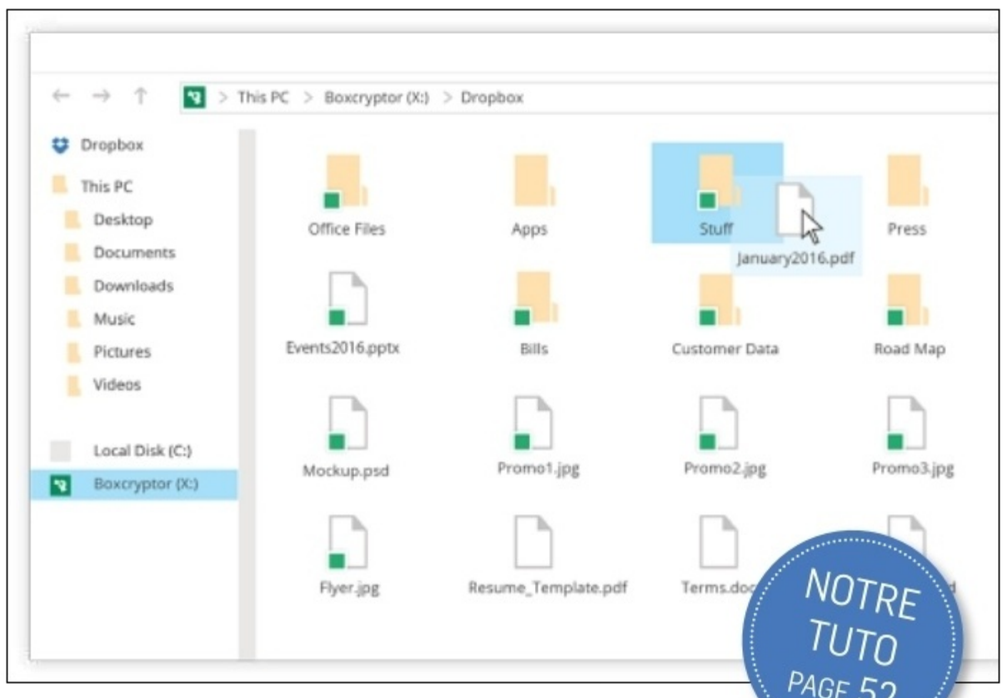
Lien : www.veracrypt.fr

Boxcryptor

> Pour le cloud

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

Lien : www.boxcryptor.com



NOTRE TUTO PAGE 52



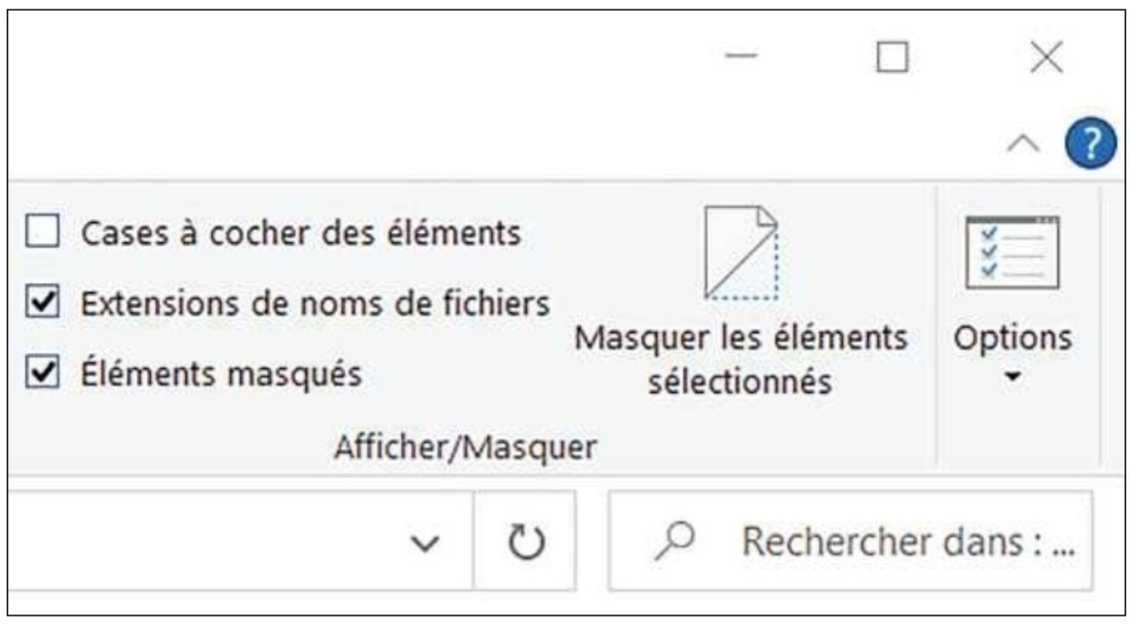
MASQUER UN DOSSIER SUR WINDOWS

PC & Fichiers

Vous pouvez cacher certains dossiers sous Windows, pourvu que les bonnes options soient activées. Suivez le guide

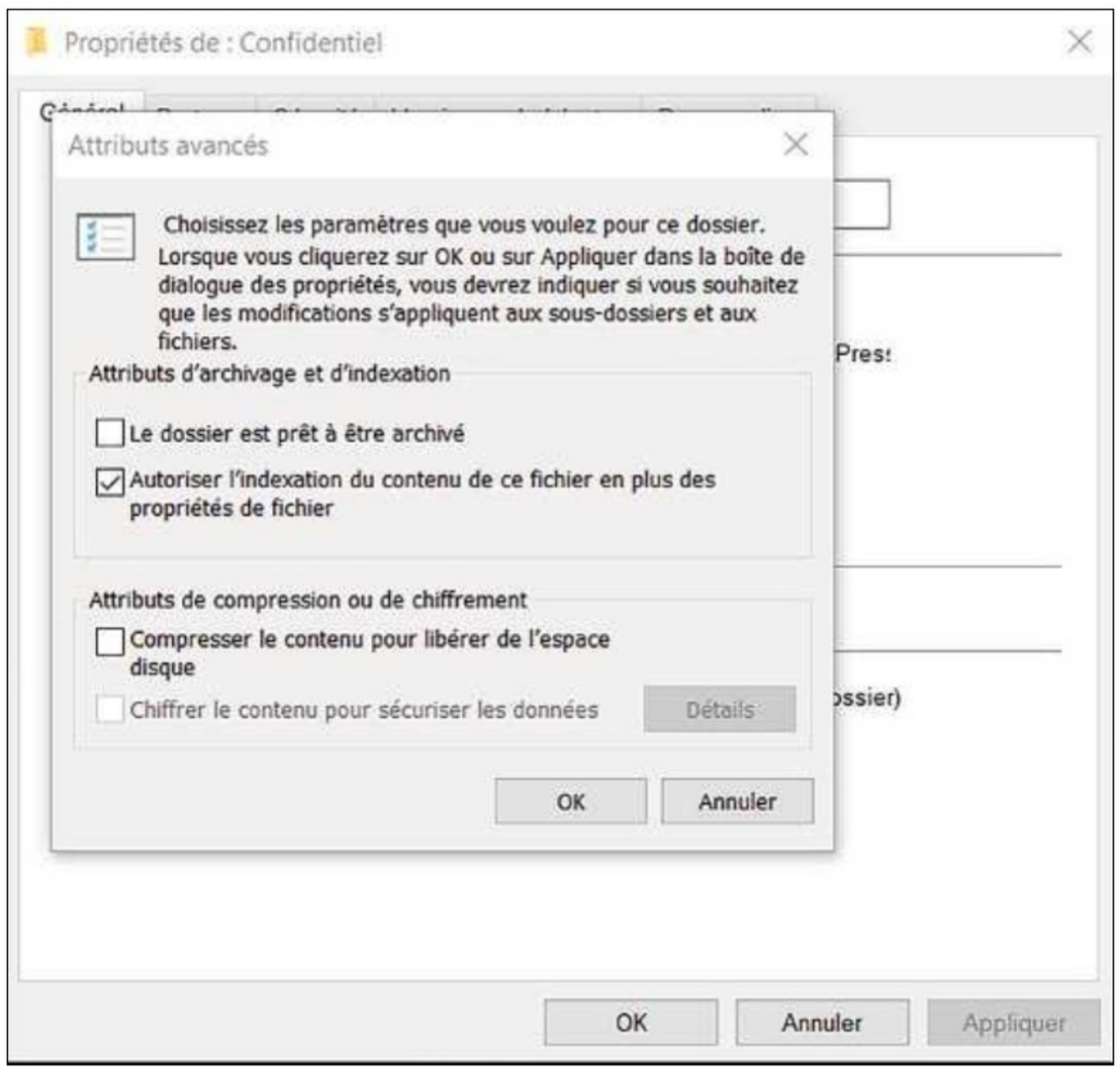
01 Masquer un dossier

Ouvrez l'explorateur de fichiers à l'endroit où se trouve le dossier à dissimuler. Cliquez sur la flèche en haut à droite pour développer le ruban. Allez dans l'onglet **Affichage**. Sélectionnez le dossier et cliquez sur **Masquer les éléments sélectionnés**. S'il est toujours visible, décochez la case **Eléments masqués**.



02 Retirer le dossier de la recherche

Si vous n'avez pas accès au ruban, faites un clic droit sur le dossier puis sélectionnez **Propriétés**. Dans la section **Général**, sous la rubrique **Attributs**, cochez la case **Caché**. Pour aller plus loin et retirer le dossier et les fichiers qu'il contient de la recherche Windows, cliquez sur **Avancé...** et décochez **Autoriser l'indexation du contenu de ce ficher**. Cliquez sur **OK**



WINDOWS

2 min

Facile

PC & Fichiers

CHIFFREZ VOTRE CLÉ USB AVEC ROHOS

Protégez le contenu de votre clé USB avec ce petit utilitaire ultra-sécurisé.

