N°66

Casser les codes et décrypter l'info

PIRATE INFORMATIQUE

Déc. 2025 / Fév. 2026

IA
PRENDRE LE CONTRÔLE SUR CHATGPT

PREMIUM SANS PAYER
HACKEZ YOUTUBE !

NE SOYEZ PLUS UNE VICTIME
PASSEZ EN MODE HACKER !
100% GRATUIT

PERFORMANCES
TOP 10 ASTUCES POUR DÉBRIDER SON PC

BLACK DOSSIER
LE GUIDE *(non)* OFFICIEL DES MEILLEURES ASTUCES POUR WHATSAPP

ANONYMAT
CHANGER D'IDENTITÉ SUR LE WEB

SOMMAIRE

BLACK DOSSIER 11–21

LE GUIDE *(non)* OFFICIEL DES MEILLEURES ASTUCES POUR WHATSAPP

HACKING

ANONYMAT

SOUTENEZ-NOUS !

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

PROTECTION

MULTIMÉDIA

PIRATE INFORMATIQUE
N°66

Déc. 2025 – Fév. 2026

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

Directeur de la publication :
David Côme

Directeur artistique :
Sergei Afanasiuk

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

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

Distribution : MLP
Dépôt légal : à parution
Commission paritaire : en cours
ISSN : 1969 - 8631

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

Parution : 4 numéros par an.

ÉDITO

TROIS ANS, UNE ÉTERNITÉ DÉJÀ

Trois ans. Seulement. Déjà. Depuis novembre 2022, l'arrivée de ChatGPT a compressé le temps : ce que nous pensions voir en une ou plusieurs décennies s'est imposé en un seul trimestre. Les experts ont feint la surprise, les sceptiques ont feint le calme, et pendant ce temps, l'IA a infiltré nos métiers, nos outils, nos habitudes — parfois nos angoisses — avec une discrétion d'autant plus déconcertante qu'elle s'est instillée partout.

Le plus troublant, finalement, n'est pas que les machines écrivent, codent ou prédisent. C'est qu'en trois ans, elles ont déplacé notre centre de gravité intellectuel. Apprendre à coexister avec un futur qui arrive trop tôt. Et avec un présent qui accélère parfois au-delà des capacités de compréhension et de réaction humaines. Nous avons créé une danseuse virtuose. Et quittons peut-être déjà le plateau, incapables de la suivre. Pour quel rôle ? Metteur en scène, machiniste, simple spectateur ?

Bonne lecture !

La rédaction

BOITIERS IPTV ILLÉGAUX

LA MENACE PIRATE
au cœur de votre salon ?

Une box "IPTV full chaînes pour 60 € à vie", ça ressemble au bon plan parfait. En réalité, ces boîtiers illégaux s'apparentent parfois à des chevaux de Troie posés au milieu du salon : vecteurs de malwares, portes d'entrée pour les pirates, et bombe à retardement juridique.

Les études commencent à chiffrer le phénomène : des analyses menées sur des offres IPTV pirates montrent qu'une part importante des utilisateurs (jusqu'à 30 % dans certains pays) ont été victimes d'attaques ou de fraudes après utilisation de ces services.

Derrière les flux "gratuits" se cachent souvent des applications modifiées, des dépôts pirates et des firmwares bricolés qui embarquent adwares, trojans, voire infostealers capables d'aspirer mots de passe et cookies de session.

AMAZON BLOQUE LES APPS ILLÉGALES SUR FIRE TV STICK

Amazon opère une mise à jour majeure sur son Fire TV Stick : les applications "sideloadées" promouvant le streaming illégal (notamment sportif) se voient désormais bloquées au niveau du firmware. Un coup dur porté au marché parallèle… et aux utilisateurs malins.

« *Cela s'inscrit dans le cadre de nos efforts continus pour soutenir les créateurs et protéger nos clients, car le piratage peut également exposer les utilisateurs à des logiciels malveillants, des virus et des fraudes* », explique Amazon. Car, bien sûr, les applications pirates gratuites ou au tarif ultra-agressif peuvent embarquer des malwares, des rançongiciels ou des collecteurs d'identifiants..

Du côté d'Amazon, la mesure s'appuie sur deux leviers majeurs : d'une part, le lancement du nouvel appareil Fire TV Stick 4K Select avec système d'exploitation fermé Vega OS qui empêche toute installation hors boutique officielle ; d'autre part, une mise à jour logicielle rétroactive sur les modèles existants en France et Allemagne.

LES APPLIS NON OFFICIELLES SONT BANNIES DU FIRE TV STICK 4K TANDIS QUE LES ANCIENS MODÈLES SERONT EUX AUSSI BRIDÉS PAR MISE À JOUR.

NIDS À MALWARES

Surfshark, une société de cybersécurité et fournisseur de VPN de premier plan, a publié un avis de sécurité sur les appareils IPTV illicites : "*Une fois que vous connectez une boîte IPTV non fiable à votre réseau domestique, vous devriez supposer que tout ce que vous tapez pourrait être récolté - et que l'appareil peut essayer d'observer d'autres trafics sur votre réseau*", a déclaré Miguel Fornes, expert en cybersécurité chez l'éditeur de VPN. Selon M. Fornes,

> Un service pirate, bidouillé par des pirates et à usage de M. Tout le monde. Qu'est-ce qui pourrait mal tourner ?

pour exécuter des applications piratées ou «fissurées», de nombreuses boîtes douteuses désactivent les protections Android de base telles que les vérifications vérifiées du démarrage et les vérifications d'intégrité des applications, ce qui les rend beaucoup plus faciles à compromettre. Tout ce que vous entrez sur l'appareil – connexions de streaming, comptes Google, historique de recherche, saisie vocale, même les bibliothèques de photos si elles sont liées – peut être récolté par des tiers inconnus. Sans parler des identifiants de messageries siphonnés ou comptes bancaires compromis.

Une fois connectés à votre Wi-Fi ou Ethernet domestique, ces appareils peuvent découvrir d'autres appareils sur le réseau et peuvent intercepter le trafic non chiffré, cartographier votre réseau et affaiblir votre sécurité globale. Leur micrologiciel est souvent obsolète, altéré ou non signé, et ils reçoivent rarement des mises à jour de sécurité dignes de confiance, laissant les vulnérabilités connues non corrigées.

HACKING « AGENTIQUE »

L'IA PEUT EXÉCUTER DES ATTAQUES SANS INTERVENTION HUMAINE

Fin septembre 2025, une attaque de grande ampleur a été stoppée in extremis par Anthropic : pour la première fois, des hackers ont utilisé un système d'IA pour conduire presque entièrement une intrusion — « *80 % à 90 % sans intervention humaine* », selon l'entreprise. Ce tournant marque un nouveau chapitre du cyber-conflit : l'IA n'est plus utilisée seulement pour conseiller et préparer une attaque : elle pilote elle-même le hacking.

DÉBUT DE L'ÈRE « AGENTIQUE »

Dans un billet publié en novembre 2025, Anthropic explique avoir détecté une opération de longue durée menée contre environ trente organisations — entreprises technologiques, institutions financières, agences gouvernementales. La menace ? Les attaquants ont pris pour cible le modèle Claude Code d'Anthropic et l'ont "jailbreaké" pour exécuter des actions offensives : ouvrir des portes back-door, exfiltrer des données, établir des accès persistants. Le terme "agentique" y apparaît pour décrire un système capable de planifier, décider et agir sur son propre cycle, sans supervision humaine.

« *Nous pensons qu'il s'agit du premier cas documenté d'une cyberattaque menée sans intervention humaine substantielle* », explique Anthropic. « *La vitesse et le degré d'automatisation offerts par l'IA ont quelque chose d'un peu effrayants* ».

Vous l'aurez compris, ce type d'attaques se généralisera ces prochaines années. Parmi les armes défensives, il est clair que des cyber-agents 100% IA devront être eux aussi déployer dans nos systèmes d'informations pour contrer en temps réel ceux des pirates... sans intervention humaine. Car les vitesses d'exécution et d'adaptation seront de plus en plus décorrélées de notre temps humain de réaction et de compréhension.

> « La vitesse et le degré d'automatisation offerts par l'IA ont quelque chose d'un peu effrayants » - Anthropic

TORRENTFREAK A 20 ANS :

Chronique d'un site qui a vu le Web basculer

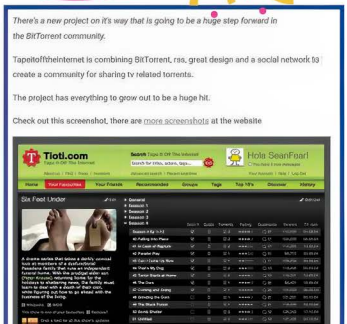
En 2005, la planète numérique découvre à quel point le P2P est devenu incontrôlable. Napster est mort, mais le protocole BitTorrent inonde nos PC à une échelle inédite. Les trackers pullulent, les fichiers ".torrent" circulent comme des pièces de monnaie. C'est dans ce contexte que naît TorrentFreak, fondé par Ernesto van der Sar, passionné d'activisme numérique. L'idée n'est pas de fournir des liens pirates — le site n'en héberge jamais — mais de documenter un phénomène social, technique et juridique.

Lorsque TorrentFreak publie son premier billet en novembre 2005, l'Internet ressemble encore à un Far West numérique. Les modems ADSL chantent au petit matin, BitTorrent est en plein essor, et The Pirate Bay vient d'entrer dans l'histoire. Les majors hurlent au pillage, les tribunaux s'agitent, la dématérialisation de la culture entre dans tous les foyers.

Dans ce chaos juvénile, un jeune Néerlandais, Ernesto van der Sar, commence à tenir ce qui ressemble alors à un carnet de bord : un site modeste, sobre, presque artisanal, qui raconte la réalité du partage numérique avec une chose rare dans ce milieu saturé : de la précision.

UNE RÉVOLUTION À ÉCRIRE

« *Lorsque les torrents ont croisé mon chemin pour la première fois, ils m'ont semblé être une véritable révolution* », explique celui qui n'était alors qu'un jeune étudiant. « *Les technologies de partage de fichiers antérieures avaient déjà montré ce qui était techniquement possible, mais la nature web des torrents a donné naissance à des communautés en ligne partout dans le monde. À cette époque, les « pirates » étaient encore considérés comme des révolutionnaires du numérique, qui libéraient l'information des contraintes physiques telles que les CD et les DVD. L'essor des sites de torrent publics et des trackers privés était fascinant à observer. En 2005, cela a finalement conduit au lancement de TorrentFreak.* »



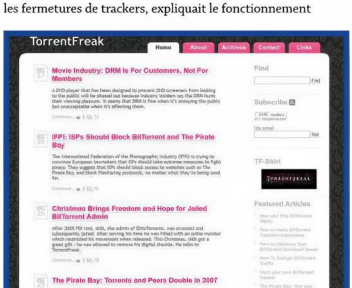
LE 12 NOVEMBRE 2005 NAISSAIT TORRENTFREAK AVEC CE PREMIER POST DÉDIÉ À UN NOUVEAU SERVICE BAPTISÉ TIOTI.COM (TAPE IT OFF THE INTERNET). TIOTI A DEPUIS DISPARU, PAS TORRENTFREAK.

Vingt ans plus tard, TorrentFreak n'a plus rien d'un blog. C'est devenu un témoin de l'histoire souterraine du Web, un média que lisent aussi bien les pirates que les juristes, les ayants droit que les chercheurs. « *TorrentFreak a commencé comme une aventure solitaire, mais après un an, Andy Maxwell nous a rejoints* », poursuit Ernesto van der Sar. « *Si de nombreuses autres personnes ont contribué au site au fil du temps, aujourd'hui, nous travaillons tous les deux de manière indépendante et restons les piliers du site, rédigeant tous les articles d'actualité* ».

ÉVOLUER POUR DURER

Entre-temps, l'industrie du piratage s'est métamorphosée plusieurs fois, mais TorrentFreak, lui, est toujours là, fidèle à cette fonction presque anthropologique : raconter comment s'organise une partie du monde que les institutions ne comprennent qu'avec retard. « *Au fil des ans, l'écosystème du partage de fichiers lui-même a changé* », confirme le fondateur. « *Le nom du site comprend toujours le mot « torrent », mais aujourd'hui, la plupart de nos articles portent sur l'écosystème plus large du piratage et les défis liés au droit d'auteur, qui n'ont plus rien à voir avec ce qu'ils étaient il y a vingt ans* ».

Ce qui frappe en relisant ses premières archives, c'est la manière dont le site a saisi très tôt l'importance du phénomène BitTorrent. Alors que la plupart des médias généralistes se contentaient d'articles alarmistes, TorrentFreak documentait les fermetures de trackers, expliquait le fonctionnement des DHT, racontait les coulisses de la scène warez. Le ton n'est jamais militant : il est observateur, presque clinique. Ernesto van der Sar aimait dire : « *Nous n'encourageons rien. Nous décrivons une réalité.* » Et c'est précisément cette neutralité studieuse qui a construit sa crédibilité.



DÈS 2007, TORRENTFREAK N'A PLUS RIEN D'UN BLOG ADOLESCENT, MAIS SE STRUCTURE EN SITE D'INFOS DE RÉFÉRENCE.

DU PARTAGE AU PIRATAGE MAFIEUX

Au fil des années, le paysage qu'il couvre change radicalement. La grande migration du piratage — des torrents vers le streaming — occupe la décennie 2010. TorrentFreak en capte les premiers signes : l'arrivée de Popcorn Time, les hébergeurs de fichiers qui deviennent des mini-CDN, la montée des sites proposant séries et films en un clic. « *Les amateurs de piratage des débuts ont été progressivement remplacés par des individus et des groupes cherchant à gagner rapidement de l'argent, voire des millions* », regrette Ernesto van der Sar. « *Cela a introduit davantage d'éléments criminels dans le milieu du piratage, qui continuent de sévir aujourd'hui* »,

> Le site est devenu une mémoire vivante de deux décennies de conflits autour de l'accès à la culture

20 ANS EN CHIFFRES ET EN DATES

2005 : Naissance du site
+ de **15000** articles publiés
+ de **100** décisions judiciaires majeures documentées
1 média cité dans Wired, BBC, Guardian, NYT...
0 lien illégal publié depuis sa création

2005-2012 : Âge d'or du protocole de partage de fichiers BitTorrent

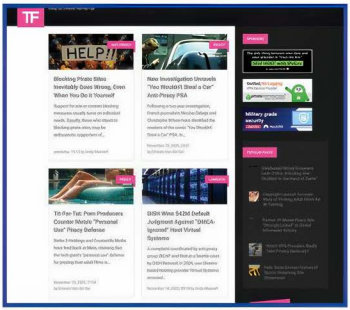
2012-2020 : Bascule vers le streaming

2020 – 2025 : Invasion des boîtiers IPTV et des applications « all-in-one »

2005 VS 2025 : DEUX INTERNET, DEUX MONDES

> 2005 : trackers BitTorrent, eMule, MP3, DivX, disques durs USB, firewall Windows XP.

> 2025 : IPTV illégale, CDN détournés, streaming chiffré, boîtiers Android rootés, 5G, lossless, blocages DNS dynamiques, surveillance automatisée par IA.

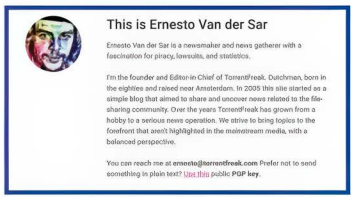


TORRENTFREAK EN NOVEMBRE 2025, 20 ANS APRÈS SA CRÉATION.

Puis vient la troisième mutation, plus brutale encore : l'explosion de l'IPTV illégale, ces boîtiers Android vendus sur les marchés ou sur Telegram, où un abonnement de quelques euros promet l'accès à tout le sport mondial. TorrentFreak en révèle la mécanique interne : infrastructures éclatées sur plusieurs continents, revendeurs anonymes, panels de gestion, réseaux criminels qui utilisent ces flux comme façade technique pour d'autres activités.
Dans l'industrie culturelle, certains ont longtemps regardé TorrentFreak comme un "site pirate", avant d'admettre qu'il jouait un rôle essentiel. Les cabinets juridiques qui traquent les infractions s'en servent comme baromètre. Les chercheurs universitaires y piochent des données historiques. Même les grandes plateformes de streaming y trouvent des informations pour anticiper les tendances. Le site est devenu, presque malgré lui, une mémoire vivante de deux décennies de conflits autour de l'accès à la culture.

NEUTRE NE VEUT PAS DIRE SANS COMBATS À MENER

Ce qui distingue TorrentFreak, c'est sa capacité à comprendre les zones grises. L'équipe sait raconter un procès sans sombrer dans la propagande, suivre les stratégies des ayants droit tout en décrivant les contournements ingénieux des utilisateurs. Elle sait aussi exposer les dérives de surveillance : les blocages DNS qui s'étendent, les régulations qui renforcent la pression sur les FAI, les gouvernements qui instrumentalisent la peur du piratage pour installer de nouveaux outils de contrôle.
En 2025, alors que les boîtiers IPTV pullulent et que les cyberattaques ciblent désormais aussi les infrastructures de piratage, TorrentFreak reste un phare dans un brouillard épais. Les journalistes du site travaillent dans l'ombre, mais leur travail éclaire. Ils documentent ce que d'autres préfèrent simplifier. Ils racontent des histoires techniques avec un sens de la nuance que l'on trouve rarement dans la presse généraliste.
Dans un monde où les débats sur le droit d'auteur se mêlent à ceux sur la surveillance, où les frontières entre légal et illégal deviennent floues au rythme des innovations, TorrentFreak reste l'un des rares espaces où cette complexité est assumée, expliquée et rendue intelligible. Et si tout cela tient encore debout, c'est sans doute grâce à l'intuition fondatrice d'Ernesto van der Sar : le piratage n'est pas une anomalie, mais un langage. Un langage qui dit quelque chose de notre rapport à la technologie, à la culture, et aux pouvoirs qui veulent la contrôler.



