WINDOWS
MACOS
ANDROID
LINUX
IOS

LE MAGAZINE DU NUMÉRIQUE

01NET

HIVER 2024 - HORS-SÉRIE 141

NUMÉRO SPÉCIAL

ÉDITION 2025

LE GRAND GUIDE DE LA SÉCURITÉ

RANSOMWARES
PIRATAGE
VIRUS
PHISHING
MOTS DE PASSE
DONNÉES PERSONNELLES

Protégez votre PC et votre vie privée

+ 40 ASTUCES INDISPENSABLES

pour Windows, Android, internet, macOS, iOS...

Dom : 7 € - Belux : 6,5 € - Ch : 10,6 FS
Can : 10,99 $ca - Port Cont : 6,9 €
Mar : 68 Dh - Tun : 9,9 Tnd

CPPAP L 15053 - 141 H - F : 5,90 € - RD

Jamais vu ça

-5 €/mois et par plateforme de streaming

remise cumulable,
sur tous les abonnements
avec ou sans pub[1].

La Fibre Orange vous offre des mois et des mois de plaisir sur Netflix, Disney+ et Max

Disponible avec l'offre Livebox Max.

Offre soumise à conditions, engagement 12 mois, en France métropolitaine. Avec l'offre Livebox Max à 57,99 €/mois (prix hors promotion), sous réserve d'éligibilité, avec décodeur compatible (frais de mise en service : 40 €). Souscription de la ou des plateformes en plus auprès d'Orange dans un délai de 3 mois suivant la mise en service de l'offre Livebox Max et activation du compte de la plateforme selon les conditions générales d'utilisation de chacune. Remise(s) appliquée(s) sur la facture Orange. Liste des plateformes au 10/10/24 susceptible d'évolution. Perte de la remise en cas de résiliation après les 3 mois. Frais de résiliation Livebox : 50 €. Détails et tarifs sur orange.fr

(1) Hors Netflix Essentiel. Shogun ©2024 Disney et ses sociétés affiliées.

orange™ est là

(IN)SÉCURITÉ NUMÉRIQUE

Le 18 septembre, l'explosion coordonnée de milliers de bipeurs au Liban a entraîné la mort de huit personnes et causé au moins 2 750 blessés. L'attaque, attribuée aux services secrets israéliens, ciblait les membres du Hezbollah, le parti religieux et groupe paramilitaire soutenu par le régime iranien. Deux jours plus tard, l'histoire se répétait, avec l'explosion de talkies-walkies piégés cette fois. Des opérations hybrides, tout à la fois conventionnelles, car mettant en œuvre des explosifs, et cyber, puisque déclenchées à distance. En s'équipant d'appareils radio aussi minimalistes, le Hezbollah espérait pourtant protéger ses communications de tout acte de piratage du Mossad, éviter que ses hauts dirigeants soient géolocalisés et éliminés à cause de leurs échanges sur leurs téléphones portables… Cet épisode acte définitivement l'intrusion du numérique comme arme à part entière dans les conflits. Une arme létale dans le cas présent, mais aussi un instrument de désinformation massive utilisé par les belligérants pour discréditer leurs ennemis et manipuler les opinions. Un moyen silencieux, ô combien efficace, de paralyser à distance des systèmes de distribution d'électricité, des centrales nucléaires, des hôpitaux, des entreprises, des systèmes bancaires…

ANTON SELEZNEV/ISTOCKPHOTO

L'ARME NUMÉRIQUE EN PREMIÈRE LIGNE. En février dernier, un rapport des Nations unies s'inquiétait des cyberattaques menées par la Corée du Nord en vue de financer son programme nucléaire. Une stratégie à part entière, pilotée par l'Unité 180, un service placé sous la direction de l'agence de renseignement extérieure, qui compterait 6 800 hackers occupés à créer et déployer des *ransomwares*, à dévaliser des cryptomonnaies dans le monde entier. L'ONU recense ainsi 58 attaques qui auraient rapporté, au total, trois milliards d'euros au régime de Pyongyang, dont 620 millions de dollars issus du seul piratage d'Axie Infinity, un univers virtuel reposant sur des jetons numériques (NFT). Une situation pas si étonnante, les États mis à l'index par les grandes nations n'ayant pas attendu le numérique pour adopter des pratiques mafieuses et utiliser, par exemple, la contrebande de pétrole ou d'opium afin de contourner les embargos et se procurer des devises. Les outils ont simplement évolué, le numérique limitant les risques et étendant significativement le terrain de jeu.

DE LA BLAGUE DE POTACHE À LA CYBERCRIMINALITÉ. À l'origine, le premier virus était pourtant bien inoffensif. Conçu en 1971 par Bob Thomas, un salarié de l'entreprise Bolt, Beranek and Newman – une société américaine qui occupe une place à part dans l'histoire de l'informatique puisqu'elle est à l'origine du réseau Arpanet, l'ancêtre d'internet –, ce petit programme se propage en affichant un simple message sur les ordinateurs connectés à Arpanet : « *Je suis Creeper, attrapez-moi si vous pouvez.* » Une blague et rien de plus. Creeper s'avère en effet sans danger, incapable de se dupliquer. Un pas est franchi dans les années 1980, quand le virus Jérusalem (du nom de la ville où il se manifeste pour la première fois) frappe des milliers d'ordinateurs personnels dont il efface les programmes, conduisant l'éditeur allemand G Data Software à développer un logiciel antivirus, Ultimate Virus Killer 2000. En 2007, une nouvelle menace émerge : les rançongiciels qui réinventent la prise d'otages, à l'image de Petya qui bloque des milliers d'entreprises et occasionne un milliard d'euros de dommages. ● **LA RÉDACTION**

sommaire

HORS-SÉRIE #141 NOV.-DÉC. 2024

SÉCURITÉ 8

COUVERTURE : ©ISTOCKPHOTO/DENIS NOVIKOV

55 TRUCS ET ASTUCES

SHUTTER M/ISTOCKPHOTO

Téléchargez les applis Android et/ou iOS testées dans ce numéro en scannant leur QR Code avec votre smartphone.

Pour accéder aux sites mentionnés, tapez leur adresse bit.ly dans la barre d'adresse de votre navigateur. Le signe Ø représente un zéro.

01NET

01NET MAGAZINE 16, rue des Rasselins 75020 Paris
STANDARD : 01 77 37 72 20

ABONNEMENTS 0
Tél. : 01 70 37 31 74 (du lundi au vendredi de 9 h à 18 h)
Service client : abonnement.01net@groupe-gli.com

Abonnez-vous sur www.kiosque01.fr
22 numéros France : 69 euros TTC (TVA 2,10 % incluse)
France Étudiant : 59 euros TTC (TVA 2,10 % incluse)
sur justificatif d'une carte d'étudiant en cours de validité
France avec 6 hors-séries : 89 euros TTC (TVA 2,10 % incluse)
Suisse : www.edigroup.ch – Belgique : www.edigroup.be
Autres pays : www.kiosque01.frr

ÉDITION DÉLÉGUÉE
Agence de presse **alchimie médias** - infos@alchimiemedias.com
www.alchimiemedias.com

RÉDACTION
DIRECTRICE DE LA PUBLICATION
JACQUELINE GALANTE

RÉDACTEUR EN CHEF
JEAN-MARIE PORTAL jmportal@01netlemag.com

ONT COLLABORÉ À CE NUMÉRO
Alchimie Médias, Olivier Brault, Stéphane Joly, Thierry Lavanant, Sandrine Liger, Stéphane Philippon, Vediteam.

RÉGIE PUBLICITAIRE MEDIAOBS
44, rue Notre-Dame-des-Victoires 75002 Paris
Tél. : 01 44 88 97 70
DIRECTRICE GÉNÉRALE ADJOINTE COMMERCE SANDRINE KIRCHTHALER
DIRECTEUR DE PUBLICITÉ BENJAMIN COURCHAURE bcourchaure@mediaobs.com
ACCOUNT MANAGER (publicité pour le digital) MATHIS MEHEUT mmeheut@mediaobs.com

DIFFUSION
CHEF DE PRODUIT VENTE AU NUMÉRO
ÉRIC BOSCHER eb@groupepropress.fr
SERVICE DES VENTES (réservé aux dépositaires et marchands de journaux)
PROPRESS CONSEILS
15, rue Claude Tillier 75012 Paris
Tél. : 01 44 69 82 82

IMPRIMÉ EN FRANCE
PAR MAURY 45330 Malesherbes Cedex

01NET est édité par la société 01NET MAG
SAS au capital de 10 000 euros.
Principal actionnaire : 2BCG média

PRÉSIDENT 2BCG média,
représenté par JACQUELINE GALANTE
DIRECTRICE GÉNÉRALE PASCALE BRELIER
DIRECTEUR ÉDITORIAL JEAN-FRANÇOIS BALAINE
DIRECTEUR DE CRÉATION NICOLAS CANY

SIÈGE SOCIAL
16, rue des Rasselins
75020 Paris

Siret : 799 351 341 00042
Code APE : 5813Z

Commission paritaire : 0326 K 78311 -
ISSN 2266-7989
Dépôt légal : à parution
Distribution : MLP

AUDIENCE MESURÉE PAR ACPM
4 212 000 lecteurs (OneNext 2022 S2, L12)

Les prix affichés dans nos pages sont donnés à titre indicatif.
Une réaction, une question ? courrier01@01netlemag.com

L'impression de 01NET est réalisée à l'aide d'encres blanches labellisées Blue Angel.
Magazine imprimé sur du papier certifié PEFC. Origine du papier : France.
Taux de fibres recyclées : 100 %. Eutrophisation, PTot : 0,008 kg/tonne.
Le papier est issu de forêts gérées durablement et de sources contrôlées. pefc-france.org

EYELIGHTS

DES AUTOS ET DES PUCES

Les voitures électriques ont été les stars du Mondial de l'auto. Toujours plus autonomes et connectées, elles visent à devenir plus abordables.

Les constructeurs et les équipementiers ont mis les petits plats dans les grands pour éblouir les centaines de milliers de visiteurs du Mondial de l'auto, à Paris. Les passionnés ont pu découvrir de nouveaux modèles et rêver devant des prototypes. Une fête de la « bagnole » très attendue après l'annulation de l'édition 2020, en raison de l'épidémie de Covid, et un salon 2022 en configuration minimale. Emportés par l'enthousiasme général, les exposants ont oublié, en l'espace de dix jours, la conjoncture morose, entre des ventes en berne et le renforcement des règles sur les émissions de CO_2 au sein de l'Union européenne qui pourrait coûter jusqu'à 15 milliards d'euros de pénalités aux constructeurs européens. Malgré des parts de marché en baisse, les voitures électriques trônaient en majesté sur la plupart des stands, attirant la lumière des projecteurs et les visiteurs, à l'image de Renault dont les R4 et R5 réinventées ont remporté haut la main la palme du succès populaire. Si la ligne de la R4 E-tech se nourrit des influences de la 4L, la technologie est bien contemporaine, avec un moteur électrique partagé avec la R5 E-Tech, une batterie nickel-manganèse-cobalt, une calandre lumineuse, des écrans numériques tactiles, un assistant virtuel, les services de Google intégrés…

LES ÉCRANS PRENNENT LE POUVOIR. Au-delà de la motorisation et des batteries, les véhicules électriques ont accéléré la transition numérique de l'automobile. Les écrans tactiles grandissent, se multiplient, autorisent un nombre croissant d'interactions et de réglages. Jusqu'à déclencher la marche avant ou arrière comme sur la dernière Tesla Model 3! Une tendance semble se dessiner avec l'installation d'écrans devant le passager, destinés à gérer les fonctions de divertissement (musique, vidéo) ou la climatisation. On retrouve ces dispositifs chez Mercedes avec le MBUX, un écran long d'un mètre quarante qui court sur toute la largeur de la planche de bord, mais aussi chez Xpeng, une start-up chinoise qui exposait au Mondial de l'auto les SUV G6 et G9, deux modèles désormais disponibles en France. Les écrans panoramiques devraient se généraliser dans un avenir proche. On se souvient du système d'affichage tête haute présenté par la start-up toulousaine Eyelights au CES de Las Vegas, en début d'année, qui transforme le pare-brise en écran de réalité augmentée afin de fournir des infos au conducteur sans qu'il ait à quitter la route des yeux. Malgré toutes ces innovations, la voiture autonome n'a fait l'objet d'aucune démonstration à Paris. Pas même de Tesla, dont le système Full Self-Driving, disponible aux États-Unis, attend toujours le feu vert réglementaire pour rouler en Europe.

LES ÉNERGIES DU FUTUR. À défaut de se faire conduire par un taxi autonome, les passionnés ont pu découvrir ce qui constituera peut-être l'une des énergies du futur avec l'Alpine Alpenglow Hy6, un prototype de voiture de sport équipé d'un moteur V6 alimenté en hydrogène, et les piles à combustible de Symbio. Cette dernière entreprise est d'ailleurs partenaire du projet MissionH24, qui prévoit d'aligner une *hypercar* à hydrogène aux 24 heures du Mans en 2027. ●

EN BREF

Gare à la marche

Intel va supprimer 18 000 emplois, soit 15 % de ses effectifs. Depuis le début de l'année, l'entreprise a perdu la moitié de sa valeur en Bourse, alimentant la rumeur d'un rachat par son rival Qualcomm.

Collection 2025

L'iPhone 16 est disponible depuis le 20 septembre. Ses principales nouveautés ?Un bouton Capture pour déclencher l'appareil photo, et des fonctions d'IA indisponibles en France. Tarif : dès 970 euros.

Coup de tonnerre

On ne l'espérait plus ! Thunderbird arrive enfin sur nos mobiles. Mozilla a publié une version bêta de son client de messagerie sur le Play Store d'Android s'appuyant sur l'appli open source K-9 Mail.

C'est Lunar

Les PC portables équipés des puces Lunar Lake d'Intel sont là. Gravées en trois nanomètres par TSMC, celles-ci intègrent une unité de traitement neuronal compatible avec l'IA Copilot+ de Microsoft.

LE MEILLEUR DU SON. Shokz et Nothing améliorent le rendu **des écouteurs à « oreilles libres »**, tandis que Samsung renforce sa technologie **de réduction de bruit**.

Les finitions impressionnent. Le seul doute concerne la durabilité du cache amovible en plastique qui protège l'accès au port de recharge USB-C.

SHOKZ

OPENRUN PRO 2

IL NE MANQUE PLUS DE BASSES

Plus confortables que jamais avec leur arceau en titane ultraléger, les OpenRun Pro 2 corrigent le principal défaut des casques à conduction osseuse, à savoir des basses peu présentes, grâce à une conception hybride. Ils utilisent désormais deux haut-parleurs, l'un à conduction osseuse assigné à la reproduction des aigus et des médiums, l'autre à conduction aérienne chargé de délivrer les graves. À l'écoute, le résultat s'avère convaincant. Même si la qualité audio reste un cran en dessous de ce que proposent de bons écouteurs intra-auriculaires, il devient possible de profiter de sa musique dans de bonnes conditions d'écoute. L'autre avancée notable concerne l'intégration attendue d'une prise USB-C pour la recharge en lieu et place du connecteur magnétique propre à la marque.

bit.ly/3ZOjcGo – Shokz – 200 €

NOTHING EAR (OPEN)

OUVERTS SUR LE MONDE

Les écouteurs à « oreilles libres » sont décidément en vogue. Nothing s'y met à son tour avec les Ear (open), qui empruntent les codes graphiques caractéristiques de la marque, avec l'utilisation de plastique transparent pour le couvercle du boîtier de rangement et de recharge, le corps des écouteurs qui laisse voir les haut-parleurs et certains composants. Nothing rend une copie réussie. Les Ear (open) se placent d'emblée parmi les modèles à architecture ouverte les plus efficaces en matière de qualité sonore, de confort, d'autonomie (environ huit heures entre deux recharges) et de filtrage des bruits ambiants lors des conversations téléphoniques.

bit.ly/4dNbznj – Nothing – 150 €

SHOKZ

SAMSUNG

GALAXY BUDS3 PRO

L'ESPRIT DE FAMILLE

Avec les Galaxy Buds3 Pro, Samsung comble son retard sur les AirPods Pro, la référence en matière d'écouteurs sans fil à réduction de bruit. L'atténuation des bruits ambiants et le mode transparence sont au niveau de ce que propose Apple.
Même bilan en ce qui concerne la restitution sonore, très équilibrée, avec des graves présents sans excès. Samsung réserve également certaines options à son écosystème. Un téléphone sous OneUI récent est nécessaire pour profiter de la connexion multipoint, de l'appairage rapide, du mode audio spatial avec suivi des mouvements de la tête, des codecs haute définition ou encore de la traduction à la volée assurée par l'intelligence artificielle Galaxy AI.

bit.ly/4ewcHwK – Samsung – 250 €

SÉCURITÉ, MIEUX VAUT PLUS QUE MOINS

Beaucoup de particuliers font encore le minimum en matière de sécurité informatique, s'estimant être suffisamment prudents dans leurs pratiques pour éviter les attaques cyber. Et jugeant probablement que celles-ci n'arrivent qu'aux autres dès lors que l'on prend soin d'installer une suite de sécurité ou, à défaut, d'activer Windows Defender, le module de sécurité de Microsoft qui ne cesse de s'étoffer. Si les utilisateurs sont des cibles pour les escrocs du web dans le cadre de leurs usages personnels d'un ordinateur ou d'un téléphone, ils courent des risques plus grands encore en entreprise. Publié en mars, le baromètre de la cybersécurité 2023 réalisé par le cabinet Cyblex Consulting pour Docaposte révèle qu'une entreprise sur cinq admet avoir déjà subi une cyberattaque.

Faire le bon choix

20 % de victimes, c'est aussi la proportion – on n'imagine pas qu'il s'agisse d'une coïncidence – de décideurs qui pensent leur entreprise très exposée aux risques cyber, quand 28 % se sentent peu ou pas menacés. Dans le détail, plus la société compte de salariés, plus la cybersécurité est érigée en priorité. Un niveau de sensibilisation qui varie du simple au quadruple entre les grandes entreprises (plus de 1 000 salariés) et les TPE (moins de 20). Comment expliquer ces disparités ? Par la présence ou l'absence de collaborateurs entièrement dévolus à la gestion des systèmes informatiques bien sûr, ces professionnels étant formés aux problématiques de la cybersécurité. Un point que l'on retrouve du côté des particuliers. Les « geeks », en bons passionnés de nouvelles technologies, prennent la menace au sérieux et mettent tout en œuvre pour éviter les ennuis. C'est aussi le cas, très souvent, chez les béotiens, dont l'absence assumée de connaissances techniques nourrit une prudence peut-être excessive. Mais en matière de sécurité, le mieux n'est jamais l'ennemi du bien ! ●

ID-WORK/ISTOCKPHOTO

LES
TEMPS FORTS

DIFFICULTÉ
VARIABLE
TEMPS
VARIABLE
DOMAINE
SÉCURITÉ

La protection des ordinateurs contre les menaces du web ne doit pas être sous-estimée à l'heure où fleurissent les rançongiciels, l'hameçonnage et les logiciels espions.

EXPLOITEZ LE MEILLEUR DES SUITES ANTIVIRUS

Difficile de trancher sur le choix d'une suite de sécurité tant les possibilités sont nombreuses et la concurrence féroce. L'une des plus connues a pourtant disparu des principaux comparatifs et tests : l'antivirus de Kaspersky, un éditeur dont le siège social est à Moscou et qui pâtit de la situation géopolitique. Les autorités françaises ont en effet, dès 2022, mis en garde ses clients quant aux potentielles cyberattaques venant de Russie et visant les professionnels et les particuliers. Vous ne trouverez donc pas l'application dans ce dossier. Tous les outils cités dans ces pages bénéficient d'excellentes notes en matière de protection et de performance aux évaluations réalisées régulièrement par l'organisme indépendant AV-Test. Quelle que soit la suite de sécurité de ce dossier que vous choisirez, vous aurez donc l'assurance d'être bien protégé. Votre choix doit donc porter sur d'autres critères.

N'OUBLIEZ PAS LE VPN ! Si vous êtes néophyte, tablez sur une interface grand public à l'image de celle d'Avast, Bitdefender ou McAfee. Si vous êtes un amateur éclairé qui aime optimiser les fonctions avancées d'une application, préférez Norton 360 ou la suite d'Eset. Sachez que la plupart des applications proposent, en plus du client destiné à sécuriser les ordinateurs, PC et Mac, une protection des smartphones grâce à des applications mobiles associées. Il en va de même de l'anonymisation du surf sur internet par les VPN intégrés qui masquent votre adresse IP. Les programmes s'accompagnent en outre d'extensions qui veillent sur les navigateurs et bloquent les menaces propagées par les sites internet. Certaines suites se démarquent en associant des services additifs. McAfee signale les éventuelles fuites de données émanant de mots de passe compromis ; Avast et Eset déploient des fonctions de surveillance du réseau local. Votre choix est aussi affaire de prix. Prenez garde aux abonnements qui, après un an à prix cassé, peuvent venir doubler la note ! Pensez à décocher les cases de reconduite automatique et n'hésitez pas à changer de protection si vous repérez une offre plus avantageuse. ●

BOÎTE À OUTILS POUR CE PAS À PAS, NOUS AVONS UTILISÉ LES ÉLÉMENTS SUIVANTS

PC

Connexion internet

Norton 360, F-Secure Total, Bitdefender, Avast Premium Security

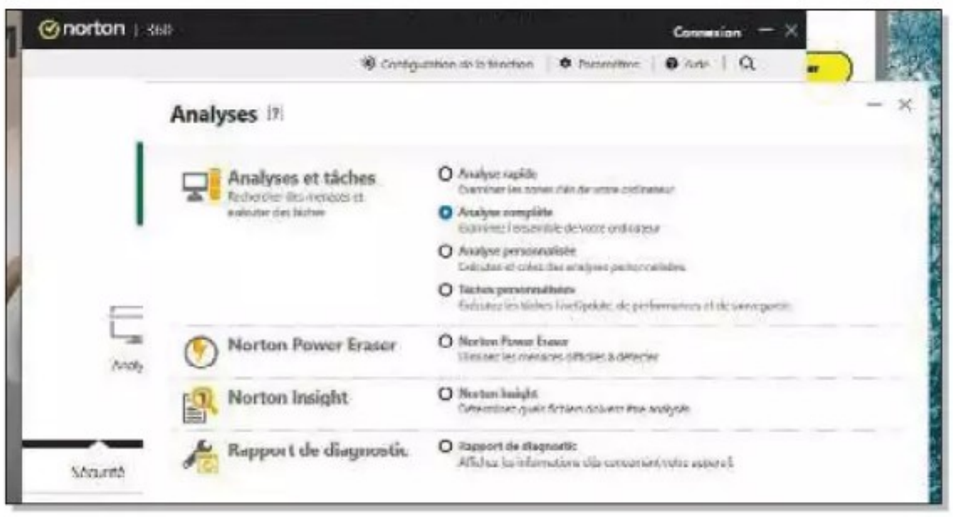
McAfee Total Protection, Eset Smart Security, Proton VPN

CONFIEZ VOTRE SÉCURITÉ À NORTON 360

Bénéficiant d'une interface grand public et de services de pointe, cette suite de référence en cybersécurité protège efficacement les ordinateurs et les appareils nomades des particuliers et des entreprises.

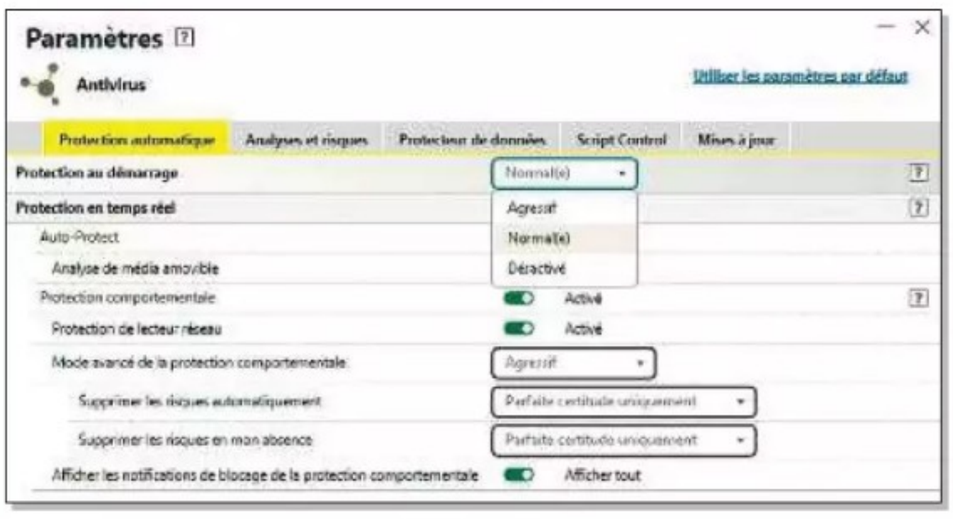
1 LANCEZ LA PREMIÈRE ANALYSE

S'il n'existe pas de version gratuite de Norton, il est toutefois possible de tester la suite de sécurité (bit.ly/4ebmkAN) durant quatorze jours avant de confirmer l'abonnement. Nous avons opté pour la version « standard » dans le cadre de ce dossier. Au lancement initial, la signature des virus s'actualise automatiquement. Effectuez une première recherche en allant sur **Ouvrir** et en cliquant sur la flèche noire pointant vers le bas. Choisissez **Analyses** et cochez la case **Analyse complète**. Celle-ci risque d'être longue, mais en déployant le menu **Mon ordinateur doit**, il est possible de forcer sa mise en veille une fois qu'elle est terminée. La flèche à droite du bouton **Ouvrir** permet d'accéder au menu **Performances, Sécurité** afin d'être certain d'être correctement protégé.