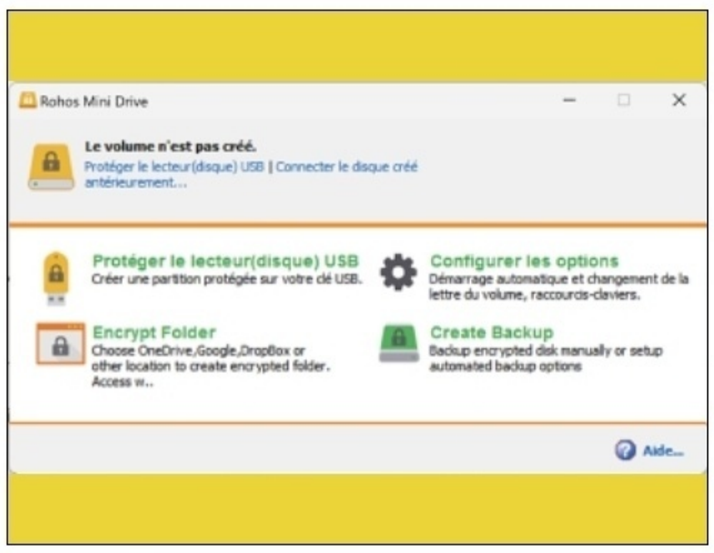
ROHOS MINI DRIVE
rohos.com

10 min

Moyen

Rohos Mini Drive est destiné à ceux qui souhaitent sécuriser des fichiers sensibles sur une clé USB en créant une partition chiffrée. Ce logiciel est idéal pour les professionnels qui transportent des informations confidentielles, garantissant que les données restent protégées même en cas de perte ou de vol du périphérique. Le chiffrement est en AES 256 bits et la partition chiffrée sur votre support USB est cachée. C'est-à-dire qu'en cas de vol, on se saura pas quoi chercher et cracker sans une analyse plus approfondie. Vous avez juste besoin de fournir un mot de passe pour y accéder. En un seul clic, vous pouvez enregistrer votre premier fichier dans un volume protégé. Le chiffrement est automatique et à la volée pour les suivants. Dans les options, choisissez d'utiliser Rohos sans droits d'administrateur, ce qui vous permettra d'accéder aux données chiffrées sur n'importe quel ordinateur. La version gratuite est limitée à 2 Go de partition sécurisée.

PREMIÈRE CONFIGURATION DE VOTRE VOLUME CHIFFRÉ



01 Installation

Depuis le site de Rohos, téléchargez et installez en français le programme depuis **Téléchargement de la configuration**. Ouvrez Rohos Mini Drive, vous êtes prêt à configurer votre première clé USB.



02 Votre clé

Insérez votre support externe USB. Revenez sur l'interface de Rohos puis cliquez sur **Protéger le lecteur(disque) USB**. Si vous n'avez qu'une unité connectée, Rohos la sélectionnera automatiquement par défaut. Si vous en possédez plusieurs, à vous de choisir celle que vous voulez configurer. Vous devrez d'abord définir votre mot de passe.

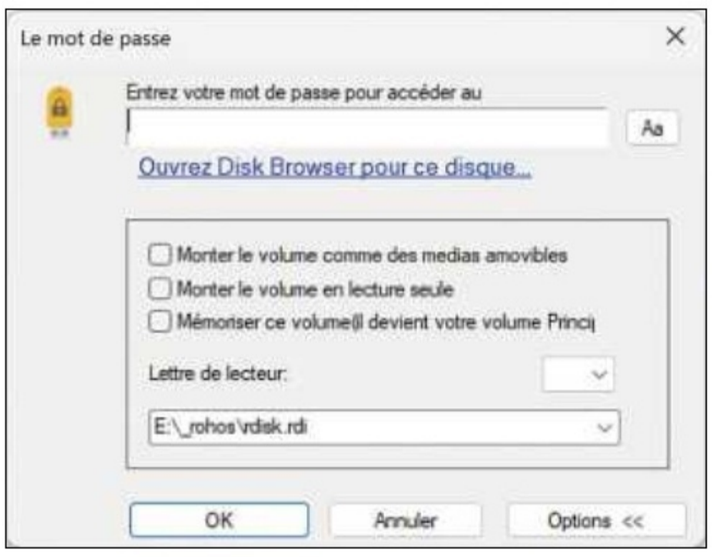


03 Espace chiffré

Via **Détails**, vous pouvez définir l'espace qui sera alloué à votre partition protégée. Dans la version gratuite de Rohos Mini Drive, cet espace est de 2 Go. Une fois défini, cliquez sur **Ok** puis sur cliquer sur **Créer un volume** dans la fenêtre principale. Rohos s'occupe de créer le volume crypté demandé. Cela peut prendre quelques dizaines de secondes.

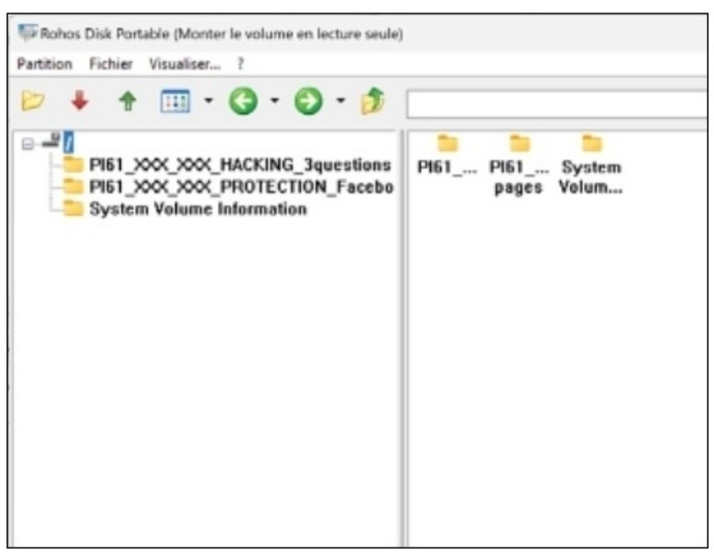


AVEC ROHOS MINI DRIVE



04 Accéder à votre volume

Une fois le volume créé, vous devrez cliquer sur l'icône Rohos Mini.exe sur votre clé USB pour y accéder. Votre mot de passe vous est alors demandé pour voir et interagir avec ce que contient votre volume. Si vous travaillez sur votre PC, pas de souci, mais si vous ouvrez ce volume sur un autre terminal, vous devrez disposer des droits d'administrateur.



05 Interface de gestion portable

L'option **Ouvrez Disk Browser pour ce disque** vous permet d'utiliser la version portable de Rohos Mini Drive sur n'importe quel PC sans droit d'administrateur. Et vous aurez besoin, bien sûr, de votre mot de passe. Cette interface permet également de créer des conteneurs de disques virtuels et des conteneurs cryptés cachés.



06 Et même le cloud !

Via l'interface principale, vous aurez accès aux **Options**, à la possibilité de créer automatiquement des backups chiffrés mais aussi de cibler votre service de cloud pour y créer un volume chiffré via votre interface PC. Cliquez sur **Encrypt Folder > Choose Location** pour définir ce dernier. Un nouveau mot de passe dédié à ce nouvel espace vous sera demandé.



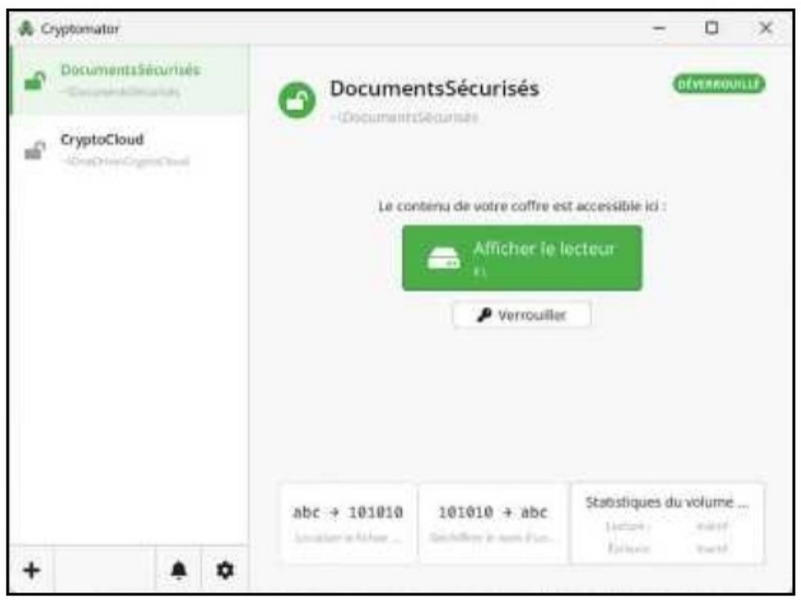
CRYPTOMATOR :

PROTÉGEZ VOS DOSSIERS SENSIBLES SUR PC ET DANS LE CLOUD



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

À l'heure où le stockage dans le cloud est devenu un réflexe — notamment avec OneDrive intégré par défaut à Windows 11 — la question de la confidentialité de nos données n'a jamais été aussi cruciale. Les fichiers personnels, les documents de travail ou les archives sensibles que nous synchronisons dans le nuage peuvent être vulnérables s'ils ne sont pas protégés correctement.
La gageure est de savoir chiffrer et sécuriser par mot de passe un dossier sur votre PC… tout en s'assurant que sa synchronisation sur le cloud bénéficiera de la même protection !
C'est ici que Cryptomator entre en scène. Ce logiciel libre, développé par l'équipe allemande de Skymatic, offre une solution élégante et robuste pour protéger en local vos dossiers avec un chiffrement de bout en bout, sans vous priver des avantages du cloud. Si vous utilisez un service de cloud (comme OneDrive, Dropbox, Google Drive…) qui synchronise et sauvegarde une partie du contenu de votre PC, Cryptomator s'occupe de tout de façon transparente sans que vous ayez à vous en occuper. Il vous assurera que personne, pas même le fournisseur de cloud, ne puisse lire vos fichiers.