ERNESTO VAN DER SAR ET ANDY MAXWELL SONT LES DEUX PILIERS DE TORRENTFREAK. LES DEUX FONT PEU DE PUBLICITÉ SUR LEURS PERSONNES... MAIS PEUVENT ÊTRE LE PLUS SIMPLEMENT DU MONDE CONTACTÉS PAR EMAIL. DÉLICIEUSEMENT OLD SCHOOL.

« Aujourd'hui, la personne d'une vingtaine d'années qui a lancé TorrentFreak est à quelques années de ses 50 ans », confie-t-il. *« C'est une pensée effrayante, mais en même temps une bénédiction. (...) D'une certaine manière, j'ai le sentiment que TorrentFreak a déjà accompli sa mission. C'est une pensée rassurante, mais j'ai l'intention de maintenir le site en ligne indéfiniment. C'est l'œuvre d'une vie, non seulement pour moi, mais aussi pour Andy. »*

POURQUOI LES AVOCATS, LES FAI ET LES AYANTS DROIT LISENT TORRENTFREAK

Parce que ses enquêtes révèlent ce que peu d'autres médias savent : les stratégies de contournement, l'état réel des réseaux pirates, les effets concrets de la régulation, les chiffres non publiés sur le piratage mondial. TorrentFreak sert de boussole, même à ceux qui combattaient initialement son existence. Les technologies pirates à un instant T ont aussi deux valeurs cardinales pour les industriels du divertissement :

1) Elles inventent souvent des outils et solutions souples et économiques qu'ils intègreront eux-mêmes plus tard (le P2P est encore aujourd'hui souvent utilisé même dans la distribution de solutions VoD et streaming) ;

2) Elles forment des cohortes de futurs consommateurs à l'usage du dématérialisé. C'est le piratage qui a créé le besoin et la réceptivité des utilisateurs aux offres de distributions numériques légales qui ont, quelques années plus tard, inondé nos salons.

IPTV : DU PIRATAGE ARTISANAL À L'INDUSTRIEL

Ce n'est plus un "site de streaming pirate", mais une infrastructure industrielle. À l'automne 2025, des analystes de Silent Push ont documenté un réseau IPTV clandestin s'étendant sur plus de 1 000 noms de domaine et plus de 10 000 adresses IP, actif depuis des années. Derrière, on trouve des panels IPTV clé en main (XuiOne, Tiyansoft) loués à des revendeurs dans le monde entier, alimentant des milliers de boîtiers et d'abonnements illégaux.

Le réseau redistribue du contenu premium : Netflix, Disney+, Amazon, Apple TV+, grandes ligues sportives… Le tout appuyé sur une infrastructure distribuée, avec DNS alternatifs, rotation de domaines, hébergement éclaté dans plusieurs juridictions, et serveurs parfois liés à des acteurs basés en Afghanistan ou dans d'autres zones peu coopératives.

Ce que montrent ces enquêtes, c'est que le piratage IPTV n'est plus une petite économie parallèle : il s'agit d'un écosystème criminel structuré, mixant vente d'abonnements, publicité frauduleuse, revente de données d'utilisateurs et parfois distribution de malwares. Les sommes brassées se chiffrent en milliards de dollars par an.

FAILLES ZERODAY

Trend Micro distribue plus d'1 M$ aux hackers éthiques

L'édition 2025 de Pwn2Own Irlande a frappé fort : les chercheurs en sécurité offensive ont mis au jour 73 vulnérabilités zero-day uniques, touchant routeurs, smartphones, NAS, objets connectés et caméras. Au total, Trend Micro a distribué 1 024 750 dollars de récompenses.

Parmi les exploits marquants : la compromission d'un Samsung Galaxy S25, permettant d'accéder à la caméra et à la géolocalisation, et le "SOHO Smashup" de l'équipe Team DDOS, qui a enchaîné huit failles sur un routeur et un NAS QNAP. L'équipe Summoning décroche le titre de Master of Pwn avec 187 500 dollars.

Trend Micro souligne que ces découvertes offrent aux fabricants environ 71 jours d'avance pour corriger les failles avant qu'elles ne soient potentiellement exploitées. La prochaine édition, consacrée à l'automobile, se tiendra à Tokyo en janvier 2026.

AUTOMOBILE

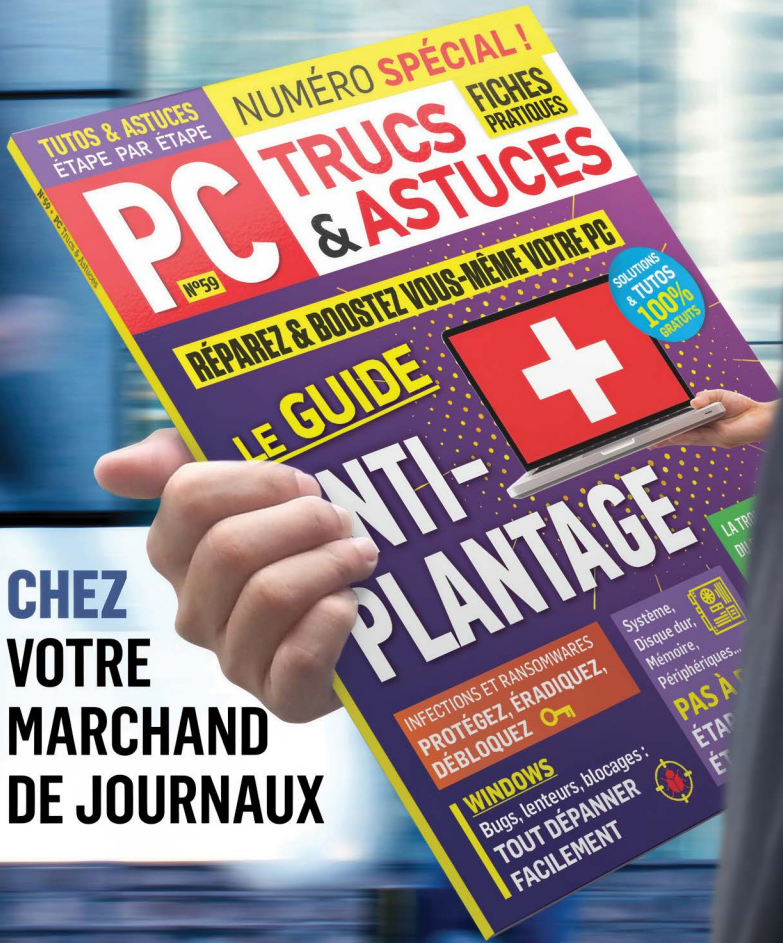
GANG FRANCO-ITALIEN

ARRÊTÉ POUR PIRATAGE DE VOITURES DE LUXE

Un réseau franco-italien spécialisé dans la fabrication d'outils de piratage automobile a été démantelé en novembre dernier. Les enquêteurs ont interpellé cinq suspects accusés d'avoir produit et vendu des dispositifs électroniques capables de déverrouiller à distance des véhicules premium comme BMW, Range Rover ou Mercedes. Selon la police italienne, ces appareils, inspirés des techniques de hacking keyless, permettaient de capturer ou cloner le signal des clés numériques, puis d'envoyer des commandes frauduleuses aux voitures.

L'affaire illustre la convergence bien connue ces dernières années entre hacking et criminalité "physique" : les voleurs n'ont plus besoin de forcer une serrure, mais d'exploiter des failles radio et des protocoles mal sécurisés. Les dispositifs saisis étaient vendus plusieurs milliers d'euros sur des canaux chiffrés et expédiés dans toute l'Europe sous couvert d'outils de diagnostic automobile. Pour les constructeurs, c'est un signal d'alarme : la sécurité des véhicules connectés se joue désormais autant dans le chiffrement que dans la carrosserie.

L'INFORMATIQUE FACILE
POUR TOUS !



CHEZ VOTRE MARCHAND DE JOURNAUX

VIE PRIVÉE, SÉCURITÉ ET ANONYMAT

LE GUIDE DES MEILLEURES ASTUCES POUR PILOTER WHATSAPP COMME UN PRO

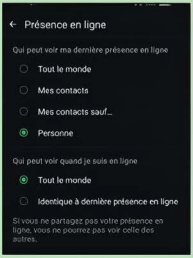
Connaissez-vous les techniques et fonctions Whatsapp qui vous donnent le contrôle total sur la messagerie instantanée ? Vie privée, protection et anonymat : avancez sur Whatsapp en utilisant les meilleures astuces pour discuter et échanger en maîtrisant l'art de savoir qui peut voir quoi, quand et pour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

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.



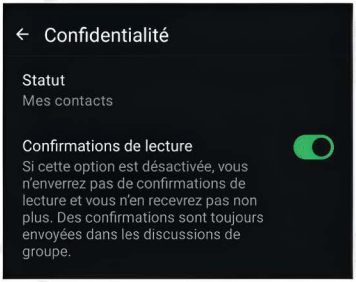
Sous **Qui peut voir ma présence en ligne**, sélectionnez **Personne** si vous souhaitez que personne ne voie plus vos heures de présence. Si vous préférez limiter la visibilité à vos proches, optez pour **Mes contacts sauf...** et excluez les curieux.

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.

PROTÉGER DES DISCUSSIONS SENSIBLES PAR UN MOT DE PASSE

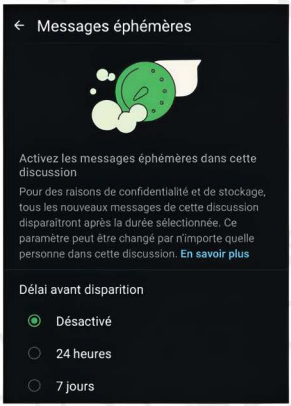
Certaines conversations ne regardent que vous. Depuis 2024, WhatsApp permet de verrouiller une discussion spécifique dans un dossier caché, accessible uniquement par empreinte ou code.

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.

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.

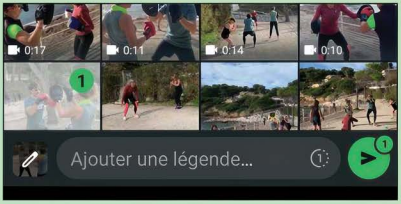
Ouvrez une discussion, puis appuyez sur le nom du contact et accédez à **Messages éphémères**. Choisissez une durée : **24 heures**, **7 jours** ou **90 jours**. Tous les nouveaux messages de ce chat seront supprimés automatiquement à l'expiration du délai. Cette option s'applique aux nouveaux messages,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



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.

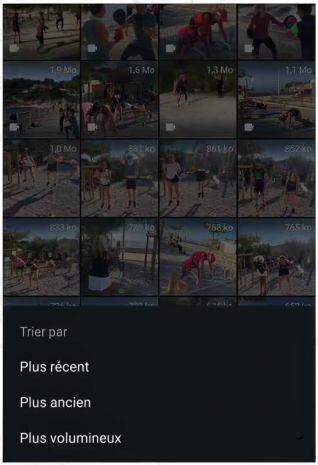
Lors d'un envoi d'un vocal, photo ou vidéo, touchez l'icône "**1**" à droite de la zone de légende. Vous verrez apparaître la mention **Photo/Vidéo à vue unique**. Envoyez le fichier : le destinataire devra l'ouvrir immédiatement, et ne pourra plus le consulter ensuite. WhatsApp bloque aussi les captures d'écran pour ce type de média, renforçant la confidentialité de l'échange.



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.



BLOQUER ET SIGNALER UN CONTACT MALVEILLANT

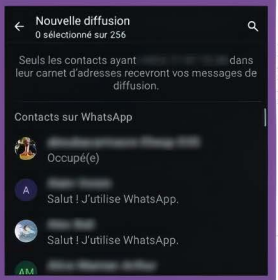
Spam, harcèlement, usurpation : bloquer un contact est la première défense. Cela coupe tout canal de communication, tout en signalant le comportement à WhatsApp.

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.

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.

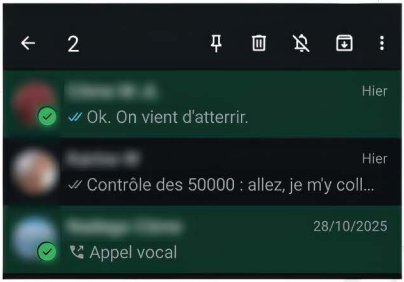
Sur l'écran principal, appuyez sur les trois points en haut à droite puis sur **Nouvelle diffusion**. Sélectionnez les contacts concernés (jusqu'à 256). Envoyez votre message : chacun le reçoit individuellement, comme un message privé.



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.

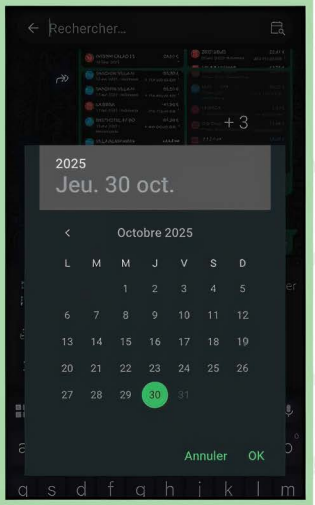
Depuis l'écran principal, effectuez un appui long sur la ou les discussions à épingler. Touchez l'icône épingler en haut de l'appli (en forme de punaise). Vous pouvez en épingler jusqu'à cinq (au lieu de trois auparavant).



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.



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 »

PRATIQUE

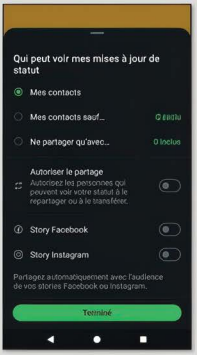
Apparus en 2017 pour concurrencer les "stories" d'Instagram et Snapchat, les statuts WhatsApp permettent de publier des contenus temporaires visibles pendant 24 heures : textes, photos, vidéos, GIFs ou même messages vocaux. Ces publications apparaissent dans l'onglet Statut et s'effacent automatiquement 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.

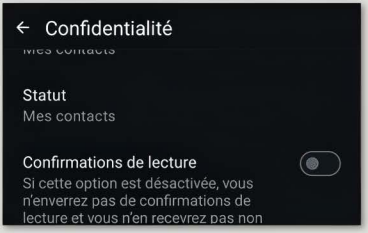
Ouvrez WhatsApp, allez dans **Actus** puis créez votre statut. Avant de publier, allez dans l'onglet **Statut** en bas à gauche. Trois options s'affichent : Mes contacts (par défaut) ; **Mes contacts sauf...** (pour exclure certaines personnes) ; **Ne partager qu'avec...** (pour créer une audience restreinte). 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.

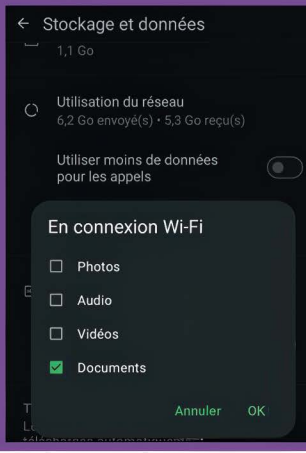
Sur Android, les statuts visionnés sont stockés temporairement dans le dossier caché : **/WhatsApp/Media/.Statuses**. Ouvrez un explorateur de fichiers (Files, Solid Explorer...) ou explorez votre mobile depuis un PC puis copiez le fichier souhaité avant qu'il ne soit supprimé. Sur iPhone, utilisez une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

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.

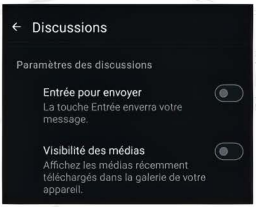
Allez dans **Paramètres > Stockage et données.** Sous **Téléch. Auto. des médias**, vous allez pouvoir piloter exactement ce qui ne peut être sauvegardé sans votre accord (vous devrez lancer le chargement manuellement – ou pas ! - à chaque nouvelle réception. Par exemple, ici, **Aucun média** en données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

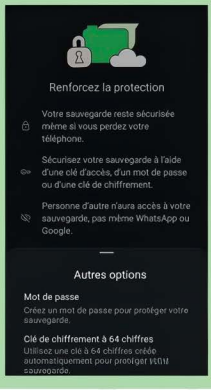
Les sauvegardes de conversations sont très pratiques, mais lorsqu'elles partent sur le cloud, elles perdent le bénéfice du chiffrement de bout en bout. En cas de piratage ou de demande judiciaire, vos discussions et contenus multimédias peuvent être accessibles en clair.

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.