2 AMÉLIOREZ LA PROTECTION

Cliquez sur l'onglet des **Paramètres** dans le menu supérieur puis sur **Antivirus**. Positionnez la protection au démarrage en mode **Normal(e)** puis le mode avancé de la protection comportementale sur **Agressif**. Validez avec le bouton **Appliquer**. Accédez à l'onglet **Analyses et risques**. Déroulez le menu **Analyse de lecteur USB** et optez pour **Activé**. Enfin, dans la section **Configurer** d'**Analyse complète,** choisissez la planification **Quotidienne**.



3 BÉNÉFICIEZ D'UN NAVIGATEUR ROBUSTE

Sur l'accueil, cliquez sur le bouton **Installer** faisant face à l'intitulé Private Browser. Une fois le navigateur de Norton en place, pointez sur **Ouvrir** puis sur le bouclier bleu à droite. Activez le curseur de l'Agent de confidentialité, puis dirigez-vous vers **Blocage basique**, **Paramètres**. Cochez la case **Blocage modéré**. Revenez à l'accueil du Centre de sécurité et de confidentialité et effectuez un nettoyage en choisissant **Lancer Cleaner**, **Supprimer les données**.

4 DEVENEZ INDÉTECTABLE SUR LA TOILE

La dernière étape de sécurisation de votre machine et du surf sur internet passe par la mise en place du VPN maison, inclus dans l'abonnement standard. Cliquez sur le bouton **Activer** de l'accueil. Par défaut, celui-ci utilise un emplacement en France pour déporter votre accès à internet. Si vous préférez être connecté à un autre pays, pointez sur la flèche à droite de Désactiver puis sur **Région VPN**. Sélectionnez une nouvelle région. Les paramètres du VPN proposent également de bloquer le suivi publicitaire et l'activation automatique du dispositif d'anonymisation lorsqu'il détecte des réseaux non sécurisés (**VPN automatique**). Enfin, utilisez le mode **Arrêt d'urgence** pour être certain que vos données ne seront pas compromises en cas de déconnexion du VPN.

Gardez vos logiciels à jour

Maintenant que la configuration antivirus est optimale, passons à la sécurité des logiciels installés. Depuis la page l'accueil de Norton 360, pointez sur le bouton **Analyser** du Gestionnaire de mises à jour. Activez le curseur de mise à jour automatique. Si Norton signale des applications obsolètes, cliquez sur **Mettre à jour**. Certaines peuvent être exclues ou non prises en compte. Allez sur l'onglet **Autres programmes** pour actualiser la liste en ajoutant ou supprimant des éléments.

STANISLAV CHEGLEEV/ISTOCKPHOTO

ADOPTEZ ET OPTIMISEZ F-SECURE TOTAL

La société finlandaise F-Secure assure la sécurité de plus de 30 millions d'usagers. Sa suite de sécurité est particulièrement complète, facile à configurer et **classée parmi les plus efficaces au palmarès d'AV-Test**.

1 METTEZ À JOUR LA BASE DE SIGNATURE

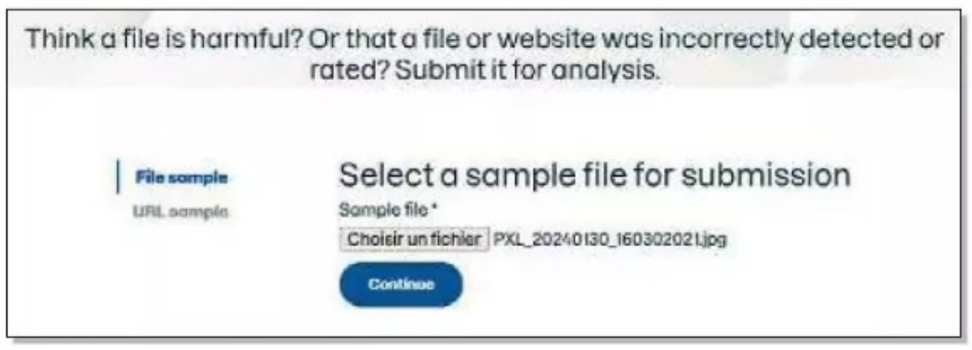
Allez sur la page de téléchargement de la version d'essai du programme (bit.ly/47BUhrI) pour installer la suite de sécurité. Indiquez que vous souhaitez protéger votre appareil. À la page d'accueil du programme, cliquez sur le bouton **Démarrer** sous **Protection des appareils** et pointez sur **Paramètres**. Accédez à l'option autorisant les droits d'administrateur pour pouvoir agir sur l'ensemble des fonctions F-Secure. Dirigez-vous vers les **Mises à jour** en colonne gauche et actualisez la base de signature des virus.

2 DÉMARREZ DES ANALYSES PLANIFIÉES

Le bon point de F-Secure est que la plupart des options de protection avancée sont activées par défaut, ce qui n'est pas forcément le cas de tous ses concurrents. Seule la fonction d'analyse périodique doit être lancée manuellement. Depuis l'écran d'accueil, ouvrez les **Paramètres d'analyse** en mode administrateur et pointez sur le curseur de l'analyse planifiée. Définissez la périodicité, cochez la case **Exécuter la tâche dès que possible** et fermez le panneau des paramètres.

3 AJOUTEZ L'EXTENSION À VOTRE NAVIGATEUR

F-Secure bénéficie d'une extension compatible avec les principaux navigateurs du marché. Vous trouverez ce module dans les paramètres de l'application, à la section **Protection contre les fraudes**. Déroulez cette page vers le bas et cliquez sur le lien menant vers votre navigateur (Chrome, Edge, Firefox). Un nouvel onglet pointant vers le module complémentaire s'affiche. Installez ce dernier pour bénéficier d'une protection bancaire ainsi qu'un mode de recherche sûr, SafeSearch.

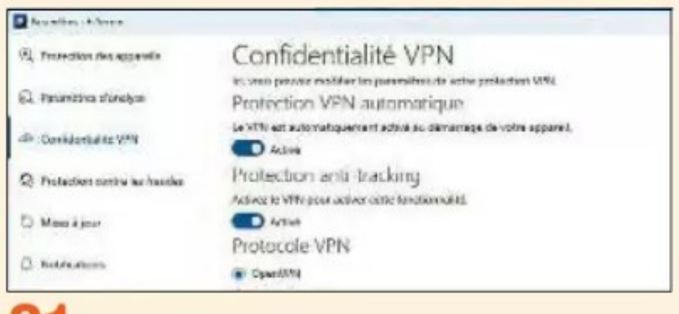


4 ENVOYEZ DES ÉCHANTILLONS

Si un fichier semble infecté, il est possible de le transmettre à F-Secure pour une analyse extérieure qui préservera votre ordinateur. Cliquez sur **Protection des appareils**, **Envoyer un échantillon**, **Choisir un fichier**. Validez le transfert avec **Continue**, **Yes** et saisissez des informations complémentaires (type de fichier, problème rencontré, etc.). Finalisez l'envoi avec **Upload**. Attendez le retour de l'analyse. Dans ce laps de temps, profitez-en pour lancer une analyse complète depuis le menu **Analyse antivirus**.

PAS À PAS EXPRESS — RÉGLEZ LE VPN

Comme la plupart des suites de sécurité payantes, celle de F-Secure intègre un VPN **qu'il convient de mettre en service** et de paramétrer correctement.

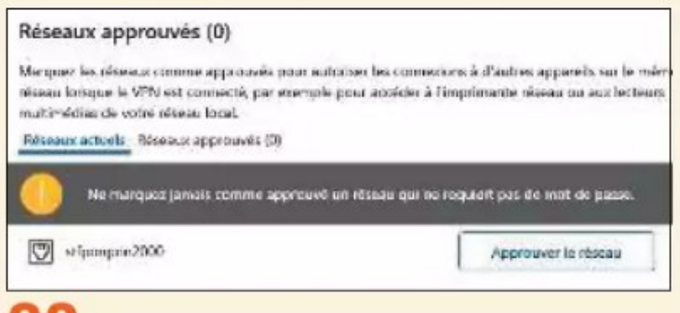


01. Démarrez le réseau privé virtuel

Dirigez-vous vers les paramètres depuis l'écran d'accueil de la suite et passez en mode administrateur. Pointez sur **Confidentialité VPN** en colonne gauche et activez les curseurs **Protection VPN automatique** et **Protection anti-tracking**.

02. Changez de protocole

La section Protocole VPN est associée par défaut à OpenVPN. Il est préférable de lui substituer le protocole **IKEv2**, plus stable et plus rapide. Activez par ailleurs le curseur **Killswitch** afin de limiter l'exposition aux failles de protection.



03. Approuvez les réseaux connus

Si votre ordinateur est relié à un réseau familial, il convient d'accorder l'accès à d'autres appareils, de façon, par exemple, à utiliser une imprimante partagée. Cliquez sur **Sélectionner les réseaux**, puis approuvez le réseau local identifié.

TRAVAILLEZ SANS CRAINTE AVEC BITDEFENDER

L'éditeur roumain peaufine sa suite Total Security depuis près d'un quart de siècle. **Des améliorations régulières l'ont hissée sur le podium des solutions de cybersécurité** les plus efficientes.

1 OBTENEZ LA VERSION D'ESSAI

La suite de sécurité Bitdefender bénéficie d'une version d'essai. Allez sur la page bit.ly/4dfhf99 et identifiez-vous à l'aide d'un compte Google ou Microsoft pour créer un compte. Pointez sur **Tableau de bord** à gauche, cliquez sur le lien **Obtenir la version d'essai** et procédez à l'installation de l'application sur votre ordinateur. Au lancement initial, effectuez une analyse de l'appareil et cochez la case d'essai du produit durant 30 jours.

2 PARAMÉTREZ L'ANTIVIRUS

Depuis l'accueil, pointez sur **Protection** et ouvrez l'antivirus. Cliquez sur l'onglet **Avancés**. Nous vous conseillons d'activer les curseurs d'analyse des archives et des secteurs d'amorçage. Allez dans l'onglet **Paramètres** et réglez la surveillance des disques réseau sur **Analyse automatique** si votre PC fait partie d'un réseau familial. Faites de même pour la section des CD & DVD.

Optez pour le bon profil

Les outils additifs se trouvent au sein du menu **Utilitaires**. La fonction **Optimisation en 1 clic** supprime les fichiers inutiles. Utilisez la commande **Destructeur de fichiers** afin de supprimer définitivement tous les éléments sélectionnés par vous-même, la section **Paramètres** des profils pour ajuster les options de sécurité en fonction de vos activités du moment. Chacune d'elles (Travail, Jeu, Film, etc.) bénéficie de configurations propres. Le profil Travail propose par exemple de reporter les tâches de maintenance et de mises à jour, quand le profil Jeu ajuste l'alimentation de l'ordinateur.

3 DÉMARREZ LES ANALYSES

Depuis l'accueil, lancez une analyse de vulnérabilité. Vous saurez ainsi si vos applications sont à jour. Poursuivez avec une analyse du système qui a pour but de passer en revue les fichiers enregistrés sur l'ordinateur et les périphériques de stockage USB et réseau. Pointez ensuite sur **Protection** à gauche et activez les défenses contre le cryptomining et les ransomwares. Terminez par une analyse de vulnérabilité avec **Ouvrir**, **Démarrer l'analyse**.

4 PROTÉGEZ VOTRE VIE PRIVÉE

En colonne gauche, visitez le menu consacré à la **Vie privée**. Celui-ci se compose de six sections. Ouvrez l'Anti-tracker. Si vous utilisez plusieurs navigateurs, installez-le sur ces derniers. Pointez ensuite sur **Paramètres** de la section **Protection vidéo & audio**. Accédez à l'onglet éponyme et activez les curseurs de notification d'accès à la webcam et au micro.

5 DEVENEZ INVISIBLE GRÂCE AU VPN

La suite inclut un VPN masquant votre adresse IP sur internet. Vous le trouverez dans le menu **Vie privée**. Cliquez sur **Ouvrir le VPN**, **Connexion**. Pointez sur **Activer la fonction Kill Switch** et sur son curseur associé. Visitez la section **Bloqueur de publicités et de traceurs**. Activez les deux curseurs présents. Continuez la configuration en allant sur **Auto-connexion**. Forcez la connexion du VPN en choisissant le mode **Démarrage de l'appareil**. Activez également sa mise en route en cas de **Wi-Fi non sécurisé**.

PLACEZ-VOUS SOUS L'AILE D'AVAST

Plus complète que la version gratuite, qui se résume à un (très bon) antivirus, l'édition premium de la suite de sécurité tchèque est **testable pendant 30 jours, sans avoir à enregistrer de carte bancaire.**

1 PROGRAMMEZ DES ANALYSES CIBLÉES

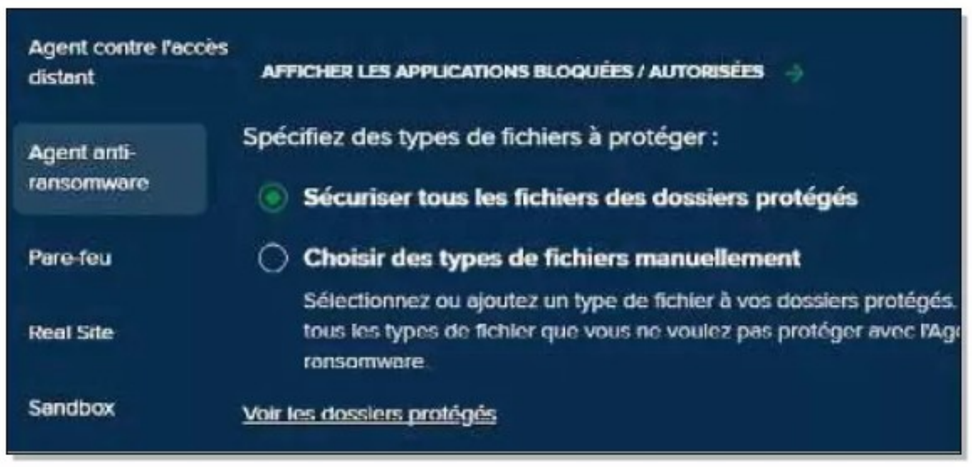
Rendez-vous à l'adresse bit.ly/3ZB9lny et pointez sur **Essayer pendant 30 jours**. Procédez à l'installation. Le volet gauche de l'écran d'accueil présente les principaux menus de sécurité. Pointez sur **Protection, Analyse antivirus, Scan au démarrage, Préparer l'analyse** et redémarrez le PC. Cette fonction détecte des menaces et les supprime avant même le démarrage du système. Retournez dans le menu **Analyse antivirus** et optez pour **Analyse ciblée**. Si vous soupçonnez qu'un virus se cache dans un dossier, sélectionnez cet emplacement et lancez l'analyse ciblée avec **OK**. Utilisez les analyses personnalisées pour définir le type (complet, rapide…) et la fréquence (journalière, mensuelle) de la surveillance.

2 BLOQUEZ LES PROGRAMMES MALVEILLANTS

Dans **Protection**, accédez à la section **Agents de sécurité**. Cliquez sur l'icône des paramètres et positionnez le curseur sur **Haute sensibilité** pour les malwares, les indésirables et les outils. Revenez sur le premier onglet et cochez les cases **Activer le mode renforcé, Activer l'Agent anti-rootkits, Activer l'Agent anti-exploits.** Dans la partie réservée aux types d'éléments à analyser, cochez **Tous les fichiers.**

3 ÉVITEZ LES RANÇONGICIELS

Entrez dans le menu **Protection**, puis dirigez-vous vers l'onglet **Agent anti-ransomware.** Cliquez sur l'icône en forme d'engrenage à droite et cochez l'option **Mode strict.** Vous devrez peut-être autoriser l'accès au PC pour les logiciels que vous connaissez et que vous savez sans dangers. Cette sécurité renforce la protection des applications non approuvées. Poursuivez et terminez en cochant **Sécuriser tous les fichiers des dossiers protégés.**



4 SÉCURISEZ VOTRE BOÎTE MAIL

Déroulez le menu **Confidentialité**, **Alertes piratage**. Activez l'option **BreachGuard** afin de surveiller d'éventuels piratages liés à l'adresse mail utilisée pour la création de votre compte Avast. Si des fuites sont découvertes, changez le mot de passe immédiatement. Par ailleurs, dans **Protection**, adoptez une veille de votre boîte de messagerie depuis la **Protection e-mail**. Renseignez une adresse et connectez le compte à Avast. Celui-ci vous signalera tout courriel suspect, toute tentative d'hameçonnage et d'éventuels malwares cachés. Par ailleurs, il est possible d'afficher vos statistiques de protection depuis l'onglet **Menu**, **Mes statistiques**. Vous découvrirez le nombre d'attaques empêchées ainsi que les menaces en quarantaine.

Protégez votre réseau familial

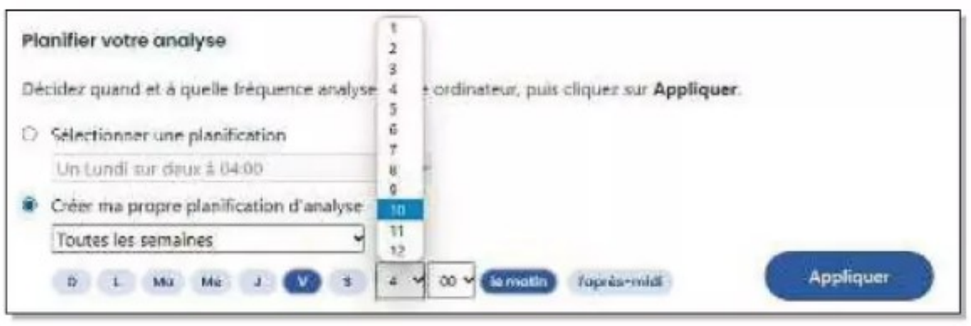
Avast établit une veille du réseau local à la recherche d'éventuelles brèches. Allez sur **Inspecteur réseau** dans **Protection** et cliquez sur **Analyser le réseau**. Quand elle détecte de potentiels risques, l'application vous propose des solutions. Effectuez une seconde passe (**Réanalyser le réseau**) qui peut faire ressortir d'autres appareils actifs connectés. Pointez sur **Terminé** puis vérifiez que les curseurs **Toujours analyser** et **Surveiller ce réseau** sont activés.

DRESSEZ DES BARBELÉS AVEC MCAFEE

Parmi les plus anciennes du marché, la suite américaine garde bon pied bon œil. **La version Total Protection est même la seule à évaluer le niveau de protection des appareils**, en suggérant des axes d'amélioration.

1 PLANIFIEZ VOS EXAMENS

Installez la version d'évaluation gratuite (bit.ly/3zsBe6x) en indiquant votre adresse mail. Lancez une première analyse complète en visant les points dans l'angle de l'encadré **Antivirus**. Cliquez sur **Voir les détails, Types d'analyse**. Une fois la recherche achevée, poursuivez en planifiant de futurs scans périodiques. Dirigez-vous vers **Analyse planifiée** et cochez **Créer ma propre planification d'analyse**. Définissez une périodicité et validez (**Appliquer**).



2 NETTOYEZ VOTRE ORDINATEUR

McAfee Total Protection peut aider votre machine à fonctionner sans ralentissements. Accédez aux options de l'encadré **Suppression des traces de navigation, Voir les détails, Paramètres**. Certains fichiers système méritent d'être cochés afin d'être nettoyés. C'est le cas du Registre, du cache de miniatures et des cookies. Cochez également la case **Eléments supprimés** de la partie **E-mail**. Cliquez sur **Appliquer, Nettoyer**. Vérifiez les éléments sélectionnés avant de valider avec **Continuer**.

3 VERROUILLEZ VOTRE IDENTITÉ NUMÉRIQUE

L'encadré consacré à l'identité nécessite de créer le mot de passe du compte. Cliquez sur l'icône avatar en colonne gauche puis sur **Mon abonnement, Rendez-vous dans Mon compte**. Choisissez un sésame fort. Revenez sur l'accueil et pointez sur **Protection de l'identité**. La page qui s'affiche invite à vérifier que le mot de passe n'est pas compromis en ligne. Allez sur **Vérifier maintenant, Me montrer, Traiter les violations de données**. Si c'est le cas, changez le mot de passe associé au site web affiché.

4 OPTIMISEZ LES APPLIS ET VÉRIFIEZ LE RÉSEAU

Parmi les fonctionnalités de McAfee, il en est une qui permet d'accélérer les performances de certaines applications du PC. Cliquez sur **Ma protection** en colonne gauche puis sur **Optimiseur d'applications**. Procédez à l'installation qui nécessite de se déconnecter de Total Protection. Redémarrez puis revenez dans ce même menu pour voir si McAfee a optimisé certaines applis. Allez sur **Ma protection, Mon réseau domestique**. Chaque appareil actif est mentionné ainsi que son type et adresse MAC.

PAS À PAS EXPRESS — BONIFIEZ VOTRE SCORE DE PROTECTION

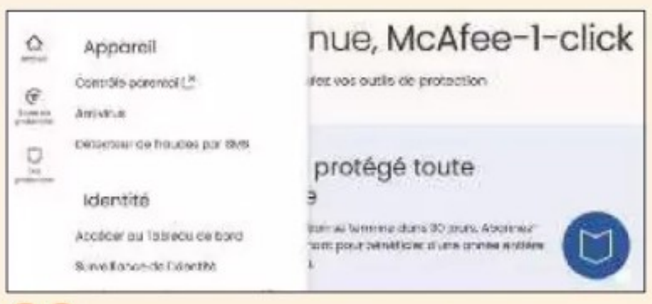
McAfee est le seul à délivrer une note globale de sécurité, de 0 à 1 000, pour chacun de ses membres. Tous peuvent améliorer leur score en réalisant des actions de prévention et de sécurité.

01. Découvrez votre note

Cliquez sur **Consultez votre score de protection** depuis l'accueil puis **Accéder au Centre de protection McAfee**. Sur la page web qui s'affiche, vérifiez votre note en allant sur **Score de protection** en colonne gauche.

02. Tentez de l'améliorer

McAfee propose de réaliser diverses actions pour booster votre score, comme vérifier les comptes à risque, activer la protection sur le web, résoudre les violations de données… Déroulez la page vers le bas pour les enclencher.



03. Ajoutez des barrières

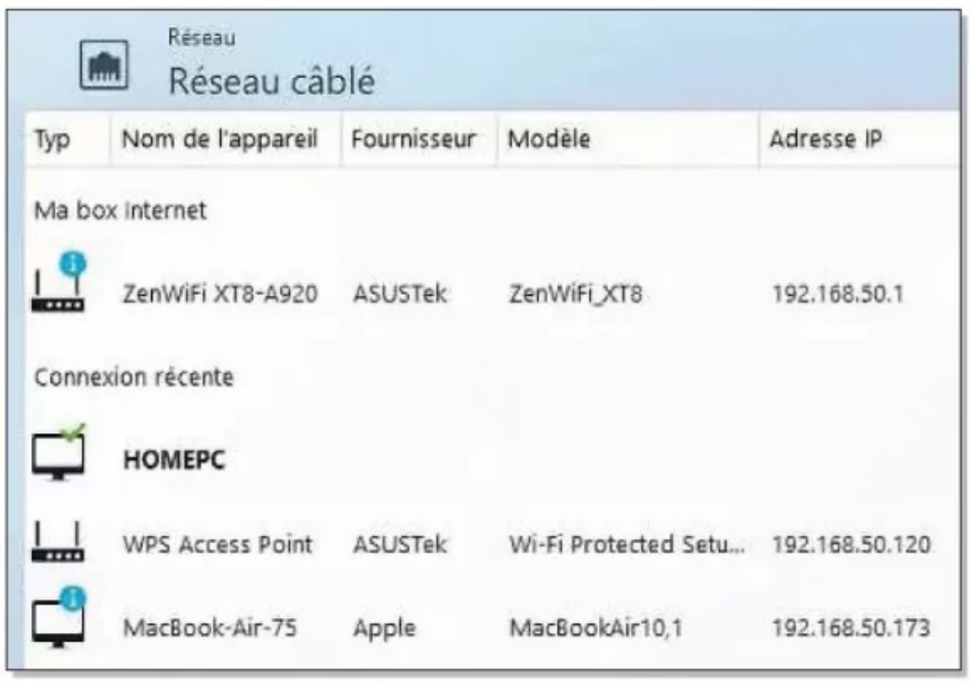
Chaque action que vous entreprenez fait grimper votre score. Pointez sur **Ma protection** en colonne gauche. Vous pouvez installer un contrôle parental, un VPN, une protection web du navigateur…

ENTREZ DANS LA BULLE ESET SMART SECURITY

Actif depuis les années 1990, cet acteur de la cybersécurité slovaque fait lui aussi toujours partie des premiers de la classe lors des comparatifs effectués par la société AV-Test. **Une valeur sûre.**

1 CHOISISSEZ LE TYPE D'ANALYSE

Installez la version d'essai de la version premium (bit.ly/3zm57FH) en prenant soin de cocher la case d'activation de la détection des applis potentiellement indésirables. Créez un compte client. Terminez en vous connectant avec le bouton **Essayer gratuitement**. Engagez une première analyse de l'ordinateur depuis la colonne gauche. Déroulez le menu **Analyses avancées** et pointez sur **Analyse personnalisée**. Choisissez les éléments à scanner et optez pour **Analyse approfondie** dans le menu **Profil**.