OPEN SOURCE, MAIS ULTRA INTUITIF

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

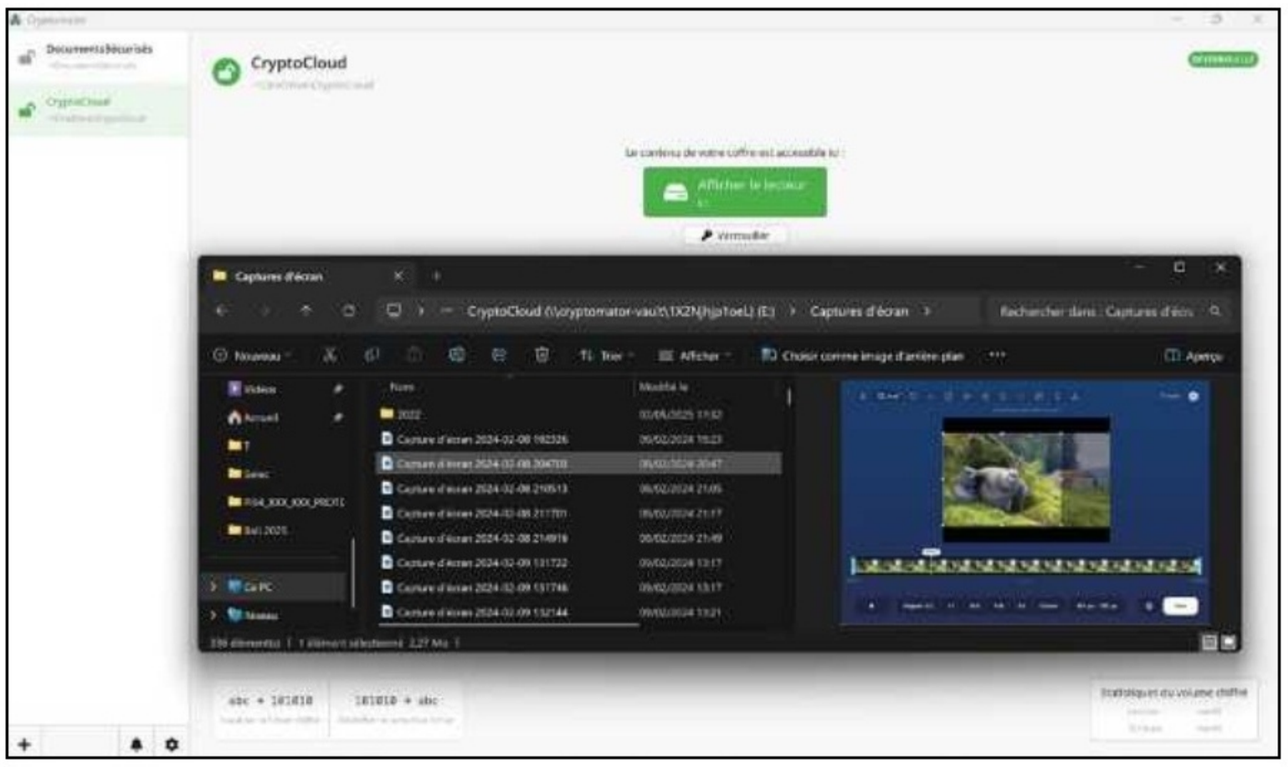
Dès son installation, Cryptomator vous permet de créer ce qu'il appelle un "coffre" (ou vault, en anglais). Il s'agit d'un répertoire spécial, protégé par mot de passe, qui se comporte comme un disque virtuel une fois ouvert. Ce coffre peut être situé n'importe où sur votre disque dur, y compris dans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

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

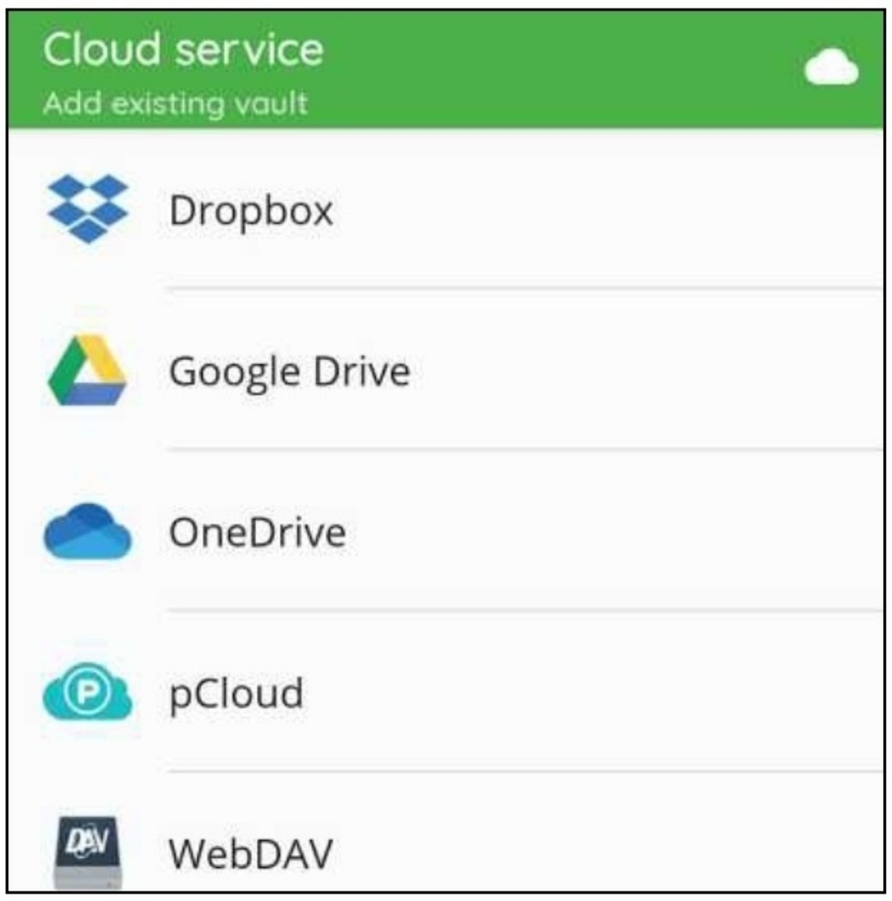
PENSÉ POUR LE CLOUD, MAIS AUSSI POUR LE LOCAL

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

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



Dans un dossier protégé, chaque fichier est chiffré individuellement : quand vous modifiez un élément, la synchronisation ne concernera que cette modification.



Si Cryptomator est gratuit sur iOS, sa version Android est elle payante, à 19,99 € pour un usage illimité et avec les fonctions premium déverrouillées.

À SAVOIR

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

PC & Fichiers

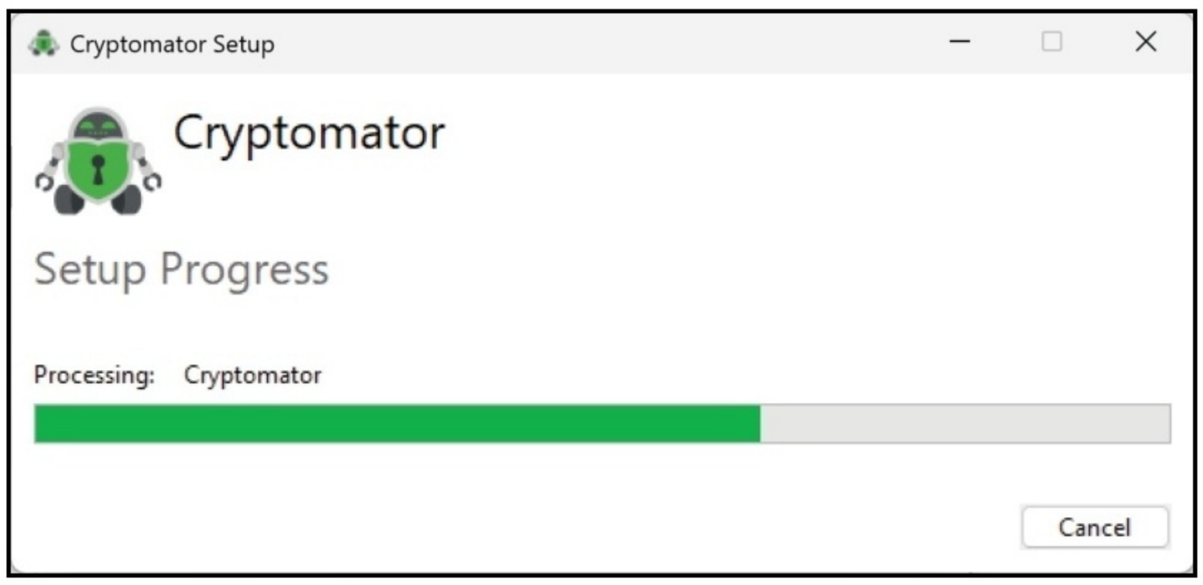
PROTÉGEZ VOS DOSSIERS EN LOCAL

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

01

Installation de Cryptomator

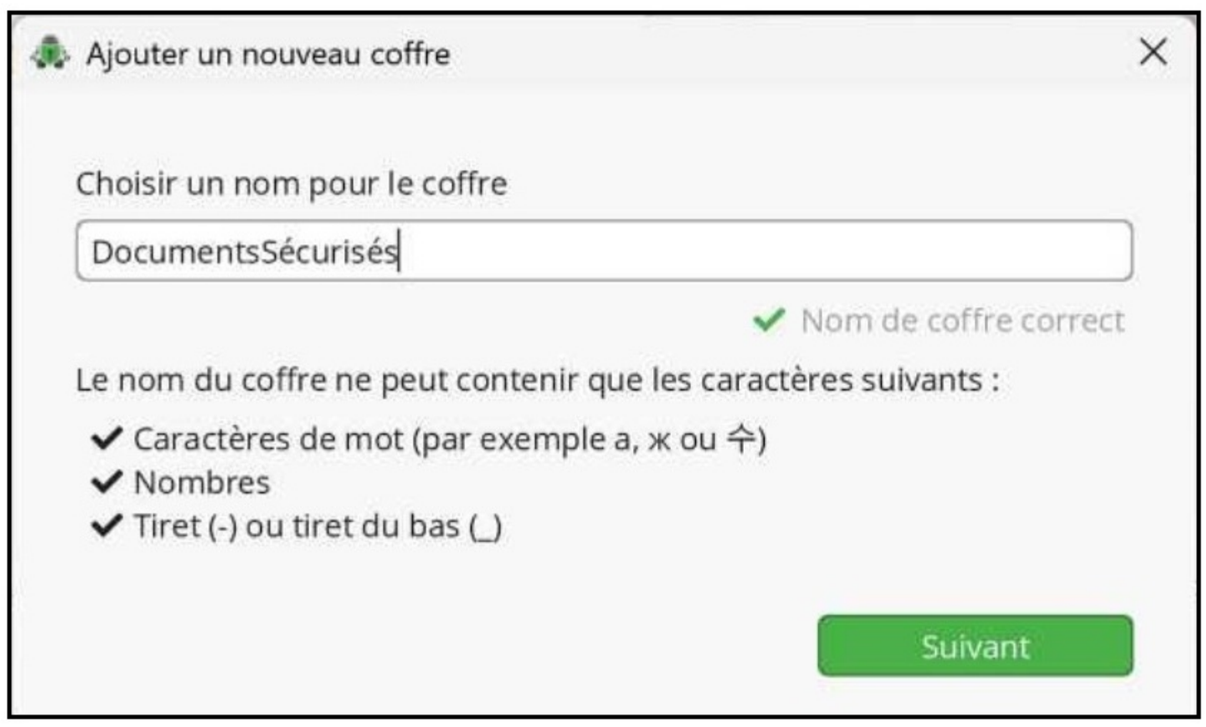
Téléchargez la dernière version de Cryptomator pour Windows depuis le site officiel. Lancez l'installateur et suivez les instructions. Une fois installé, ouvrez Cryptomator.