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

PRATIQUE

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

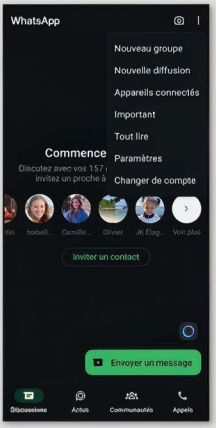
Ouvrez votre Whatsapp habituel puis passez par les trois points du menu en haut à droite de votre fenêtre d'accueil. À côté de votre profil, à droite, appuyez sur le petit « + ». L'option **Ajouter un compte** apparaît. Poursuivez, acceptez les conditions Whatsapp et continuez.

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 !



PIRATE INFORMATIQUE

JE SOUTIENS
LE COMMERCE DE PROXIMITÉ,

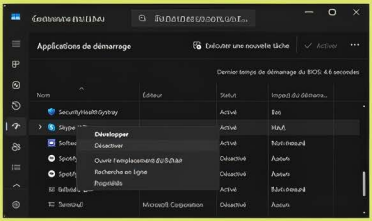
JE VAIS CHEZ MON MARCHAND DE JOURNAUX

Direct éditeurs

10 ASTUCES FACILES POUR CORRIGER LES LENTEURS ET BLOCAGES

Démarrage interminable, menus qui répondent au ralenti, applications longues à se lancer... Ces lenteurs peuvent transformer l'expérience Windows 11 en cauchemar quotidien. Heureusement, elles sont souvent causées par des programmes gourmands, des réglages mal optimisés ou un entretien négligé du système. Voici comment redonner une seconde jeunesse à votre PC.

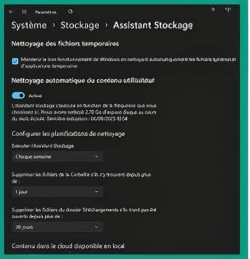
Identifier les programmes qui ralentissent le démarrage



Appuyez sur **Ctrl + Maj + Échap** et, dans le **Gestionnaire des tâches**, allez sur l'icône **Applications de démarrage** dans la barre latérale. Désactivez les applications non essentielles (ex. Spotify, Teams, Adobe Updater...) en passant par un clic droit sur celle(s) de votre choix. Moins de programmes lancés au démarrage = démarrage plus rapide.

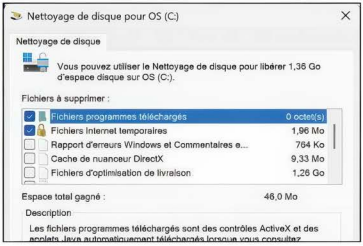
Nettoyage automatique

Via les **Paramètres** puis **Système > Stockage**, activez l'**Assistant de stockage** pour automatiser ce nettoyage. En cliquant sur l'Assistant, vous pourrez même configurer ses modalités d'exécution (fréquence, etc.).



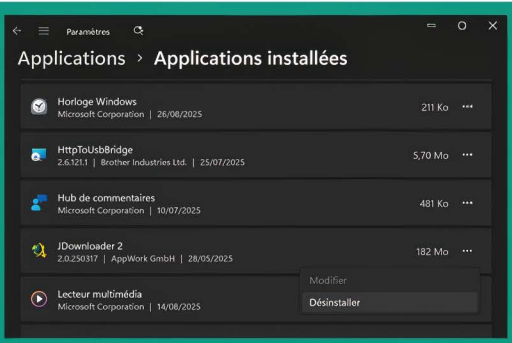
Nettoyer manuellement le disque système

Tapez **Nettoyage de disque** dans la recherche Windows. Supprimez fichiers temporaires, caches et anciennes mises à jour.



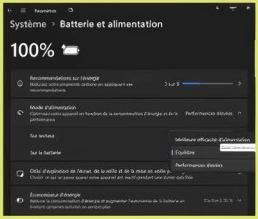
Désinstaller les logiciels inutiles

Passez par **Paramètres > Applications > Applications installées**. Supprimez les programmes que vous n'utilisez plus via les trois petits points situés en face. Chaque logiciel prend un espace de stockage inutile et vous avez peut-être oublié que vous avez autorisé certains à communiquer avec l'extérieur, gérer une catégorie de fichiers ou données présentes sur votre PC, etc., ce qui consomme des ressources pour rien !



Vérifier la gestion d'alimentation

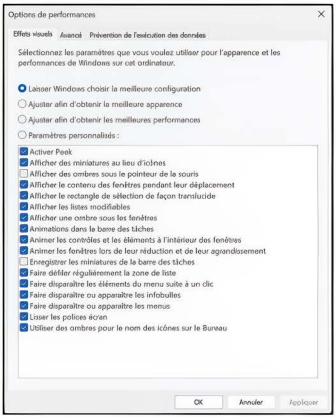
Via les **Paramètres,** passez par **Système > Batterie et alimentation**. Dans **Modes d'alimentation**, que ce soit sur **Batterie** ou **Secteur,** choisissez au minimum le mode **Équilibre** ou directement **Performances élevées** si disponible et si votre batterie dispose d'une bonne autonomie. Le mode **Meilleure efficacité d'alimentation** privilégie la faible consommation énergétique et peut réduire la fréquence CPU et donner une impression de lenteur.



Un peu plus bas, ouvrez le bloc **Economiseur d'énergie**. Il vous permettra d'affiner encore la gestion des performances et de l'autonomie de la batterie notamment lorsque cette dernière descend sous un certain seuil.

Désactiver les animations et effets visuels superflus

Les effets de transition et de transparence alourdissent l'affichage, surtout sur les PC avec peu de RAM ou un GPU intégré. Appuyez sur **Win + R** et tapez **sysdm.cpl** puis **Ok**. Dans l'onglet **Paramètres système avancés**, dans la section **Performances**, cliquez sur **Paramètres**. Choisissez **Ajuster afin d'obtenir les meilleures performances** ou personnalisez en décochant : Animer les fenêtres, Fond transparent, etc.



Réduire le nombre d'onglets ouverts dans le navigateur

Chrome, Edge et Firefox stockent chaque onglet dans un processus distinct ce qui entraine une forte consommation de RAM.

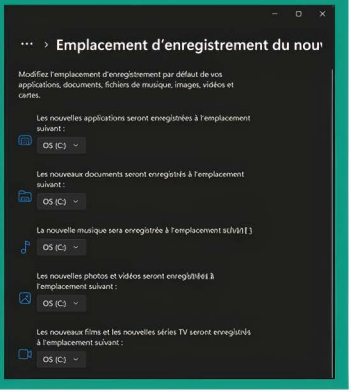
Dans Edge : **Paramètres > Système et performances,** activez **Mettre les onglets en veille**.

Dans Chrome : Utilisez une extension comme **The Great Suspender** pour mettre en pause les onglets inactifs.

Dans Firefox : Installez le module **Auto Tab Discard**. Vous pourrez piloter finement quoi mettre en veille, quoi conserver actif, etc.

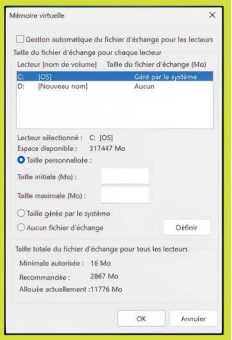
Changer le disque par défaut pour les nouveaux programmes

Votre disque dur principal commence à saturer ? Vous pouvez choisir de changer la destination par défaut des nouveaux programmes à installer ou même la destination par défaut de tous les nouveaux contenus que vous rapatriez. Dans **Système > Stockage > Paramètres de stockage avancés**, allez dans **Emplacement d'enregistrement du nouveau contenu**. Définissez un autre disque pour les applis, documents, musiques, etc.



Optimiser la mémoire virtuelle

Un PC avec peu de RAM (4 ou 8 Go) peut saturer et ralentir lors du multitâche. Vous pouvez booster la mémoire virtuelle via une extension matérielle, par un simple réglage Windows ! Appuyez sur **Win + R** et tapez **sysdm.cpl** puis **Ok**. Dans l'onglet **Paramètres système avancés**, dans la section **Performances**, cliquez sur **Paramètres**. Allez dans **Avancé > Mémoire virtuelle** et cliquez sur **Modifier**. Décochez **Gestion automatique**, sélectionnez votre SSD et définissez une taille personnalisée (ex. Taille initiale = RAM × 1,5 ; Taille max = RAM × 3). Résultat : Windows utilise le SSD comme extension de RAM, réduisant les plantages et lenteurs en usage intensif.



Optimiser le refroidissement du PC portable

Un PC portable qui chauffe bride son processeur (throttling), réduisant les performances. Utilisez un support ventilé avec ventilateurs intégrés. Évitez également les surfaces molles (lit, canapé) qui bloquent les aérations. Enfin, nettoyez régulièrement les grilles de ventilation à l'air comprimé. De manière générale, gardez en tête que les puces et processeurs fonctionnent mieux à basse température.

QUI SONT (VRAIMENT) LES HACKERS EN 2026 ?

Derrière le mot « hacker » se cache une galaxie variée d'acteurs — certains au service de la sécurité, d'autres poussés par le profit ou l'idéologie. En 2025, cette diversité s'est accentuée avec la démocratisation des outils et l'émergence de modèles économiques underground. Voici leur cartographie.

Parce que chaque profil implique des stratégies différentes de défense, comprendre ce que sont ces hackers — leurs outils, motivations et business models — c'est déjà s'armer intellectuellement. Un script kiddie en masse peut exploiter une faille IoT non patchée. Un acteur RaaS peut transformer une brèche locale en catastrophe. Un hacktiviste peut exposer vos données sans vous viser directement. Et un bug bounty bien mené peut renforcer vos défenses.

BLACK HATS : LES CRIMINELS NUMÉRIQUES

Ce sont les hackers « classiques » que l'on associe souvent à des braquages numériques, rançongiciels, vols de données. Leur motivation : l'argent, la revente de données ou la monétisation d'accès illégaux. Par exemple, en début 2025, le groupe LockBit revendiquait une attaque contre une municipalité américaine, exigeant plusieurs millions de dollars en crypto pour restituer les données. Leurs méthodes incluent désormais la double extorsion : non seulement chiffrer les fichiers, mais aussi menacer de publication des données volées si la rançon n'est pas payée.

WHITE HATS : LES GARDIENS VIGILANTS

Ce sont les hackers « éthiques » : experts en sécurité, pentesters, chercheurs travaillant pour des entreprises

ou via programmes de bug bounty. Leur mission : détecter les failles avant qu'elles ne soient exploitées, alerter les organisations, renforcer les défenses. Dans le domaine, **HackerOne** et **Bugcrowd** restent des plateformes phares où des chercheurs indépendants décrochent des primes importantes pour la découverte de vulnérabilités critiques. En 2025, un chercheur indépendant a décelé une faille 0-day chez un constructeur IoT majeur, évitant potentiellement des millions de victimes.

GREY HATS : ENTRE LES LIGNES

Ces hackers oscillent entre légalité et provocation. Ils peuvent révéler une faille sans autorisation, publier des preuves de vulnérabilité sans exploitation malveillante, ou pousser une entreprise à corriger sous pression médiatique. Un cas récent (fin 2024) : un chercheur a mis au jour une vulnérabilité critique dans une application bancaire, l'a publiée publiquement après un délai raisonnable, ce qui a suscité débats sur l'éthique dans la communauté.

HACKTIVISTES & ACTEURS IDÉOLOGIQUES

Le hacking comme instrument de cause politique, sociale ou idéologique. On pense à des attaques par déni de service, exfiltration de documents pour dénoncer des abus, ou sabotage symbolique. En 2023–2024, le groupe Anonymous Sudan a revendiqué des cyberattaques contre des infrastructures gouvernementales pour protester contre des mesures internes. Ces opérations permettent aux hackers de mêler discours politique et évolution technologique.

SCRIPT KIDDIES & OPÉRATEURS « LOW EFFORT »

Ce segment s'appuie sur des kits prêts à l'emploi, des scripts téléchargés, des plateformes automatisées : même sans compétences approfondies, l'utilisateur lance des attaques basiques. L'essor des kits « ransomware-as-a-service » (RaaS) rend ces outils accessibles à des profils non techniques. Une étude d'Akamai en 2025 note que certains groupes malveillants recrutent des affiliés non techniques pour lancer des attaques simples à grande échelle.

L'ÉCOSYSTÈME ET L'ÉCONOMIE SOUTERRAINNE

> Marchés de données, accès et identités : Dans les recoins sombres du dark web, on achète et vend : identifiants, accès RDP, bases de données piratées, bitcoins volés, etc. En 2024, le marché Genesis Market, spécialisé dans la revente de cookies de session volés, a été démantelé après une enquête internationale. Ce type de marché montre que le hacking est devenu une économie sophistiquée de la revente d'accès.

> Kits, "as-a-service" et mutualisation du crime : La commercialisation de kits ransomware, DDoS, phishing prêts à l'emploi rend le hacking accessible. Un opérateur sans compétence technique

peut « louer » un service illégal. Le modèle RaaS (Ransomware as a Service) est emblématique : le développeur fournit le malware et prend une commission sur chaque rançon, l'affilié exécute l'attaque. Ainsi, la barrière à l'entrée du hacking baisse, multipliant le nombre d'acteurs.

> La légitimité du bug bounty : Dans le camp légal, les programmes de bug bounty (**HackerOne**, **Synack**, **YesWeHack**...) fédèrent une communauté globale. Une faille critique peut rapporter des dizaines voire centaines de milliers de dollars. Certaines entreprises poussent même des bug bounties ouverts à tous, encourageant une chasse collaborative aux vulnérabilités. Cela transforme des hackers en contributeurs à la sécurité collective.

ÉVOLUTIONS & TENDANCES À SUIVRE !

À l'horizon 2026, ce ne sont plus seulement les techniques classiques qui comptent : les hackers adoptent des stratégies hybrides, tirent parti de l'intelligence artificielle, visent la chaîne d'approvisionnement logicielle, et préparent déjà le terrain pour l'ère du quantique. Chaque tendance porte son lot de défis — et d'opportunités pour qui sait anticiper.

1# Automatisation accrue : l'IA comme bras armé du hacker

L'un des changements les plus marquants : l'essor des attaques pilotées par l'IA. Plutôt que d'opérer manuellement, les hackers développent des scripts, agents ou modèles qui mènent automatiquement la reconnaissance, la génération de leurres personnalisés (phishing, spear-phishing), voire l'adaptation dynamique à des défenses en temps réel.
Un article de TechRadar relate qu'en 2025, des systèmes de balayage automatisé ont été observés à hauteur de 36 000 scans par seconde — un bond de 16,7 % par

« Nous passons d'une IA utilisée comme outil d'efficacité à une IA capable de prendre des décisions autonomes en matière de sécurité. Ce changement est à la fois puissant et risqué. »

Timothy Youngblood, CISO (Astrix Security)

rapport à l'année précédente — visant prioritairement des services vulnérables comme RDP ou des appareils IoT mal configurés.
Dans le domaine de la recherche, une revue (Red Teaming with Artificial Intelligence-Driven Cyberattacks) montre que les techniques d'IA sont utilisées pour accélérer l'exécution d'attaques, pour générer des tentatives de phishing plus crédibles, ou pour analyser des foisonnements de données afin de repérer des cibles d'intérêt.
La menace est double : non seulement l'IA permet à un hacker de faire plus, plus vite, mais elle peut aussi masquer ses traces, en adaptant ses actions pour éviter les systèmes de détection anormaux.

2# Attaques hybrides : le mélange social + technique + deepfake

Une autre tendance forte : l'attaque hybride, c'est-à-dire la combinaison de plusieurs vecteurs (ingénierie sociale, intrusion technique, deepfake, etc.) dans la même campagne. Le hacker ne se contente pas de spammer, il infiltre, observe, exploite un faux visuel ou vocal, et frappe avec précision. Par exemple, des campagnes de vishing deepfake (imitations vocales réalistes) se multiplient : un

« patron » appelle un employé en urgence pour demander un virement. Kevin Mandia (fondateur de Mandiant) a prévenu qu'une attaque entièrement pilotée par des agents IA pourrait survenir à court terme — difficile à retracer car l'outil masquerait l'identité humaine derrière.
Une stratégie hybride automatisée pourrait s'articuler comme suit :
- Collecte de données publiquement accessibles (réseaux sociaux, fuites de données).
- Génération automatique d'un message crédible (IA).
- Appel deepfake (vocal) pour crédibiliser la demande.
- Exploitation technique (ouverture de routeur, injection dans une session, accès aux comptes maîtres).
Cette approche rend la défense plus difficile car il faut contrer plusieurs vecteurs simultanément : vigilance humaine, filtre technique, authentification forte, reconnaissance de deepfake.

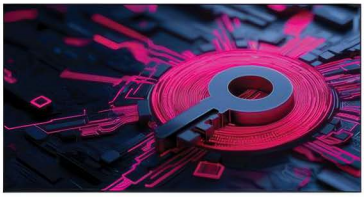
3# Ciblage de la chaîne d'approvisionnement logicielle

Une tendance désormais incontournable : au lieu de viser directement une entreprise ou un utilisateur, les hackers attaquent les fournisseurs, bibliothèques, composants tiers ou plateformes logicielles, pour contaminer en aval. Le fameux exemple de SolarWinds (2020) reste un cas d'école,

mais la méthode se répand. En 2025, certaines attaques ont été détectées où des mises à jour corrompues dans des modules open source ont injecté des backdoors dans des milliers d'installations. Le piège : quand une librairie largement utilisée est compromise, l'impact est diffusé largement. Cette tendance oblige les entreprises à surveiller non seulement leur propre sécurité, mais celle de leurs fournisseurs, à auditer les composants tiers et à intégrer la notion de software supply chain security (sécurité de la chaîne logicielle).