2 SURVEILLEZ LE RÉSEAU LOCAL

Depuis le menu **Aperçu** de l'accueil, pointez sur **Inspecteur réseau**. Dirigez-vous vers **Analyser votre réseau, Analyser tout, Lancer l'analyse**. Vous devriez recevoir une notification indiquant que l'environnement est sécurisé. La liste des connexions s'affiche. Certaines peuvent être surmontées d'une icône bleue. Cliquez sur l'appareil concerné et sur **Afficher** pour obtenir des détails.

Configurez ThreatSense

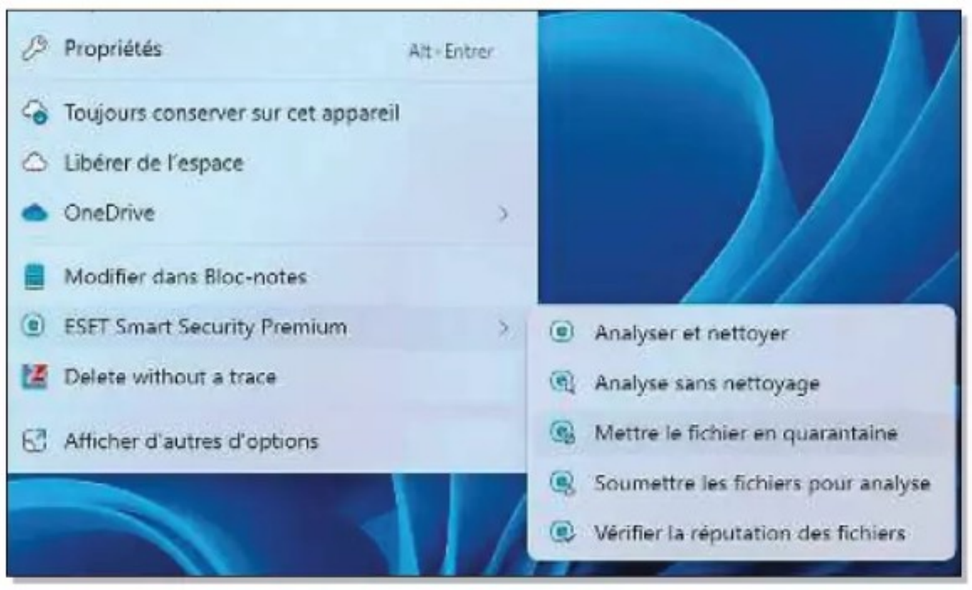
Eset offre la possibilité aux amateurs éclairés de personnaliser finement la défense de l'ordinateur. Les commandes se situent dans **Configuration, Protection de l'ordinateur**. Pointez sur l'une des icônes représentant des engrenages à droite. Le menu **Configuration avancée** propose d'engager la sécurité additive. Accédez à la **Protection en temps réel du système de fichiers** et ouvrez **ThreatSense**. Activez le curseur **Heuristique avancée/Signatures ADN**. Dans la section **Protections**, il est possible de redéfinir les seuils de détection sur **Offensif** ou **Équilibré**. Allez dans la section **Analyses des logiciels malveillants** et réglez l'analyse à la demande sur **approfondie**.

3 CRÉEZ UN FAUX COMPTE WINDOWS

Dans le menu **Configuration**, pointez sur **Outils de sécurité**. Activez tous les curseurs. Grâce à l'**Antivol**, il est possible de créer un compte fantôme (faux compte Windows) qui va appâter un éventuel voleur tentant d'utiliser votre PC. Vous serez ainsi prévenu si cela se produit. Définissez un pseudo et validez avec **Créer**.

4 CHIFFREZ VOS DONNÉES DANS UN LECTEUR VIRTUEL

Il est possible de protéger les fichiers sensibles dans un lecteur virtuel chiffré. Depuis **Aperçu**, cliquez sur **Secure Data, Créer un lecteur virtuel chiffré**. Choisissez un emplacement de destination et sa capacité en Mo ou Go. Créez un mot de passe et validez. Glissez vos fichiers personnels dans ce lecteur. Secure Data autorise également la création de dossiers protégés sur des clés USB.



5 FAITES ANALYSER UN FICHIER

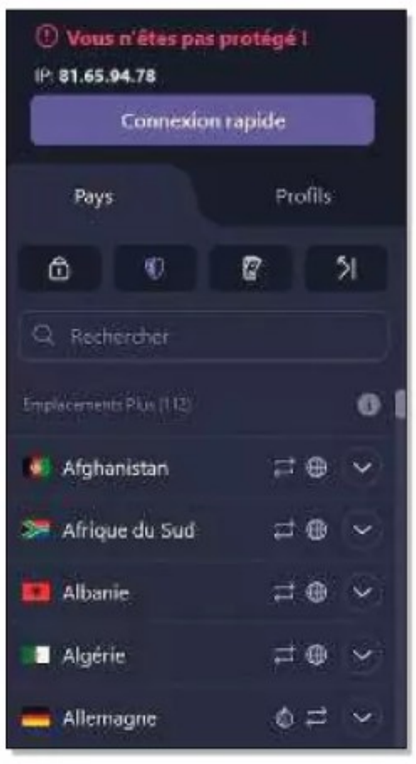
Vous avez reçu un fichier suspect ? Plusieurs options s'offrent à vous. Commencez par opérer un clic droit sur son icône et choisissez **ESET Smart Security**. Dans le sous-menu joint, engagez une première analyse. Si des doutes subsistent, pointez sur **Vérifier la réputation des fichiers, Soumettre les fichiers pour analyse**. Il sera vérifié sur les serveurs d'Eset. Si vous êtes certain qu'il s'agit d'un élément malveillant, optez pour sa mise en quarantaine.

NAVIGUEZ SOUS LES RADARS AVEC PROTON VPN

Les utilisateurs de ce VPN suisse bénéficient des lois les plus strictes en matière de protection de la vie privée. **La version payante apporte des fonctions supplémentaires et une meilleure vitesse de navigation.**

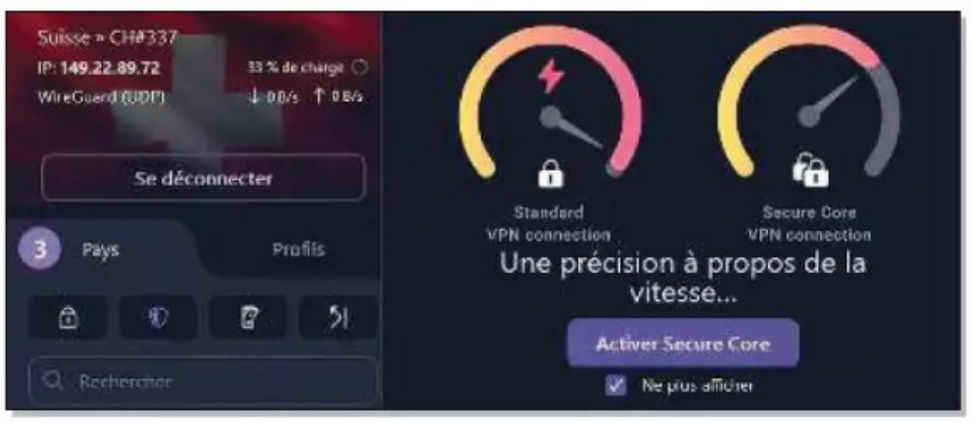
1 DÉMARREZ LE RÉSEAU VIRTUEL

L'offre VPN de Proton (protonvpn.com/fr) inclut une version gratuite sans publicité ni limitation de données ou de vitesse. Simple et pratique, elle suffit à protéger un poste informatique sans bénéficier des fonctionnalités de la version payante. Celle-ci (bit.ly/4gAwi01) inclut notamment la prise en charge du protocole P2P, bénéficie de vitesse de navigation jusqu'à 10 Gbit/s et permet de se connecter à des milliers de serveurs basés dans 110 pays. Créez un compte puis téléchargez la solution VPN (bit.ly/3BdnInE). Indiquez vos identifiants dans la fenêtre de connexion. La carte mondiale affiche les serveurs Proton sur la planète. Dans un premier temps, cliquez sur le bouton **Connexion rapide**.



2 PRÉFÉREZ DES PAYS RESPECTUEUX DE LA VIE PRIVÉE

Lorsque la connexion est établie, zoomez avec la molette pour voir précisément l'emplacement du serveur. Passez à un autre pays en cliquant sur l'une des icônes violettes puis **Se connecter**. Si le transfert de données doit absolument être sécurisé, pointez sur le cadenas **Secure Core** et activez la protection additive. Dans ce cas, le trafic risque d'être ralenti car rerouté par des pays « sûrs ».

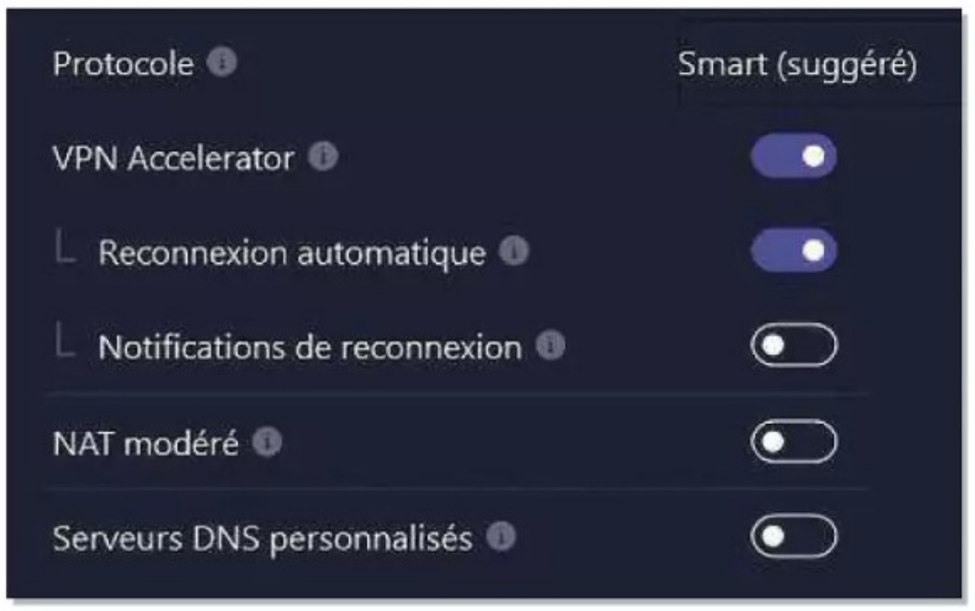


3 DÉBARRASSEZ-VOUS DES PUBS ET TRACEURS

Parmi les fonctionnalités du VPN suisse, celle de bloquer les réclames et les malveillants n'est pas à sous-estimer. Cliquez sur l'icône bouclier (**NetShield**) et pointez sur **Bloquer les logiciels malveillants, publicités et traqueurs**. Par ailleurs, nous vous conseillons d'activer l'option **Arrêt d'urgence (kill switch)** pour éviter de voir vos données compromises en cas de coupure du VPN.

4 ACCÉLÉREZ LES ÉCHANGES DE DONNÉES

Si vous êtes du genre joueur, vous devriez apprécier la fonctionnalité **Redirection de port** (icône de droite sous l'onglet **Profils**) qui accélère les flux de données lors des jeux en ligne et des transferts de fichiers torrent. Un nouveau numéro de port apparaîtra au-dessus du bouton de déconnexion. À vous de le renseigner dans votre client BitTorrent. Par ailleurs, en accédant aux **Paramètres** du VPN depuis les traits horizontaux en haut à gauche, vous pouvez bénéficier des versions bêta en avant-première en activant le curseur éponyme. L'onglet **Connexion** donne accès à l'option **NAT modéré** que nous conseillons de désactiver si vous ne jouez pas en ligne.



5 METTEZ UN FICHIER SOUS QUARANTAINE

Vous avez reçu un fichier qui paraît suspect ? Plusieurs options s'offrent à vous. Commencez par opérer un clic droit sur son icône et choisissez **ESET Smart Security**. Dans le sous-menu joint, engagez une première analyse. Si des doutes subsistent, pointez sur **Vérifier la réputation des fichiers**, **Soumettre les fichiers pour analyse**. Il sera vérifié sur les serveurs Eset. Si vous êtes certain qu'il s'agit d'un élément malveillant, optez pour sa mise en quarantaine.

Établissez des profils

Pointez sur l'onglet **Profils**, **Créer un profil**. Sélectionnez un type de connexion (Standard, Secure Core, P2P pour l'échange de fichiers de pair à pair, Tor pour naviguer caché sur ce réseau mondial décentralisé). Donnez-lui un nom explicite puis choisissez le pays de connexion ainsi qu'un serveur (le plus rapide par défaut). Il est aussi possible de sélectionner un protocole particulier comme **Stealth** qui permet de contourner la censure internet. Validez avec **Enregistrer**.

DIFFICULTÉ ÉLEVÉE
TEMPS 30 MIN
DOMAINE INTERNET

RENDEZ VOTRE RÉSEAU WIFI IMPÉNÉTRABLE

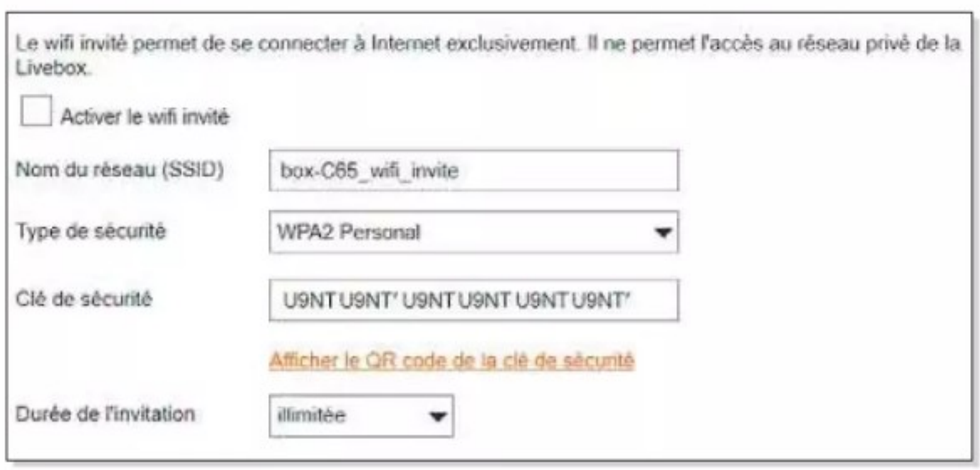
Veillez à dresser une forteresse autour de votre réseau domestique. Certains voisins peuvent être tentés de siphonner la bande passante de votre Wifi, pour naviguer sans payer, ou plus grave, pour se livrer à des actes malveillants.

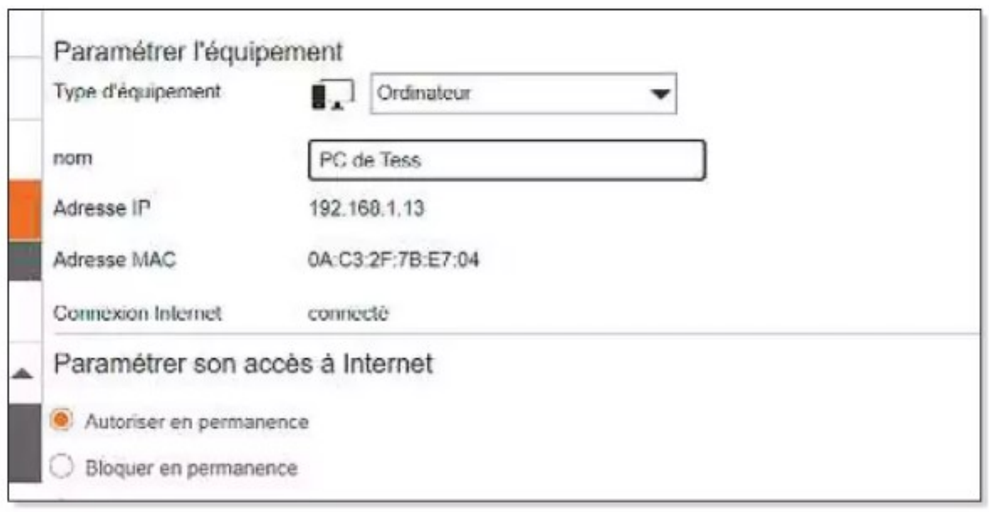
1 DISSIMULEZ VOTRE SSID

Le Service Set IDentifier est le nom de votre routeur, celui que vous cherchez dans la liste des réseaux disponibles quand vous raccordez un nouvel appareil en Wifi. Pour dissimuler le SSID, il faut accéder à l'interface d'administration de la box depuis un navigateur connecté à internet via la box (entrez l'adresse livebox pour Orange, mabbox.bytel.fr pour Bouygues, mafreebox.freebox.fr pour Free, monmodem pour SFR). Accédez aux paramétrages Wifi et décochez **Diffuser le nom** ou activez **Cacher le SSID** selon votre appareil. Rendez-vous ensuite dans les paramètres avancés et vérifiez, dans **Type de sécurité**, que vous êtes en WPA2 ou WPA3, sinon, sélectionnez-le.

2 UTILISEZ UN VPN ET LE MODE INVITÉ

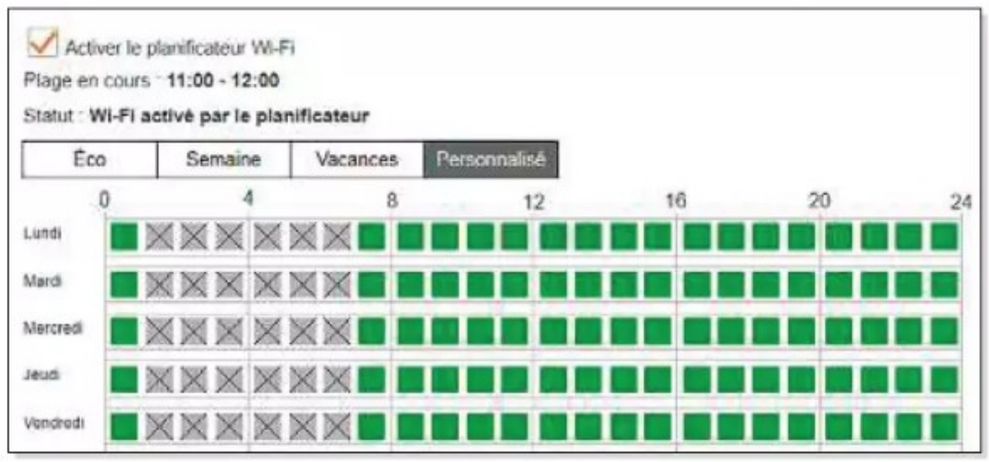
Si vous surfez avec un VPN, un hacker potentiel n'a alors affaire qu'à des données indéchiffrables. Sachez que certains navigateurs tels que Brave ou Opera intègrent un VPN. En revanche, vous devez recourir à une solution payante pour en ajouter un à votre routeur, et par conséquent protéger tous les accès à votre réseau domestique, y compris ceux des objets connectés. Dans le cas d'un assistant personnel, d'une sonnette ou d'une smart TV par exemple, privilégiez, si votre box en dispose d'un, le réseau Wifi invité de cette dernière. De cette manière, l'accès à internet est autorisé mais le réseau privé demeure isolé.





3 VÉRIFIEZ LES APPAREILS CONNECTÉS

Depuis l'interface d'administration de votre box *(voir étape 1)*, vous accédez à la liste des équipements connectés. Tout appareil inconnu, ou que vous n'utilisez plus, doit absolument être supprimé du réseau domestique. Ne laissez pas de place au doute : cliquez sur le matériel concerné et optez pour **Bloquer**. Certains dispositifs ont parfois des intitulés fantaisistes. Procédez par élimination. Commencez par bloquer l'appareil non identifié, quitte à rétablir l'accès lorsque vous êtes certain qu'il s'agit d'un périphérique sûr. Profitez-en pour renommer le matériel en question afin de mieux l'identifier à l'avenir.



4 PLANIFIEZ LES HEURES D'ACCÈS

La meilleure sécurité pour le Wifi demeure encore de ne pas en avoir ! Reste qu'il n'est pas possible de relier tous les appareils en Ethernet. Mais rien ne vous empêche de décider des plages horaires durant lesquelles le Wifi est fonctionnel ou non. Accédez à l'interface de votre box internet et trouvez le planificateur. Là, vous pouvez désactiver le Wifi dans le courant de la nuit ou durant la journée, lorsque personne n'est à la maison. Une solution qui ne convient pas toutefois si vous disposez de caméras de surveillance ou d'un portier connecté en Wifi. Dernier conseil, veillez à maintenir vos appareils à jour, y compris le routeur.

EMTEC

X210 ELITE

USB-C™ 3.2 Gen2

Faites équipe avec le SSD portable X210, le champion de la sauvegarde des moments les plus précieux !

Jusqu'à **500** Mo/s*

X210 GAMING

USB-C™ 3.2 Gen2

Digne des plus grands exploits, le SSD portable X210G sera votre meilleur allié sur tous les terrains numériques !

Jusqu'à **1100** Mo/s*

Retrouvez tous nos produits sur **www.emtec-international.com**

USB Type-C™ and USB-C™ sont des marques déposées de USB Implementers Forum.
*Les performances peuvent varier en fonction de l'utilisation et du matériel

DIFFICULTÉ
MODÉRÉE
TEMPS
20 MIN
DOMAINE
INTERNET

ÉVITEZ LES PIÈGES DES RÉSEAUX PUBLICS

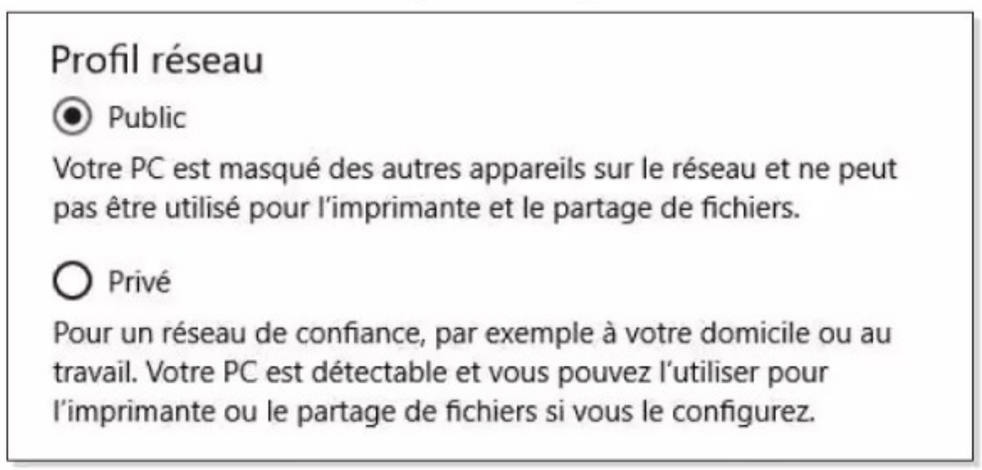
À défaut de disposer d'un VPN, **il existe des précautions élémentaires et des réglages susceptibles d'éloigner les utilisateurs malveillants** quand on se connecte à un point d'accès sans fil dans l'espace public.

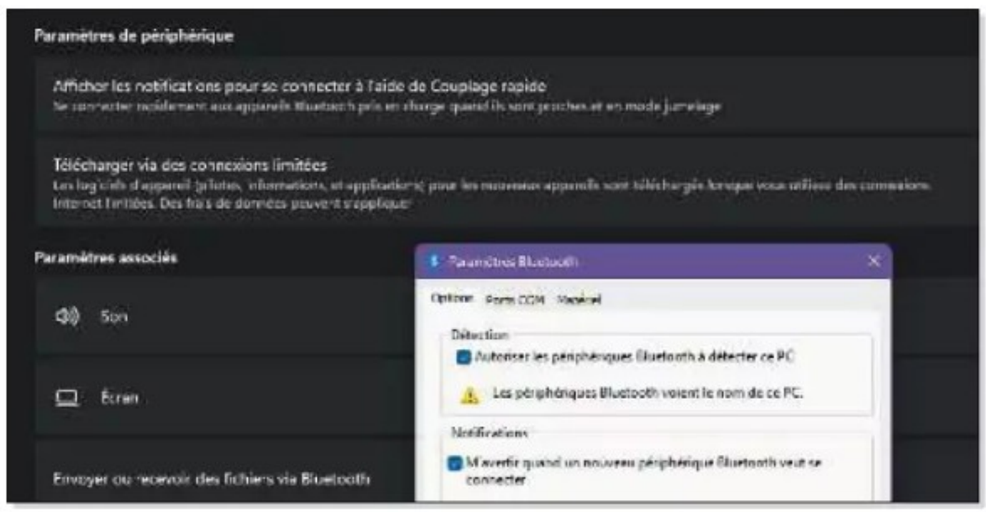
1 EMPÊCHEZ LA CONNEXION AUTOMATIQUE

Pour éviter que votre PC ne bascule sur les réseaux publics auxquels vous vous êtes déjà connecté, ouvrez les paramètres de Windows, cliquez sur **Réseau** et **Internet, Wi-Fi, Gérer les réseaux connus**. Sélectionnez un point d'accès et décochez **Connexion automatique lorsque le réseau est à portée**. N'hésitez pas non plus à **masquer** les « *hotspots* » dès que vous n'en avez plus l'usage. Toujours sur la page **Gérer les réseaux connus**, actionnez le bouton **Oublier** à droite du nom du point d'accès du lieu que vous venez de quitter. Vous pouvez aussi compliquer l'identification de votre PC en activant **Adresses matérielles aléatoires** sur la page des propriétés du réseau Wifi.