02

Création d'un nouveau coffre

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





CRYPTOMATOR
cryptomator.org

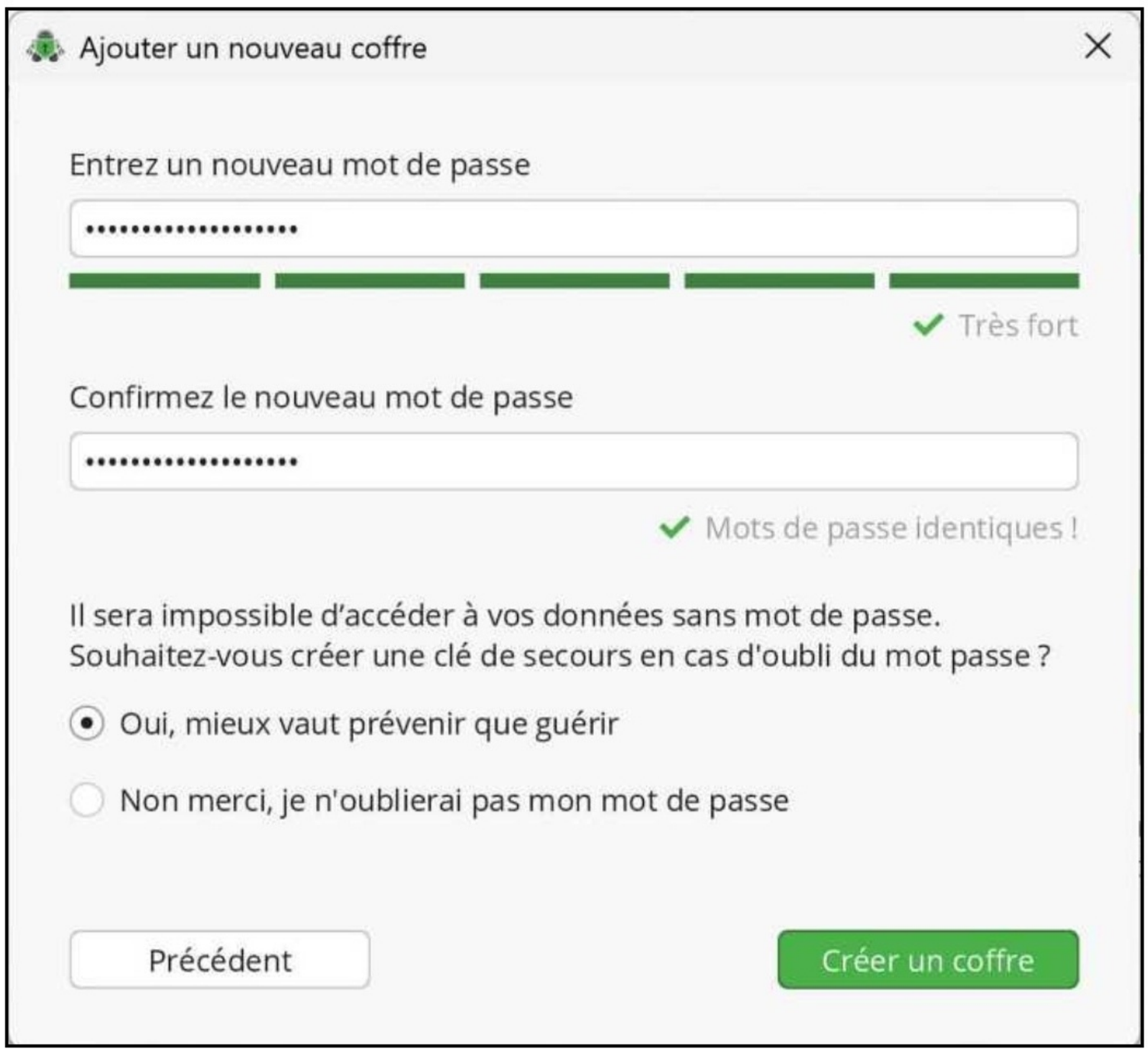
10 min

Facile

AVEC CRYPTOMATOR

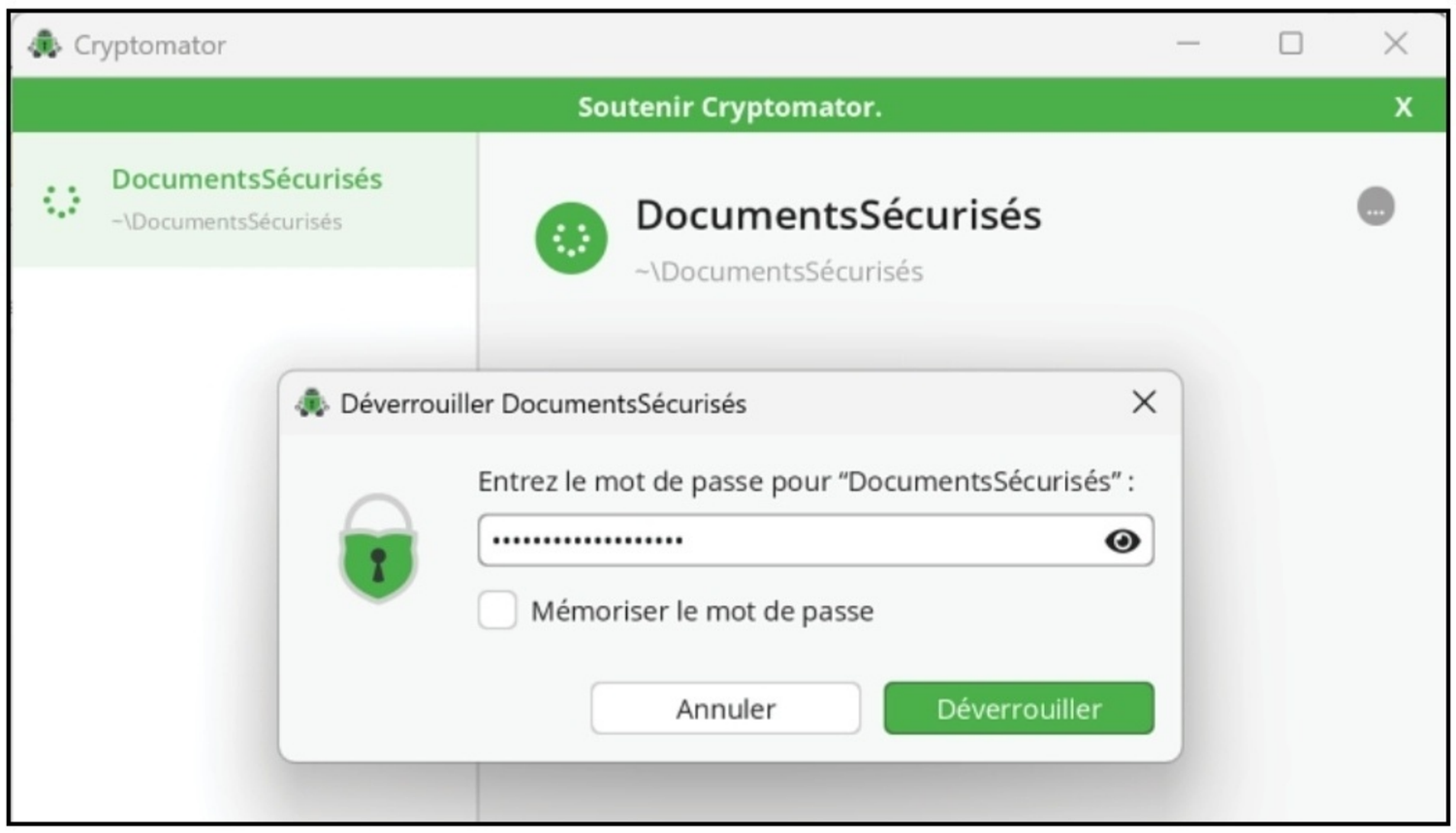
03 Votre mot de passe

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



04 Utilisation du coffre

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



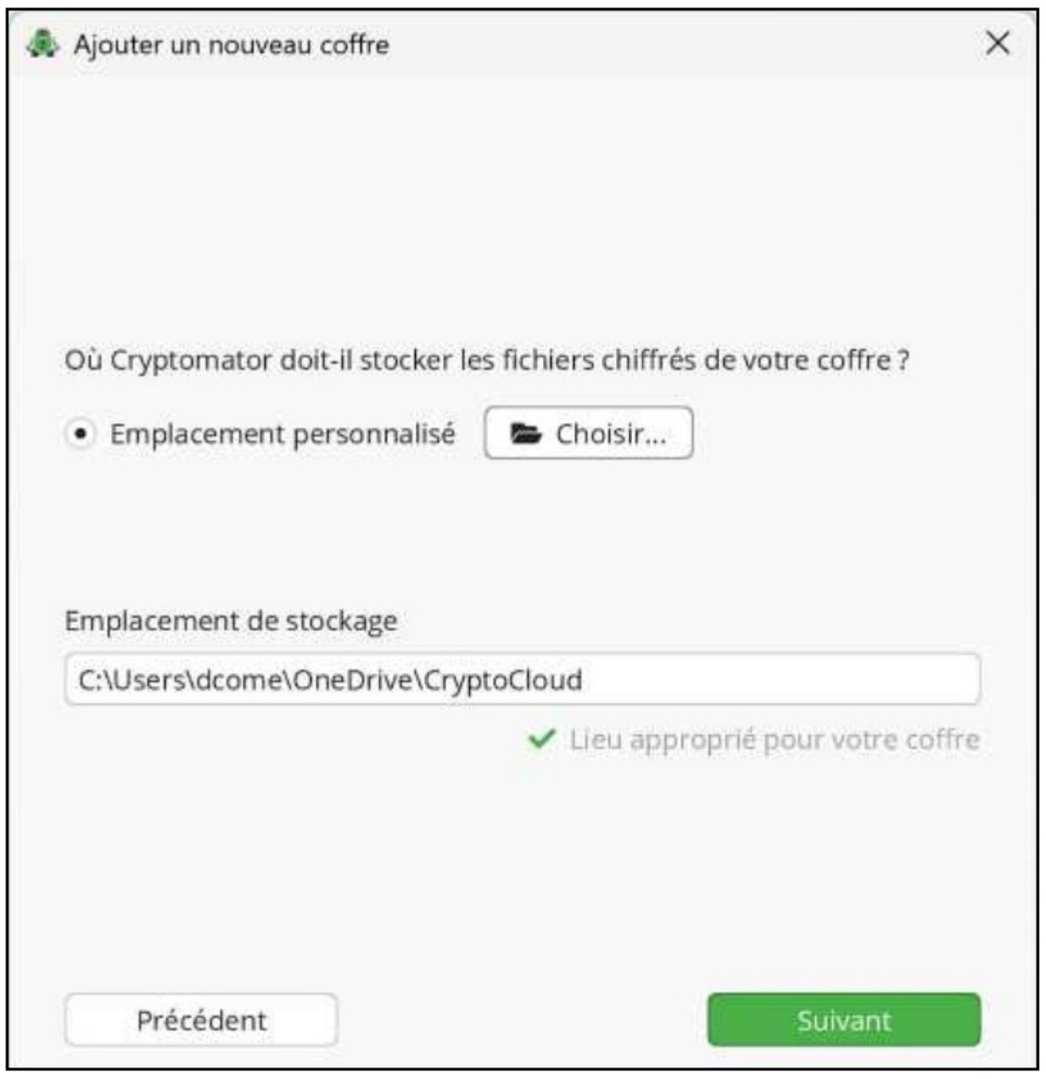
PC & Fichiers

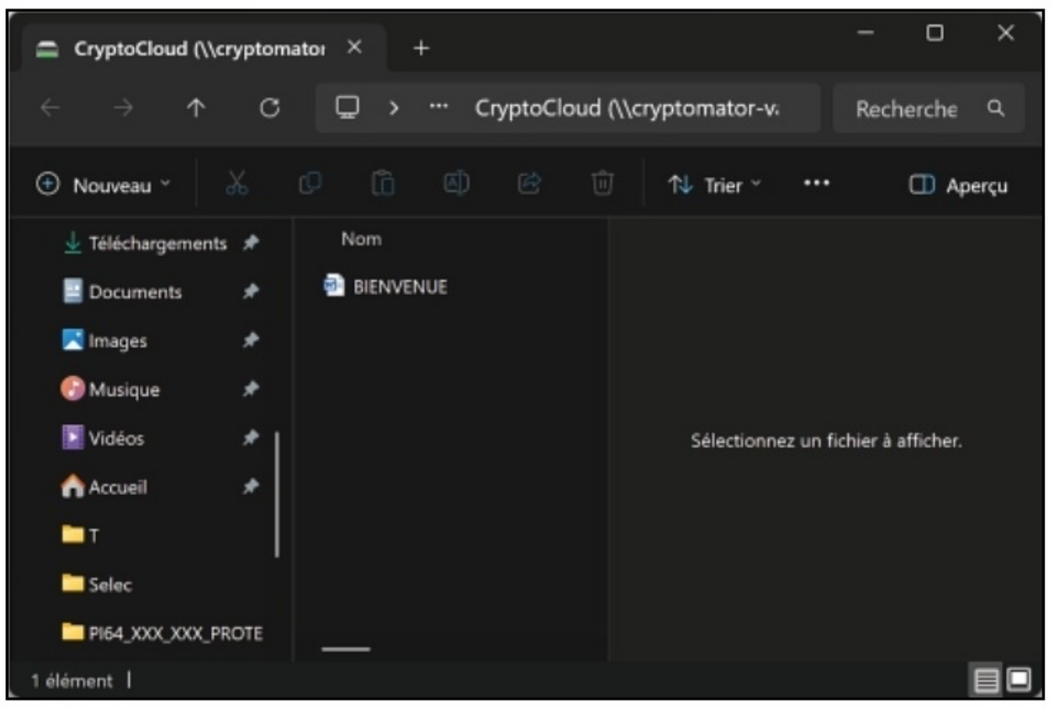
Nous avons choisi OneDrive, mais le tuto suivant fonctionnera aussi avec les autres grands services de cloud. Vous créerez un nouveau coffre-fort chiffré, mais, cette fois-ci, stocké dans votre dossier OneDrive local. Vos fichiers protégés seront ainsi synchronisés automatiquement avec votre cloud.

UTILISEZ CRYPTOMATOR SUR PC AVEC ONEDRIVE

01 Création d'un nouveau coffre-fort

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





02 Lecteur virtuel

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

Accès depuis un autre appareil

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

CONSEILS

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

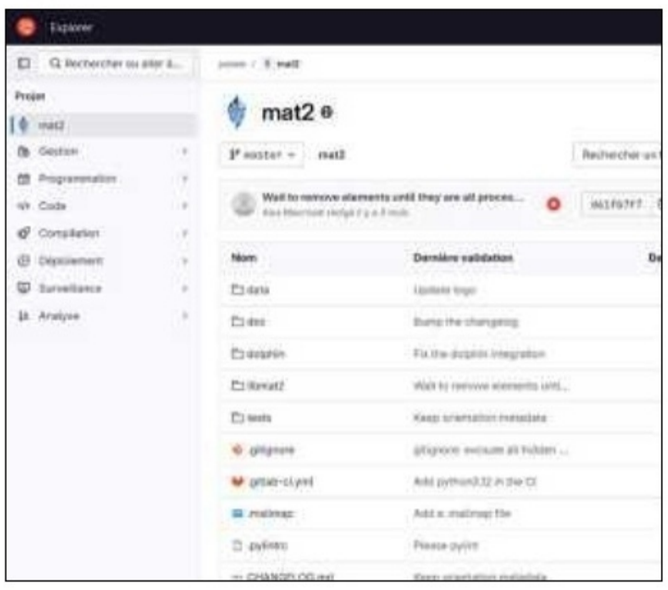
PC & Fichiers

TOP 3 OUTILS POUR SUPPRIMER LES TRACES DE VOS FICHIERS MULTIMÉDIA

Dans cet article, nous vous présentons trois outils – tous gratuits – pour limiter ou effacer les traces contenues dans vos photos et vos vidéos.

MAT2 (Metadata Anonymisation Toolkit) : L'ANONYMISEUR « TOUT EN UN »

MAT2 est une boîte à outils libre spécialement conçue pour anonymiser divers formats (images, PDF, audio, vidéo…). Très simple d'utilisation sur Linux (une interface graphique est disponible) et

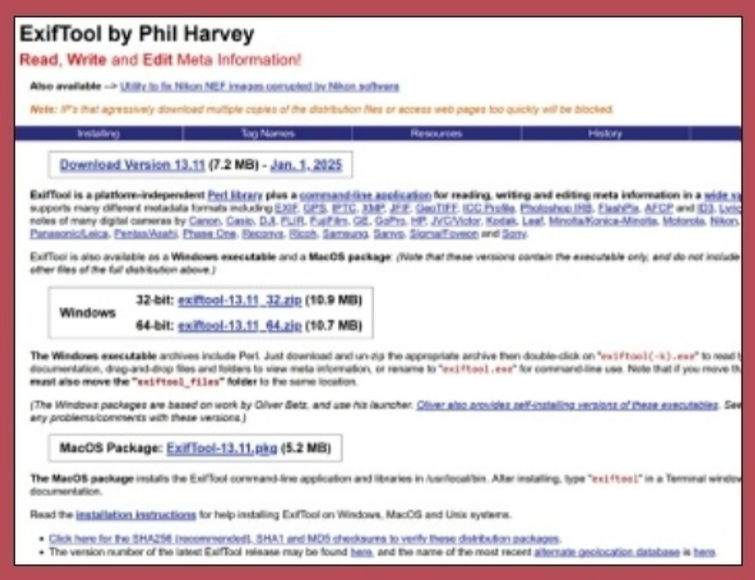