4# Transition post-quantique et attaques anticipées

Enfin, les hackers ne regardent pas seulement le présent : ils anticipent le futur quantique. L'idée est simple mais redoutable : collecter aujourd'hui des données chiffrées (ex : transmissions chiffrées, backups), puis stocker ces archives pour les déchiffrer plus tard, lorsque les ordinateurs quantiques seront disponibles. On appelle cela l'attaque « store now, decrypt later » (stocker maintenant, décrypter plus tard).
La conséquence : toute organisation digne de ce nom devra bientôt fonctionner en mode « crypto-agile » — capable de basculer entre algorithmes classiques et post-quantique sans rupture de service.



LES FAUX SITES DE MARQUE DE PLUS EN PLUS FACILES À CRÉER

Nous vous en parlions dans les pages précédentes de l'automatisation accrue de certaines attaques et escroqueries en ligne grâce à l'IA. Nous faisons un focus ci-dessous sur la création de plus en plus simple de faux sites qui reprennent tous les codes de marques bien connues pour tromper leurs victimes.

Les chercheurs de Norton alertent sur la prolifération de faux sites Web dédiés aux attaques de phishing. Baptisés "VibeScams" par la célèbre société américaine de sécurité informatique, ces sites de phishing paraissent authentiques, recopiant parfaitement le design, la structure et l'apparence d'un véritable site. Et pourtant, ces créations ne demandent aucune connaissance de code ou de piratage de la part des escrocs. Couplés à l'IA, les générateurs de sites Web leur permettent de créer des répliques parfaites de sites légitimes, en quelques minutes seulement.

FACILITÉ ET RAPIDITÉ EFFRAYANTES

En pratique, un simple prompt tel que « crée un site Web qui ressemble à Amazon.fr » suffit désormais pour générer en quelques secondes un site de phishing soigné, avec les couleurs, la structure et même les liens de bas de page d'un site que les utilisateurs associent instinctivement à une marque de confiance.

Certaines plateformes de création de sites Web recréent même un site entier à partir d'une capture d'écran fournie par l'arnaqueur – d'une page d'accueil à un panier. Ils permettent généralement également une localisation parfaite de la langue, permettant aux escrocs de cloner instantanément l'apparence et la sensation d'un site légitime dans plusieurs langues.

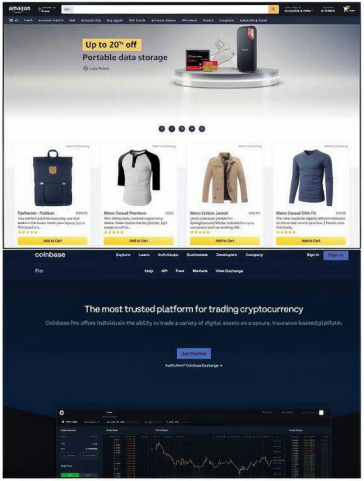
UNE VAGUE MONTANTE

En 2025, Norton déclare avoir notamment bloqué plus de 140 000 sites malveillants générés par IA et détecté en moyenne 580 nouveaux sites de phishing par jour. Toujours selon la société américaine, les États-Unis, la France, le Brésil, l'Allemagne et le Japon étaient les pays parmi les plus touchés.

Ces faux sites usurpent souvent l'identité de marques comme connues, à travers de fausses notifications ou SMS pour inciter les victimes à ouvrir ces pages de connexion frauduleuses, dans le but ultime de dérober leurs identifiants et données bancaires. Cette technique est particulièrement efficace sur mobile, où les URL sont plus difficiles à vérifier et où un design visuel simple suffit souvent à convaincre.

CRÉATION DE FAUX SITES PAR IA : QUELS PRIX ?

La gamme d'offres payantes est vaste, allant de 0,5 $ par mois à 500 $ par mois, avec une variété de niveaux gratuits et / ou de périodes d'essai. Certains fournisseurs offrent également des offres à vie pour 249 $ ou 599 $.



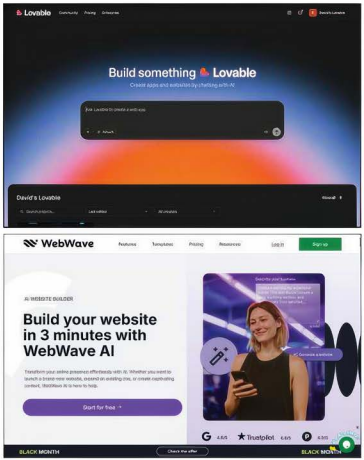
VOICI CI-DESSUS DES EXEMPLES DE SITES WEB, IMITANT RESPECTIVEMENT AMAZON ET COINBASE, GÉNÉRÉS AVEC UN OUTIL DE CRÉATION DE SITES WEB DOPÉ À L'IA.

Cette nouvelle vague d'outils de construction Web axés sur l'IA a considérablement abaissé la barrière à l'entrée pour les cybercriminels, démocratisant l'accès à des opérations sophistiquées de clonage et d'escroquerie sur les sites. Non plus limitées à ceux qui ont une connaissance de HTML, CSS et JavaScript, ces plateformes permettent à toute personne disposant d'une connexion Internet de répliquer des marques de confiance, des portails bancaires ou des interfaces d'échange avec une fidélité alarmante. La facilité et la rapidité de ce processus non seulement accélèrent la prolifération des sites Web frauduleux, mais rendent également de plus en plus difficile pour les utilisateurs de faire la distinction entre les sites Web authentiques et malveillants.

> Même les pirates du dimanche peuvent désormais créer de faux sites de qualité en quelques minutes

Le visiteur retrouve d'un coup d'œil les bonnes couleurs, l'espacement, le placement du logo et les liens de pied de page minuscules. C'est suffisant pour inciter les gens à remettre des informations d'identification voire bancaires, et c'est pourquoi cette vague d'escroqueries se propage si rapidement.

Norton a identifié les plateformes de créations Web que les attaquants exploitent selon ses détections. Toutes sont des plateformes légitimes et de confiance… mais le prix d'entrée est tellement bas et le résultat tellement simple à obtenir qu'elles sont détournées de leur usage initial par les escrocs. Norton cite par exemple Lovable, Elementor, Flazio, Softr, Webflow et WebWave, entre autres.



LOVABLE ET WEBWAVE FONT PARTIE DES PLATEFORMES DE CRÉATION DE SITES WEB ASSISTÉES PAR IA PARMI LES PLUS POPULAIRES.

DES CIBLES PRIVILÉGIÉES

Les sites d'arnaque typiques comprennent les échanges de cryptomonnaies, les portails d'investissement, les sites bancaires, les plateformes de médias sociaux, les services de livraison, les sites d'achat et bien plus encore.

Près de la moitié des sites Web détectés par Norton étaient des pages de phishing traditionnelles usurpant l'identité de portails de connexion familiers comme Microsoft, Gmail ou Amazon. Environ un quart a ciblé l'espace de la cryptomonnaie, soit en imitant les échanges populaires tels que Coinbase, Binance et MetaMask, soit en faisant la promotion d'escroqueries à l'investissement basées sur la cryptomonnaie. Le reste comprenait des arnaques plus générales et d'autres pages malveillantes.

Créer une clé de réinitialisation du mot de passe

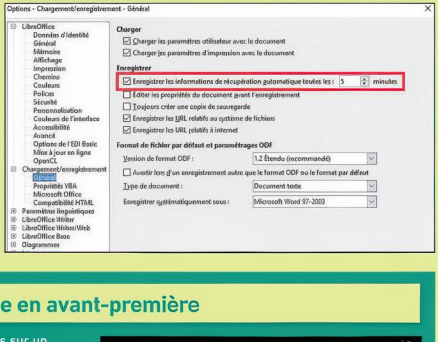
> Avec Windows

Vous avez peur d'oublier votre mot de passe Windows ? Toutes les versions de l'OS permettent de créer une clé à stocker sur un support amovible. Appuyez sur **Ctrl + Alt + Suppr** pour avoir accès au menu **Modifier un mot de passe** puis **Créer un disque de réinitialisation de mot de passe**. Insérez un périphérique USB et choisissez-le dans la liste. Tapez ensuite votre mot de passe actuel et laissez Windows s'occuper de placer le fichier **userkey.psw** sur la clé. Faites un essai en pressant **Win + L**. Votre session sera verrouillée. Tapez un mauvais sésame, validez et choisissez **Réinitialiser le mot de passe**. Connectez alors le périphérique contenant le fichier sus-nommé.

Retrouver un texte non sauvegardé

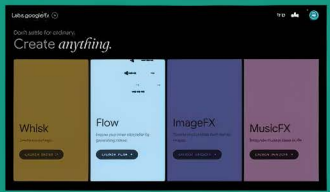
> Avec LibreOffice Writer ou Word

Vous avez presque fini les 25 pages de votre rapport, et tout d'un coup, panne de courant ? Pour être sûr de récupérer une version récente de votre document, allez dans **Outils > Options > Chargement/enregistrement** (Writer) ou **Fichiers > Options > Enregistrement** (Word) et mettez 5 minutes à **Enregistrer les informations de récupération automatique toutes les**.



Accéder aux outils d'IA Google en avant-première

Si vous tombez sur labs.google/fx, vous n'êtes pas sur un énième site obscur de « fake IA gratuite », mais bien dans le laboratoire créatif officiel de Google. C'est ici que la firme teste et regroupe ses outils génératifs dédiés à l'image, la musique et la vidéo, avant (éventuellement) de les intégrer à des produits plus grand public. Un hub vitrine, expérimental, puissant… et volontairement discret. On y retrouve aujourd'hui quatre outils phares : **ImageFX** (texte → image), **MusicFX** (texte → musique et boucles audio), **Flow** (génération de vidéos cinématographiques avec le modèle Veo), **Whisk** (remix et composition visuelle à partir d'images de référence).



Ici son testés des fonctions et modes opératoires qui n'existent pas encore dans les outils IA officiels de Google. Certaines apparaissent et disparaissent ainsi régulièrement !

Tous sont accessibles gratuitement via un compte Google, dans les pays éligibles, et réservés aux utilisateurs de 18 ans et plus.

Lien : labs.google/fx

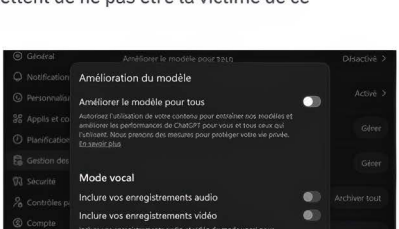
TUTO

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

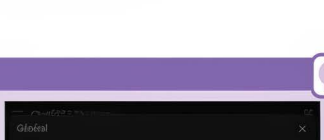
Passez par **Paramètres > Gestion des données > Améliorer le modèle pour tous**. Et désactiver. Vous noterez que ce réglage inclut aussi les enregistrements audio et vidéo. Vous empêchez ainsi OpenAI d'utiliser vos nouveaux échanges pour améliorer ses modèles : un bon réflexe pour des contenus sensibles (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".

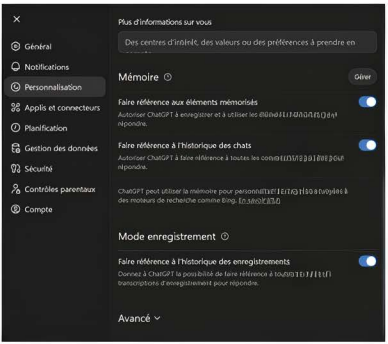
ATTENTION AUX LIENS PARTAGÉS



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.



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).

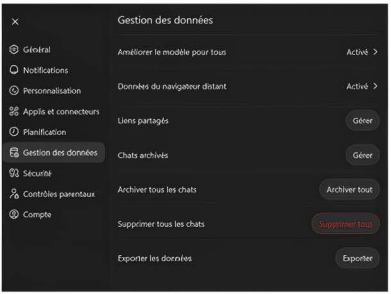
LE PRIVACY PORTAL D'OPENAI, QU'EST-CE QUE C'EST ?

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.

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.



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).

SÉLECTION

TOP 5 OUTILS POUR CONTRÔLER SES DONNÉES

Reprendre le contrôle, ce n'est pas disparaître du Web. Ces cinq outils — de l'export de données à la configuration du système — constituent un kit d'autodéfense numérique grand public, gratuit et complémentaire. Le plus efficace ? Les combiner : un audit global avec Takeout, un nettoyage social avec Exodus et MyPermissions, puis une désinfection locale via BleachBit et ShutUp10++.

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

MYPERMISSIONS > Le détective des connexions cachées

CONSEIL

Relancez ces outils tous les trois à six mois, et vous verrez que la "vie privée numérique" n'est pas un mythe, mais une discipline.

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.

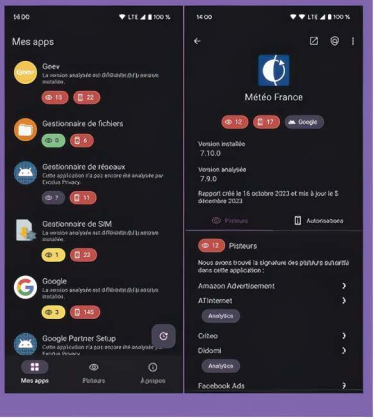
Lien : https://mypermissions.com

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.

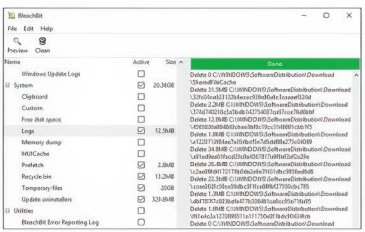
Lien : https://exodus-privacy.eu.org



BLEACHBIT > Nettoyer le PC comme on vide un grenier

Après les traces en ligne, place à celles qui dorment sur votre disque dur. Sous Windows comme sous Linux, des gigaoctets de fichiers temporaires, caches et journaux racontent votre activité. Le logiciel libre BleachBit agit comme un grand ménage de printemps numérique.
Il ne se contente pas d'effacer les cookies : il nettoie en profondeur les dossiers temporaires, les historiques de navigateurs, les journaux système, et peut même écraser l'espace libre du disque pour rendre la récupération difficile. Avant de supprimer, il propose une prévisualisation détaillée, idéale pour les utilisateurs prudents.
Entièrement gratuit et open source, BleachBit est transparent et léger. Il ne protège pas de l'espionnage en ligne, mais il réduit la quantité d'informations exploitables localement — une étape souvent négligée dans la protection de la vie privée.

Lien : www.bleachbit.org

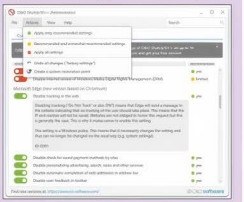


O&O SHUTUP10++

> Rendre Windows moins bavard

Windows 10 et 11 collectent, par défaut, une foule de données : diagnostics, télémétrie, suggestions, historique d'activité... Le tout réparti dans des menus labyrinthiques. L'utilitaire gratuit O&O ShutUp10++ centralise ces réglages et les rend enfin lisibles.
Dès l'ouverture, il affiche une longue liste d'options classées par catégories (confidentialité, sécurité, mises à jour, Edge, localisation...). Chaque ligne est accompagnée d'une explication claire et d'une recommandation : appliquer, ignorer ou conserver. En un clic, on peut adopter le profil "recommandé" qui coupe la majorité des fonctions de traçage.
L'outil crée un point de restauration avant toute modification, ce qui permet de revenir en arrière sans stress. Son avantage : il ne s'installe pas ; il s'exécute simplement.
Sa limite : une configuration trop radicale peut désactiver certaines fonctions utiles (ex. Windows Update). Utilisé avec mesure, ShutUp10++ offre un compromis rare entre confort et confidentialité.

Lien : www.oo-software.com/en/shutup10



SÉLECTION

TOP 3 SERVICES

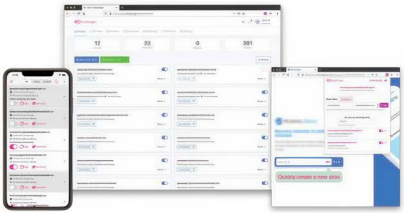
CRÉEZ UNE IDENTITÉ NUMÉRIQUE JETABLE

Formulaires d'inscription, newsletters, tests en ligne, boutiques douteuses… À chaque clic, notre vraie identité numérique se fragmente et s'expose. Pour éviter ce profilage permanent, il existe des outils capables de créer des identités jetables. Leur usage n'a rien d'illégal : il s'agit simplement de reprendre la main sur ce que l'on choisit de dévoiler.

SIMPLELOGIN > L'ART DU DOUBLE NUMÉRIQUE

Imaginez un service capable de générer à la volée des adresses e-mail alias : cinema@votre-nom.alias, voyage@votre-nom.alias… Quand un site vous écrit, SimpleLogin fait le relais sans jamais révéler votre véritable adresse. Si un alias commence à recevoir du spam, vous le supprimez et tout disparaît.
Racheté par Proton en 2022, SimpleLogin reste open source et dispose d'une offre gratuite solide : création illimitée d'alias, transfert de courriels et réponses anonymes depuis l'alias. L'application mobile Android/iOS complète l'écosystème.
Ses forces ? Une conception claire, une transparence exemplaire et un ancrage européen : les données sont hébergées en France et en Suisse, sous juridiction RGPD. Seule contrainte : au-delà d'un certain volume d'envois, la version payante devient nécessaire. Mais pour un usage grand public, SimpleLogin est aujourd'hui la référence du mail masqué éthique.