2 GARDEZ LE BON PROFIL

Le profil réseau est généralement public quand vous vous connectez pour la première fois en Wifi. Mais mieux vaut s'en assurer, car cette option empêche la détection de votre appareil sur le réseau et l'activation du partage de fichiers. Dans les paramètres de Windows 11, pointez sur **Réseau et Internet**, **Wi-Fi**, **Propriétés de Nom du réseau**, puis sous **Type du profil de réseau**, cochez **Réseau public**. Windows 10 vous demande quant à lui s'il s'agit d'un réseau public lors de la connexion à un hotspot. Pour vérifier le statut d'une connexion, allez dans **Paramètres**, **Réseau et Internet**, cliquez sur **État** sous le nom du réseau, puis sur **Propriétés**.





3 PROTÉGEZ VOTRE BLUETOOTH

Pour empêcher qu'un utilisateur ne se connecte à votre ordinateur via Bluetooth et collecte des données à votre insu, rendez-vous dans les paramètres de Windows 10 et choisissez **Périphériques**, **Paramètres Bluetooth avancés**, **M'avertir lorsqu'un appareil Bluetooth veut se connecter**. Désactivez l'option **Autoriser les périphériques Bluetooth à détecter ce PC**. Ainsi, votre ordinateur restera invisible pour les matériels situés à portée de Bluetooth. Dans Windows 11, ces mêmes options se trouvent sur la page **Paramètres**, **Bluetooth et appareils**, **Appareil** et **Plus de paramètres Bluetooth**.

4 VEILLEZ AUSSI SUR VOTRE MOBILE

Si vous utilisez le partage de connexion de votre téléphone pour naviguer sur internet et envoyer des mails depuis votre PC, pensez à sécuriser les échanges sur le mobile. Prenez l'habitude de désactiver le Bluetooth dès que vous n'en avez pas l'usage. Dans le cas d'un appareil sous Android, déployez le volet des réglages rapides et effleurez la vignette ou l'icône **Bluetooth** pour couper ce mode de transmission. Sur un iPhone, l'opération s'effectue dans le centre de contrôle en touchant l'icône **Bluetooth**. Dans les réglages, pressez aussi **Airdrop**, puis **Réception désactivée** ou **Contacts uniquement**.

DIFFICULTÉ
MODÉRÉE
TEMPS
30 MIN
DOMAINE
SYSTÈME

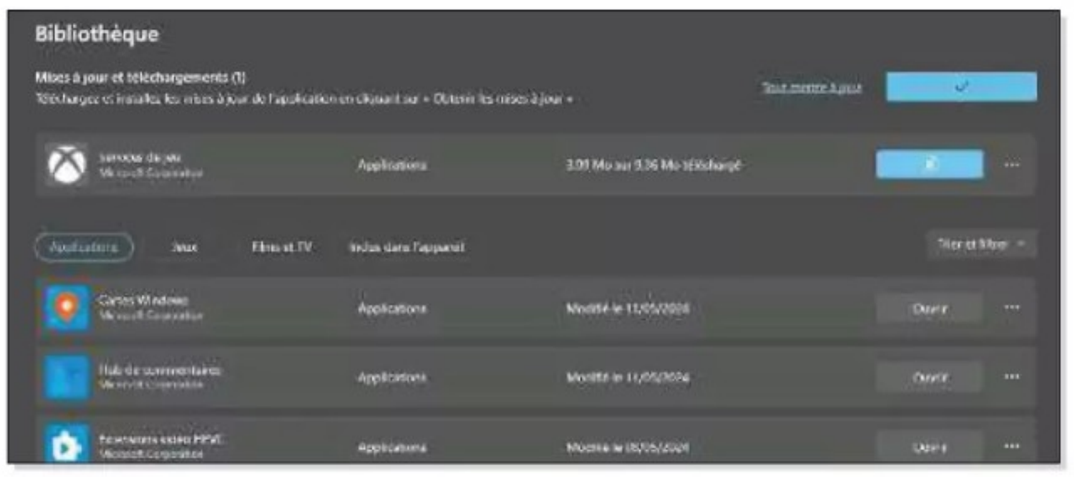
GARDEZ VOS LOGICIELS À JOUR

Même si Windows et de nombreux programmes intègrent un dispositif de mise à jour automatique, **certaines applications nécessitent une intervention de votre part.**

astuce 1

VÉRIFIEZ LA BIBLIOTHÈQUE DU MICROSOFT STORE

La boutique de Windows n'opère pas systématiquement la mise à jour des logiciels qui y ont été téléchargés. Pour vous assurer de disposer des dernières versions, lancez le Microsoft Store, puis cliquez en bas de la fenêtre sur l'onglet **Bibliothèque**, **Obtenir les mises à jour**. Ouvrez par exemple une application du pack Office, pointez sur **Fichier**, **Compte** et sur l'icône **Options de mise à jour**, **Mettre à jour**. Cette même icône propose de désactiver les mises à jour si un problème de sécurité a été identifié et de suivre les modifications apportées par Microsoft en choisissant **Afficher les mises à jour**.



astuce 2

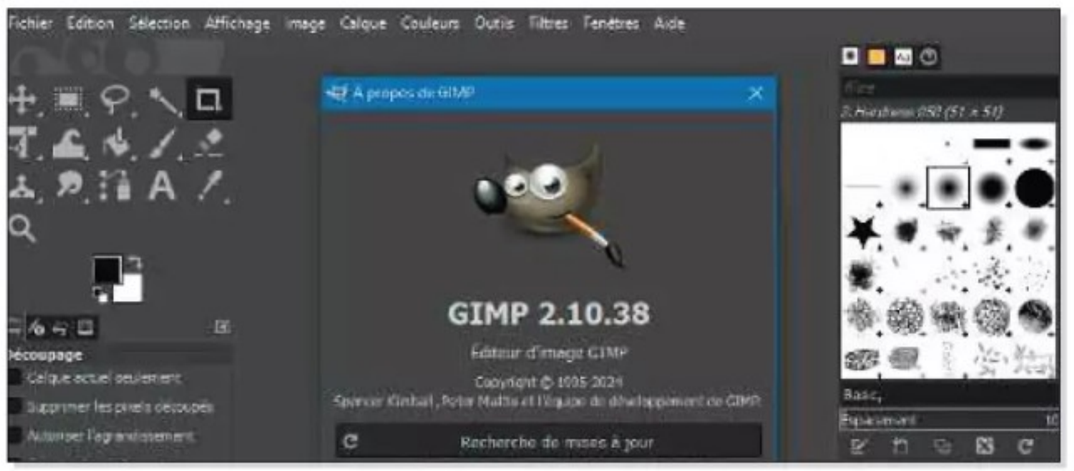
ACTUALISEZ VOS NAVIGATEURS

Les mises à jour ne sont pas automatiques ou prennent parfois du temps à se répandre sur tous les appareils. Avec Google Chrome, cliquez sur les trois points en haut à droite de la fenêtre, puis sur **Paramètres**, **À propos de Chrome** pour installer d'éventuels correctifs. Il suffit de relancer le navigateur pour en profiter. Avec Microsoft Edge et la plupart des butineurs reposant sur le noyau Chromium, la procédure est identique. Si vous utilisez Opera, déroulez le menu **O** présent en haut à gauche de la fenêtre et choisissez **Mise à jour et récupération**, **Vérifier les mises à jour**.

astuce 3

RECHERCHEZ DE NOUVELLES VERSIONS

Tout dépend de la façon dont vous avez acquis le programme installé sur votre système. Pour une application comme Gimp, si vous êtes passé par le Microsoft Store, il faut retourner sur ce dernier pour lancer la mise à jour *(lire étape 1)*. Si vous l'avez obtenu sur le site de l'éditeur ou une plateforme de téléchargement, rendez-vous dans l'application, cliquez sur **Aide**, **À propos de Gimp** et **Recherche de mise à jour**. D'autres utilitaires tels que VLC se mettent à jour au lancement, mais pour vous assurer d'utiliser la dernière version, cliquez sur **Aide** et **vérifier les mises à jour**.



astuce 4

PARAMÉTREZ WINDOWS UPDATE

Rendez-vous dans les **Paramètres** de Windows et pointez sur **Mise à jour et sécurité**, **Windows Update**. Sélectionnez les **Options avancées** et activez le mode **Recevoir les mises à jour d'autres produits Microsoft lorsque vous mettez à jour Windows**. Les périphériques et composants ont eux aussi besoin de leurs utilitaires pour se mettre à jour. La carte vidéo, par exemple, passe par l'outil Geforce Experience s'il s'agit d'un modèle Nvidia, ou Adrenalin dans le cas d'une carte AMD. Même les casques, claviers et souris nécessitent un utilitaire pour intégrer les correctifs de leur *firmware*. Nous vous conseillons donc de les installer… et de les garder à jour !

DIFFICULTÉ
MODÉRÉE
TEMPS
VARIABLE
DOMAINE
SÉCURITÉ

RENFORCEZ LA CONFIDENTIALITÉ DE VOS DONNÉES

Dès que vos appareils s'allument, **le regard inquisiteur de Google, Amazon, Facebook, Apple, Microsoft… plane sur vous.** Évitez cette surveillance en réduisant l'exposition de vos données.

Dès que l'on se connecte à internet, il est pratiquement impossible d'échapper à l'espionnage des géants de la tech. Surtout lorsqu'on se comporte en « bon père de famille », sans chercher à se cacher. Ce sont précisément ces vies numériques bien ordonnées qui intéressent Google, Microsoft, Apple, Facebook, Amazon… et leur assurent des revenus considérables via la vente des données privées, qui servent ensuite à diffuser des publicités ciblées. Chacune de nos activités en ligne, telles que liker une publication, installer une application ou consulter un site web, sont minutieusement analysées et utilisées pour la création de profils publicitaires qui deviennent de véritables mines d'or pour les annonceurs. Il suffit de jeter un coup d'œil aux détails du module d'antipistage du moteur de recherche DuckDuckGo pour mesurer l'ampleur de la collecte d'informations ! Les tentatives de suivi sont constantes. L'espionnage se prolonge même lorsque les applications ne sont pas actives. C'est le cas, par exemple, avec celle de Météo France. Non contente d'enregistrer les habitudes de ses usagers, celle-ci prend la liberté d'autoriser les traceurs de sociétés externes à établir des profils toujours plus précis de ses clients.

PAS QUESTION DE BAISSER LES BRAS. Se protéger du pistage en ligne, c'est défendre nos vies privées et celles de nos proches. Cela commence par faire un sérieux tri dans les données – parfois oubliées – que nous stockons sur nos appareils. Dans un second temps, il faut mettre en place des mesures de protection autour des informations sensibles. Ces différentes barrières, intégrées pour certaines aux systèmes d'exploitation des appareils et aux navigateurs, n'offrent pas des garanties absolues. Elles contribuent toutefois à la tranquillité digitale. Certains utilisateurs jugeront sans doute de tels dispositifs insuffisants. La solution passera alors par l'abandon des services et outils liés aux géants de la tech, qu'il s'agisse de passer de Windows à Linux ou de « dégoogelisé » l'environnement de son smartphone Android. Un choix radical, réservé aux amateurs avertis, mais qui éloigne les grandes oreilles de Google et consorts. ●

BOÎTE À OUTILS POUR CE PAS À PAS, NOUS AVONS UTILISÉ LES ÉLÉMENTS SUIVANTS

PC ou Mac

Téléphone Android ou iPhone

Application CCleaner, DuckDuckGo, Greenify, PrivaZer, Proton VPN

ÉTAPE 1

UTILISEZ LES RÉGLAGES INTÉGRÉS AUX APPAREILS

Conscients des attentes des utilisateurs, **les géants de la tech invitent les utilisateurs à réduire l'exposition de leurs données…** avec modération bien sûr !

GOOGLE

1 EFFACEZ LES HISTORIQUES D'ACTIVITÉ ET DE POSITION

Connectez-vous à votre compte Google (bit.ly/3SJCRnH) et accédez à la section **Faire un Check-up Confidentialité**. Cliquez sur **Activité sur le Web et les applications**. Déroulez le menu **Désactiver** et choisissez **Désactiver et supprimer l'activité**. Validez et réglez le délai de suppression sur trois mois. Passez ensuite à la rubrique **Voir toutes les commandes relatives à l'activité** pour désactiver et supprimer l'historique des positions enregistré par vos appareils mobiles. Faites de même avec l'historique de YouTube en sélectionnant la commande **Suspendre**. Pointez sur **Gérer l'activité** pour afficher un résumé des dernières modifications.

2 DÉSACTIVEZ LA PUBLICITÉ PERSONNALISÉE

Cliquez sur **Mes préférences publicitaires**, puis sur **Activé** et **Désactiver**. Vous ne verrez ainsi plus de publicités personnalisées et vos données personnelles (âge, activité Google, etc.) ne seront plus utilisées pour cibler les annonces. Vérifiez également que votre compte Google n'est pas associé à des entreprises externes autorisées à vous espionner. Revenez sur la page d'accueil en pointant sur l'avatar en haut à droite de la fenêtre et cliquez sur **Gérer votre compte Google**. Accédez à **Gérer vos données et votre vie privée, Données des applis et services que vous utilisez, Applis et services tiers**. Passez en revue les acteurs liés à votre compte et supprimez les connexions superflues avec la flèche › à droite.

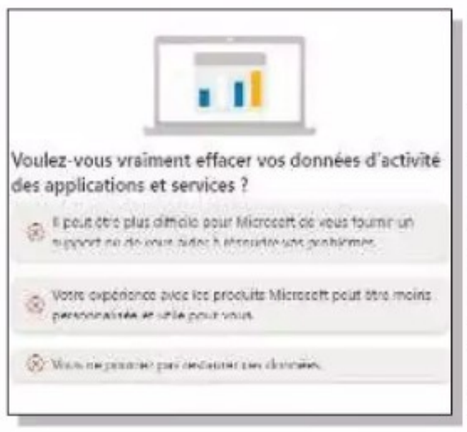
MICROSOFT

1 INTERDISEZ LES DONNÉES FACULTATIVES

Dans les paramètres de votre PC (**Windows+I**), **Confidentialité et sécurité**, déroulez le volet **Général** des **Autorisations de Windows** et désactivez les quatre curseurs associés. Revenez à la page précédente, cliquez sur **Diagnostics et commentaires** et suspendez le mode **Envoyer des données de diagnostic facultatives**. Répétez l'opération pour la section **Expériences personnalisées**. Intéressez-vous aussi au menu **Supprimer les données de diagnostic**. Retournez enfin à la première page de **Confidentialité et sécurité** pour désactiver et effacer l'**Historique des activités**.

2 CONFIGUREZ LE TABLEAU DE BORD DE CONFIDENTIALITÉ

Toujours dans le menu **Confidentialité et sécurité**, cliquez à présent sur **Général**, **Tableau de bord de confidentialité**. Le navigateur internet se lance automatiquement et vous mène à la page de gestion des comptes Microsoft. Saisissez vos identifiants de connexion pour accéder au menu de confidentialité. Utilisez la section **Gérer vos données d'activité** afin de réduire votre empreinte sur les serveurs Microsoft. Déroulez le menu **Activité de localisation, Gérer**. Choisissez une fréquence d'effacement tous les trente jours, puis affichez l'activité des applications et services et pointez sur **Effacer toutes les activités de l'application et du service**. Au bas de la page, désactivez le mode **Revoir les paramètres d'une publicité**.



PAS À PAS EXPRESS FAITES LE MÉNAGE DANS VOS APPAREILS APPLE

Si le fabricant des **Mac adopte une politique moins agressive** en matière de collecte des données que ses rivaux, cela ne signifie pas pour autant qu'il s'en désintéresse !

01. Suspendez les annonces personnalisées

Ouvrez les réglages de l'iPhone. Accédez à la section **Confidentialité et sécurité**, **Publicité Apple** et suspendez les annonces spécialisées. Revenez en arrière, effleurez **Analyse et améliorations** et désactivez les quatre curseurs.

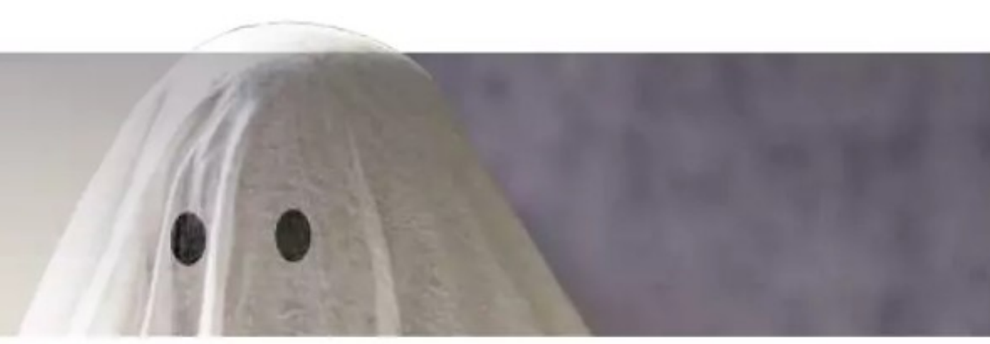
02. Révoquez les accès des applications

Sur la page **Réglages**, effectuez une requête sur le terme **Contrôle de sécurité**. Effleurez **Gérer les partages et les accès**, **Continuer**, **Étape 2 Accès des apps**. Cochez les applis dont vous souhaitez révoquer l'accès à votre compte Apple.

03. Stoppez les analyses de l'iCloud

Connectez-vous à votre compte Apple depuis un Mac (bit.ly/3SJRlE5). Depuis la page **Identifiant Apple**, désactivez l'analyse iCloud dans le menu **Confidentialité**. Suivez le lien **Gérer vos données** pour obtenir une copie des infos enregistrées.

ANDREY POPOV/ISTOCKPHOTO



ÉTAPE 2

SUPPRIMEZ LES DONNÉES PRIVÉES DE WINDOWS

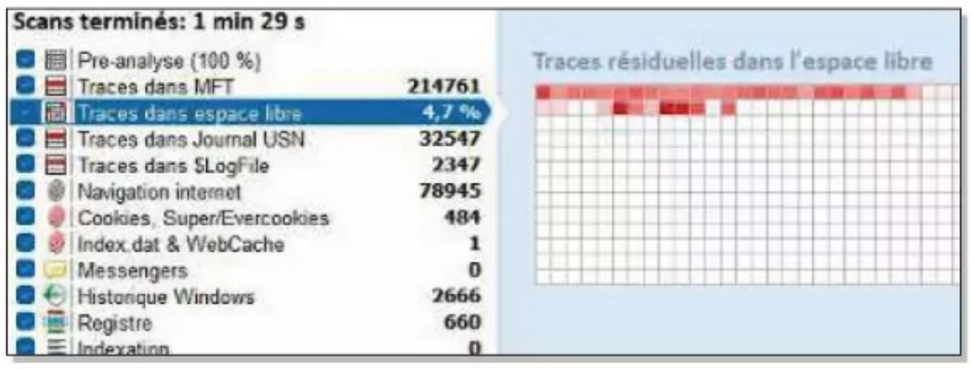
N'attendez pas que Microsoft efface l'intégralité de votre vie privée.
Pour cela, mieux vaut s'en remettre à une application tierce comme PrivaZer.

1 CONFIGUREZ PRIVAZER LORS DE L'INSTALLATION

Installez la version gratuite de PrivaZer (bit.ly/3SFx7eC). La procédure intègre 18 étapes qui servent à optimiser le fonctionnement de l'application. Commencez en choisissant l'option **Utilisateur avancé** du menu **Quel genre d'utilisateur êtes-vous ?** Cochez la case **Oui, raccourcis invalides + Liste des plus utilisés** dans **Nettoyage**. Continuez en optant pour le **Vidage de la corbeille sans trace** à chaque nettoyage du PC et la **Suppression des historiques des logiciels de bureautique** et **photos/images**. Pour rendre invisible la liste des fichiers et dossiers récemment ouverts dans l'Explorateur de Windows, cochez la case **Oui**. Acceptez l'effacement de l'historique du navigateur et des pages ouvertes lors de la dernière session.

2 RAYEZ LES ÉLÉMENTS INDÉSIRABLES

Poursuivez les réglages de PrivaZer en autorisant une sélection intelligente des cookies et en supprimant l'intégralité du WebCache où est conservée toute votre activité sur internet en arrière-plan. Acceptez le nettoyage du WebCache, des Shellbags, du SRUM (*system resource usage manager*) et l'effacement des anciennes versions de Windows, Windows Update et Windows Prefetch. Gardez l'hibernation du PC et validez vos choix avec **Enregistrer**. Lancez une première analyse en cliquant sur **OK**. PrivaZer affiche les cookies qu'il juge utile. Si vous souhaitez effacer l'un de ces éléments, sélectionnez-le et pointez sur **Supprimer**. Reprenez le cours de l'analyse.



3 EFFECTUEZ UN NETTOYAGE EN PROFONDEUR

PrivaZer vous demandera de fermer votre navigateur internet afin de purger l'historique des sites visités. Une fois l'analyse terminée, un bilan s'affiche donnant l'occasion d'apprécier l'ampleur des traces que vous laissez derrière vous ! L'application recense une vingtaine de points critiques. Il vous appartient de décider ou non d'appliquer les recommandations. Nous vous recommandons de conserver en bloc les préconisations. Pensez en revanche à cocher l'option **Créer un point de restauration** avant de cliquer sur le bouton **Nettoyer**. Pour des données ultra-confidentielles, pointez sur **Options de nettoyage**, **Réécriture sécurisée** et cochez le mode **Disque dur**. Déroulez le menu **1 PASSE** et choisissez la méthode **3 PASSES USA DOD 5220.22-M**. Validez avec **Nettoyage normal**.

4 ÉTENDEZ L'ANALYSE À VOS PÉRIPHÉRIQUES DE STOCKAGE

Après un premier nettoyage réussi, redémarrez le PC et lancez PrivaZer. Demandez-lui de se pencher sur le cas d'un disque dur externe, d'une clé USB ou d'une carte mémoire en allant sur **Scanner en profondeur**. Désignez le type d'appareil et lancez l'analyse. Vous pouvez également exiger de l'application qu'elle cherche des traces spécifiques telles que les activités internet ou des logiciels. Accédez au menu **Programmées** pour planifier des nettoyages automatiques chaque semaine ou mois, à l'onglet **Nettoyage** des **Options avancées** pour ajuster les paramètres de suppression (normale ou sécurisée) et définir le nombre de passes.

Faites table rase sur Mac

Il n'existe pas de version de PrivaZer adaptée à macOS. Les utilisateurs d'ordinateurs Apple peuvent cependant se tourner vers Mac Cleaner (bit.ly/46eexgP). Payant (48 € à vie), celui-ci s'occupe de supprimer les fichiers inutiles, comme le cache et les journaux système, l'historique de localisation des utilisateurs, les cookies, les recherches, les téléchargements. Il gère également les plug-ins et les extensions, les programmes indésirables et les fichiers cachés. L'interface grand public facilite la prise en main. Si vous préférez une application gratuite, tournez-vous vers la version Mac de CCleaner (bit.ly/3uaWvP4) pour venir à bout des éléments indésirables de votre système.

ÉTAPE 3

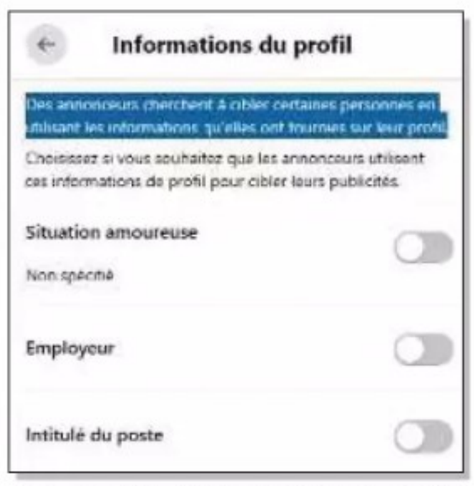
EMPÊCHEZ LES RÉSEAUX D'EXPLOITER VOTRE VIE NUMÉRIQUE

Il est ardu, voire impossible, de dissimuler ses données privées sur les réseaux sociaux. **Cependant, des outils tels qu'Off Facebook Activity permettent d'en effacer une partie.**

1 SUPPRIMEZ VOS ACTIVITÉS EN DEHORS DE FACEBOOK

En naviguant sur le web, vous êtes traqué, et les sites visités partagent souvent vos activités avec Meta. Vous pouvez limiter cette mise en commun en pointant sur votre avatar, puis sur **Paramètres et confidentialité**, **Paramètres**, **Vos informations Facebook** en colonne gauche et enfin **Activités en dehors de Facebook**. Un menu vous invite à dissocier certaines activités et à effacer l'activité passée. Dans le premier cas, cochez les cases des entreprises liées à votre compte pour couper court à toute relation. Anticipez vos interactions à venir en allant sur **Gérer l'activité future** et en cochant la case de dissociation.