fonctionnel aussi sur d'autres systèmes via des conteneurs ou émulation. Installez MAT2 (directement depuis les dépôts officiels de plusieurs distributions Linux ou via Flatpak). Glissez-déposez vos fichiers dans l'interface pour lancer l'anonymisation. MAT2 crée des copies nettoyées, en supprimant les informations sensibles (balises EXIF, métadonnées PDF, etc.).

Lien : https://0xacab.org/jvoisin/mat2

ExifTool : NETTOYER LES MÉTADONNÉES DE VOS PHOTOS

Cet utilitaire en ligne de commande permet de lire, d'éditer et de supprimer les métadonnées (EXIF) contenues dans les images (format JPEG, PNG…), mais aussi dans d'autres types de fichiers. Gère un grand nombre de formats et offre des commandes très précises, idéales pour automatiser le nettoyage de gros volumes de photos. Sous Windows, après avoir télécharger l'utilitaire, il faudra passer par l'invite de commandes et exécuter : **exiftool -all= Chemin/vers/fichier.jpg**



Cette commande efface toutes les métadonnées EXIF.

Lien : exiftool.org

Shutter Encoder : RÉENCODER ET PURGER LES MÉTADONNÉES DE VOS VIDÉOS



Ce logiciel gratuit et en français permet de convertir de nombreux formats vidéo et audio. Durant la conversion, Shutter Encoder supprime la plupart des métadonnées, réduisant ainsi votre empreinte numérique tout en optimisant la taille du fichier. Dans les options avancées du logiciel, activez l'option pour effacer ou limiter les métadonnées et lancez l'encodage.

Lien : www.shutterencoder.com/fr/

PC & Fichiers

EFFACEZ VOS TRACES AVEC GLARY

Glary Tracks Eraser efface la multitude de traces laissées par l'utilisation quotidienne de votre ordinateur. Des petits bits de mémoire enregistrés à droite et à gauche dont vous n'avez pas conscience, mais qui, collectés et mis bout à bout, en disent beaucoup sur vous, votre profil et vos habitudes.