Lien : https://simplelogin.io



ANONADDY > L'ALTERNATIVE LIBRE DES PURISTES

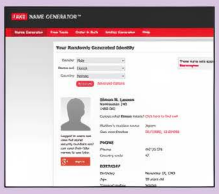
Né dans la mouvance open source, AnonAddy reprend le même principe que SimpleLogin, mais dans une approche encore plus indépendante. Vous créez une adresse alias unique — par exemple magazine@anonaddy.me — et le service redirige les messages vers votre vraie boîte sans jamais la dévoiler. La différence ? AnonAddy peut être auto-hébergé, une rareté précieuse pour les utilisateurs qui veulent un contrôle total.
Sa version gratuite autorise 20 alias et 10 réponses anonymes par mois, ce qui suffit largement à la plupart des usages quotidiens. L'interface, plus sobre, s'adresse à un public un peu plus technique, mais reste intuitive. Côté sécurité, tout est chiffré en transit et les logs sont minimaux. La seule faiblesse : son serveur principal est basé au Royaume-Uni, donc soumis à des législations différentes du RGPD, même si la politique de confidentialité reste exemplaire.

Lien : https://anonaddy.com

FAKE NAME GENERATOR > DEVENEZ QUELQU'UN D'AUTRE EN UN CLIC

Quand un site vous demande prénom, adresse et date de naissance pour un simple téléchargement, mieux vaut ne pas toujours dire la vérité. Fake Name Generator produit instantanément de fausses identités crédibles : nom, adresse, téléphone, âge, carte d'identité, profession… Vous choisissez le pays, le sexe, la langue, et l'outil invente un double numérique cohérent.
Ce générateur, libre d'accès et sans inscription, a un succès phénoménal : plus de 100 millions d'identités créées depuis sa création. Les données sont fictives, mais parfaitement formatées pour passer les formulaires web. En revanche, il ne faut jamais utiliser ces informations pour nuire ni pour de fausses déclarations administratives : l'outil est destiné à protéger sa vie privée, pas à usurper celle d'autrui.

Lien : www.fakenamegenerator.com

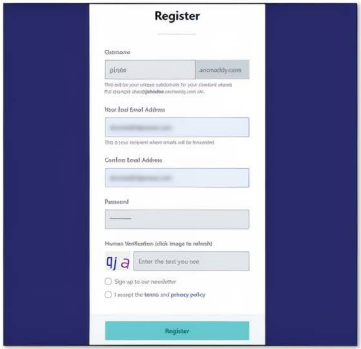


VOTRE PREMIER ALIAS AVEC ANONADDY

PRATIQUE

01 NOM DE DOMAINE ET MAIL PRINCIPAL

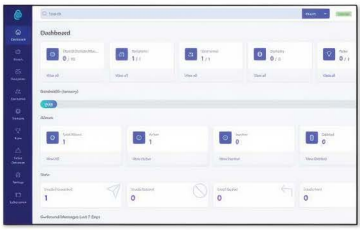
Créez un compte et personnalisez votre alias : en version gratuite, le service vous fournit un nom de



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

02 ALIAS À LA VOLÉE

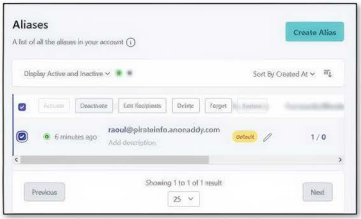
Une fois sur le tableau de bord de votre compte, vous vous demandez sans doute comment créer votre premier alias ? Pas besoin ! La prochaine fois que vous enregistrerez un email sur un service Web, mettez celui qui vous passe par la tête sur ce modèle : **monalias@votrenomdedomaine.anonaddy.com.** Ici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



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

03 GESTION

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



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

04 RÉPONSE ANONYME

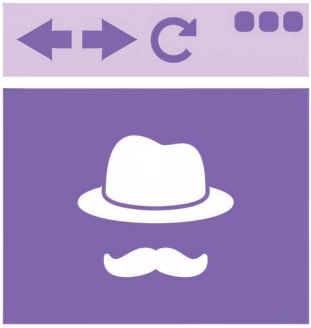
Et vous pouvez bien sûr renvoyer des emails avec cet alias, sans que votre email réel ne soit visible. Vous restez sur votre email principal et utilisez simplement l'option de réponse au mail reçu via votre alias. AnonAddy se charge

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

DÉCRYPTAGE

LE MYTHE DE LA NAVIGATION PRIVÉE

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 !

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.

> Beaucoup ont confondu "discrétion locale" et "invisibilité globale". Or c'est précisément là que le mythe commence.

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.

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.

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.

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
- L'historique local n'est pas enregistré
- Les cookies ne sont pas conservés après fermeture
- Les recherches ne sont pas ajoutées au navigateur
- Les sessions simultanées sont possibles (ex. deux comptes Gmail)

Ce qu'elle NE PROTÈGE PAS
- Votre adresse IP reste visible pour les sites
- Votre FAI voit toujours vos connexions
- Le fingerprinting fonctionne toujours
- Les trackers publicitaires continuent de vous profiler
- Les fuites DNS, WebRTC ou scripts tiers restent actives

EFFACEZ L'HISTORIQUE DE NAVIGATION SUR amazon

INFOS Où le trouver ? [Amazon.fr]
Difficulté :

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

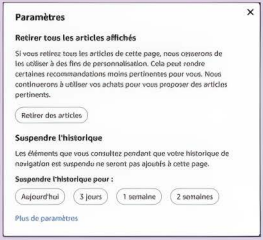
Une fois loggué, ce n'est pas forcément le plus intuitif selon votre terminal (PC ou mobile). Amazon n'a pas très envie que vous lui enleviez cet historique qui en dit tellement sur vous. Les deux accès les plus simples sont, soit via le lien en bas du bloc **Continuez vos achats** sur la page d'accueil,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

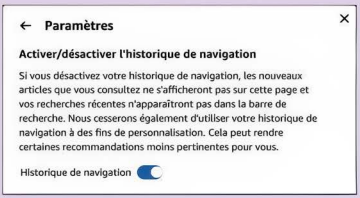
03 SUPPRIMER OU BLOQUER TEMPORAIREMENT

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**.



Oui,
recycler mes papiers, c'est utile.

Pour l'environnement

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

Le recyclage de papier, c'est :

3 fois moins d'eau*

3 fois moins d'énergie*

* comparé à la fabrication de papier non recyclé

Pour l'emploi

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

Collecte

Papeterie

Centre de tri

Découvrez le recyclage du papier sur www.consignesdetri.fr

CITEO

Le nouveau nom d'Eco-Emballages et Ecofolio

TOUT SAVOIR SUR RÉCUPÉRATION MACHINE RAPIDE,

La nouvelle trousse de survie de Windows 11

Depuis cet été, Windows 11 embarque une arme inédite contre les pannes système critiques : la Récupération Machine Rapide. Conçue pour relancer un PC incapable de démarrer, cet outil de réparation express via le cloud promet de sauver vos données et d'éviter une réinstallation fastidieuse. Voici tout ce qu'il faut savoir pour l'utiliser efficacement.

Qui n'a jamais connu ce scénario cauchemar : un PC qui refuse de démarrer après une mise à jour ratée, un pilote corrompu ou un disque qui lâche ? Jusqu'ici, les solutions étaient laborieuses : clé USB d'installation, réinitialisation complète, parfois perte de données. Récupération Machine Rapide (Quick Machine Recovery en anglais) change la donne en proposant une restauration automatique, guidée et sans support externe, directement depuis les serveurs Microsoft. Introduite avec Windows 11 24H2 (KB5062660), cet outil répare automatiquement un PC qui ne démarre plus en recherchant un correctif ciblé via le cloud (WinRE). Elle est activée par défaut sur Home et configurable sur Pro/Entreprise.

Récupération Machine Rapide vise trois objectifs :

1) **Réparer un Windows qui ne démarre plus :** en téléchargeant une image saine du système.

2) **Simplifier les procédures de dépannage :** plus besoin de préparer un média USB ou d'avoir des connaissances techniques poussées.

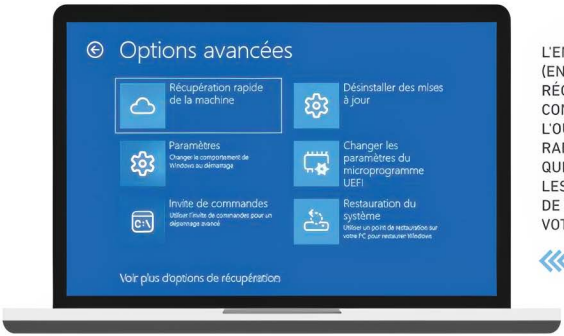
3) **Sécuriser les données :** vos fichiers personnels peuvent être conservés, selon l'option choisie.

En clair, il s'agit d'un "reset cloud intelligent", mais optimisé pour les situations d'urgence.

DÉCLENCHEMENT

Si Windows ne démarre pas : l'option s'affiche automatiquement après plusieurs échecs de boot. Si Windows démarre encore : vous pouvez passer par **Paramètres > Système > Récupération.** Dans **Démarrage avancé,** cliquez sur **Redémarrez maintenant.**

Via l'interface de redémarrage, passez par **Dépannage** et **Options avancées** pour accéder à la **Récupération Machine Rapide**.



L'ENVIRONNEMENT WINRE (ENVIRONNEMENT DE RÉCUPÉRATION WINDOWS) CONTIENT DÉSORMAIS L'OUTIL "RÉCUPÉRATION RAPIDE DE LA MACHINE" QUI TENTERA DE FIXER LES CRASHS MAJEURS DE VOTRE SYSTÈME SANS VOTRE INTERVENTION.

PRÉREQUIS

Si vous possédez l'une des dernières versions de Windows 11, la Récupération Machine Rapide est installée et est activée par défaut. Vous pouvez le vérifier en allant dans **Paramètres > Système > Récupération > Récupération machine rapide**.

Il vous faudra cependant une connexion Internet stable et fonctionnelle pour que ce service puisse être efficace. Mais si mon PC ne démarre plus du tout nous direz-vous ? Quand le PC ne démarre plus, après plusieurs échecs, Windows entre dans l'Environnement de récupération (WinRE) et lance automatiquement l'outil ce qui permet d'établir une connexion réseau, l'envoi d'un diagnostic minimal, les téléchargement et application d'un correctif si une solution connue existe. À défaut, Windows retente selon un intervalle défini ou bascule sur Réparation du démarrage classique.

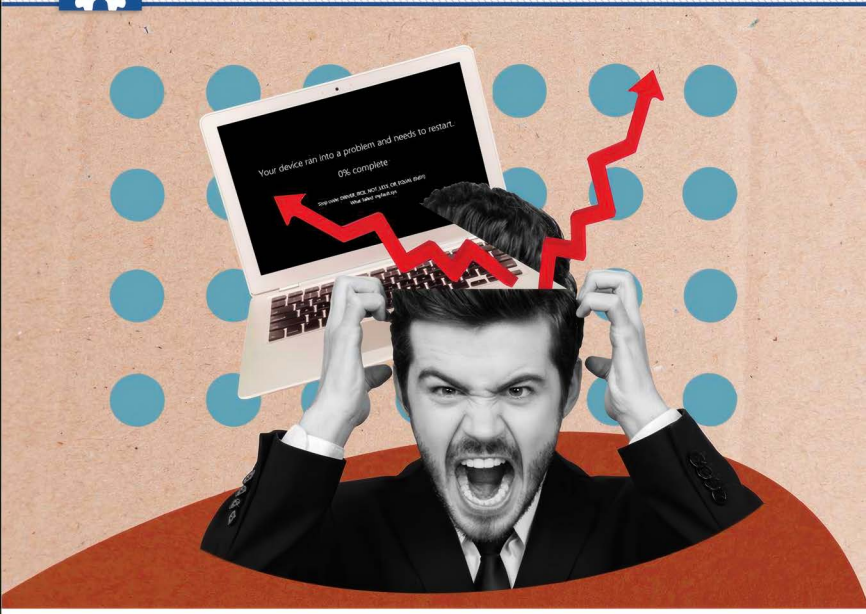
Il vous faudra enfin prévoir un espace disque d'au moins 4 à 6 Go pour les téléchargements nécessaires (taille de l'image système).

CHOIX DU MODE

Lors de la tentative de réparation par Récupération Machine Rapide, vous aurez la possibilité de **Conserver mes fichiers** (Windows est réparé, vos documents restent intacts) ou de **Tout supprimer** (repartitionne et réinstalle un Windows vierge, idéal pour les machines fortement corrompues ou revendues).

L'outil télécharge une image propre de Windows adaptée à votre version. La réinstallation automatisée, les pilotes et mises à jour critiques sont réappliqués. Le PC redémarre plusieurs fois, puis affiche un environnement prêt à l'emploi.

Depuis l'été 2025, Windows propose une solution automatisée et pilotée dans le cloud pour faire face au crash de votre ordinateur… Plus besoin d'être un expert pour tenter la réparation en local.



QUE FAIRE FACE À UN ÉCRAN NOIR DE CRASH

(ANCIENNEMENT ÉCRAN BLEU) ?

Depuis la mise à jour Windows 11 24H2, l'« écran bleu de la mort » (BSOD) a laissé place à un écran noir de crash. L'aspect visuel change, mais la fonction reste identique : signaler une erreur critique du système avec un code d'arrêt. Voici comment identifier les causes et résoudre les plantages répétés.

À compter de la version Windows 11 24H2, Microsoft a remplacé le légendaire Blue Screen of Death (BSOD – le fameux « écran bleu ») par un écran de crash au visuel noir — parfois surnommé Black Screen of Death (BkSOD) ou Unexpected Restart Screen.

POURQUOI CE CHANGEMENT VISUEL ?

Microsoft a fait le choix de changer son écran bleu iconique (et synonyme de panique intense) pour aligner l'interface de crash avec le thème sombre de Windows 11, dans une démarche de modernisation visuelle. Et sans doute aussi pour réduire le stress visuel causé par l'écran bleu classique tout en offrant une expérience plus «normalisée» avec le reste de l'OS. Mais le contenu diagnostic reste : codes d'arrêt, pilotes en cause, voire QR code. Et pour les professionnels IT, rien ne change : les outils de diagnostic classiques (WinDbg, Event Viewer, minidumps, etc.) continuent à fonctionner comme avant.

Et alors… doit-on toujours parler d'"écran bleu" ? Oui, dans le langage courant (BSOD), surtout en contexte de dépannage. Mais pour être précis, on devrait maintenant parler de « écran noir de crash » ou « écran de redémarrage inattendu ».

CONSEIL

Un BSOD peut cacher un problème matériel : surchauffe CPU/GPU, alimentation instable, SSD défaillant. Utilisez en complément de notre tutoriel des outils de monitoring gratuits (ex. **HWMonitor**, **CrystalDiskInfo**) pour vérifier températures et l'état de vos disques. Un PC qui plante toujours malgré réinstallation de Windows est souvent victime d'un composant matériel défectueux.

LES 10 PRINCIPAUX CODES D'ARRÊT WINDOWS 11

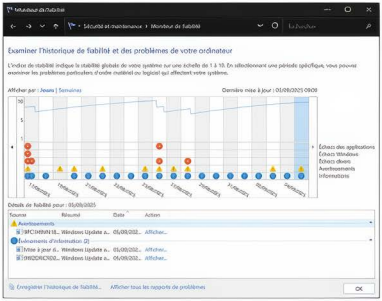
Ce tableau récapitule les principaux codes d'arrêt rencontrés lors d'un écran noir de crash (anciennement BSOD) sous Windows 11, leurs causes probables et les solutions recommandées. Il constitue un aide-mémoire pratique pour le dépannage.

Code d'arrêt	Cause probable	Solution recommandée
MEMORY_MANAGEMENT	Défaillance de la RAM, overclock instable	Tester la RAM avec Diagnostic mémoire Windows, retirer ou remplacer la barrette fautive
CRITICAL_PROCESS_DIED	Processus système essentiel corrompu (fichiers ou pilotes)	Exécuter sfc /scannow et DISM, mettre à jour Windows et pilotes
DRIVER_IRQL_NOT_LESS_OR_EQUAL	Pilote réseau, audio ou stockage en conflit	Identifier le pilote fautif via BlueScreenView, mettre à jour ou désinstaller le pilote
SYSTEM_SERVICE_EXCEPTION	Erreur dans un pilote graphique ou antivirus	Mettre à jour le pilote GPU, désinstaller temporairement l'antivirus tiers
PAGE_FAULT_IN_NONPAGED_AREA	RAM défectueuse ou pilote accédant à une zone mémoire interdite	Vérifier la RAM, tester sans overclock, mettre à jour les pilotes suspects
KMODE_EXCEPTION_NOT_HANDLED	Pilote incompatible ou mal codé	Identifier le pilote mentionné, réinstaller ou remplacer par la version stable
VIDEO_TDR_FAILURE (nvlddmkm.sys / atikmpag.sys / igdkmd64.sys)	Pilote graphique (NVIDIA, AMD, Intel) qui plante	Mettre à jour/désinstaller et réinstaller le pilote GPU, vérifier la température de la carte graphique
INACCESSIBLE_BOOT_DEVICE	Windows ne détecte plus le disque système (bootloader corrompu, pilote stockage manquant)	Vérifier le BIOS/UEFI (mode AHCI/RAID), exécuter chkdsk, réparer le démarrage depuis WinRE
DPC_WATCHDOG_VIOLATION	Temps d'attente dépassé par un pilote ou un SSD	Mettre à jour les pilotes SATA/NVMe, vérifier l'état du SSD avec CrystalDiskInfo
BAD_POOL_HEADER	Gestion mémoire défectueuse (pilotes, antivirus, RAM)	Mettre à jour pilotes, désinstaller logiciels récents, tester la RAM

Bonus > Si le code mentionne directement un fichier (ex. nvlddmkm.sys), il s'agit du pilote concerné. Rechercher ce fichier dans Google donne rapidement l'indice du matériel à corriger (NVIDIA, AMD, Intel, etc.).