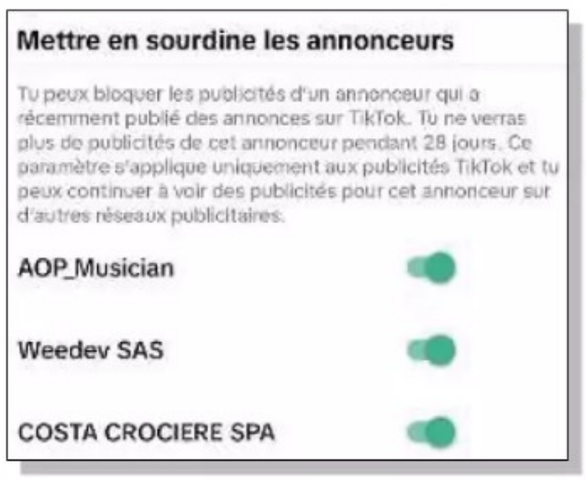
2 RÉDUISEZ LA PUBLICITÉ CIBLÉE



Les publicités sur Facebook sont par défaut personnalisées. Vous pouvez basculer ce paramètre intrusif vers une option générique qui réduit l'utilisation de vos données. Accédez au menu **Confidentialité** en colonne gauche des paramètres. Cliquez sur **Vérifier certains paramètres importants**. L'assistant de confidentialité apparaît. Dirigez-vous vers la section **Vos préférences publicitaires sur Facebook**, **Continuer**, **Suivant**. Désactivez les quatre curseurs d'informations du profil. Poursuivez en réglant les interactions sociales sur **vous-même uniquement**. Enfin, visitez la section **Les paramètres de vos données Facebook** et supprimez les éventuels sites web et applications auxquels vous vous êtes connectés.

3 MINIMISEZ VOTRE EMPREINTE SUR TIKTOK

Le réseau social chinois de partage de vidéos cible votre profil pour proposer des réclames adaptées. Empêchez ce suivi en effaçant l'activité que les annonceurs ont partagée avec vous en dehors de TikTok. Ouvrez l'application, accédez à votre profil en bas à droite et pointez sur les traits horizontaux en haut de la page, puis sur **Paramètres et confidentialité**, **Publicités**. Décochez l'option **Publicités personnalisées**. Effacez ensuite votre activité dans la rubrique **Gérer tes données hors TikTok**. Rendez-vous pour finir dans la section **Mettre en sourdine les annonceurs** et décochez les sociétés qui ont récemment publié des annonces sur la plateforme.



4 EMPÊCHEZ LINKEDIN DE TROP S'INCRUSTER

Le réseau professionnel LinkedIn, détenu par Microsoft, espionne vos interactions sociales dans le but d'afficher des publicités ciblées. Dans l'application mobile du service, effleurez votre avatar, allez dans **Préférences**, **Données relatives à la publicité** et désactivez le curseur **Données du profil pour la personnalisation des publicités**. Pointez ensuite sur **Catégories de centres d'intérêt** et désactivez cet autre curseur. Répétez l'opération pour les différentes entrées du menu **Données tierces**. Vous avez aussi la possibilité de contrôler et d'effacer vos données en modifiant certains paramètres depuis l'aide en ligne (bit.ly/3ME0n1m).

PAS À PAS EXPRESS

LIMITEZ AU MAXIMUM VOTRE EXPOSITION SUR X

Depuis le rachat de Twitter par Elon Musk, **le réseau social est plus libéral que jamais** en termes de collecte et d'utilisation des données personnelles. La prudence s'impose.

01. Réglez les options de confidentialité

Ouvrez la version web de l'application dans un navigateur et saisissez vos identifiants. Pointez sur **Plus**, **Paramètres et support**, **Paramètres et confidentialité**, **Confidentialité et sécurité** et rejoignez la section **Partage des données et personnalisation**.

02. Mettez de l'ordre dans le partage de données

Décochez la case **Intérêts** et **Publicités personnalisées** dans **Préférences en matière de publicité**. Cochez le mode **Refuser les cookies non nécessaires** du menu suivant. Désactivez ensuite l'option **Identité déduite** et interdisez le partage de données avec les partenaires commerciaux.

03. Interdisez l'exploitation de votre identité

Rendez-vous dans **Sécurité et accès au compte**, **Applications et sessions**, **Applications connectées** et révoquez les privilèges alloués aux services et logiciels tiers. Désactivez également le mode **Identité déduite** dans **Appareils et Applications connectées**.

ÉTAPE 4

FERMEZ VOS COMPTES META, GOOGLE, MICROSOFT...

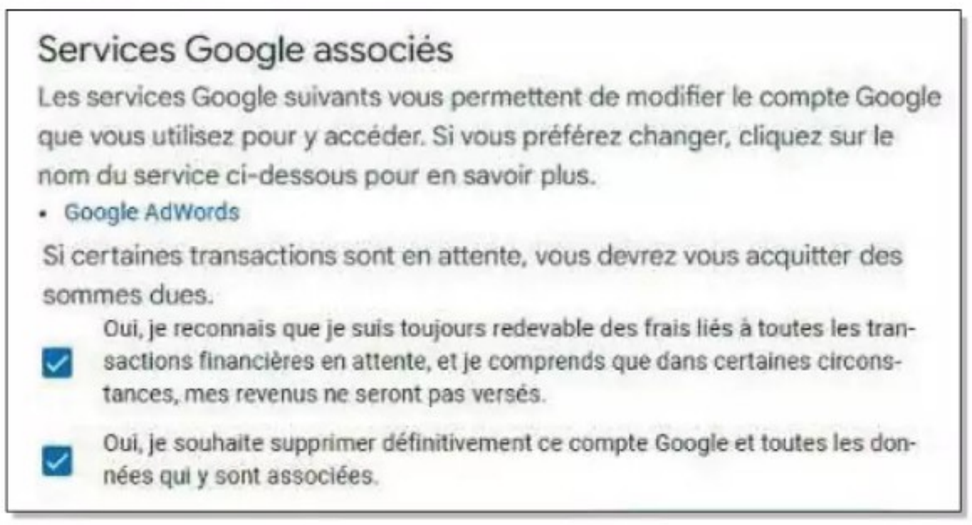
Il existe une **solution imparable à la collecte de données** : clore définitivement les comptes qui vous lient à Windows, Facebook, Instagram...

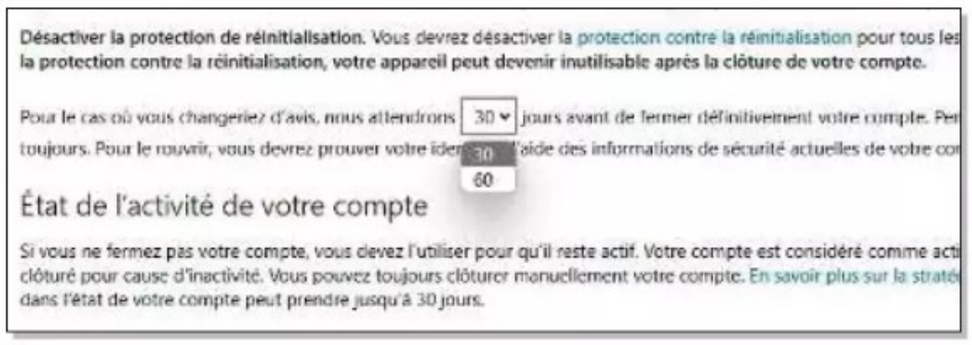
1 PRIVEZ META DE VOS DONNÉES PERSONNELLES

Un compte Facebook ou Instagram peut à tout moment être désactivé temporairement. Cependant, la collecte des données continue, Meta estimant que la désactivation ne signifie pas le retrait du consentement au traitement des données. Mieux vaut donc le supprimer comme suit : cliquez sur votre avatar puis sur **Paramètres et confidentialité, Paramètres, Espace Comptes** en haut à gauche. Allez sur **Informations personnelles** en colonne gauche et sur **Propriété et contrôle du compte, Désactivation ou suppression**. Pointez sur **Facebook** ou **Instagram** et cochez la case de **suppression définitive**. Pensez à télécharger vos informations comme proposé, avant de confirmer son effacement.

2 OUBLIEZ GOOGLE

La suppression d'un compte Google est synonyme de handicap. Plus de Gmail, plus de services Google sur votre téléphone Android, plus d'espace de stockage Drive. Pensez-y avant de vous lancer. Ouvrez votre compte Microsoft (bit.ly/3MEhrUY) et cliquez sur **Données et confidentialité** en colonne gauche. Déroulez la page jusqu'en bas et pointez sur **Supprimer votre compte Google** dans la rubrique **Plus d'options**. Une page récapitulative indique le contenu qui sera effectivement effacé. Vous devez ensuite cocher les différentes cases d'acceptation avant de procéder. Un lien de téléchargement vous sera adressé afin que vous téléchargiez une archive de vos données avant leur effacement définitif.





3 PASSEZ-VOUS DE MICROSOFT

Renoncer complètement à l'écosystème Microsoft peut aussi sembler un peu fou. Il existe pourtant des solutions pour remplacer Windows, à commencer par les différentes distributions Linux, Ubuntu en tête, mais aussi les logiciels de la suite Office et la messagerie Outlook. Pour résilier un compte Microsoft, rendez-vous sur la page de clôture disponible à l'adresse bit.ly/3QWWIhL et entrez vos identifiants. L'interface propose de télécharger les données et de désactiver le dispositif de protection qui bloque la réinitialisation des appareils Windows associés au compte. Vous êtes également libre de définir le délai de clôture effectif (après 30 ou 60 jours). Cliquez sur **Suivant** et suivez la procédure, qui inclut notamment l'annulation des abonnements actifs (Microsoft 365, Skype), indispensable préalable à la fermeture du compte.

4 DITES ADIEU À MESSENGER, TIKTOK ET WHATSAPP

Vous avez beau vous désinscrire de Facebook et Instagram, Messenger reste quant à lui actif. Pour procéder à la clôture du compte, ouvrez l'application, déroulez le volet de menu et touchez l'icône des paramètres, et **Espace Comptes, Informations personnelles, Propriété et contrôle du compte, Désactivation ou suppression**. En ce qui concerne TikTok, effleurez votre profil en bas à droite, les traits horizontaux pour accéder à la page **Paramètres et confidentialité**, puis **Compte, Désactiver ou supprimer le compte, Supprimer définitivement le compte**. Quant à WhatsApp, la démarche est simple : lancez l'application, appuyez sur les points en haut à droite, accédez à **Paramètres, Compte, Supprimer le compte**. Indiquez votre numéro de téléphone avant de procéder à la clôture.

Exercez votre droit à la suppression des données personnelles

Le droit à l'effacement des données privées en ligne est énoncé dans l'article 17 du règlement européen sur la protection des données. En conséquence, vous pouvez exiger des organisations et entreprises commerciales qu'elles suppriment les informations vous concernant dès lors lorsque vous exercez votre droit d'opposition ou retirez le consentement sur lequel repose le traitement de ces données. La Commission nationale de l'informatique et des libertés accompagne cette démarche en fournissant des modèles de courriers (bit.ly/30C92mi) adaptés à chaque situation et destinés à être envoyés aux sites web, commerçants en ligne et réseaux sociaux qui détiennent ou sont à l'origine de la publication des données. De nombreux acteurs proposent désormais des pages spécialement conçues pour enregistrer les demandes de suppression. C'est le cas de Facebook (bit.ly/40AnNur), Google (bit.ly/3G0b8r8) ou du moteur de recherche Bing (bit.ly/47uFVrR).

ÉTAPE 5

OPTIMISEZ LA PROTECTION DE VOS FICHIERS

Maintenant que le nettoyage des données privées est acté, il reste à se protéger des futures tentatives de suivi. **Un jeu d'enfants avec un VPN et DuckDuckGo.**

1 ÉLIMINEZ LES CONTENUS INUTILES

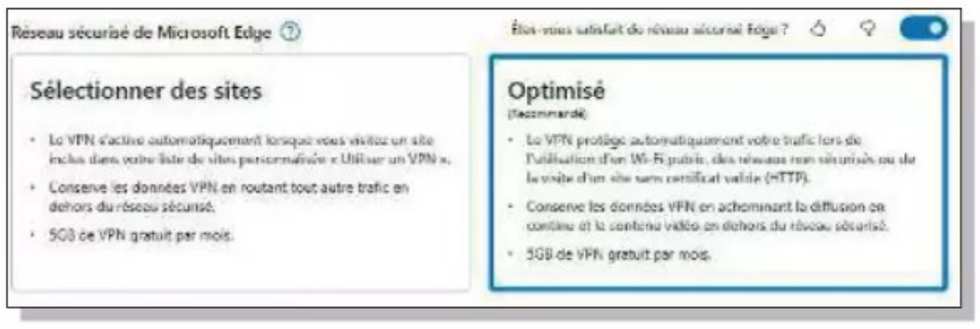
Sur Android, une première solution consiste à utiliser l'appli **Files by Google** pour gagner de précieux gigaoctets d'espace. Allez sur le menu **Nettoyer** et faites la chasse aux doublons, captures écran, vieilles photos, fichiers téléchargés… Cela fera un peu moins de données à espionner ! Pour aller plus loin, iPhone compris, installez l'appli CCleaner et lancez un nettoyage global (**Smart Scan**) du contenu du mobile. Prenez le temps de retirer photos, vidéos, contacts inutiles, fichiers enregistrés en cache, données d'applications. Et comme CCleaner aussi vous espionne, pensez à la supprimer de l'appareil après utilisation.

2 RÉDUISEZ L'ACTIVITÉ EN ARRIÈRE-PLAN DES APPLICATIONS

Sous Android, ouvrez les **Paramètres**. Accédez à **Google**, **Annonces**, **Confidentialité des annonces** et désactivez les différents curseurs. Réinitialisez l'identifiant publicitaire. Désactivez ensuite les applications qui fonctionnent en arrière-plan, collectent et transmettent des flux de données à leur éditeur. Pour cela, accédez aux paramètres de l'appareil et pointez sur **Applications**, puis sur **Accès spéciaux des applis**, **Données sans restrictions**. Désactivez l'ensemble des options. En parallèle, sollicitez l'excellente application Greenify qui force la mise en veille des applications grâce à son bouton **Zzz**. Les éléments actifs en arrière-plan sont automatiquement arrêtés.

3 RÉDUISEZ LES ACCÈS ET FLUX DE DONNÉES

Les applications peuvent potentiellement accéder au capteur photo, à la position du téléphone, au micro… Pour vérifier ces autorisations, appuyez longuement sur les icônes des applications que vous utilisez régulièrement. Sélectionnez l'option **i** (Infos) et accédez aux **Autorisations**. Les options disponibles varient selon les applications. Elles se limitent parfois à l'envoi des notifications. Si la gestion s'étend à d'autres accès, nous recommandons de restreindre les privilèges au maximum. Touchez le type d'accès (Position, Micro, etc.), cochez la case **Autoriser seulement si l'appli est utilisée** ou **Ne pas autoriser**. Sur iPhone, vous pouvez réduire les flux générés par les applications en choisissant le mode **Données réduites** : rendez-vous dans les réglages du mobile et touchez **Données cellulaires**, **Options**, **Mode de données** et **Mode Faibles données**.



4 CACHEZ-VOUS DERRIÈRE UN VPN

Le navigateur Microsoft Edge a récemment ajouté un VPN gratuit (dans la limite de 5 Go de données mensuelles). Dans ses paramètres, activez le curseur **Réseau sécurisé** et pointez sur **Optimisé**. Mozilla en propose aussi un pour Firefox, mais il est payant (bit.ly/46h3wvd). Sinon, tournez-vous vers Opera, qui incorpore lui aussi un VPN, mais gratuit, activable via une icône située dans la barre de menu. L'utilisateur peut en outre choisir une position géographique (Europe, Asie ou Amérique) afin de contourner certains filtres de services en ligne.

PAS À PAS EXPRESS

PASSEZ SOUS LES RADARS GRÂCE À DUCKDUCKGO

Le moteur de recherche DuckDuckGo, disponible sur ordinateurs et téléphones, **bloque les traceurs, efface les données de navigation en un clic** et évite que les applications vous suivent.

01. Réduisez les cookies

Installez le navigateur DuckDuckGo (bit.ly/2tkEz1V) sur votre ordinateur. Cliquez sur les points en haut à droite, puis sur **Settings**. Dans **Privacy**, cochez la case **Cookie Consent Pop-ups** afin de limiter le dépôt de cookies et d'augmenter la confidentialité.

02. Effacez instantanément

Le raccourci **Fire Button** disponible sur les versions pour ordinateurs et téléphones (bit.ly/47fukwW) du navigateur constitue une arme antitraceurs efficace. La commande ferme automatiquement tous les onglets et efface les données enregistrées durant la navigation.

03. Activez l'antisuivi

Installez le navigateur DuckDuckGo sur votre mobile. Effleurez les points en haut à droite et rejoignez la page **Paramètres**. Dans le menu **Confidentialité**, touchez **Protection contre le suivi des applications**. Le nombre de tentatives de suivi s'affiche instantanément.

DIFFICULTÉ MODÉRÉE
TEMPS 40 MIN
DOMAINE SYSTÈME

SAUVEGARDEZ LE CONTENU DE VOTRE PC

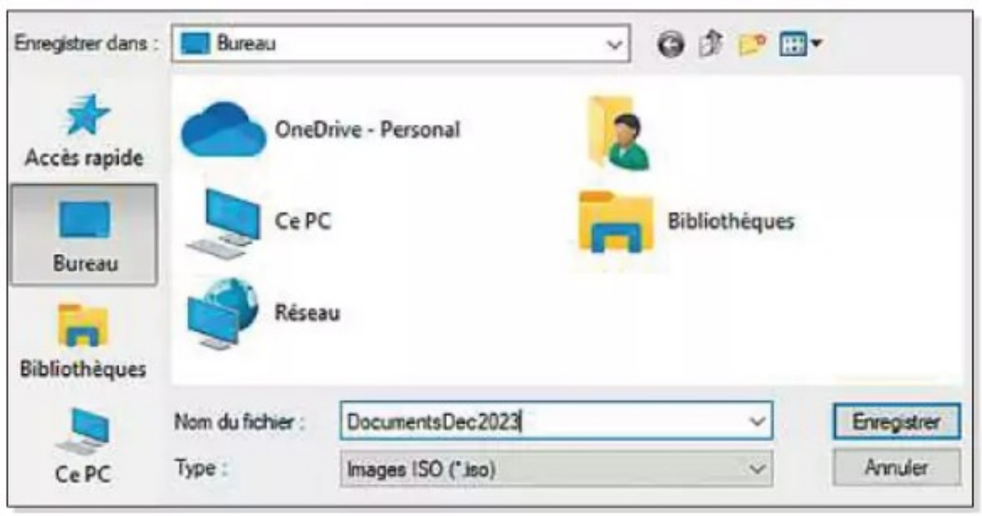
Pour ne plus perdre aucune donnée, nous ne cessons de vous inciter à réaliser des sauvegardes. **Une en local, sur un disque dur externe, l'autre conservée loin du domicile pour prévenir vols et incendies.**

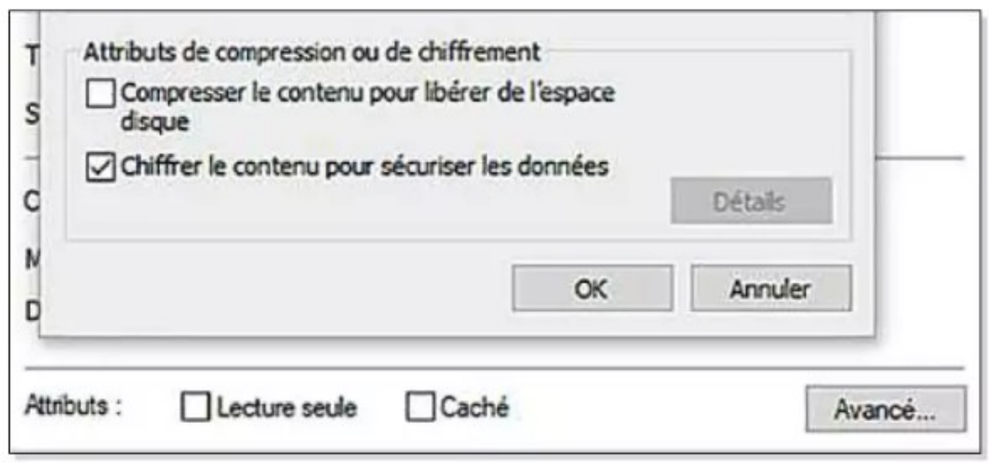
1 INSTALLEZ L'APPLICATION WINCDEMU

Il existe différentes méthodes pour effectuer des sauvegardes de fichiers, en recourant à un utilitaire spécialisé ou en procédant par copier-coller vers un périphérique de stockage externe. Vous pouvez aussi confier vos données à un service cloud européen chiffré et soumis au RGPD (pCloud, kDrive, etc.). S'il s'agit de sécuriser de grandes quantités d'informations, voire une ou plusieurs partitions entières, mieux vaut créer des images ISO que vous protégerez. Allez sur le site bit.ly/48jVFhV pour télécharger et installer WinCDEmu. Assurez-vous de disposer de Windows 11 Professionnel - le menu de création d'images ISO est absent de Windows 11 Famille.

2 CRÉEZ LA PREMIÈRE ISO

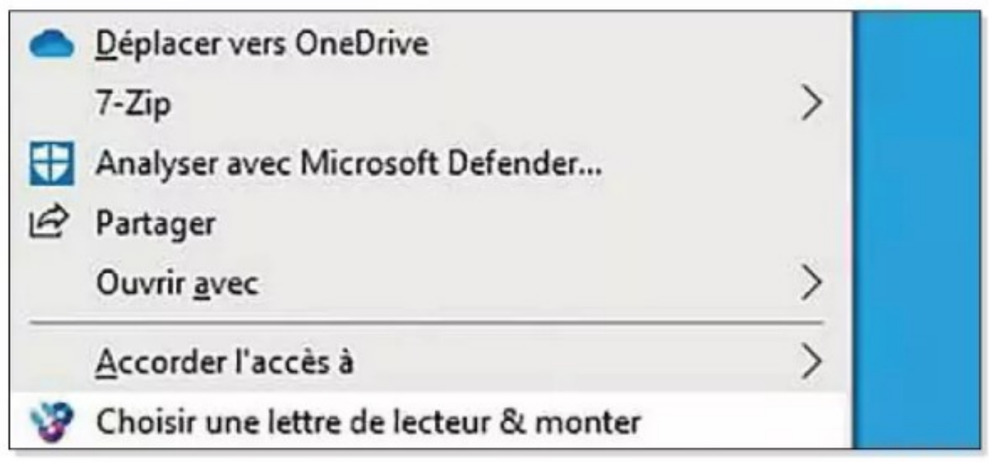
Ouvrez l'Explorateur de fichiers (**Windows** + **E**) et accédez au dossier à sauvegarder. Si vous rangez vos textes, photos et vidéos dans les librairies de Windows, il vous suffit de sélectionner le dossier utilisateur de votre compte à la racine du disque système. Effectuez ensuite un clic droit sur cet emplacement et pointez sur **Build an ISO image**. Une fois l'archive générée, cliquez sur le fichier. Celui-ci affiche des propriétés semblables à un volume de stockage (clés USB, disques durs internes et externes). Vous pouvez en l'état faire un clic droit sur le fichier ISO et graver l'image disque sur un DVD, par exemple. Avant cela, apportons un niveau de sécurité en plus.





3 CHIFFREZ L'IMAGE DISQUE

Opérez un clic droit sur le fichier, pointez sur **Propriétés**. Accédez à l'onglet **Général** et dans la section **Attributs**, choisissez **Avancé**. Cochez l'option **Chiffrer le contenu pour sécuriser les données**. Validez avec **OK** et **Appliquer**. Continuez en actionnant **Chiffrer le fichier uniquement** et le bouton **OK**. L'icône du fichier ISO affiche alors un cadenas. Le fichier ne peut s'ouvrir que sur votre PC. Vous pouvez aussi verrouiller un document ou un dossier grâce à une appli de compression avec une protection par mot de passe comme 7-Zip ou WinZip ou à un logiciel de chiffrement tel que BitLocker ou VeraCrypt.



4 ACCÉDEZ AU CONTENU DE L'ARCHIVE ISO

Le fichier ISO peut maintenant être copié sur un périphérique de stockage externe et confié à un proche. Personne d'autre que vous ne sera en mesure d'accéder à son contenu. Si vous perdez vos données et l'usage de la sauvegarde conservée chez vous sur un support externe ou dans le cloud, récupérez le disque de secours abritant l'image ISO. Branchez-le à votre ordinateur, affichez le contenu dans l'Explorateur de fichiers de Windows et effectuez un clic droit sur l'ISO. Pointez ensuite sur **Propriétés du fichier** et sélectionnez le cadenas ouvert pour déverrouiller. Il reste alors à opérer un clic droit sur l'image et à opter pour **Choisir une lettre de lecteur & monter** pour retrouver l'ensemble de vos documents.

PROTÉGEZ LES DOCUMENTS WORD ET EXCEL

Les mots de passe ont deux fonctions dans Office : interdire l'ouverture d'un document ou en autoriser l'accès en empêchant toute modification par un tiers.