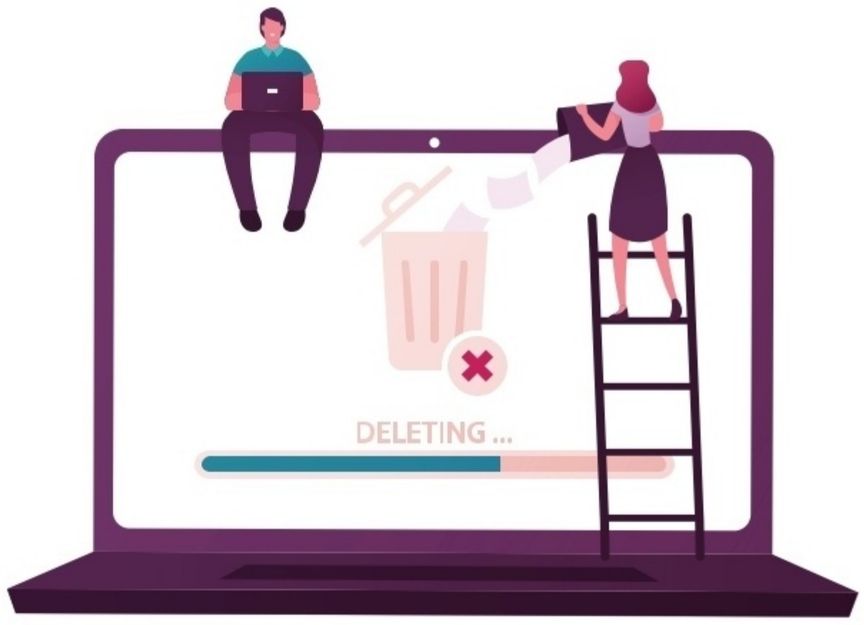
GLARY TRACKS ERASER
www.glarysoft.com

10 min

Facile

Glary Tracks Eraser a pour but principal de protéger la confidentialité des utilisateurs en supprimant les traces d'activités laissées sur l'ordinateur. L'éditeur, Glarysoft, n'est plus à présenter. Il propose depuis des années des solutions aussi populaires qu'efficaces en termes de sécurité informatique et de protection de la vie privée. Pour les particuliers, ses logiciels gratuits offrent souvent des fonctions que l'on retrouve habituellement dans des utilitaires payants.

Glary Tracks Eraser va fouiller les entrailles de votre PC pour trouver et effacer à la demande des données qui peuvent compromettre votre identité et votre vie privée. Il s'agit par exemple de :
- L'historique de navigation sur le web ;
- Les fichiers temporaires ;
- Les cookies ;



- Les fichiers journaux (logs) ;
- Les entrées de registre inutiles ;
- Les fichiers récemment ouverts.

En effaçant ces données, Glary Tracks Eraser vise à protéger les informations personnelles des utilisateurs contre les regards indiscrets et les menaces potentielles telles que le vol d'identité et les atteintes à la vie privée. Il peut être utilisé à la fois à des fins préventives, pour maintenir la confidentialité au quotidien, et de manière réactive, après une session de travail ou de navigation pour effacer les traces d'activités.

MAIS C'EST QUOI EXACTEMENT LES FICHIERS TEMPORAIRES ?

Vous en entendez souvent parler sans savoir forcément de quoi il en retourne. Les fichiers temporaires, ou fichiers «temp», sont des fichiers créés par des programmes pour stocker temporairement des informations. Ils servent à optimiser le fonctionnement des logiciels et des systèmes d'exploitation en fournissant un espace de travail temporaire. Une fois leur utilité terminée, ils sont censés être supprimés automatiquement. Toutefois, il arrive souvent qu'ils restent sur le disque dur, occupant ainsi un espace précieux.

FONCTION DES FICHIERS TEMPORAIRES

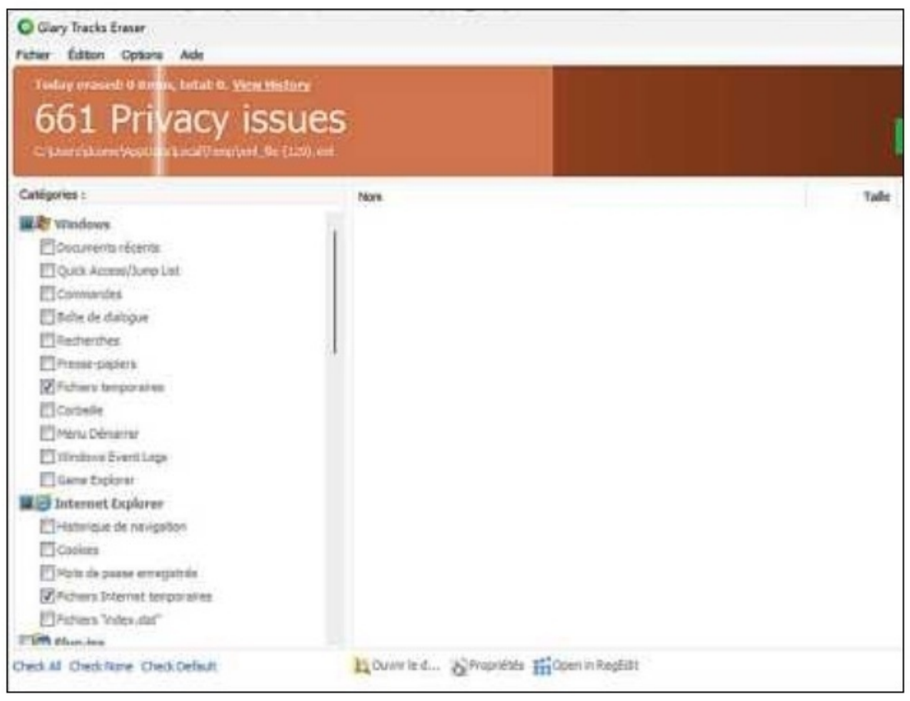
- Amélioration des performances : Les fichiers temporaires permettent aux programmes de fonctionner plus efficacement. Par exemple, lors de l'installation d'un logiciel, des fichiers temporaires sont créés pour stocker des données intermédiaires nécessaires à l'installation.

- Sauvegarde temporaire : Lorsqu'un document est ouvert et en cours de modification, les logiciels créent des fichiers temporaires pour sauvegarder automatiquement les changements. Cela permet de prévenir la perte de données en cas de fermeture inopinée du programme ou de panne du système.

- Gestion des caches : Les navigateurs web créent des fichiers temporaires pour stocker des éléments de pages web visitées. Cela permet de charger les pages plus rapidement lors de visites ultérieures en récupérant les éléments depuis le cache plutôt que de les télécharger à nouveau.

Lorsque les fichiers temporaires ne sont pas supprimés automatiquement, ils peuvent s'accumuler et occuper une quantité importante d'espace disque, ralentissant ainsi le système. Mais ils posent aussi un gros souci de confidentialité, car ils contiennent un grand nombre d'infos sur vos activités actuelles ou passées.

SCAN ET NETTOYAGE AVEC GLARY TRACKS ERASER



01 Scan au démarrage

Lancez Glary Tracks Eraser. Le premier scan s'attaque par défaut aux fichiers temporaires que l'on peut supprimer sans risque pour le système ou nos données. Le logiciel vous demandera de fermer les applications qu'il scanne (navigateur, client de messagerie, etc.) afin d'aller au bout de son process.



02 Autres scans préconfigurés

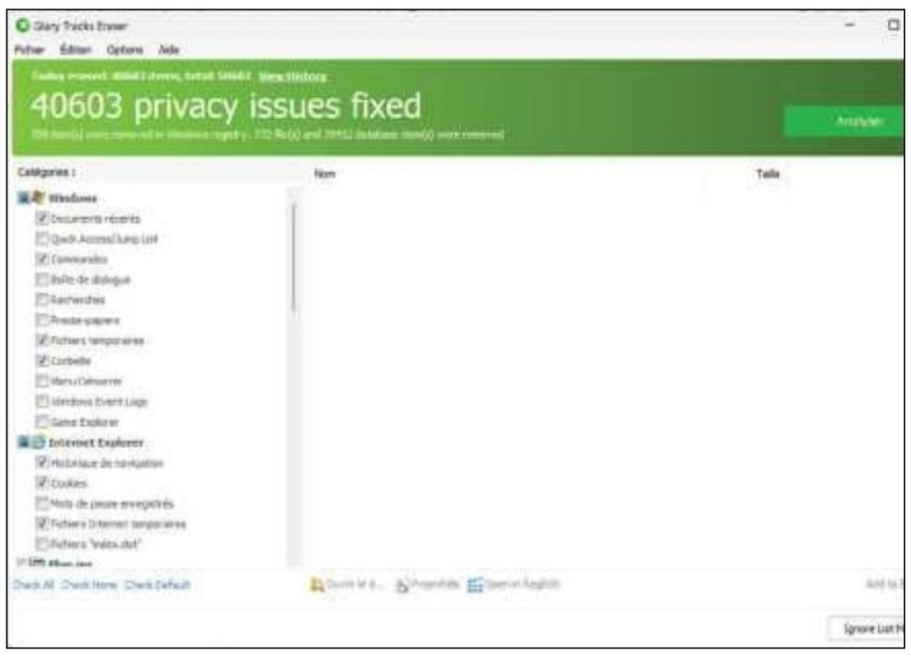
Si vous souhaitez vous attaquer à l'ensemble des traces laissées sur votre PC, vous pouvez cliquer sur **Check All** en bas à gauche de la fenêtre. Attention, vous risquez de supprimer des éléments de registre ou des cookies par exemple qui vous simplifiaient la vie jusqu'à présent. **Check None** vous permet de tout décocher. **Check Default** revient à la configuration de scan initiale.

Glary propose plusieurs niveaux de scan pour fouiller plus ou moins en profondeur votre ordi.



03 Ou scan manuel

Vous pouvez bien sûr effectuer votre choix manuellement en cochant et décochant les entrées qui vous semblent pertinentes. En cliquant dans la colonne de gauche sur l'un des Items, vous afficherez à droite plus d'infos sur ce qui sera supprimé par Glary Tracks Eraser. Cliquez sur **Relancer l'analyse** en haut à droite pour scanner précisément votre choix final.



04 Nettoyage

Une fois ce scan effectué,vous pouvez cliquer sur **Nettoyer**. Glary Tracks Eraser vous liste en haut le résultat final de son action. Le lien **View History** vous permettra de revoir ce qui a été supprimé lors de vos précédents nettoyages.