TUTO PRATIQUE

DIAGNOSTIQUER ET FIXER LE PROBLÈME CRITIQUE

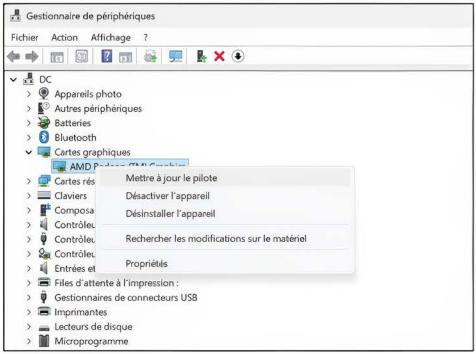


01› IDENTIFIER LE CODE D'ARRÊT

Notez le code affiché sur l'écran noir (ex. MEMORY_MANAGEMENT, CRITICAL_PROCESS_DIED). Après redémarrage, ouvrez le **Moniteur de fiabilité** (tapez **fiabilité** dans la recherche Windows) pour retrouver l'incident. Les minidumps (**C:\Windows\Minidump**) conservent les détails utiles pour l'analyse.

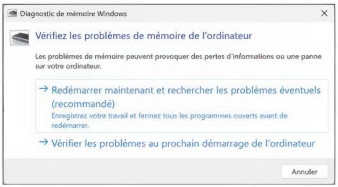
02› METTRE À JOUR WINDOWS ET LES PILOTES

Allez dans **Paramètres > Windows Update > Installez les correctifs**. Via **Gestionnaire de périphériques** : mettez à jour les pilotes essentiels (GPU, chipset, stockage, réseau). Les pilotes graphiques sont parmi les premiers responsables des crashs récurrents.



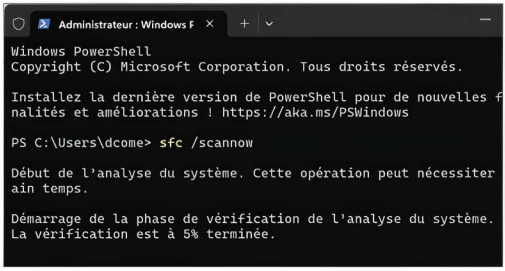
CONSEIL

Parfois, ce sont les périphériques externes qui posent problème. Imprimantes, disques USB, dongles peuvent provoquer un conflit pilote : débranchez tout sauf clavier/souris et testez la stabilité pour identifier, périphérique par périphérique, celui qui provoque ces crashs intempestifs.



03› VÉRIFIER LA MÉMOIRE VIVE (RAM)

Tapez **Diagnostic de mémoire Windows**. Lancez le test (cela implique le redémarrage de votre PC). Si des erreurs apparaissent, testez vos barrettes une par une et remplacez la défectueuse.



04 › RÉPARER LES FICHIERS SYSTÈME

En **Invite de commandes (admin)**, lancez successivement :

sfc /scannow

DISM /Online /Cleanup-Image / RestoreHealth

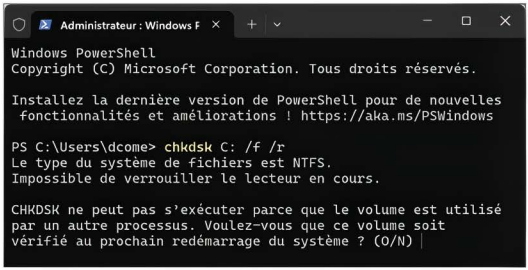
Ces outils corrigent les fichiers Windows corrompus qui provoquent des plantages.

05 › VÉRIFIER LE DISQUE DUR / SSD

Ouvrez encore l'**Invite de commandes (admin)**. Tapez :

chkdsk C: /f /r

Le scan au prochain redémarrage vérifie et répare les erreurs disque.



ASTUCE

Si aucun crash n'apparaît en mode sans échec, cela vous permet de diagnostiquer que le coupable est soit un pilote soit un service tiers. Pour tester le mode sans échec, passez par **Paramètres > Système > Récupération > Démarrage avancé > Redémarrer maintenant**.

06 › DERNIERS RECOURS

Si aucune des solutions précédentes n'a fonctionné, il vous faudra passer par une restauration du système à un point stable. Si les crashs persistent, vous pourrez même réinitialiser votre PC (avec conservation de vos fichiers) en utilisant la Restauration machine rapide (**Lire page 44**).

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

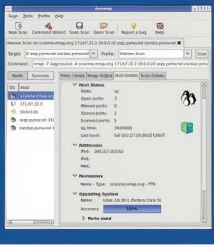
Home Assistant centralise les objets connectés de dizaines de marques (Philips Hue, Xiaomi, Somfy, Shelly, TP-Link, Aqara…) dans une interface unique. Pour l'utilisateur, c'est l'équivalent d'une « tour de contrôle » : on voit quels appareils sont actifs, leur état réseau, leur dernière activité et, 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.

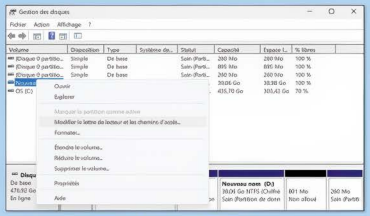
Lien : https://nmap.org

RESTAURER UN SSD/HDD QUI DISPARAÎT APRÈS UNE MISE À JOUR

Après certaines mises à jour (ex : KB5063878), des utilisateurs de Windows 11 signalent la disparition de leur SSD ou disque dur : volumes introuvables, périphériques absents de l'Explorateur. Pas de panique : voici la marche à suivre pour diagnostiquer et récupérer vos données.

01 DISQUE DÉTECTÉ ?

Faites un clic droit sur l'icône du menu **Démarrer > Gestion des disques**. Si le disque apparaît mais sans lettre, assignez-en une (clic droit **> Modifier la lettre de lecteur et les chemins d'accès**). Si le disque est « Non alloué », passez à l'étape 3.



02 GESTIONNAIRE DE PÉRIPHÉRIQUES

Toujours via un clic droit sur l'icône du menu **Démarrer**, allez **à Gestionnaire de périphériques > Lecteurs de disque**. Si le disque est listé avec un ⚠, faites **Mettre à jour le pilote** via un clic droit.

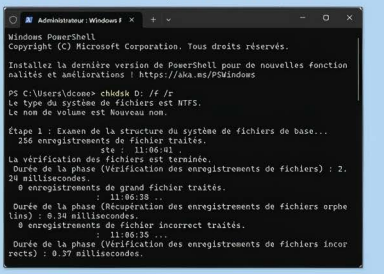
CONSEIL

Si le volume est reconnu comme « Non alloué » ou partition supprimée : vous pouvez aussi utiliser un logiciel de récupération gratuit (ex. TestDisk ou Recuva) pour restaurer la table de partition ou récupérer les fichiers. Sauvegardez sur un autre support avant toute écriture.

03 VÉRIFIER L'INTÉGRITÉ DU DISQUE

Ouvrez l'Invite de commandes (admin) et tapez : **chkdsk X: /f /r**

Remplacez « X » par la lettre du lecteur concerné. Cela répare les erreurs de fichiers et marque les secteurs défectueux.



04 DÉSINSTALLER LA MISE À JOUR

Si le souci est apparu immédiatement après une mise à jour : allez dans **Paramètres > Windows Update > Historique de mise à jour** et descendez jusqu'à **Désinstaller des mises à jour**. Sélectionnez le patch incriminé (ex. KB5063878), redémarrez. Attendez un correctif ultérieur avant de le réinstaller.

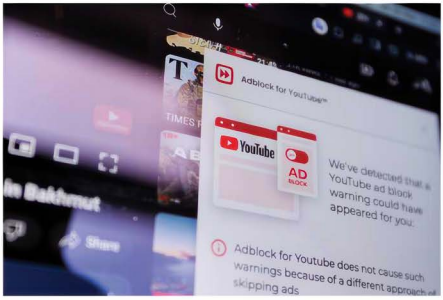
HACKEZ YOUTUBE !

DÉBRIDEZ LA PLATEFORME, VIREZ LES PUBS ET LE PROFILAGE

Mods et clients alternatifs vous donnent accès à YouTube… sans les abus que la plateforme américaine nous impose. Plutôt que de quitter YouTube, et si vous repreniez le contrôle et profitiez, en plus, de fonctionnalités inédites ?

YouTube est devenu insupportable. Et ce n'est pas toi qui as changé. Tu veux regarder un tuto, un concert, une conf tech, un replay… tu te retrouves coincé entre deux pubs non skippables, des pop-ups qui s'énervent contre ton bloqueur, des recommandations qui t'aspirent dans un vortex de contenus que tu n'as jamais demandés, et un pistage permanent greffé à ton compte Google. Depuis 2023, la plateforme a durci la guerre aux adblockers, renforcé ses mécanismes de suivi, et réservé des fonctions de base (lecture en arrière-plan, téléchargement, confort) à YouTube Premium.

YouTube abuse de son hégémonie et multiplie les dérives. Dîtes stop.



Résultat : une partie des utilisateurs – particulièrement les plus geeks, mais aussi un public averti et lassé – a commencé à contourner le problème. Pas en fuyant YouTube, quasi impossible, mais en contournant son interface officielle. C'est là qu'entrent en scène trois familles d'outils :

- **Les mods YouTube :** des versions modifiées de l'appli Android ;

- **Les clients alternatifs :** applications et services indépendants tournés vers la vie privée ;

- **Les apps orientées TV :** qui réinventent l'expérience sur grand écran.

YOUTUBE EST ALLÉ TROP LOIN

Le problème ne se résume plus à "il y a des pubs". Personne ne s'étonne qu'un service gratuit se finance. Ce qui crispe, c'est le combo de tout ce qu'il y a de plus détestable en termes de marchandisation de votre attention. La saturation publicitaire est devenue la règle, plus l'exception : coupures multiples, formats intrusifs, répétition, placement au milieu des vidéos longues. Le traçage systématique s'est développé à l'image d'une pieuvre : historique, temps de visionnage, centres d'intérêt, appareil, localisation approximative, comportements croisés avec tout l'écosystème Google. Face à TikTok, le géant américain utilise désormais les mêmes armes délétères pour vous rendre accrocs et si possible débiles : recommandations infinies, Shorts omniprésents, algorithme qui pousse ce qui retient plutôt que ce qui intéresse. Enfin, la pression anti-bloqueurs vous transforme en criminels : messages d'alerte, limitation de lecture pour ceux qui osent filtrer.

PEUT-ON PROFITER DE YOUTUBE SANS YOUTUBE ?

En même temps, la position ultra-hégémonique de YouTube le rend incontournable et c'est ce qui autorise la plateforme à toutes ces dérives. Mais sachez que vous pouvez profiter de YouTube sans accepter le package complet pub + tracking + contraintes Premium. Derrière les termes « Mods » et « Alternatives Front-end » se cachent des projets qui vous donnent accès aux vidéos YouTube, aux chaînes auxquelles vous êtes abonnés, aux mêmes fonctions… mais en court-circuitant la machine à vampiriser. Attention, chacune de ses solutions s'accompagne de compromis, de risques, et de zones grises juridiques. C'est précisément ce qu'on va démêler.

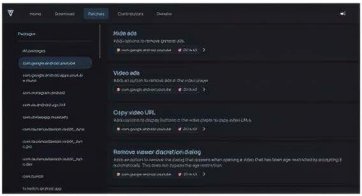
MODS YOUTUBE : LA CHIRURGIE LOURDE SUR L'APPLI OFFICIELLE

Les "mods" YouTube sont les plus spectaculaires, les plus puissants, et les plus sensibles. L'idée est simple à résumer, plus complexe à assumer : on prend l'appli YouTube officielle Android, on la patch, on retire ce qui gêne, on ajoute ce qui manque.

Dans la pratique, ces mods peuvent supprimer la publicité, autoriser la lecture en arrière-plan, intégrer SponsorBlock pour zapper les segments sponsorisés, forcer certains réglages vidéo, nettoyer l'interface, etc. Mais ils le font en contournant les règles du service. Et YouTube est bien décidé à avoir leur peau.

REVANCED : L'HÉRITIER ASSUMÉ DE VANCED

ReVanced est le nom qui revient partout. Contrairement à Vanced à l'époque, il ne distribue pas une app toute faite, mais des patches open source et un Manager permettant de modifier toi-même l'APK officiel de YouTube. En langage simple : tu télécharges YouTube, tu appliques ReVanced par-dessus, et tu obtiens un YouTube propre et dépollué !



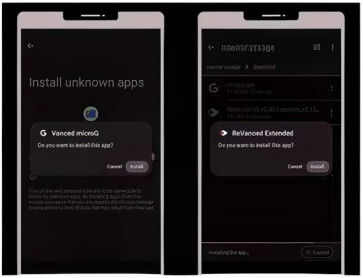
C'est l'approche la plus transparente et la plus propre techniquement. Mais le cadre reste le même : tu modifies une appli propriétaire et, tu bloques la monétisation, tu t'éloignes des conditions d'utilisation de Google.

Lien : https://revanced.app/

REVANCED EXTENDED : LE MOD DE CEUX QUI MODDENT LES MODS

Pour les plus extrêmes, ReVanced Extended pousse plus loin : plus d'options, intégration avec Magisk, réglages fins, tweaks en profondeur. C'est l'outil de ceux qui considèrent Android comme un terrain de jeu intégral. C'est puissant, mais c'est clairement un monde pour utilisateurs avancés : root, Zygisk, contournements plus agressifs. Et donc une règle d'or : si tu ne comprends pas ce que tu actives, tu ne joues pas avec.

Lien : https://github.com/NoName-exe/revanced-extended

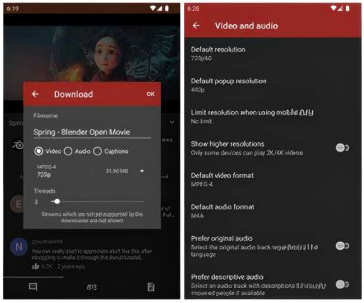


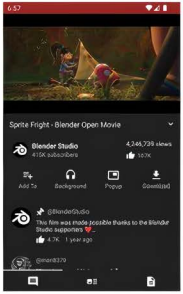
CLIENTS ALTERNATIFS : YOUTUBE FILTRÉ, PROXIFIÉ, DÉGOOGLISÉ

Autre approche, plus élégante : ne pas toucher à l'appli officielle, mais changer de porte d'entrée. Les clients alternatifs n'essaient pas de "pirater" YouTube, ils servent d'interface entre toi et la plateforme. C'est simplissime : l'utilisateur ouvre l'app ou le site alternatif, il se charge de récupérer la vidéo, et d'afficher le contenu demandé. Il peut y avoir quelques pubs et scripts de tracking mais de façon non abusive et surtout transparente, sans obligation de se connecter à son compte Google.

NEWPIPE : LE YOUTUBE MINIMALISTE DES APPAREILS DÉGOOGLISÉS

Sur Android, NewPipe est devenu une petite institution. Open source, léger, il lit YouTube sans Google Play Services, sans traçage invasif, sans compte obligatoire. L'utilisateur peut s'abonner, créer des listes, suivre des chaînes, télécharger localement des vidéos et de l'audio (toujours avec la question légale selon les contenus), limiter les permissions au strict nécessaire.



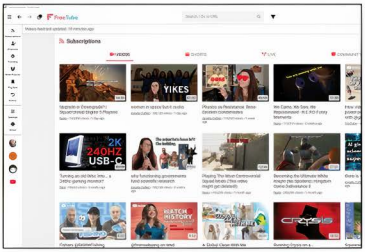


C'est l'outil rêvé des smartphones dégooglisés, des ROM custom, des lecteurs exigeants qui veulent juste... regarder des vidéos sans être aspirés. En contrepartie, pas de commentaires postés, pas de sync avec ton vrai compte Google, et parfois quelques bugs lorsque YouTube change de mécanique interne.

Lien : https://newpipe.net/

FREETUBE : LA MÊME PHILOSOPHIE SUR PC

Côté ordinateur, FreeTube applique la même logique : un client desktop open source qui te permet de naviguer sur YouTube comme d'habitude, mais en gardant l'historique et les abonnements en local, sans exposer ton profil à Google. C'est sobre, efficace, parfait pour les gros consommateurs qui veulent un environnement dédié, scriptable,



contrôlable. Là encore, il faut accepter les limites : si YouTube change certaines briques, il faut attendre la mise à jour.