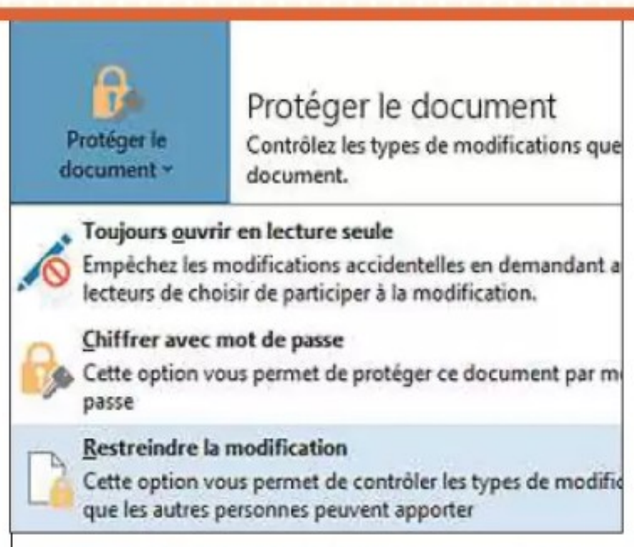
DIFFICULTÉ MODÉRÉE
TEMPS 10 MIN
DOMAINE BUREAUTIQUE

1 VERROUILLEZ L'ACCÈS À UN FICHIER WORD

Affichez le document à protéger et déroulez le menu **Fichier**. Pointez sur **Informations** à gauche, puis sur **Protéger le document**. Dans la liste, sélectionnez **Chiffrer avec mot de passe**. Saisissez la combinaison de votre choix, validez avec **OK** et confirmez le mot de passe. Mémorisez-le car il n'existe aucun moyen de le récupérer en cas d'oubli.

2 VERROUILLEZ UN CLASSEUR EXCEL

Ouvrez un document. Cliquez sur **Fichier, Informations, Protéger le classeur** et **Chiffrer avec mot de passe**. Excel propose d'appliquer un verrouillage sélectif en associant des mots de passe différents à chacune des feuilles. Vous pouvez le faire depuis la page **Informations** du fichier en choisissant **Protéger la feuille active** ou directement à partir du classeur : effectuez un clic droit sur l'onglet de la feuille concernée au bas de la fenêtre et pointez sur **Protéger la feuille**.



Restreindre les modifications empêche les changements de mise en forme.

3 ÉDITEZ UNE FEUILLE PROTÉGÉE

Contrairement à un classeur verrouillé, une feuille protégée reste lisible, mais il n'est pas possible d'y apporter des changements. Pour l'éditer, cliquez sur **Fichier, Informations, Protéger le classeur** et **Ôter la protection**. Saisissez le mot de passe et validez. Sinon, opérez un clic droit sur l'onglet de la feuille et choisissez **Ôter la protection**.

4 RETIREZ LA PROTECTION

Pour supprimer le verrouillage appliqué à un document Word ou à un classeur Excel, ouvrez le fichier, cliquez sur **Fichier, Informations, Protéger le document** et **Chiffrer avec mot de passe**. Pas de commande de suppression ? Eh non ! Il faut effacer le mot de passe et confirmer avec **OK**.

CHIFFREZ LES DONNÉES AVEC VERACRYP

Le chiffrement reste le moyen le plus sûr pour assurer la confidentialité des données de votre PC. **Optez pour une approche radicale** en cryptant l'ensemble du disque système.

DIFFICULTÉ ÉLEVÉE
TEMPS 60 MIN
DOMAINE SYSTÈME

1 SÉLECTIONNEZ LE DISQUE OU LA PARTITION

Commencez par installer VeraCrypt, disponible sur le site veracrypt.fr, dans la section **Téléchargements**. Lancez le programme et accédez au menu **Système, Chiffrer la partition/le disque système**. Vous pouvez choisir le mode **Caché** si vous avez peur que l'on vous demande de lever le chiffrement de votre PC sous la contrainte ou vous en tenir au mode **Normal**. Déroulez l'assistant en pointant sur **Suivant**. Dans la fenêtre **Zone à chiffrer**, sélectionnez **Chiffrer la partition du système Windows**. Si le disque dur n'abrite qu'une seule partition, les deux options aboutissent au même résultat. Dans la fenêtre des systèmes d'exploitation, cochez **Amorçage**, à moins qu'il ne s'agisse d'une configuration multiboot où plusieurs systèmes d'exploitation cohabitent.

2 TESTEZ LE CHIFFREMENT

Cliquez sur **Suivant** pour accéder à la page **Options de chiffrement**. Conservez les options par défaut, puis pointez sur **Afficher le mot de passe** avant de le créer. VeraCrypt active en effet par défaut le clavier américain et il est impossible de changer de langue. Notez précieusement le code secret. Déplacez ensuite la souris comme demandé et déroulez l'assistant. L'appli vous encourage à créer un disque de secours. Récupérez le fichier Zip généré et copiez le contenu de l'archive sur une clé USB formatée en Fat32. Une fois le disque de secours vérifié, cliquez sur **Suivant** au bas de la fenêtre **Mode de nettoyage**. Actionnez le bouton **Test**. Windows redémarre et vous invite à entrer votre mot de passe. À l'issue de l'analyse, il ne reste plus qu'à appliquer le chiffrement via la commande **Crypter**.

Un mot de passe est requis pour accéder au disque de secours.

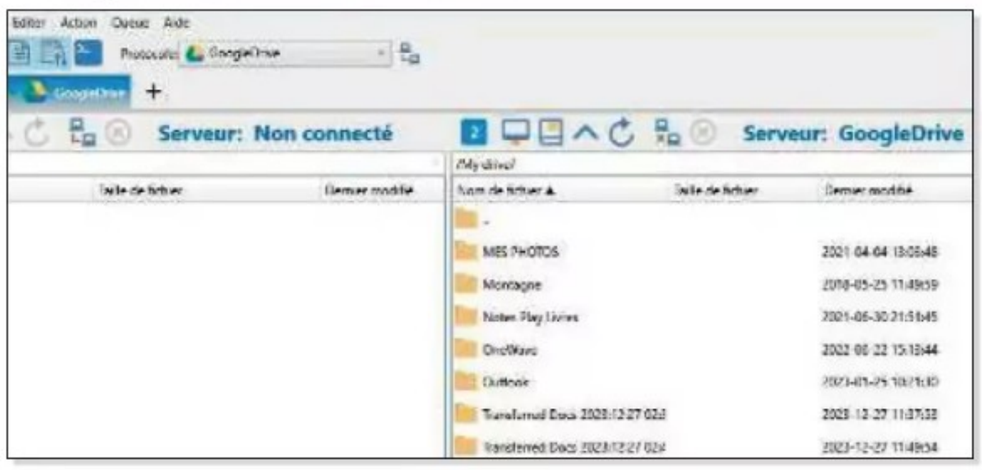
DIFFICULTÉ
MODÉRÉE
TEMPS
30 MIN
DOMAINE
CLOUD

CONSERVEZ VOS FICHIERS DANS LE CLOUD

Vous ne prendrez jamais assez de précautions. Et si vous utilisiez vos comptes **Microsoft et Google pour multiplier les copies de sauvegarde** de vos fichiers les plus sensibles…

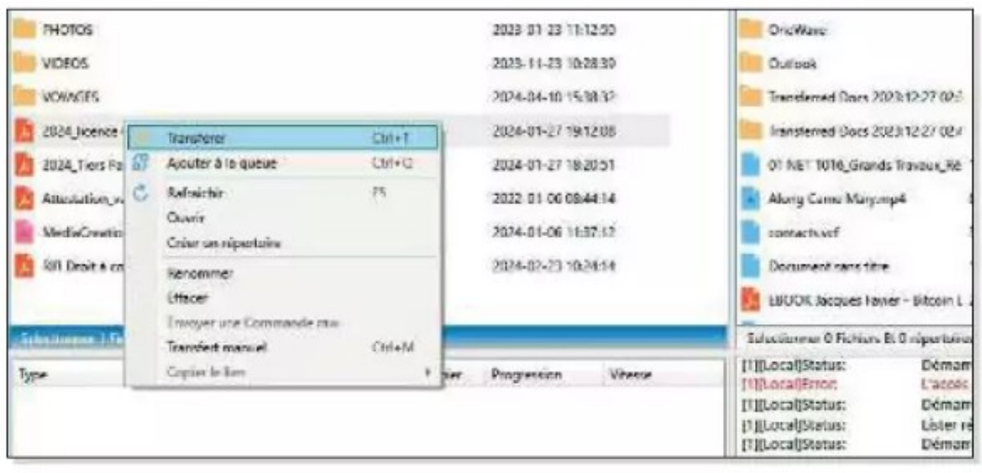
1 CONNECTEZ GOOGLE DRIVE AU SERVEUR FTP

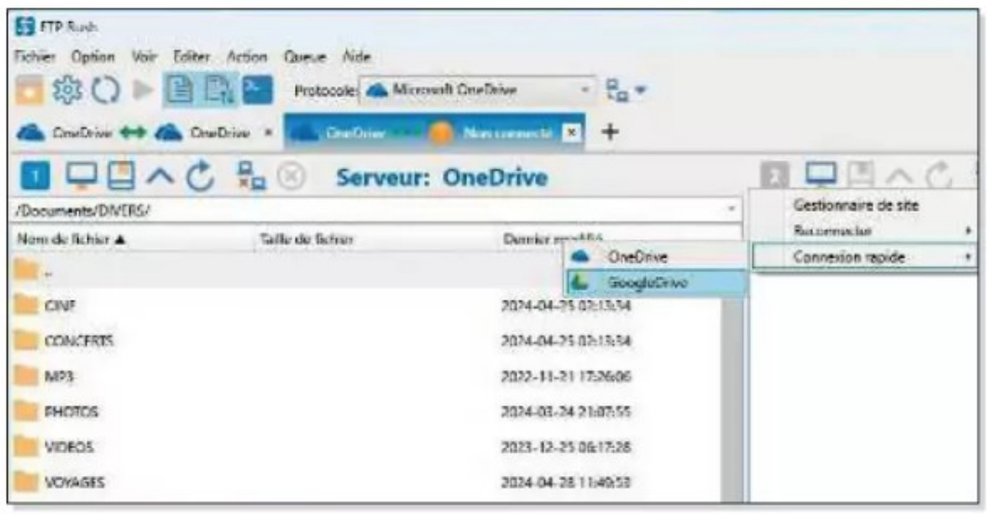
Pour des transferts entre les services cloud ou depuis un disque dur, nous allons employer le protocole FTP, un peu désuet mais toujours utile. Installez l'utilitaire gratuit FTP Rush v3 (bit.ly/3y0FUQØ) dans sa version Windows NET Framework. Lancez l'application, déroulez le menu **Protocole** et choisissez **Google Drive** - FTP Rush est aussi compatible avec OneDrive et Dropbox. Validez ce choix en pointant sur l'icône **Connecter**. Autorisez le logiciel à accéder à votre espace en ligne et cochez l'option **Tout sélectionner**. Fermez l'onglet et retournez sur la page d'accueil du client FTP. Double-cliquez sur **My Drive** pour afficher le contenu de votre Drive.



2 TRANSFÉREZ UN FICHIER DU PC VERS LE CLOUD

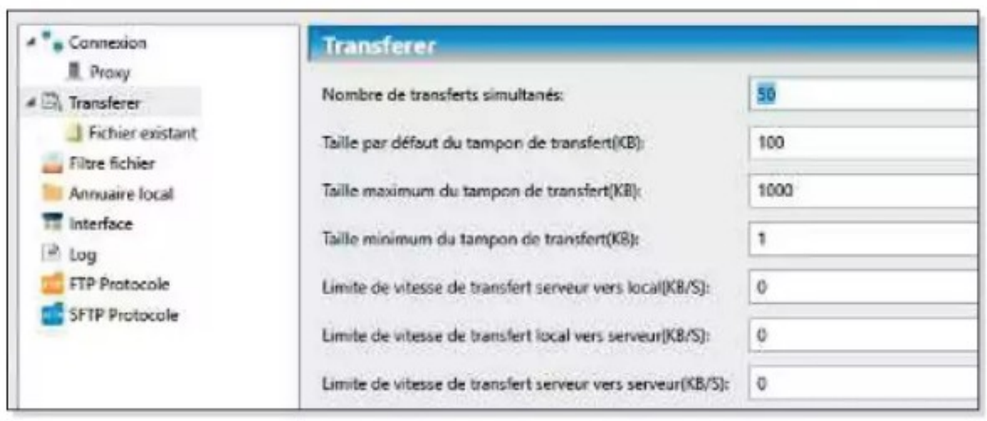
Désignez l'emplacement où seront enregistrés les éléments que vous voulez sauvegarder. Cliquez ensuite dans le volet de navigation qui occupe la moitié droite de la fenêtre et donne accès au contenu du PC, comme l'indique la mention **Local**. Parcourez l'arborescence du PC en utilisant l'icône **Dossier parent** située en haut de la liste. Sélectionnez un disque (C:/, D:/, etc.), pointez sur **~Documents** et choisissez l'élément à sauvegarder (un fichier ou un dossier). Opérez un clic droit sur son nom et actionnez la commande **Transférer** pour lancer la copie. Vous pouvez suivre l'avancée des opérations et retrouver l'historique de votre activité au bas de la fenêtre.





3 ÉCHANGEZ DES ÉLÉMENTS ENTRE GOOGLE DRIVE ET ONEDRIVE

Vous l'avez compris, l'interface de FTP Rush reprend un principe cher aux gestionnaires de fichiers, avec une fenêtre partagée en deux parties que l'on associe chacune à un disque local ou à un espace de stockage en ligne. Pour transférer des contenus entre deux services cloud, cliquez sur l'icône **Basculer vers mode serveur** dans la barre d'outils du volet jusqu'ici lié au disque local. Déroulez le menu **Protocole** et optez pour OneDrive ou Dropbox. Autorisez FTP Rush à accéder à cet espace et cliquez sur **Connecter**. Répétez le processus de copie décrit précédemment.



4 GÉREZ VOS ESPACES DANS FTP RUSH

Cet utilitaire peut se substituer aux webapps de Drive, OneDrive et Dropbox. Ainsi, pour définir un nouveau dossier, effectuez un clic droit dans le volet lié au service concerné et choisissez la commande **Créer un répertoire**. Donnez un nom à cet emplacement et validez avec **OK**. Le menu contextuel propose également de renommer ou d'effacer des éléments. Les modifications sont synchronisées sur tous les appareils associés au compte cloud. FTP Rush intègre des options de gestion de la bande passante de la connexion internet. Allez dans le menu **Options (Ctrl+O)** et explorez la section **Transférer** pour limiter la vitesse de transfert et éviter de ralentir vos autres activités, ou augmenter le nombre de transferts simultanés.

FAITES LE POINT SUR VOS VERSIONS DE LOGICIELS MICROSOFT

Garder ses programmes à jour est un bon moyen de défense contre les logiciels malveillants. Mais encore faut-il qu'ils soient encore pris en charge par l'éditeur de Windows.

DIFFICULTÉ MODÉRÉE
TEMPS 15 MIN
DOMAINE SYSTÈME

1 IDENTIFIEZ VOTRE VERSION DE WINDOWS

Windows 10 ou 11 ? S'agit-il de l'édition Professionnel, Famille ou Éducation ? Dans les paramètres, cliquez sur **Mise à jour et sécurité, Activation** (Windows 10) ou sur **Système, Informations Système** (Windows 11). Vous pouvez aussi saisir « Winver » dans la zone de recherche du menu **Démarrer** et valider avec **Entrée**.

2 AFFICHEZ VOTRE NUMÉRO DE DÉCLINAISON D'OFFICE

La version de la suite bureautique de Microsoft s'affiche sur l'écran de démarrage des applis. Si vous avez manqué cette info, une fois Word ou Excel ouvert, déroulez le menu **Fichier** et cliquez sur **Compte**. Repérez la mention **Information sur le produit** et notez le numéro de version sous **Produit activé**.

3 VÉRIFIEZ LA DATE DE FIN DU SUPPORT

Le site de Microsoft renseigne sur la date de fin du support technique de l'ensemble des produits de la marque. Rendez-vous sur bit.ly/3pLUØQQ, cliquez sur **Rechercher** et entrez les informations recueillies aux étapes précédentes. Nous constatons ainsi que Windows 10 Home et Pro bénéficient du support technique jusqu'au 14 octobre 2025.

Sélectionnez un produit pour trouver les dernières versions et mises à jour.

4 METTEZ VOS PRODUITS À JOUR

Le passage à Windows 11 nécessite de disposer d'un matériel compatible. Il existe bien des astuces pour contourner les limitations, mais cela suppose une réinstallation totale et la perte des données et des applis. Si votre suite Office est sur le point de devenir obsolète et de se voir privée des mises à jour de sécurité, cliquez sur **Changer de licence** de la page **Fichier**, **Compte** et adoptez une mise à jour plus récente (l'opération est payante).

REMODELEZ L'INTERFACE DE WINDOWS DEFENDER

Vous goûtez peu l'ergonomie de l'antivirus de Windows 11 ? Alors pilotez les fonctions de sécurité de votre PC **avec l'utilitaire DefenderUI.**

DIFFICULTÉ MODÉRÉE
TEMPS 15 MIN
DOMAINE ANTIVIRUS

1 AJUSTEZ LES PARAMÈTRES DE L'APPLICATION

Ouvrez votre navigateur et rendez-vous sur le site **defenderui.com**. Cliquez sur **Download Free** pour télécharger le programme et l'installer. Au premier lancement, l'interface s'affiche en anglais. Nous vous conseillons de basculer les menus en français en utilisant le menu déroulant des langues. Pointez sur le mode **Recommandé**. Ce profil applique des réglages par défaut aptes à répondre aux besoins du plus grand nombre – des paramètres qui peuvent être modifiés ultérieurement. Vous arrivez ensuite sur la page d'accueil de l'utilitaire où sont regroupées les options d'analyse. Cliquez sur **Mise à jour des signatures**, puis **Scanner** pour lancer une recherche de virus. Choisissez le mode **Basic**. Les options en jaune ne sont pas actives, comme l'accès contrôlé au dossier, efficace contre les ransomwares, mais susceptible de gêner le bon fonctionnement de certaines applis.

DefenderUI centralise les options de l'antivirus de Windows.

2 CRÉEZ UN PROFIL UTILISATEUR

Déroulez le menu **Profil recommandé** présent au sommet de la fenêtre et sélectionnez **Profil agressif** pour hausser le niveau de sécurité de Windows et bénéficier du contrôle de l'accès aux dossiers ou empêchez drastiquement l'installation des applications non reconnues. Si aucun des scénarios par défaut ne vous agrée, pointez sur **Profil agressif** et choisissez cette fois l'option **Profil personnalisé**. DefenderUI vous propose d'ajuster à votre guise les paramètres de sécurité du PC. Une fois que vous avez terminé, cliquez sur la disquette pour enregistrer le profil. Les plus experts peuvent pousser la personnalisation en explorant le contenu des onglets **Avancé** et **Règles ASR**.

DIFFICULTÉ
VARIABLE
TEMPS
VARIABLE
DOMAINE
SYSTÈME

EXHUMEZ DES FICHIERS ENVOLÉS

Quand de précieuses données disparaissent, il est facile d'être pris d'un vent de panique. Reprenez vos esprits. **Dans bien des cas, celles-ci ne sont pas détruites à jamais.**

Les fichiers et les dossiers conservés dans un disque dur, le cloud ou un téléphone ne disparaissent jamais par hasard. Il existe toujours une cause à l'origine de leur évanouissement. Ils peuvent avoir été placés dans la corbeille par inadvertance, transférés dans un autre dossier ou sur un disque secondaire. Auquel cas une recherche approfondie devrait suffire à remettre la main dessus. En revanche, si la corbeille a été vidée ou la clé USB nettoyée, le problème devient plus ardu. Mais, là encore, rien n'est perdu. Même dans le cas des périphériques externes, il est possible de retrouver des données effacées au moyen du Terminal de Windows. Et il existe des utilitaires qui rendent possible, dans certains cas, la récupération des données. Attention toutefois, le résultat est loin d'être garanti à 100 %. Quant aux espaces de stockage en ligne, ils conservent les éléments supprimés durant un mois, ce qui laisse une marge de manœuvre conséquente aux étourdis.

MIEUX VAUT PRÉVENIR QUE GUÉRIR. Pour autant, il n'est jamais certain que ces solutions fonctionnent à tous les coups. Il apparaît donc primordial de prévenir la catastrophe. Commencez par vous protéger des hackeurs en actualisant périodiquement votre système ainsi que votre suite de sécurité. Pensez ensuite à automatiser une copie de vos bibliothèques sur un disque externe grâce à une application du type AOMEI Backupper. Pour plus de sécurité, il est préférable de débrancher le périphérique de l'ordinateur entre deux sauvegardes. Vous pouvez aussi investir dans un serveur de stockage en réseau (NAS) qui va, comme son nom l'indique, stocker l'intégralité du disque principal dans un second voir un troisième volume. Les NAS de la série J du fabricant taïwanais Synology permettent, par exemple, d'effectuer des protections complètes de données pour moins de 300 euros. Du côté des smartphones, l'utilisation d'applis de gestion de fichiers en parallèle de la connexion à Google Drive ou iCloud facilite grandement la récupération des éléments égarés ou effacés récemment. De quoi vous sauver la vie… numérique ! ●

BOÎTE À OUTILS POUR CE PAS À PAS, NOUS AVONS UTILISÉ LES ÉLÉMENTS SUIVANTS

PC ou Mac

Téléphone Android ou iPhone

Applications CX Explorateur de fichiers, Data Recovery, Dropbox, ES Files Explorer, Files by Google, iTunes, OneDrive, Recuva

DÉCLENCHEZ L'OPÉRATION SAUVETAGE SUR VOTRE PC

Quand un élément disparaît de l'ordinateur, il n'est pas forcément perdu à tout jamais. **À moins d'avoir reformaté le disque dur, il existe des solutions de récupération,** plus ou moins complexes et efficaces.

1 VÉRIFIEZ LA CORBEILLE

Vous n'arrivez plus à remettre la main sur un fichier ? Ouvrez la corbeille. Vous y avez peut-être glissé les contenus par erreur, auquel cas il suffit d'actionner la commande **Restaurer** pour les réinstaller dans leur emplacement d'origine. La disparition peut aussi être liée à un défaut de rafraîchissement du Bureau : le dossier est bien là, mais il n'apparaît pas. Faites un clic droit sur une zone vierge et pointez sur **Actualiser** pour l'afficher de nouveau. Si vous avez déplacé les éléments par erreur, ouvrez l'Explorateur de fichiers (**Windows + E**). Cliquez sur **En savoir plus**, **Options**. Dirigez-vous vers l'onglet **Rechercher** et cochez les options disponibles. Appliquez les modifications et lancez votre recherche.

2 CHERCHEZ DANS L'EXPLORATEUR DE FICHIERS

Si vous savez dans quelle bibliothèque l'élément a été copié, sélectionnez l'emplacement en colonne gauche et indiquez son nom dans la zone de recherche en haut à droite. En présence d'un grand nombre de résultats, utilisez l'en-tête **Trier** pour filtrer la liste par type, date, taille… Si la recherche exclut des volumes, déroulez le menu **Options de recherche**, **Modifier les emplacements indexés**, **Modifier**. Cochez les cases des périphériques actifs et validez avec **OK** avant de relancer la recherche. Quand l'élément s'affiche dans les résultats, opérez un clic droit sur son nom et choisissez **Ouvrir l'emplacement du fichier.**

3 RESTAUREZ LE SYSTÈME

Si vous êtes sûr d'avoir détruit un élément par mégarde, impossible de le retrouver avec les manipulations décrites ci-dessus (à moins d'utiliser un service cloud, *voir p. 61*). Votre seule chance de remettre la main sur le fichier consiste à revenir à un état antérieur du système. À condition qu'il existe une sauvegarde. Pour savoir si c'est le cas, pointez sur la loupe en barre des tâches et effectuez une recherche sur le terme **point de restauration**. Cliquez sur **Créer un point de restauration**. Accédez à la **Restauration du système**, **Suivant**. Cette fenêtre mentionne les éventuelles sauvegardes, leur date de création et type. Choisissez l'une d'elles pour démarrer la restauration.

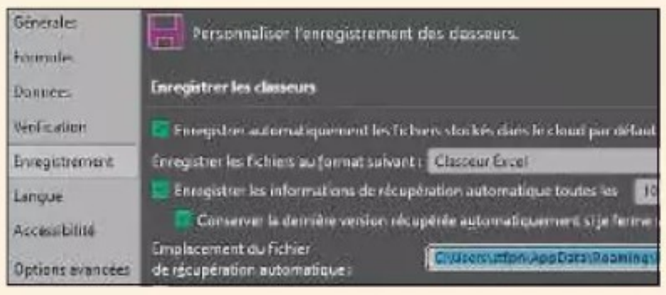
4 TENTEZ VOTRE CHANCE AVEC RECUVA

Téléchargez l'application de récupération de données Recuva (bit.ly/3Uww1Ba) dans sa version gratuite. Durant l'installation, cochez la case **Enable Deep Scan**. Cliquez sur **Switch to advanced mode**, **Options**. Choisissez le français dans le menu **Language**. Agrandissez la fenêtre. Utilisez le champ de recherche en indiquant le nom de l'élément égaré. La colonne **État** fait état du niveau de récupération, tandis que l'onglet **Info**, à droite, mentionne son emplacement. Si votre fichier fait partie du lot, opérez un clic droit sur son nom, pointez sur **Récupérer les éléments surlignés** et choisissez l'emplacement de destination.