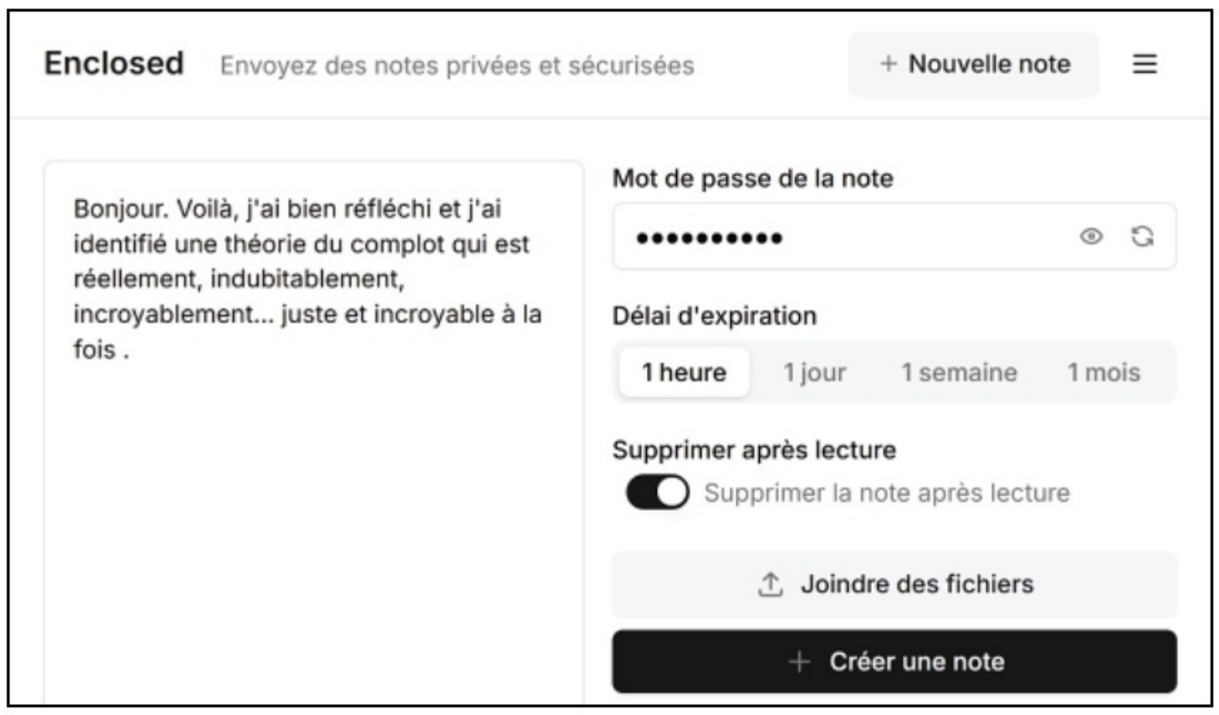
PC & Fichiers

ENVOYEZ UNE NOTE CHIFFRÉE AVEC ENCLOSED

Enclosed chiffre de bout en bout vos notes et documents associés afin de les partager en deux clics. C'est simple, efficace et même l'esthétique est soignée !

01 Créer la note

Écrivez simplement votre texte, joignez des fichiers si nécessaire, définissez un mot de passe et un délai avant autodestruction. Vous pouvez même demander la suppression juste après lecture. Cliquez ensuite sur **Créer une note**.



02 Envoyer et déchiffrer

Enclosed génère un lien que vous pourrez conserver le délai imparti ou envoyer à un contact. Ce dernier aura besoin d'un mot de passe pour déchiffrer votre envoi et accéder à la note.



ENCLOSED
enclosed.cc

2 min

Facile

CHIFFREZ UN FICHIER EN LIGNE AVEC FILELOCK

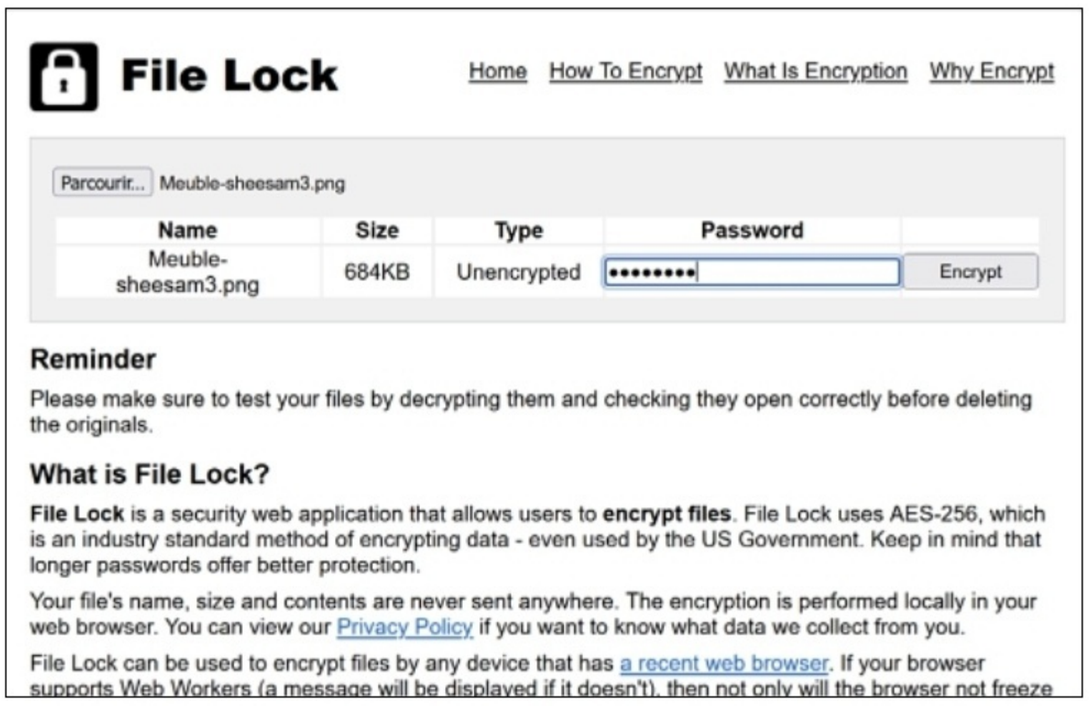
Besoin de chiffrer et d'envoyer rapidement un fichier sécurisé sans passer par un logiciel complexe ? Utilisez Filelock, un service 100% en ligne qui fait le job en deux étapes.



FILELOCK
filelock.org

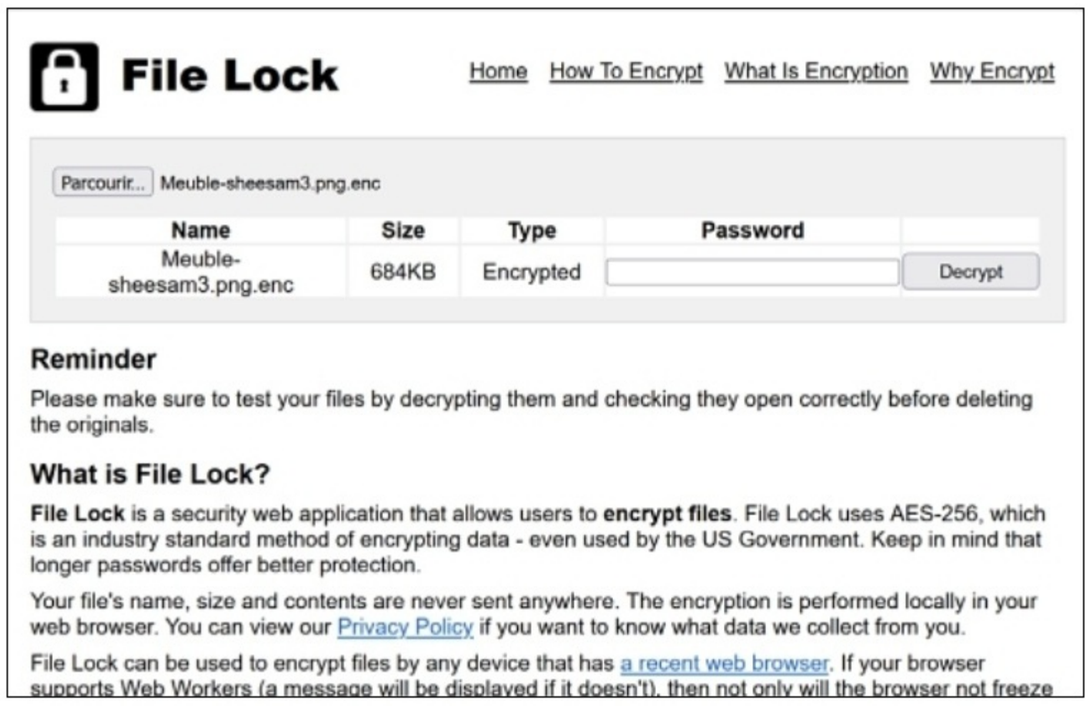
2 min

Facile



01 Chiffrer

Cliquez sur **Parcourir** et sélectionnez sur votre PC le fichier à protéger. Saisissez un mot de passe (à ne pas oublier!) et cliquez simplement sur **Encrypt**. Votre fichier chiffré sera enregistré avec une extension **.enc**.



02 Déchiffrer

Pour ouvrir votre fichier, vous - ou votre contact - repasserez par le site de Filelock et chargerez à nouveau le fichier .enc via **Parcourir**. Sauf que, cette fois-ci, le site le reconnait comme chiffré et vous propose de le déchiffrer en cliquant sur **Decrypt**... Et vous devez bien sûr posséder le bon mot de passe.

PC & Fichiers

EMPREINTE DIGITALE : VENDRE SON ÂME À GOOGLE ?

Comment fonctionne le déverrouillage par empreinte digitale sur nos appareils Android ? Est-ce une solution sécurisée ? Qui peut y avoir accès ou la récupérer à notre insu ?

Si votre téléphone est équipé d'un lecteur d'empreinte digitale, sur l'écran ou à l'arrière de votre smartphone, vous pouvez l'utiliser pour déverrouiller votre appareil, certaines applications ou autoriser des paiements en ligne. Ce système de déverrouillage est plus rapide et pratique que le renseignement d'un code. Attention cependant, contrairement à l'intuition, la protection par empreinte digitale est considérée, à raison, comme moins sécurisée que le verrouillage par code. Des techniques simples existent pour copier votre empreinte digitale ! Comme dans un mauvais film, il suffit de vous tendre un verre et de le récupérer pour avoir une chance de la reproduire.

Pratique et intégré

Tous les smartphones Android disposant de cette fonction s'appuient sur des matériels et capteurs différents, choisis par chaque fabricant. Mais la plupart utilisent ensuite le système logiciel intégré par Android (et donc par Google) pour gérer la reconnaissance et les autorisations. Sur Android 15, vous pouvez ajouter jusqu'à cinq empreintes par appareil, utile pour enregistrer plusieurs doigts, mais aussi pour autoriser l'accès à plusieurs personnes d'une même famille par exemple.