Lien : https://freetubeapp.io/

INVIDIOUS / PIPED : YOUTUBE VIA UN PROXY (OU TON PROPRE SERVEUR)

Dernière famille : Invidious et Piped, des frontends web. Vous continuez de regarder YouTube, mais depuis un autre domaine, qui agit comme intermédiaire filtrant. Les utilisateurs avertis peuvent même héberger leur propre instance sécurisée avec, à la clé, la possibilité de contrôler les logs. C'est très séduisant sur le papier. Mais sur les instances publiques, il faut rappeler une chose simple : tu fais confiance à un proxy intermédiaire qui voit tout ce que tu fais. Avant, c'était YouTube.

Liens :

> Invidious : https://invidious.io/

> Piped : https://github.com/TeamPiped/Piped

MODS ORIENTÉS TV : REPRENDRE LE CONTRÔLE DU SALON

Sur le téléviseur, la frustration est encore plus visible : YouTube officiel sur Android TV ou sur certaines box, c'est l'autoroute à pubs. Tu es loin du clavier, sans bloqueur, captif. C'est là qu'intervient un acteur aujourd'hui incontournable : SmartTube.

SmartTube (ex-SmartTubeNext), c'est un client non officiel pour Android TV et box qui s'installe via une APK. L'objectif :offrir YouTube sans pubs, avec une vraie ergonomie TV, et un contrôle poussé de la qualité, des codecs, des réglages. C'est fluide, souvent bluffant. Mais comme pour les autres solutions non officielles, le message doit rester clair : puisque cette application n'est pas approuvée par Google, elle pourrait un jour disparaître et, pour des raisons de sécurité, il faut toujours télécharger son APK depuis le site et GitHub officiels.

Lien : **https://smarttubeapp.github.io/**

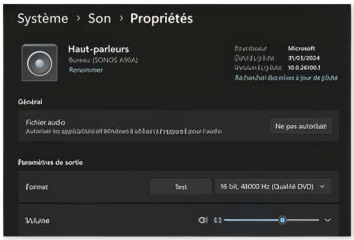
TUTO

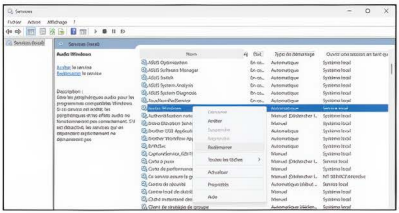
CORRIGEZ LE SON ABSENT SUR WINDOWS 11

Plus de son dans les haut-parleurs ou le casque ? C'est l'un des problèmes les plus fréquents de Windows 11. Mauvais périphérique par défaut, pilote audio défectueux ou service bloqué peuvent être en cause.

01 › PÉRIPHÉRIQUE DE SORTIE

Faites un clic droit sur l'icône du volume dans la barre des tâches, en bas droite. Passez par **Paramètres audio**. Dans **Choisissez l'emplacement de lecture**, sélectionnez votre périphérique (ex. Haut-parleurs Realtek, Casque Bluetooth, etc.). Cliquez sur ce périphérique et testez avec le bouton **Test** pour vérifier la sortie.



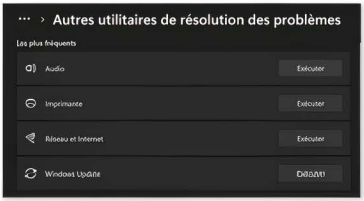


02 › RELANCER LE SERVICE AUDIO

Appuyez sur **Win + R**, tapez **services.msc** puis **Ok**. Trouvez **Audio Windows**. Vérifiez qu'il est en cours d'exécution et en mode **Automatique**. Si besoin, clic-droit et faites **Redémarrer**.

03 › PILOTE AUDIO

Appuyez sur **Win + X** et allez dans **Gestionnaire de périphériques**. Ouvrez **Contrôleurs audio, vidéo et jeu**. Clic droit sur votre carte son et choisissez **Mettre à jour le pilote**. Si ça ne change rien : passez par **Désinstaller l'appareil** puis redémarrer (Windows réinstalle le pilote automatiquement).



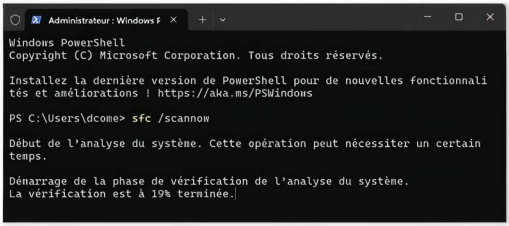
04 › DÉPANNEUR AUDIO INTÉGRÉ

Allez dans **Paramètres > Système > Résolution des problèmes > Autres utilitaires**. Cliquez sur **Audio > Exécuter**. L'outil corrige automatiquement des paramètres erronés ou redémarre les composants audio.

05 › PÉRIPHÉRIQUES EXTERNES

Pour un casque Bluetooth : supprimez et réassociez l'appareil (**Paramètres > Bluetooth**).

Pour un écran HDMI/DisplayPort : vérifiez que la sortie **Haut-parleurs HDMI** est sélectionnée.



06 › DERNIER RECOURS

Exécutez en **Invite de commandes (admin)** :

sfc /scannow

DISM /Online /Cleanup-Image /RestoreHealth

Si le problème persiste, envisagez une restauration système ou l'utilisation de **Récupération machine rapide** (**lire page 44**).

TUTO

CASTEZ ET/OU CAPTUREZ VOTRE ÉCRAN EN NAVIGATION PRIVÉE

Caster son écran (ou faire une simple capture d'écran) est par défaut impossible sur Android en navigation privée. Comment désactiver cette protection pour diffuser sur tous vos écrans sans renoncer au mode incognito ?

En mode navigation privée / Incognito, Firefox et Chrome activent un flag Android appelé FLAG_SECURE sur la fenêtre privée. Ce flag dit au système : tu n'as pas le droit de faire des captures d'écran, enregistrer l'écran ou afficher ce contenu sur un écran non sécurisé (cast/mirroring). Résultat : captures bloquées, écran noir en mirroring ou cast, même si le reste du téléphone est visible. L'objectif n'est pas de vous embêter, mais de protéger des données sensibles : recherche perso, comptes, contenus potentiellement confidentiels ou professionnels, et d'éviter qu'une appli tierce, une TV partagée ou un service distant ne puisse enregistrer ces pages à votre insu.

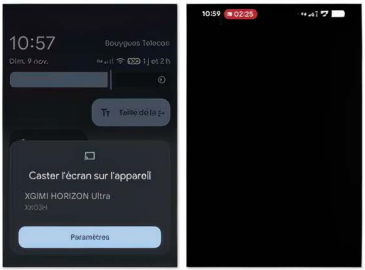
Il s'agit d'une protection Android par défaut qui a son intérêt… mais qui se trouve être très limitante quand l'utilisateur est en mode privé mais souhaite tout de même faire des captures d'écran ou diffuser son contenu sur une TV, un projecteur, etc. depuis son téléphone ou sa tablette.

> Outre une protection de vos métadonnées et de vos historiques, la navigation privée bloque aussi par défaut les possibilités de cast, de mirroring, d'enregistrements ou de capture d'écran.

ÉCRAN NOIR

En mode Cast ou Mirroring, l'écran du navigateur apparaîtra noir (ou flouté) sur l'écran tiers (alors que le reste de l'écran du téléphone ou les autres applications sont, eux, bien visibles.

Tant que ce flag est actif, aucune appli de mirroring et de cast classique ne pourra afficher l'onglet privé. Idem pour les captures d'écran ! Heureusement, sur Firefox, il est possible de désactiver facilement cette protection. Sur Chrome, cela dépendra de votre appareil.



EN MODE PRIVÉ, TOUTE TENTATIVE DE CAST SE SOLDE PAR UN ÉCRAN NOIR.

CAST/SCREENSHOT EN NAVIGATION PRIVÉE AVEC FIREFOX

PRATIQUE

01 › PARAMÈTRES

Ouvrez Firefox, passez par le Menu puis **Paramètres > Navigation privée**. Activez **Autoriser les captures d'écran en navigation privée**. Fermez puis réouvrez Firefox.

02 › FLAG SECURE DÉSACTIVÉ

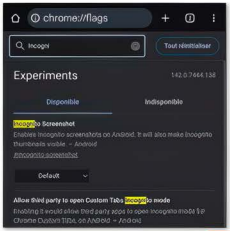
Revenez en navigation privée sur la page désirée. Ce réglage retire le FLAG_SECURE et permet désormais les captures, l'enregistrement et le mirroring/cast (hors contenus protégés type DRM vidéo ou sécurisation du site lui-même, comme pour une banque).

CAST/SCREENSHOT EN NAVIGATION INCOGNITO AVEC CHROME

PRATIQUE

01 › TROUVER LE FLAG

Par défaut, le mode Chrome Incognito bloque lui aussi les captures d'écran et la diffusion cast. Dans la barre d'adresse de Chrome, tapez **chrome://flags** puis **Entrée**. Cherchez **Incognito Screenshot**.

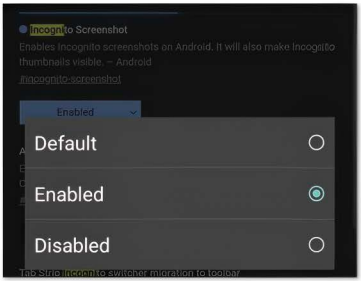


À SAVOIR

Sur un téléphone Android sans surcouche, cette astuce fonctionne parfaitement. Mais selon la marque de votre mobile ou tablette, vous n'aurez peut-être pas accès à ce flag.

02 › DÉSACTIVER

Passez-le en **Enabled** puis cliquez sur **Relancer**. Après avoir redémarrer Chrome, le nouveau paramètre doit être activé. Allez dans une fenêtre en navigation privée et testez.

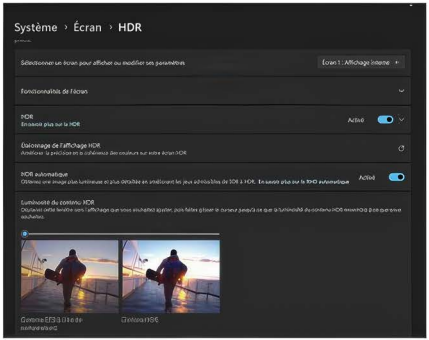


Capturer une vidéo de jeu
> Avec Xbox Game Bar

Enregistrer vos parties sans installer OBS ou d'autres logiciels lourds peut sembler compliqué. Sachez que la Xbox Game Bar, préinstallée sur Windows 11, permet d'enregistrer votre écran pendant les jeux, de prendre des captures et d'accéder à un mini tableau de bord de performance. Appuyez sur **Windows + G** pour ouvrir la barre, cliquez sur le bouton **Enregistrer** (ou **Windows + Alt + R** pour un raccourci direct). Par défaut, vos vidéos sont enregistrées dans **Vidéos > Captures**.

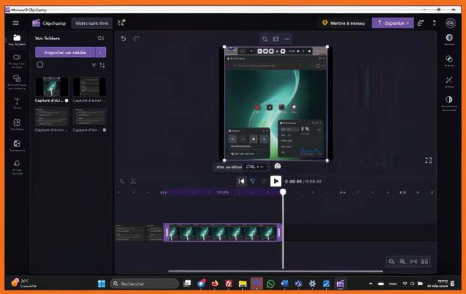
Activer le HDR automatique
> Pour booster l'image des vidéos et jeux

Même avec un bon écran, les couleurs semblent ternes dans certains jeux ou vidéos. Windows 11 peut activer automatiquement le HDR (plage dynamique étendue) sur les écrans compatibles. Cela vous apportera une meilleure luminosité, des contrastes renforcés ainsi que des noirs plus profonds dans les contenus compatibles. Attention, certains (dont nous faisons partie) trouvent que le HDR est génial pour les jeux mais enlève aussi un grain et une identité graphique à de nombreux films. A magner avec précaution donc. Allez dans **Paramètres > Système > Écran.** Activez le **HDR** et **HDR Automatique** si vous souhaitez que les contenus compatibles soient traités sur ce mode sans intervention manuelle de votre part. Fans les options, vous pourrez même calibrer votre HDR pour un rendu plus personnalisé.



Créer un diaporama photo avec musique
> Depuis l'application Photos

Vous voulez faire une vidéo souvenir avec vos photos et musiques sans installer de logiciel complexe. L'application native **Photos** de Windows permet de créer facilement des diaporamas animés avec fond sonore, titres, transitions, effets. Ouvrez **Photos. Sélectionnez les photos de votre choix puis** cliquez sur **l'icône Créer une vidéo en haut de l'interface**. La solution ClipChamp s'ouvre et vous permettra d'ajouter musique, effets, transition, etc. grâce à une interface de montage simplifiée. Exportez la vidéo dans le format souhaité une fois que vous êtes satisfait !

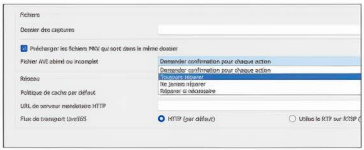


Télécharger une vidéo Facebook ou Insta — Avec SnapSave

Impossible de regarder une vidéo sans connexion ? Certaines plateformes ne proposent pas de téléchargement. SnapSave vous permet de télécharger gratuitement des vidéos de Facebook ou Instagram en MP4 ou MP3. Parfait pour une vidéo de cuisine, un tutoriel ou une musique à regarder hors ligne. Allez sur **https://snapsave.app/fr** et collez l'URL de la vidéo choisie. Choisissez la qualité ou audio seul puis cliquez tout simplement sur **Télécharger**.

Améliorer la lecture d'un fichier vidéo corrompu > Avec VLC Media Player

Une vidéo refuse de s'ouvrir ou plante régulièrement pendant la lecture ? VLC, lecteur libre et gratuit, propose une fonction de réparation automatique des fichiers AVI, en plus de lire quasiment tous les formats et de lire un certain nombre de



fichiers incomplets ou mal encodés. Ouvrez votre vidéo AVI avec VLC. Si une alerte apparaît, choisissez **Réparer**. Réglez ce comportement par défaut dans Outils > **Préférences > Entrée/Codecs.** Dans le menu déroulant **Fichier AVI abîmé ou incomplet**, vous pouvez choisir **Toujours réparer** ou **Réparer si nécessaire.**

Lien : www.videolan.org/vlc/

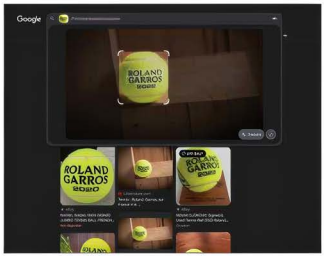
Ajouter des sous-titres à vos vidéos > Avec Kapwing

Kapwing propose d'ajouter manuellement ou automatiquement des sous-titres à n'importe quelle vidéo via une interface intuitive. La version gratuite permet de traiter des vidéos de maximum 4 minutes. Idéal pour vos vidéos YouTube, stories ou contenus pédagogiques. Allez sur **www.kapwing.com/tools/subtitles** et importez votre vidéo. Cliquez sur **Générer automatiquement** ou **ajoutez les textes manuellement**. Exportez enfin votre vidéo avec les sous-titres incrustés.

Retrouver l'origine d'une image en ligne > Avec Google Images (Recherche inversée)

Vous avez trouvé une image intrigante (personne, lieux, produit) mais ne connaissez ni son auteur, ni son contexte ? La recherche inversée d'images de Google permet d'identifier la source d'une photo, ses déclinaisons, ou les sites où elle a été publiée. Pour lancer votre recherche, cliquez sur l'icône de l'appareil photo dans la barre de recherche, collez l'URL de l'image ou importez un fichier puis consultez les résultats similaires ou exacts. N'oubliez pas d'utiliser la fonction de cadrage pour identifier une personne ou un produit spécifique sur une image plus large !

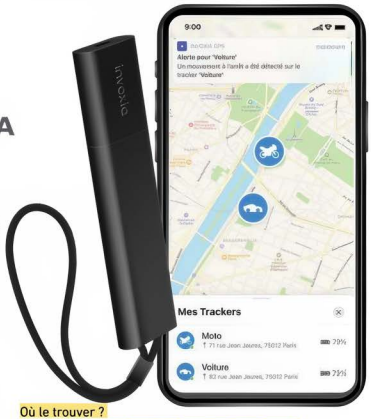
Lien : https://images.google.com



Invoxia Tracker GPS Classic Edition 2026

UN VRAI TRACKER GPS ANTIVOL... QUI VA JUSQU'AU BOUT ?

ON LE POSE DANS UN COIN, ON L'OUBLIE... JUSQU'AU JOUR OÙ IL SAUVE UNE MOTO À 8 000 €, UN FOURGON PRO OU UN SAC PHOTO. LE TRACKER GPS CLASSIC EDITION 2026 D'INVOXIA EST EXACTEMENT PENSÉ POUR CE SCÉNARIO : UN OUTIL DISCRET, À LARGE AUTONOMIE, SANS CARTE SIM ET EXPLOITABLE PAR LES FORCES DE L'ORDRE OU VOTRE ASSURANCE.