PAS À PAS EXPRESS

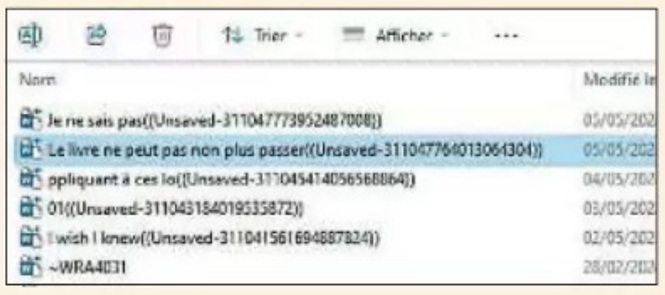
RESTAUREZ DES DOCUMENTS OFFICE

La suite bureautique de Microsoft renferme quelques astuces pratiques pour remettre la main sur des fichiers Word, Excel ou PowerPoint.



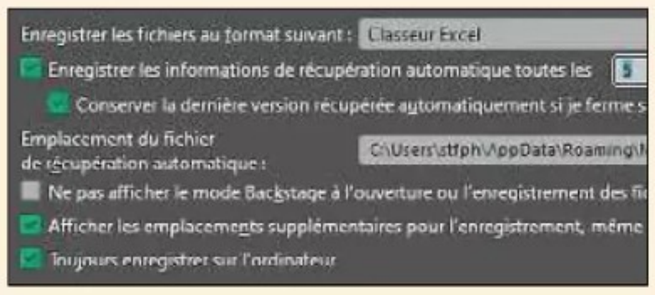
01. Repérez l'emplacement du fichier de récupération

Depuis Word ou Excel, dirigez-vous vers le menu **Fichier**, **Options** et cliquez sur **Enregistrement** en colonne gauche. Le chemin par défaut vers l'emplacement de la dernière version du fichier s'affiche. Pensez à cocher la case **Conserver la dernière version**.



02. Accédez aux derniers éléments enregistrés

Ouvrez l'Explorateur de fichiers et suivez l'emplacement désigné (généralement depuis **Ce PC**, **C:**, **Utilisateurs**). Les derniers éléments récupérés y sont conservés. Opérez un clic droit sur son nom et pointez sur **Ouvrir**. Enregistrez-le dans le dossier de votre choix.



03. Activez la sauvegarde automatique

Les documents Office peuvent être enregistrés toutes les minutes. Dans la fenêtre des options de Word et Excel, cochez la case supérieure et indiquez le délai entre deux sauvegardes. Activez également le mode **Toujours enregistrer sur l'ordinateur**.

KOSTAKOSTOV/ISTOCKPHOTO

PARTEZ EN CHASSE DE FICHIERS SUR VOTRE MAC

Comme toujours avec Apple, la convivialité de l'interface facilite les opérations de recherche et de récupération de fichiers, dossiers ou applications.

1 LANCEZ LES PREMIÈRES RECHERCHES

Lorsque vous ne voyez plus un fichier ou dossier sur votre Mac, il se peut qu'il ait été glissé dans la Corbeille par inadvertance. S'il ne s'y trouve pas, effectuez une première recherche via le Finder en pointant sur le menu **Aller**, **Récents**. Déroulez la section **Effectuer des opérations** et choisissez **Trier par** et **Date de dernière ouverture**. Basculez l'affichage sous forme de colonnes pour bénéficier d'une prévisualisation explicite. Si l'élément demeure introuvable, utilisez la fonction de recherche de Spotlight. Cliquez sur la loupe en haut à droite du Bureau et entrez le nom de l'élément à retrouver dans la zone de saisie. Validez avec la touche **Entrée** pour découvrir les résultats.

2 PARAMÉTREZ SPOTLIGHT ET LE FINDER

Déroulez la fenêtre Spotlight afin de visualiser les réponses par catégorie. Le fichier perdu peut se cacher parmi les documents, les photos, les messages… Il est possible que Spotlight ne fasse pas apparaître certaines catégories. Pour vous assurer qu'il étende son analyse à tous les recoins du disque dur, ouvrez le menu **Pomme**, **Réglages système**, **Siri et Spotlight**. Dans la section **Résultats de la recherche**, cochez les éventuels emplacements ignorés jusqu'ici par macOS et relancez la recherche. Quant au **Finder**, vérifiez dans les réglages que les quatre options relatives à l'affichage des éléments sont bien cochées.

3 FAITES APPEL À DATA RECOVERY

Plusieurs applications proposent d'exhumer les fichiers égarés ou corrompus. Recuva ne disposant pas de version Mac, vous devez vous tourner vers un logiciel payant - à moins que vous n'utilisiez une version un peu ancienne du système d'exploitation, auquel cas Free Any Data Recovery reste d'actualité. Sur un Mac récent, nous vous conseillons Data Recovery de EaseUs (bit.ly/3UxVb23). Lors du premier lancement, choisissez le disque à inspecter dans le volet de navigation (**Hardware Disk** correspond au disque principal), puis cliquez sur **Search for lost files**. Autorisez l'accès complet au disque, effectuez un tri ou utilisez la zone de saisie **Search**. Cochez la case de l'élément à récupérer et validez avec **Recover**.

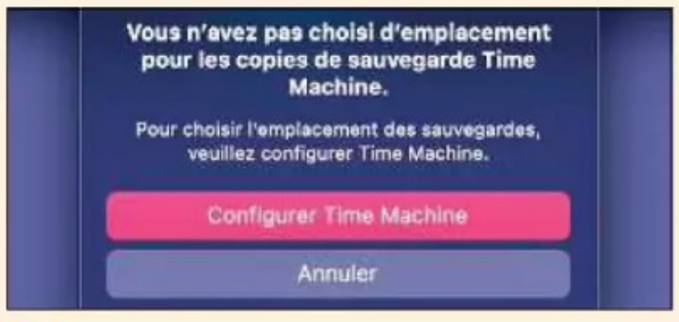
4 RECOUREZ AUX COMMANDES DU TERMINAL

Le Terminal accepte les instructions en lignes de commande. Parmi celles-ci, certaines sont dévolues à la recherche d'éléments sur les disques actifs. Ouvrez le Terminal en effectuant une requête sur son nom dans Spotlight et appuyez sur la touche **Entrée**. La commande **find** sert à lancer une analyse. Si vous vous souvenez du nom du fichier, saisissez-le, ajoutez son extension (find blabla.doc par exemple) et validez avec **Entrée**. Si vous vous souvenez de l'emplacement de l'élément ou du nom du créateur du document, n'hésitez pas à affiner la recherche en tapant ces informations. Ce qui donne, par exemple, find blabla.doc/Users/Stéphane.

PAS À PAS EXPRESS

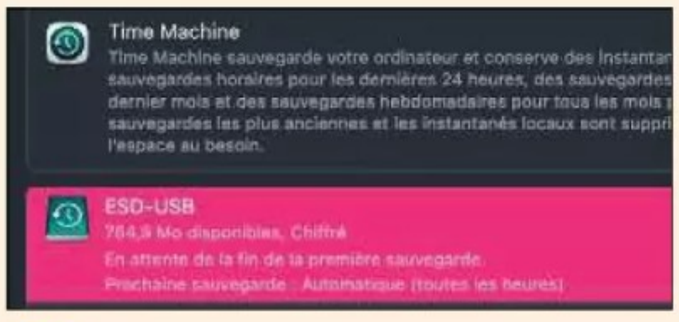
REMONTEZ LE TEMPS AVEC TIME MACHINE

MacOS propose de retrouver vos fichiers tels qu'ils étaient à une date antérieure en s'appuyant sur les sauvegardes hebdomadaires effectuées dans les mois précédents.



01. Vérifiez les sauvegardes

Effectuez une recherche sur le terme Time Machine dans Spotlight. La fenêtre d'emplacement des copies de sauvegarde apparaît. Si vous n'avez pas encore enregistré de sauvegardes périodiques, c'est le moment de passer à l'acte. Suivez la procédure de configuration.



02. Choisissez un enregistrement

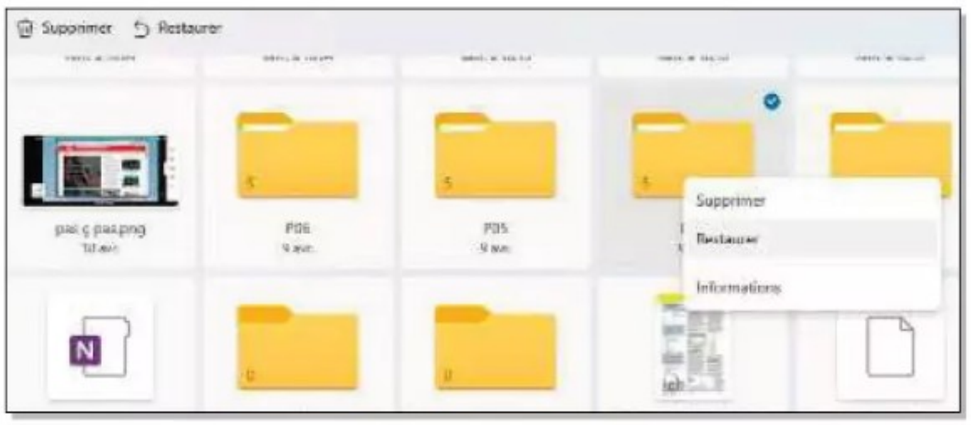
S'il existe des sauvegardes, vous pouvez y accéder à tout moment pour restaurer une version passée de votre Mac. Ouvrez de nouveau Time Machine. L'application dresse la liste des archives accessibles. Utilisez les options disponibles pour ajuster la fréquence des sauvegardes.

03. Revenez en arrière

Dans la barre de menu supérieur, pointez sur l'icône **!** entouré d'un cercle et optez pour **Parcourir les réglages Time Machine**. Une série de fenêtres apparaît. Utilisez la frise temporelle, choisissez une date et une heure et cliquez sur **Restaurer**.

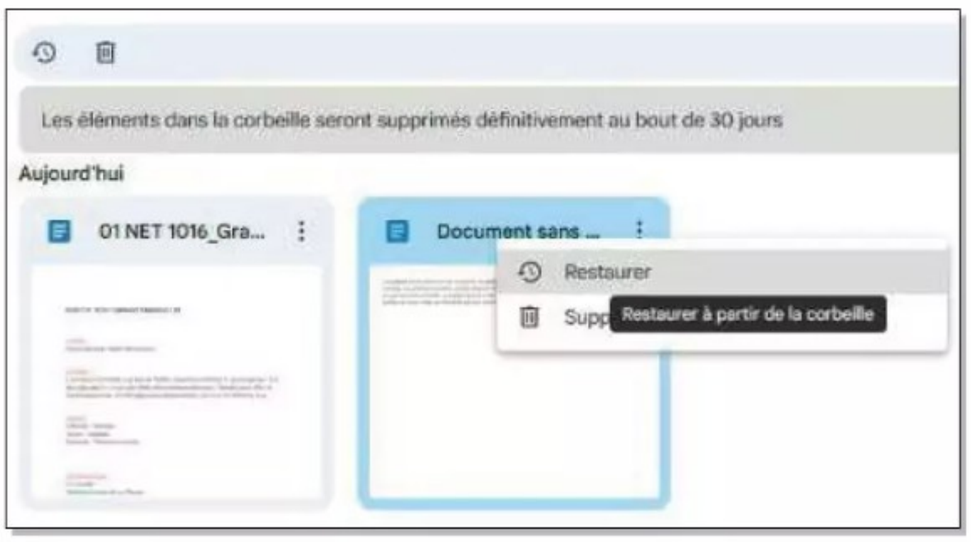
EXPLOREZ L'HISTORIQUE DU CLOUD

Les principaux services de stockage en ligne conservent un historique des versions de vos documents, ainsi qu'une copie des fichiers placés dans la corbeille.



1 EXPLOITEZ LES OPTIONS DE ONEDRIVE

Si vous disposez d'un abonnement premium au cloud de Microsoft, OneDrive (à partir de 20 €/an), vous avez une chance supplémentaire de retrouver un fichier déposé dans la corbeille. Accédez à cette dernière en opérant un clic droit sur l'icône en forme de nuage à droite de la barre des tâches. Pointez sur **Corbeille** et utilisez les options de tri (date de suppression, emplacement d'origine, etc.) ou le champ de recherche pour vous faciliter la tâche. Téléchargez le fichier sur le PC en effectuant un clic droit sur son nom et en optant pour **Restaurer**. Le document est sauvegardé par défaut sur le Bureau. Il est possible de récupérer l'intégralité de la Corbeille via l'option **Restaurer tous les éléments** du menu supérieur.

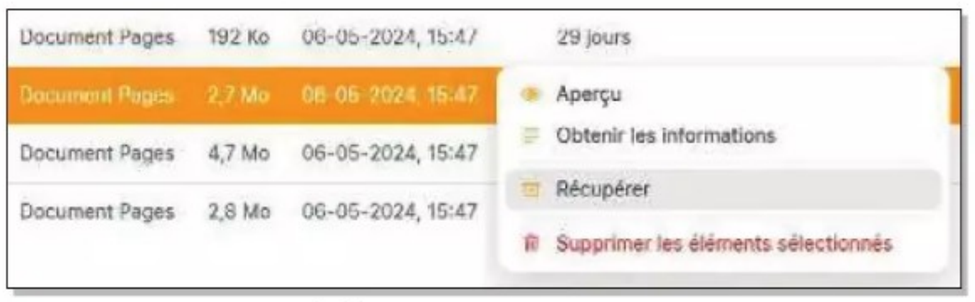


2 RÉCUPÉREZ DES FICHIERS SUR LE CLOUD GOOGLE

Google Drive propose des options similaires de restauration des fichiers égarés. Si vous n'avez pas installé l'application Drive sur votre PC, il suffit de vous connecter à votre espace cloud (bit.ly/3EHSLVi) depuis un navigateur internet, puis de cliquer sur l'icône **Corbeille** en colonne gauche. Aidez-vous des options de tri en déroulant le menu **Date de suppression/modification** pour identifier plus rapidement l'élément recherché. Si vous l'avez ferré, visez son nom. En colonne gauche, allez sur l'onglet **Détails** pour obtenir une prévisualisation de celui-ci. Opérez un clic droit sur son nom puis sur **Restaurer**. Pointez sur **Afficher l'emplacement du fichier**. Ce dernier est alors surligné dans **Mon Drive**.

3 RETROUVEZ VOS PETITS DANS DROPBOX

Dropbox est le service cloud qui bénéficie des fonctionnalités les plus diverses. Les options de récupération de fichiers en font partie. En cas de perte d'un élément, commencez par vous connecter à votre espace de stockage (bit.ly/3UKmI1M). Dirigez-vous en colonne droite vers les **Fichiers supprimés**, puis utilisez le champ de recherche. Si vous remettez la main dessus, passez le curseur sur son nom, puis cochez la case située à gauche. Validez avec le bouton **Restaurer**, puis allez sur **Tous les fichiers**. L'élément récupéré se situe à la racine du dossier **Tous les fichiers**. Si vous ne le voyez pas, cliquez sur la colonne **Nom**.



4 RASSEMBLEZ VOS ÉLÉMENTS SUR ICLOUD

Chez Apple aussi on tient à ce que les utilisateurs puissent restaurer des éléments supprimés depuis moins de trente jours. Ouvrez votre navigateur et connectez-vous à icloud.com. Allez sur **Connexion** et indiquez vos identifiants Apple ID. Sur la page d'accueil, choisissez l'application associée à l'élément égaré (Pages, Numbers, Keynote). Pointez sur **Supprimés récemment**. Effectuez un tri par nom, date ou type, passez le curseur sur le nom de l'élément à restaurer, cliquez sur les points à droite et sur **Récupérer**. Le fichier est extrait de la corbeille. Placez-vous sur l'onglet **Parcourir** pour le retrouver.

Restaurez des mails datant de plusieurs années

Les messageries Gmail et Outlook ont une mémoire d'éléphant. Une fois sur la page d'accueil de votre compte, cliquez à gauche sur **Tous les messages** et tapez ***Before:*** dans le champ de saisie, suivi de l'année de référence. Ainsi, pour rechercher les mails reçus ou envoyés avant 2010, saisissez **before:2010**. S'il existe des messages répondant à ce critère, vous les verrez réapparaître comme par enchantement ! Du côté d'Outlook, le module complémentaire Email Recovery (bit.ly/3wm9fUy) autorise la récupération des messages supprimés. Installez cet outil et activez-le depuis l'icône **Applications**. Cliquez ensuite sur **Start Recovery** et **Create Folder**. Les anciens messages s'affichent à droite.

KOSTA.KOSTOV / ISTOCKPHOTO

FOUILLEZ DANS LA MÉMOIRE DE VOTRE SMARTPHONE

Si vous n'arrivez pas à remettre la main sur **des fichiers stockés dans la mémoire** de votre téléphone, faites appel aux gestionnaires de documents disponibles dans les *stores* d'Apple et Google.

astuce 1

ANDROID | INSPECTEZ VOS DOSSIERS AVEC FILES

Si vous possédez un Google Pixel, l'appli Files installée par défaut vous permet d'effectuer une recherche fine des éléments perdus. Appuyez sur les traits horizontaux en haut à gauche. Vérifiez dans les **Paramètres** que les curseurs **Recherche intelligente** et **Afficher les fichiers masqués** soient bien activés. La barre de recherche permet de préciser la catégorie de fichiers à inspecter, tandis que l'accueil autorise l'accès immédiat aux fichiers des différentes catégories. Si vous ne possédez pas un Google Pixel, nous vous conseillons l'appli **CX Explorateur de fichiers**. Celle-ci autorise un accès instantané aux bibliothèques du mobile ainsi qu'aux fichiers sauvegardés en local ou sur une carte mémoire externe.

astuce 2

ANDROID | EFFECTUEZ DES RECHERCHES APPROFONDIES

Ouvrez CX Explorateur de fichiers. Dans **Local, Stockage principal**, ouvrez les dossiers les uns après les autres, ou utilisez la zone de saisie **Rechercher**. Soyez sûr que tous les éléments soient visibles en pointant sur les traits horizontaux puis en cochant la case **Afficher les fichiers masqués**. En touchant la flèche pointant vers le bas à droite de **Stockage principal**, il est possible de cibler un dossier. Si vous avez malencontreusement effacé des photos, vidéos et MP3, l'appli **Recuva Recover Deleted Files** peut aider à les retrouver. Donnez-lui l'accès au stockage du téléphone puis choisissez le type de fichiers à récupérer.

astuce 1

IOS | SCRUTEZ LES DIFFÉRENTS EMPLACEMENTS

Concernant les iPhone, les outils de recherche se situent dans **Fichiers**. Au bas de l'écran apparaît l'icône **Explorer**. Déroulez la section des **Emplacements** et vérifiez que l'élément ne se trouve pas dans les **Suppressions récentes**. Vous pouvez indiquer un volume précis, tel **iCloud Drive** si vous pensez qu'il a été enregistré à cet endroit. Sinon, utilisez la zone de saisie supérieure pour entamer une recherche globale. iOS propose de cibler la requête. Effleurez les points en haut à droite, dirigez-vous vers **Modifier** et désactivez les curseurs de votre choix. Si l'application Fichiers vous apparaît trop limitée, testez **ES File Explorer** (apple.co/3VeSpzm) et ses options de recherche étendues aux réseaux locaux.

astuce 2

IOS | SAUVEZ VOS DONNÉES AVEC ITUNES

Il est possible de récupérer la dernière sauvegarde de l'intégralité de l'iPhone en passant par iTunes. Installez l'application depuis le Microsoft Store et renseignez vos identifiants Apple. Connectez ensuite votre appareil à un port USB. Il doit être automatiquement détecté par iTunes. Renseignez le code PIN de l'iPhone, puis pointez sur **iPhone de** + nom de l'utilisateur et sur **Résumé** à gauche. La section Sauvegardes permet d'enregistrer l'intégralité des données du téléphone sur **iCloud** ou sur **Cet ordinateur**. Si vous possédez déjà une sauvegarde, cliquez sur **Restaurer la sauvegarde** afin de retrouver toutes vos données.

PAS À PAS EXPRESS

SAUVEGARDEZ PHOTOS ET VIDÉOS DANS LE CLOUD

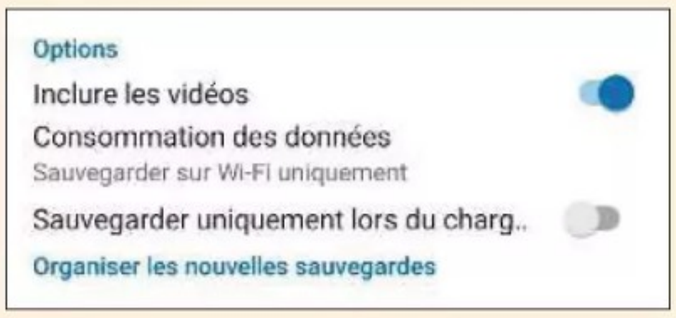
Les applis clouds telles que Dropbox et OneDrive ont la capacité d'enregistrer automatiquement sur leurs serveurs les clichés et les films capturés avec votre téléphone.

01. Installez Dropbox

Installez l'appli Dropbox sur votre mobile Android ou sur l'iPhone et entrez vos identifiants. Au lancement, répondez par l'affirmative au message vous demandant si vous souhaitez sauvegarder automatiquement les photos et vidéos de cet appareil dans Dropbox.

02. Associez OneDrive

L'opération est similaire avec le cloud de Microsoft. Après avoir installé l'application OneDrive et associé celle-ci à un compte Microsoft, appuyez sur l'icône **Photos** au bas de l'écran. Effleurez ensuite le curseur **La sauvegarde de l'appareil photo est désactivée**.



03. Gérez les sauvegardes

Confirmez l'enregistrement des photos sur l'espace OneDrive. Appuyez sur l'icône **Moi** en bas à droite. Ouvrez les **Paramètres**, pointez sur **Sauvegarde de la caméra** et indiquez si vous souhaitez inclure les vidéos, organiser les sauvegardes dans des sous-dossiers…

Le symbole bleu représente une espace

RAMENEZ À LA VIE UN DISQUE DUR ENDOMMAGÉ

Les données stockées sur un disque dur ou une clé USB peuvent soudain devenir inaccessibles à cause d'un problème matériel. Rassurez-vous, là encore, rien n'est perdu.

astuce 1

SONDEZ LE DISQUE DE STOCKAGE D'UN PC PORTABLE

Les données stockées sur un PC portable hors service ne sont pas forcément perdues. Vous pouvez extraire son disque dur en ouvrant le capot à l'aide d'un tournevis et en débranchant avec précautions les câbles d'alimentation et de données. Les disques durs et SSD installés dans les PC portables sont généralement au format 2,5 pouces ou NVMe. Pour accéder à leur contenu à partir d'un autre ordinateur, il faut vous procurer un adaptateur USB-SATA ou un boîtier USB dans lequel vous installerez le périphérique de stockage. Une fois ce dernier branché au PC, ouvrez l'Explorateur de fichiers et sélectionnez le volume parmi les lecteurs externes reconnus par Windows.

astuce 2

ACCÉDEZ AUX DONNÉES D'UN PC AVEC UN MAC OU L'INVERSE

La lecture d'un disque Windows formaté en NTFS ne pose aucun problème à un Mac. Nous vous conseillons d'actualiser le système au préalable (Sonoma 14.4.1 dans l'absolu). Branchez le périphérique qui apparaît sur le Bureau puis naviguez dans les dossiers. Il est possible d'ouvrir des photos, d'écouter des MP3 et de copier n'importe quel élément sur le Mac. En revanche, l'enregistrement de fichiers sur le disque n'est possible qu'à la condition d'installer au préalable des pilotes de périphériques depuis une application payante de ce type : bit.ly/44vbKR2. L'opération inverse se révèle plus ardue. Pour accéder au contenu d'un disque dur formaté sur Mac en APFS ou HFS+, il faut recourir à un utilitaire comme OWC MacDrive (bit.ly/4e52nMh) ou Paragon APFS for Windows (bit.ly/3Xr1N5N).

astuce 3

DEMANDEZ DE L'AIDE À UN PROFESSIONNEL

En cas de panne d'un disque dur interdisant tout accès aux données, mieux vaut faire appel à une société spécialisée qui saura extraire tout ou partie des fichiers enregistrés sur le support endommagé. Attention néanmoins, ces services, conçus à l'origine pour les entreprises, ne sont pas donnés. Nous vous conseillons de ne pas vous précipiter sur la première société venue et de solliciter systématiquement un devis. Vous pouvez vous adresser à la société Recoveo (recoveo.com), qui opère depuis plus de 20 ans, Ontrack (ontrack.com) ou Databack (databack.fr). Comptez au moins 400 euros pour une restauration complète d'un gros disque dur.

astuce 4

RÉINSTALLEZ UNE CLÉ USB MUETTE

Si le périphérique externe détenant vos données n'est plus reconnu par Windows, opérez un clic droit sur le menu **Démarrer** et ouvrez le **Gestionnaire de périphériques**. Déroulez le menu **Lecteurs de disque**. Le nom du périphérique doit s'afficher (sinon débranchez et rebranchez-le). Effectuez un clic droit sur son nom, puis visez l'option **Désinstallez l'appareil**. Débranchez puis reconnectez-le. Ouvrez l'**Explorateur de fichiers** qui devrait normalement l'afficher en colonne gauche. Si ce n'est pas le cas, revenez dans le **Gestionnaire de périphériques** et ouvrez le menu **Contrôleurs de bus USB**. Opérez un clic droit sur **Concentrateur USB générique**, **Désinstallez l'appareil**. Redémarrez le PC en maintenant une pression longue sur le bouton marche/arrêt.