UN MOT DE PASSE VOLÉ, CELA SE CHANGE. UNE EMPREINTE, ELLE, VOUS IDENTIFIERA TOUTE VOTRE VIE.

Envoyée à Google ?

Google affirme que les données liées à nos empreintes digitales sont stockées de façon sécurisée sur notre appareil et jamais partagées avec Google. Ni même avec le fabricant de notre smartphone ou avec d'autres applis installées sur notre téléphone. Lorsque Google ou un autre service veut vérifier la validité d'une empreinte, ces derniers reçoivent simplement une notification de votre appareil indiquant si l'empreinte digitale est validée ou non. Il n'y a pas d'envoi et de vérification des données biométriques dans le cloud, tout reste dans le téléphone sauf le message « Valide / Non valide ».
Mais si un fabricant de smartphones utilisant la technologie Google enfreignait ces règles de base et parvenait à enregistrer vos empreintes et à se les envoyer ? Google indique que son service doit être exécuté dans un environnement d'exécution sécurisé appelé « Trusted Exécution Environnement » et que tous les matériels concernés doivent être protégés par une règle SELinux qui rend théoriquement impossible une exfiltration des données.



En restant sur le système intégré par Android, vos empreintes restent en local, chiffrées dans un espace non connecté de la mémoire de votre appareil. Elles sont censées y être inaccessibles. Mais attentions aux applications ou aux fabricants qui utilisent leur propre système de sauvegarde et de validation.

TROIS TYPES DE CAPTEURS

Il existe aujourd'hui trois principaux types de capteurs utilisés sur nos smartphones et tablettes :

- Capteurs optiques : Les capteurs optiques utilisent une lumière pour capturer une image visuelle de l'empreinte digitale. Lorsqu'un doigt est placé sur le capteur, une caméra ou un capteur d'image enregistre l'empreinte en utilisant la réflexion de la lumière. Bien que cette technologie soit éprouvée et couramment utilisée, elle est la plus vulnérable à certaines méthodes de contournement, comme l'utilisation de fausses empreintes.

- Capteurs capacitifs : Les capteurs capacitifs mesurent les différences de capacité électrique causées par les crêtes et les vallées de l'empreinte digitale. En détectant ces variations, ils créent une image détaillée de l'empreinte. Cette méthode offre une précision élevée et est moins susceptible d'être trompée par de fausses empreintes, car elle nécessite un contact avec la peau conductrice (mais certains matériaux posés sur le doigt d'un escroc peuvent le permettre).

- Capteurs ultrasoniques : Les capteurs ultrasoniques émettent des ondes sonores à haute fréquence pour pénétrer la couche externe de la peau et capturer une image tridimensionnelle de l'empreinte digitale. Cette technologie permet une lecture précise même en présence de contaminants tels que la saleté ou l'huile, et offre une sécurité accrue en raison de la profondeur des informations capturées.



PC & Fichiers

COMMENT FONT LES PIRATES POUR REPRODUIRE UNE EMPREINTE DIGITALE ?

Comme vous l'avez deviné, le plus simple est de récupérer un objet sur lequel vous avez apposé vos doigts. Ou de prendre une photo haute définition de votre main, cela peut suffire.
Un logiciel de retouche photo est nécessaire pour nettoyer l'image et optimiser les détails de la zone ciblée. Il faut ensuite imprimer l'empreinte, le plus courant étant de le faire sur une feuille d'acétate (quelques dizaines de centimes). Le pirate déposera enfin un peu de colle à bois sur l'impression, puis retirera cette pellicule de colle une fois séchée. On se retrouve alors avec une fausse peau, prête à l'emploi, avec les empreintes. Cette technique fonctionne avec les capteurs capacitifs (lire page précédente), mais se heurte à la finesse d'analyse des nouveaux capteurs à ultra-sons.

Ces derniers sont beaucoup plus fiables puisque l'empreinte est analysée en 3D. En plus, le système peut être capable de détecter les flux de sang qui circulent au même moment dans les veines. Mais les capteurs bas et moyens de gamme, même à ultra-sons, fonctionnent sur des probabilités « faibles ». Pour faire vite et ne pas frustrer l'utilisateur, les capteurs doivent donner une réponse rapide et dans des conditions variées. Du coup, il validera une empreinte s'il la juge « suffisamment ressemblante pour être, statistiquement, celle de l'utilisateur ». Voilà qui ne nous rassure pas. Des moulages en silicone 3D et même l'usage d'encres conductrices sont déjà sur le marché pour tenter d'abuser de cette faiblesse.

Stockée en local et chiffrée

La mémoire de l'appareil où est stocké ce type de données doit être inaccessible à un tiers, à Google comme au fabricant de smartphones. Ces informations sont notamment chiffrées (le système de clés est couplé à votre empreinte) et ne doivent pas pouvoir être extraites, même après le root de l'appareil. Enfin, elles doivent aussi pouvoir être supprimées définitivement à la demande de l'utilisateur, sans possibilité de restauration. Mais attention, si vous passez par d'autres applications vous demandant de faire une capture de vos empreintes, vous devez vous assurer d'utiliser les outils intégrés d'Android et jamais un autre capteur du téléphone (photo, lumière). De la même manière, vérifiez toujours que le fabricant de votre smartphone ou tablette ne passe pas par une solution propriétaire de son cru qui serait beaucoup moins exigeante en termes de sécurité et de protection des données. Car un mot de passe corrompu, cela se change. Une empreinte volée, non, elle restera un sésame vous identifiant toute votre vie.

FORCE BRUTE : UNE MÉTHODE DE PROS



Les chercheurs de Tencent Labs et de l'université de Zhejiang ont révélé une vulnérabilité critique dans l'authentification par empreinte digitale des smartphones Android, nommée «BrutePrint». En résumé, l'idée est de soumettre des centaines voire des milliers d'empreintes au capteur jusqu'à ce que l'une d'entre-elles « matche » avec celle du propriétaire. Si tous les humains possèdent des empreintes digitales uniques, les capteurs, eux, ne fonctionnent que sous forme de probabilités peu strictes. Il suffit de trouver une empreinte qui « ressemble suffisamment » à celle d'un utilisateur pour tromper la machine.

Bases d'empreintes en libre accès

Mais, normalement, une attaque en force brute (répéter une tentative d'identification des centaines de fois jusqu'à trouver la bonne) bloque nos appareils. C'est là que BluePrint exploite une faille Android pour contourner cette mesure de sécurité et la neutraliser. Cependant, les pirates ou un service d'enquête doivent avoir le smartphone cible entre leurs mains et un équipement minimal pour lancer cette attaque. Quant aux bases de milliers d'empreintes digitales permettant de tenter ce type piratage, il est facile de les acheter… plus ou moins légalement.

CRÉER, AJOUTER OU SUPPRIMER DES EMPREINTES



01 Déverrouillage

Sur votre smartphone, allez dans **Paramètres > Sécurité et confidentialité > Déverrouillage de l'appareil**. Appuyez ensuite sur **Déverrouillage par empreinte digitale et reconnaissance faciale**. Saisissez le code de déverrouillage de votre téléphone pour accéder à cet espace sécurisé. Allez dans **Déverrouillage par empreinte digitale**.

02 Ajout ou suppression



Dans cet espace, vous accédez aux empreintes éventuellement enregistrées ou vous pouvez en créer une nouvelle en appuyant sur **+ Ajouter une empreinte**. Vous avez la possibilité de créer jusqu'à cinq empreintes différentes, qui seront toutes reconnues par votre appareil. Pour en supprimer une, il vous suffit de sélectionner la corbeille en face de celle que vous ciblez.

Changer de doigts, autoriser une autre personne à accéder à votre appareil ou simplement supprimer les autorisations déjà enregistrées : tout savoir en pratique.



03 Lecture et enregistrement

Avec **Ajouter une empreinte**, le processus d'enregistrement de votre empreinte commence. Vous devrez tapoter plusieurs fois le capteur puis varier les angles d'apposition (droite, gauche) en suivant les demandes de votre smartphone. Une fois ce processus achevé avec succès, votre empreinte est sauvegardée dans la liste des empreintes reconnues.

04 Renommer

Vous pouvez renommer chaque empreinte (pratique pour les membres d'une même famille utilisant l'appareil) en appuyant simplement sur le nom par défaut de l'empreinte enregistrée (**Doigt1**, **Doigt2**, ...) puis en modifiant son intitulé. Validez par **OK**.



CHEZ VOTRE
MARCHAND DE JOURNAUX

LES PIRATES CRYPTENT, NOS LECTEURS DÉCRYPTENT !

WI-FI,
ANONYME,
MOBILES,
HACKING,
ENCODAGE,
ANTIVOL,
CRYPTAGE,
MOTS
DE PASSE,
SURVEILLANCE



LA BIBLE DU PIRATE
5,90 €
SEULEMENT !

SORTIE EN KIOSQUES DU PROCHAIN UMÉRO :

28 MARS 2026



PC TRUCS & ASTUCES N°60

N°60 Janv. / Mars 2026

PC TRUCS & ASTUCES
est une publication
du groupe ID PRESSE.

1104, Chemin de la Batterie
13500 Martigues
E-mail : redaction@idpresse.com

Directeur de publication et rédacteur en chef :
David Côme

Directeur artistique :
Sergei Afanasiuk

Imprimé en France par :
Printed in France by :
Imprimerie Mordacq

Rue de Constantinople,
ZI du Petit-Neufpré

62120 Aire-sur-la-lys

Distribution : MLP

Dépôt légal : à parution

Commission paritaire :
0921 K 94314

ISSN : 2114 - 0898

«PC Trucs & Astuces» est édité
par SARL ID Presse,
RCS : Aix-en-Provence 491 497 665

Parution : Trimestriel
4 numéros par an

La reproduction, même partielle, des articles et illustrations parues dans «PC Trucs & Astuces» est interdite. Copyrights et tous droits réservés ID Presse. La rédaction n'est pas responsable des textes et photos communiqués. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire.

+ BONUS

SE PROTÉGER DE L'USURPATION D'IDENTITÉ

Le GUIDE 2026

Virez-moi BIG BROTHER !

Gardez le contrôle sur votre vie privée

IDPRESSE

L 15852 - 60 - F: 5,90 € - RD

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