Où le trouver ?
www.invoxia.com/product/gps-tracker-classic

Le nouvel Invoxia est un traceur pensé pour les vols réels, les assurances réelles, les procédures réelles. On le cache au fond d'une selle, derrière une garniture de coffre, dans la doublure d'un sac photo. On l'oublie. Et c'est précisément le rôle du Tracker GPS Classic Edition 2026 d'Invoxia : rester silencieux pendant des semaines, voire des mois, jusqu'au moment où quelqu'un d'autre décide de partir avec ce qui vous appartient. Là, il se réveille, documente, alerte, et vous donne enfin quelque chose de concret à opposer à la phrase terrible : « Désolé, sans piste, on ne peut rien faire. »

Pour cette édition 2026, Invoxia ne joue pas la révolution, mais l'ajustement intelligent. Le constructeur français prend son best-seller historique et le met au niveau des usages réels : le boîtier est désormais certifié IP67 et supporte la pluie, l'humidité, les motos qui dorment dehors, les coffres humides et les valises malmenées. Il abandonne bien sûr le micro-USB pour l'USB-C. L'objet reste fin, discret, suffisamment long pour être calé dans une cavité, suffisamment neutre pour disparaître. Seul bémol : pas de système de fixation prévu pour l'installer sur des parties mécaniques avec sangles ou attaches autobloquantes.

TARIFS

99 € : tracker + 1 an de connexion réseau inclus.
129 € : pack avec 3 ans de connexion
Au-delà de la période incluse : env. **4,45 €/mois**, ou **29,95 €/an** ou formule longue durée à **49,95 € pour 3 ans**.

AUTONOMIE CONTRE TEMPS RÉEL

Sous la coque, la recette reste fidèle à l'ADN de la marque : une combinaison de GPS, Wi-Fi et Bluetooth pour déterminer la position, et un envoi des données via les réseaux basse consommation type LoRa/Sigfox dans les pays couverts. Ce choix technique est assumé. On n'est pas sur un boîtier 4G/5G alimenté en permanence et qui remonte sa position toutes les dix secondes : on est sur un traceur pensé pour durer plusieurs

« INVOXIA NE REPART PAS DE ZÉRO : LE CLASSIC EDITION 2026 EST L'ÉVOLUTION DE SON TRACEUR BEST-SELLER, AVEC TROIS PROMESSES CLAIRES : MIEUX RÉSISTER AU TERRAIN (ÉTANCHÉITÉ IP67 ET COQUE PLUS ROBUSTE ; PAS DE CARTE SIM À GÉRER ; RENDRE L'ANTIVOL EXPLOITABLE EN VRAI (MODE PERDU, DOSSIER DE VOL, RADAR DE PROXIMITÉ).

CARACTÉRISTIQUES

Dimensions : 105 × 27 × 9,5 mm

Poids : 27 g

Étanchéité : certification IP67 (résistant à la poussière et à l'immersion courte)

Localisation : combinaison GPS + Wi-Fi + Bluetooth ; transmission via réseaux basse consommation (LoRa / Sigfox) dans les pays couverts, sans carte SIM.

Autonomie : jusqu'à 6 mois selon la fréquence de relevés et l'usage (modes réglables, mode intensif en cas de vol).

Recharge : port USB-C

Fonctions clés : historique des trajets, alertes de mouvement et de sortie de zone, mode Perdu (suivi intensif), radar de proximité, sonnerie, génération d'un dossier de vol (rapport + QR code pour police/assureur), IA d'analyse de mouvements.

Compatibilité : application Invoxia GPS sur Android & iOS, gestion multi-traceurs depuis un même compte.

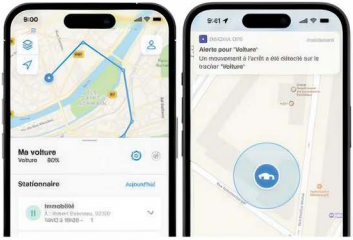
mois sur batterie, avec des points réguliers, configurables, suffisants pour suivre un véhicule volé, un deux-roues déplacé ou un bagage égaré sans vider la batterie en trois jours. C'est ce compromis – autonomie contre "temps réel absolu" – qui fait l'intérêt du Classic 2026, mais aussi sa principale limite selon l'usage qui est recherché.

UN GOÛT D'INACHEVÉ

C'est le jour où quelque chose cloche que la différence apparaît : le Classic 2026 sait détecter un mouvement suspect, un déplacement hors zone, un changement d'inclinaison d'une moto ou d'un véhicule, et envoyer des alertes suffisamment rapides pour que l'utilisateur réagisse sans passer sa nuit à rafraîchir une carte. Le fameux "Mode Perdu" pousse la fréquence de localisation lorsque le bien est en mouvement, tout en espaçant les relevés lorsqu'il est immobile, histoire d'économiser la batterie au bon moment. L'idée n'est pas de jouer à l'enquêteur en temps réel sur une carte façon film, mais de fournir un fil solide, cohérent, exploitable. Cependant, les utilisateurs seront déçus par la sonnerie intégrée, utile pour retrouver le traceur à bout portant une fois localisé. Elle s'avère être relativement discrète : une fois l'appareil bien planqué, ce n'est pas un beeper de chantier. Si votre bien volé se retrouve à l'abri de murs épais, pas sûr que votre oreille détecte la sonnerie de l'Invoxia pour franchir les derniers mètres de localisation exacte !

UN VRAI ANTIVOL, PAS UN TRACKER ESPION

Par contre, Invoxia a compris un point que beaucoup de produits concurrents ignorent : un bon traceur ne sert pas qu'à "voir sur son téléphone où est la voiture". Il doit servir à prouver, à partager, à enclencher une procédure. Le Classic Edition 2026 propose ainsi un "dossier de vol" : un rapport structuré avec historique, dernières positions et QR code, conçu pour être transmis aux forces de l'ordre et à l'assurance après dépôt de plainte. L'idée est simple, mais redoutablement pertinente : transformer un flux de données techniques en pièce exploitable dans un contexte légal.



Ce tableau reste là aussi imparfait. En pratique, le Classic 2026 dépend toujours de la qualité de couverture des réseaux bas débit : excellente sur de larges zones urbaines et axes principaux, plus incertaine dans certains environnements ruraux ou industriels isolés. Invoxia promet une compatibilité multi-pays en Europe, mais on n'est pas sur une solution "je traverse le monde sans me poser de questions". L'autre réserve tient à la promesse d'"IA embarquée" : officiellement, elle sert à mieux distinguer un déplacement anodin d'un comportement suspect. La communication reste assez opaque et rien ne permet de mesurer objectivement l'apport de cette "IA" par rapport à de bons algorithmes de détection classiques.

UN SUPER RAPPORT QUALITÉ/PRIX À L'USAGE

Reste l'aspect tarifs et coûts réels du produit : face à la concurrence, Invoxia fait le choix de la clarté, ce qui est suffisamment rare pour être mentionné. Le Tracker GPS Classic Edition 2026 est lancé à 99 € avec un an de service inclus, ou 129 € avec trois ans inclus. Au-delà de cette période, l'abonnement réseau est annoncé à 4,45 € par mois, 29,95 € par an ou 50 € pour trois ans, des montants qui restent raisonnables au regard du service rendu et du fait qu'il n'y a pas de carte SIM à gérer soi-même.

MONIMOTO 9 : eSIM POUR PLUS DE POSSIBILITÉS

Spécialiste du tracker GPS pour motos, MoniMoto propose des produits solides, étanches, précis et faits pour durer. Contrairement au l'Invoxia, son MiniMoto 9 dispose d'attaches de serrage pour le fixer discrètement sur des parties peu visibles du bien à protéger. Surtout, il dispose d'une carte eSIM internationale tout en annonçant 12 mois d'autonomie ! En plus du GPS, Monimoto peut aussi utiliser les technologies GLONASS et Telit IoT LOCATE en intérieur si ce dernier n'est pas disponible. Un badge à porter sur soi permet d'activer/désactiver le tracker à votre approche. Côté prix, le MoniMoto 9 est un peu plus cher que le Invoxia : 169 euros avec deux mois d'abonnement offerts (puis 39 € / an).

Où le trouver : **https://monimoto.com/fr**

SÉLECTION

TOP 15 Logiciels & services GRATUITS

TOP5 MOTEURS DE RECHERCHE ÉTHIQUES

DUCKDUCKGO

> Le champion de l'anti-traçage

DuckDuckGo a bâti sa réputation sur une promesse simple : ne jamais collecter ni enregistrer vos recherches. Il combine ses propres index, des données provenant de partenaires (dont Bing) et des intégrations intelligentes pour enrichir ses réponses. Les résultats sont débarrassés du "sur-ciblage" publicitaire : aucune annonce ne semble influencée par un historique passé.

Lien : https://duckduckgo.com

STARTPAGE > Les résultats de Google, sans Google

Startpage agit comme un intermédiaire : elle envoie la requête à Google pour vous, récupère les résultats et les affiche en supprimant tous les identifiants potentiels, y compris l'adresse IP. C'est un moteur idéal pour les utilisateurs qui apprécient la qualité des réponses de Google mais refusent son modèle de profilage. Startpage affiche des publicités, mais celles-ci sont contextuelles, jamais basées sur un historique.

Lien : www.startpage.com

MOJEEK > L'outsider indépendant

Mojeek est une exception rare : il possède son propre index, constitué de plusieurs milliards de pages analysées tout en insistant sur son indépendance technologique et éthique : pas de traçage, pas de personnalisation, pas de cookies. Les résultats sont bruts mais Mojeek expose des pages pertinentes sur des sujets spécialisés que d'autres moteurs ignorent. Mojeek est moins performant sur l'actualité ou les questions pratiques.

Lien : www.mojeek.com

QWANT > L'alternative européenne

Qwant veut offrir une alternative européenne aux géants américains. Sa promesse est claire : pas de cookies publicitaires, pas de traçage, pas de personnalisation. Chaque utilisateur obtient donc les mêmes résultats. Son interface est moderne et ses résultats pertinents. Qwant reste toutefois dépendant partiellement d'index externes (notamment Bing) pour certaines catégories.

Lien : www.qwant.com

BRAVE SEARCH > La recherche privée qui monte

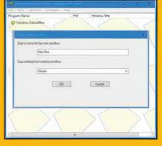
Issu du navigateur Brave, Brave Search ambitionne d'être un moteur indépendant et 100 % privé, avec son propre index alimenté par une infrastructure mondiale. Son mode "Indépendance score" indique quelle proportion des résultats provient de son propre index, un marqueur rare de transparence. Brave Search ne collecte pas de données personnelles, et ses publicités — lorsqu'elles sont activées — restent anonymisées.

Lien : https://search.brave.com

TOP5 TESTER SANS INSTALLER

SANDBOXIE PLUS

> Le bac à sable grand public

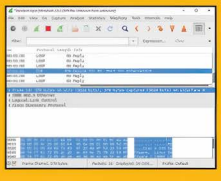


Sandboxie Plus crée une bulle isolée où lancer n'importe quel logiciel sans risquer d'altérer Windows. Idéal pour tester un programme ou visiter un site douteux : tout reste confiné et disparaît à la fermeture. Simple, rapide et gratuit, c'est la sandbox la plus accessible pour un usage quotidien.

Lien : https://sandboxie-plus.com/

FIREJAIL

> L'arme légère des utilisateurs Linux



Firejail isole les applications sous Linux grâce aux namespaces et aux profils préconfigurés. Navigateurs, messageries ou lecteurs PDF fonctionnent dans un espace restreint, sans accès aux dossiers sensibles. Léger, puissant et simple, c'est un incontournable pour sécuriser Linux.

Lien : https://firejail.wordpress.com

TOP5 OPEN DATA À LA FRANÇAISE !

DATA.GOUV.FR

> Le portail central de l'État

Portail central de l'État français, Data.gouv.fr rassemble plus de 40 000 jeux de données publics : santé, économie, transports, environnement, cartographie… La plateforme est devenue un outil clé pour comprendre la société française grâce à ses visualisations simples et ses jeux de données bruts réutilisables. On peut y créer ses propres tableaux de bord et suivre l'évolution d'indicateurs essentiels.

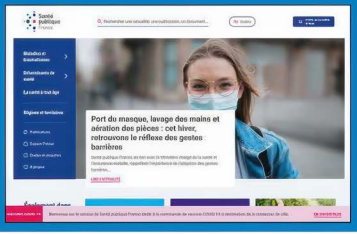
Lien : www.data.gouv.fr

SANTÉ PUBLIQUE FRANCE

> Comme son nom l'indique

Santé publique France ouvre un accès unique à des milliers d'indicateurs santé : maladies, pollution, vaccinations, mortalité, comportements à risque. Sa plateforme GEODES permet de visualiser ces données sur des cartes interactives, jusqu'à l'échelle locale. Un outil fiable, mis à jour et fondé sur des sources scientifiques validées.

Lien : www.santepubliquefrance.fr



OPEN DATA

> Paris, Lyon, Marseille, Rennes…

De nombreuses métropoles françaises disposent de leurs propres portails Open Data. Paris est la plus riche : mobilités, pollution, équipements, urbanisme, culture, consommation énergétique, stationnement, délibérations du Conseil… Ces portails locaux sont souvent plus concrets que les grandes plateformes nationales.

Lien Paris : https://opendata.paris.fr

INSEE > Les chiffres de la France à la source

Démographie, économie, emploi, prix, territoires, entreprises : l'INSEE met gratuitement à disposition l'ensemble de ses indicateurs, bases de données et publications. C'est la référence absolue pour comprendre le pays, alimenter un projet professionnel, ou analyser des tendances locales avec rigueur.

Lien : www.insee.fr

OCDE / EUROSTAT / WORLD BANK

> Institutions internationales

Ces trois plateformes donnent accès à des données premium : PIB, commerce, fiscalité, innovation, éducation, comparatifs pays, projections économiques… Elles complètent parfaitement les portails français en élargissant l'horizon aux comparaisons internationales.

Liens : https://data.oecd.org ; https://ec.europa.eu/eurostat ; https://data.worldbank.org/

WINDOWS SANDBOX

> Le laboratoire intégré à Windows 10/11 Pro

Intégré à Windows 10/11 Pro, Windows Sandbox ouvre un mini-système vierge, totalement séparé du PC. On peut y installer et tester des logiciels suspects en toute sécurité : au redémarrage, tout s'efface. Aucun réglage complexe, mais réservé aux éditions Pro/Entreprise.

CUCKOO SANDBOX

> Le microscope des fichiers suspects

Cuckoo analyse en profondeur le comportement d'un fichier dans une machine virtuelle : réseau, registre, fichiers créés, processus suspects. Plus technique, mais parfait pour comprendre si un logiciel est malveillant. Gratuit, open source, très utilisé en analyse de malware.

Lien : https://cuckoosandbox.org/

SHADOW DEFENDER

> Le "mode fantôme" qui protège tout un système

Shadow Defender place tout Windows en "mode fantôme" : installations, fichiers et réglages disparaissent au redémarrage. Parfait pour tester des programmes risqués sans conséquence. Très simple à utiliser, sa version d'essai totalement fonctionnelle suffit pour un usage gratuit.

Lien : www.shadowdefender.com

 # Casser les codes et décrypter l'info #

JE M'ABONNE à PIRATE INFORMATIQUE

LIVRAISON SOUS PLI DISCRET

OFFRE ABONNEMENT

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

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

- LIVRÉ CHEZ VOUS !
- PRATIQUE & ÉCONOMIQUE !

LES GUIDES du HACKER et du PIRATE

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

À DÉCOUPER (OU À PHOTOCOPIER), À COMPLÉTER ET À RENVOYER SOUS ENVELOPPE AFFRANCHIE À :
BII - SERVICE ABONNEMENT - 15, RUE DE MERY - 60420 MÉNÉVILLERS

☐ **Abonnement à Pirate Informatique pour 4 numéros, je joins mon règlement de 19,90 €**
☐ **Abonnement à Pirate Informatique pour 8 numéros, je joins mon règlement de 35,40 €**

☐ OUI, JE M'ABONNE :

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

☐ Je joins mon règlement par chèque à l'ordre de ID PRESSE (France uniquement)
Offre valable en France métropolitaine uniquement.

POUR NOUS CONTACTER :
abonnement.bii@gmail.com

Signature obligatoire :

Offre valable jusqu'au 31 décembre 2025. Les délais d'acheminement de La Poste varient selon les régions et pays. Conformément à la loi Informatique et Libertés du 6/1/1978, vous disposez d'un droit d'accès et de rectification quant aux informations vous concernant, que vous pouvez exercer librement auprès de ID PRESSE - 1104, CHEMIN DE LA BATTERIE - 13500 MARTIGUES

RÉDUCTION JUSQU'À -25%

LES AVANTAGES :

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

LES DOSSIERS DU

Pirate

DES DOSSIERS THÉMATIQUES COMPLETS

À DÉCOUVRIR EN KIOSQUES

PETIT FORMAT

MINI PRIX

CONCENTRÉ D'ASTUCES

100% Windows

Actuellement #Guide pratique

LE GUIDE 2026 DU HACKER

ARNAQUES

YOUTUBE

PERFORMANCES

ANONYMAT

ChatGPT

MESSAGERIES

BitTorrent

CONFIDENTIELS

OBJETS CONNECTÉS

PIRATE
INFORMATIQUE

IDPRESSE id presse
L 12730 - 66 - F: 5,90 € - RD

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