Récupérez des fichiers grâce AU TERMINAL

Lorsque vous avez effacé des données par inadvertance, nettoyé votre disque dur en profondeur ou supprimé des fichiers présents sur un disque externe, tentez de remettre la main dessus grâce à l'application Récupération de fichiers Windows du Microsoft Store (bit.ly/3ULmfwd). Celle-ci fonctionne uniquement en ligne de commandes et est réservée aux utilisateurs avertis. Vous devez indiquer tout d'abord la lettre du lecteur où ont été supprimées les données puis celle de destination. Si le périphérique n'est pas au format NTFS, ajoutez **extensive**. Autrement, tapez **regular**. Ainsi, la commande **winfr f: e:/regular** va scanner le disque f: au format NTFS, puis copier les éventuelles données effacées sur le disque E:. La commande **winfr /?** affiche toutes les commandes compréhensibles par l'application.

KOSTA KOSTOV/ISTOCKPHOTO

DIFFICULTÉ
MODÉRÉE
TEMPS
60 MIN
DOMAINE
NAVIGATEURS

RÉDUISEZ VOS TRACES SUR LE WEB

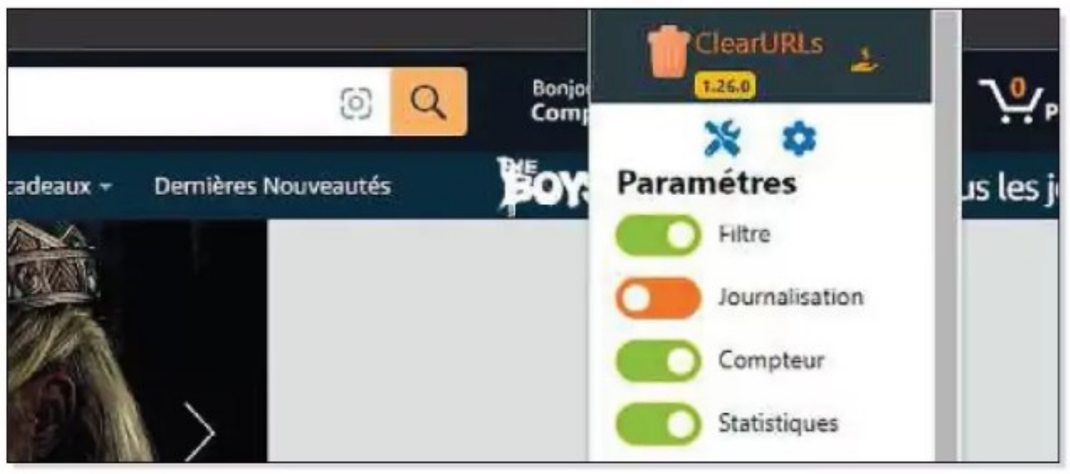
Lassé de recevoir des publicités ciblées ou des tombereaux de courriels indésirables ? **Reprenez le contrôle de vos données** lorsque vous naviguez et communiquez.

1 BLOQUEZ LE SUIVI DANS EDGE

Moins sourcilleux que Brave et Firefox, le navigateur de Microsoft permet d'ajuster le niveau de protection contre les traceurs. Dans **Paramètres**, **Confidentialité**, **Recherche et services**, imposez le mode **Strict**. Activez aussi l'option **Toujours utiliser la prévention de suivi « strict » lors de la navigation In Private** et installez le module complémentaire **uBlock Origin** (aussi disponible dans le Chrome Web Store). Ouvrez le tableau de bord de ce dernier, sélectionner **Liste de filtres** et cochez les listes référencées dans **Nuisances**, **Widgets et réseaux sociaux** et **Bannière de cookies**.

2 NETTOYEZ LES DONNÉES DE SUIVI DANS L'URL

Les réseaux sociaux, les sites d'e-commerce et les moteurs de recherche comme Google Search ajoutent à une adresse web des lignes de codes supplémentaires pour indiquer la région, l'heure ou encore l'appareil utilisé lors de votre navigation. Pour éviter de divulguer ces informations, nous vous conseillons d'adopter l'extension **ClearURLS**. Une fois installée et activée, celle-ci nettoie l'adresse mail de toutes les données susceptibles d'être utilisées par les sites. Effectuez un clic droit sur l'URL d'un site que vous visitez régulièrement et choisissez la commande **Copier sans le pistage du site**.

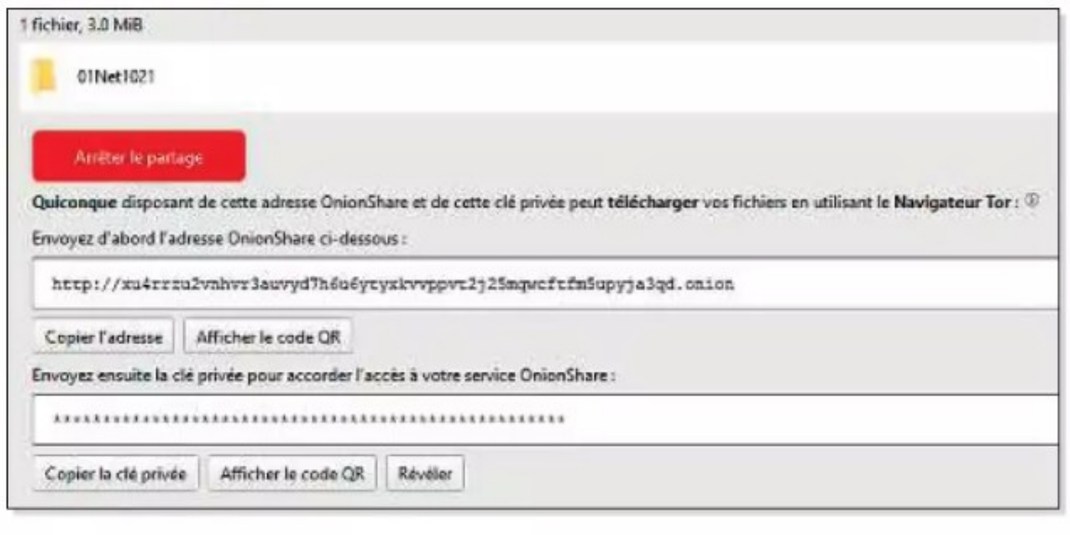


3 NAVIGUEZ AVEC TOR

Brave dispose d'un mode de navigation privée utilisant Tor, un réseau mondial et décentralisé. Mais il est possible de recourir au navigateur Tor lui-même, téléchargeable sur le site torproject.org. Ce navigateur fonctionne en permanence en mode privé, efface automatiquement les cookies et l'historique, masque votre position et votre adresse IP. Dans la barre d'adresse, l'icône **Circuit Tor** indique l'ensemble des nœuds utilisés pour masquer votre position. Cliquez dessus puis sur **Nouveau circuit Tor pour ce site** pour changer de serveurs et masquer votre position.

4 PARTAGEZ DES FICHIERS ANONYMEMENT

Il existe différentes façons de partager des fichiers en les protégeant des regards indiscrets. Vous pouvez les compresser en protégeant l'archive par un mot de passe avec un logiciel gratuit comme 7zip. Si le fichier est volumineux, nous vous conseillons de passer par Wetransfer pour l'envoi. Une autre solution consiste à recourir à l'application **OnionShare** (onionshare.org). Une fois cet outil en place, pointez sur **Connexion à Tor** et **Lancer le partage**. Glissez le fichier ou le dossier dans la fenêtre d'OnionShare et cliquez sur **Commencer le partage**. Partagez l'adresse avec les destinataires et envoyez-leur la clé de chiffrement afin qu'ils affichent les contenus dans Tor.

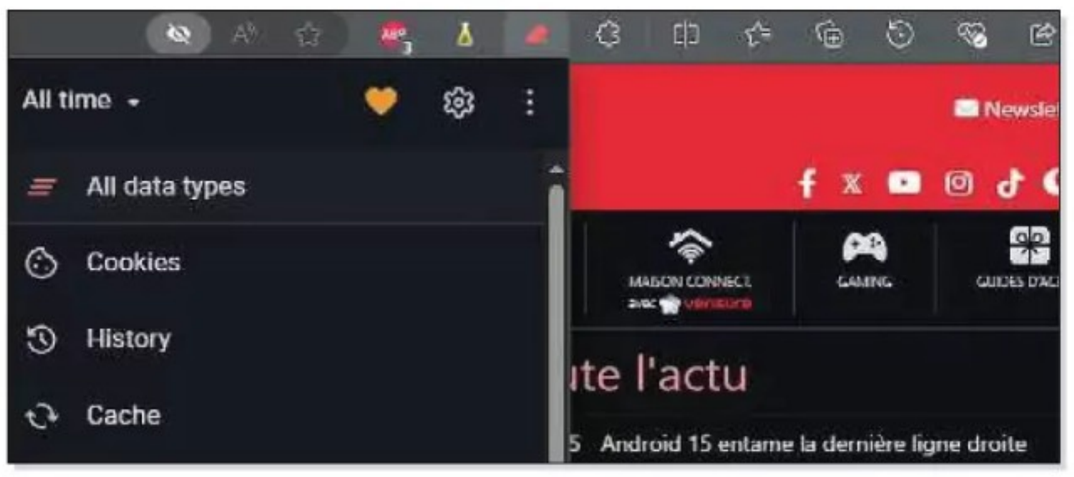


5 CHIFFREZ VOS MAILS AVEC THUNDERBIRD

Lancez le client de messagerie, cliquez sur l'icône formée de trois lignes, puis sur **Paramètres des comptes**, **Chiffrement de bout en bout**. Dans **OpenPGP**, choisissez **Ajouter une clé**, **Créer une nouvelle clé OpenPGP**. Imposez un délai après lequel les mails ne seront plus lisibles. Pointez sur **Générer la clé**, **confirmer**. Sélectionnez **Gestionnaire de clés OpenPGP**, opérez un clic droit sur votre clé et optez pour **Exporter vers un fichier** ou **Envoyer par mail**. Le destinataire doit double-cliquer sur le fichier. **asc** afin d'ajouter la clé à Thunderbird et pouvoir lire vos courriels chiffrés.

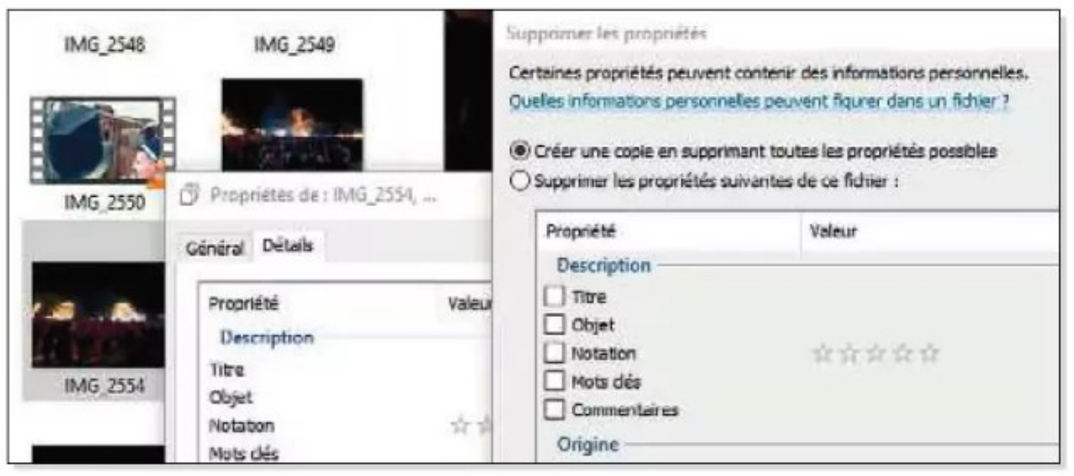
6 EFFACEZ LES DONNÉES DE VOS NAVIGATEURS EN UN CLIC

Tous les navigateurs intègrent une option servant à purger les données de navigation. Pour effectuer cette opération en un clic, installez l'extension **Clear Browsing Data** sur chacun d'eux et épingler son raccourci dans la barre des extensions. Cliquez sur l'icône, sélectionnez **All data types**, **All time** et définissez une période pour ne supprimer qu'une partie de l'historique. Cette extension peut être associée à Chrome et aux navigateurs basés sur Chromium (Edge, Brave, Opera, etc.). L'utilitaire **Ccleaner** permet aussi de nettoyer l'historique de vos navigateurs en peu de clics.



7 SUPPRIMEZ LES MÉTADONNÉES DES PHOTOS

Lorsque vous prenez un cliché, des données sont enregistrées : les références de l'appareil, les détails techniques de la prise de vue, la date et l'emplacement. Pour les supprimer, sélectionnez vos photos dans l'Explorateur de Windows. Effectuez un clic droit et pointez sur **Propriétés**, **Détails**, **Supprimer les propriétés et les informations personnelles**. Cochez **Créer une copie en supprimant toutes les propriétés possibles** et validez avec **OK**. Si vous ne souhaitez supprimer que les données de localisation, cochez **Supprimer les propriétés suivantes** et cochez les cases appropriées.



8 ÉVALUEZ LE NIVEAU DE CONFIDENTIALITÉ

Il n'est pas pratique de contourner les systèmes de suivi sans entraver la navigation. Pour tester les réglages de votre navigateur, rendez-vous à l'adresse bit.ly/4b3JSVO, cochez la case **Test with a real tracking company** puis cliquez sur le bouton **Test Your Brower**. Mis au point par l'Electronic Frontier Foundation, une ONG œuvrant pour la confidentialité des données, ce site teste la perméabilité de votre navigateur au suivi de vos informations personnelles et des données de ciblage publicitaires. Si vous ne lisez pas « *you have strong protection against Web tracking* », retour aux étapes précédentes !

9 VÉRIFIEZ VOS IDENTIFIANTS

Il existe plusieurs façons de déceler des fuites de données. Votre gestionnaire de mots de passe dispose sûrement d'une option de test. Prenons, par exemple, celui de Chrome : cliquez sur l'icône **Actualiser** et assurez-vous qu'aucun mot de passe n'a été compromis. Ceux utilisés à plusieurs reprises ou peu sécurisés sont indiqués. Prenez la peine de modifier les identifiants exposés. Pour tester votre adresse de messagerie, utilisez les sites haveibeenpwned.com, monitor.mozilla.org ou Avast (bit.ly/3VsTAeB). En cas de signalement, activez la double authentification sur les sites liés à cette adresse et préparez-vous à vider la corbeille des indésirables !

DIFFICULTÉ VARIABLE
TEMPS VARIABLE
DOMAINE SYSTÈME

Internet est devenu le terrain de jeu favori des criminels. Pour repousser leurs assauts, il convient de faire preuve de bon sens, d'adopter de bonnes pratiques et de s'appuyer sur les applications adéquates.

ÉCHAPPEZ AUX GRIFFES DES ESCROCS DU WEB

C'est toujours la même rengaine. « *Malgré les efforts de sécurisation engagés dans certains secteurs, les attaquants continuent de tirer profit des mêmes faiblesses pour s'introduire sur les réseaux, en exploitant notamment des vulnérabilités non corrigées et une trop faible maîtrise de leurs systèmes d'information par les victimes.* » Dans son dernier rapport sur les cybermenaces*, l'Agence nationale de la sécurité des systèmes d'information pointe encore et toujours du doigt les mauvaises pratiques de nombre d'internautes qui n'hésitent pas à cliquer sur les liens et les pièces jointes intégrés dans leurs courriels, sans se poser de questions. Les escrocs du numérique raffolent de ces proies un peu trop crédules qui succombent à leurs pièges (certes de moins en moins grossiers), pour lesquels il n'est pas nécessaire d'investir dans de coûteux dispositifs.

ADOPTER DE BONNES PRATIQUES. À de rares exceptions près, les tentatives d'hameçonnage ou d'arnaque commerciale s'avèrent pourtant assez faciles à identifier. Une orthographe approximative, une adresse mail farfelue doivent alerter. Rappelons d'ailleurs que les banques, les organismes publics et les opérateurs téléphoniques – appâts privilégiés des auteurs d'hameçonnage – n'invitent jamais leurs clients à leur fournir des informations personnelles par mail. Ces échanges passent par l'espace personnel en ligne et exigent une authentification en bonne et due forme. En cas de doute sur un mail ou un SMS, il est possible de signaler la tentative d'hameçonnage sur le site Phishing Initiative (bit.ly/470o7Fp), en copiant l'adresse de l'expéditeur ou le lien dans la zone de saisie prévue à cet effet. Il est toutefois probable que le bon sens ne suffise plus dans les années à venir. Les intelligences artificielles génératives risquent, en effet, d'aider les petits escrocs dans leurs sombres entreprises en générant à la pelle des mails d'hameçonnage parfaitement rédigés, de faux avis d'utilisateurs crédibles, des photos et des vidéos trompeuses… Il faut espérer que les éditeurs d'applications de sécurité déploient des IA « vertueuses » pour contrer ces nouvelles menaces. ●

* Anssi, « Panorama de la cybermenace 2023 », février 2024.

BOÎTE À OUTILS POUR CE PAS À PAS, NOUS AVONS UTILISÉ LES ÉLÉMENTS SUIVANTS

PC ou Mac · Téléphone Android ou iPhone · Navigateurs Google Chrome, Microsoft Edge · Extensions Criminal IP, AI Content Detector · Applis Téléphone d'Orange et Google, Google Messages

ÉTAPE 1

RENFORCEZ LES DÉFENSES DE VOTRE PC

Si l'être humain a souvent tendance à croire aux promesses, quand bien même elles seraient improbables, **Windows et les navigateurs déploient des défenses efficaces** où les émotions n'ont pas leur place.

1 INSTALLEZ LES MISES À JOUR

Avant d'espérer tromper leurs victimes, les logiciels malveillants doivent d'abord berner la vigilance de Windows Defender, la suite de sécurité intégrée au système d'exploitation de Microsoft, et les dispositifs de protection des navigateurs. Ces outils assurent un bon niveau de sécurité dès lors qu'ils sont maintenus à jour. Pour forcer l'installation des correctifs de sécurité et télécharger les fichiers de signatures de virus de Windows Defender, appuyez sur les touches **Windows+I**, puis cliquez sur **Windows Update, Rechercher des mises à jour**. Faites de même avec votre navigateur en choisissant **Aide, À propos de**.

2 OPTIMISEZ LA SÉCURITÉ DES NAVIGATEURS

Êtes-vous certain que le site internet que vous vous apprêtez à visiter ne présente pas de risques et qu'il ne s'agit pas d'une fausse page destinée à vous soutirer des données bancaires ou des identifiants de connexion ? Le navigateur Edge de Microsoft intègre un mode spécifique qui ajoute une couche de protection. Ouvrez les paramètres de l'application, dirigez-vous vers **Confidentialité, recherche et service** et optez pour le mode de filtrage **Strict**. Dans le cas de Google Chrome, déployez le volet **Personnaliser et contrôler**, affichez les paramètres et pointez sur **Confidentialité et sécurité, Sécurité** afin d'activer l'option **Protection avancée**. Du côté de Mozilla Firefox, l'option de filtrage **Strict** se trouve dans la section **Vie privée et sécurité** des paramètres.

3 ACTIVEZ MICROSOFT SMARTSCREEN

Le menu **Protection fondée sur la réputation** de Windows Defender protège votre PC contre les sites web malveillants, les fichiers et applications indésirables. Le module SmartScreen détermine ainsi si un élément présente un danger en le comparant à une liste de pages et de programmes de référence. Appuyez sur les touches **Windows+I** du clavier et pointez sur **Confidentialité et sécurité, Sécurité Windows, Contrôle des applications et du navigateur, Paramètres de protection fondée sur la réputation**. Activez l'intégralité des curseurs et des options affichées sur cette page avant de quitter et de redémarrer Windows.

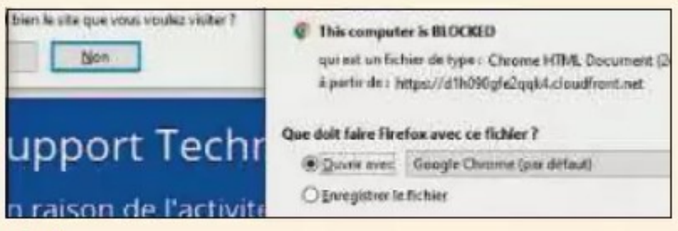
4 NE FAITES CONFIANCE QU'AUX SITES HTTPS

Les adresses des sites peu ou pas sécurisés arborent généralement le préfixe HTTP au lieu de HTTPS. L'absence du « S » final signale l'absence de chiffrement des données entre le navigateur et le serveur web distant, ce qui rend les informations échangées vulnérables. Lorsque vous vous connectez à un site, il est donc essentiel de vous assurer qu'il bénéficie d'un certificat HTTPS. Pour obtenir des informations sur le certificat d'un site, cliquez sur l'icône en forme de bouclier ou de cadenas située à gauche de la barre d'adresse. Si vous activez l'option **Toujours utiliser une connexion sécurisée** des paramètres de sécurité de Chrome, celui-ci force l'utilisation de la version HTTPS des sites ou, quand elle n'existe pas, vous demande si vous souhaitez poursuivre la navigation.

PAS À PAS EXPRESS

DÉTECTEZ LES ARNAQUES AU FAUX SUPPORT TECHNIQUE

La page web que vous venez d'ouvrir déclenche l'affichage d'un message signalant la présence d'un virus et vous incitant à contacter un numéro d'urgence pour retrouver le contrôle de son ordinateur ? Il s'agit d'une arnaque.



01. Fermez l'onglet de navigation

Si ce type de message fait craindre le pire, il suffit souvent de clore la page pour mettre un terme à la pseudo-menace. Avec Chrome, appuyez sur **Ctrl+W**. Si rien ne se passe, affichez le gestionnaire de tâches du navigateur (**Maj+Échap**), sélectionnez la page et choisissez **Arrêter le processus**.

02. Nettoyez l'ordinateur

Une fois le site clos, fermez votre navigateur et lancez Windows Defender (ou un autre antivirus) pour vous assurer qu'un logiciel malveillant n'a pas été installé sur votre PC. Supprimez ensuite l'historique du navigateur dans les paramètres de confidentialité.

03. Déposez plainte

Si vous avez paniqué et contacté le numéro d'urgence, faites opposition sans tarder auprès de votre banque, puis dénoncez les faits sur le site Pharos (bit.ly/44PVQzD). Vous pouvez aussi déposer une plainte au commissariat et appeler Info Escroqueries au 0 805 805 817.

VECTORDESIGNART2019, DIAMOND DOGS/ISTOCKPHOTO

ÉTAPE 2

IDENTIFIEZ LES FAUX COMMERÇANTS

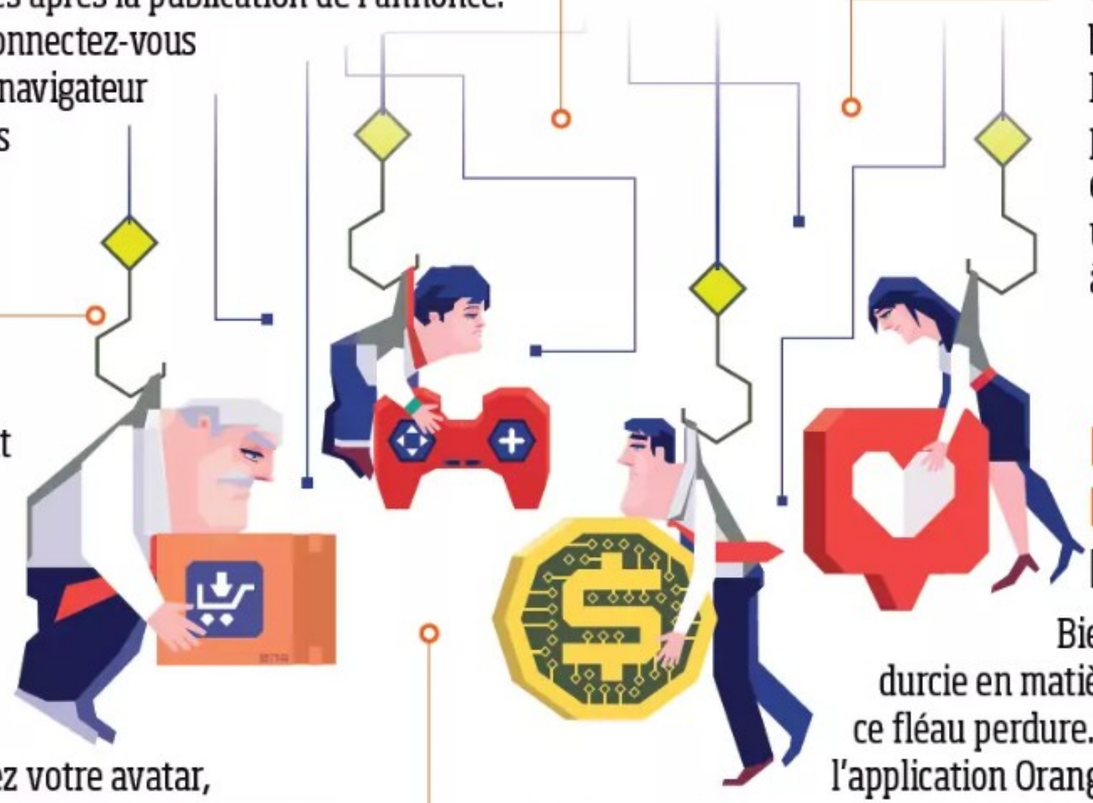
Les escrocs du web investissent tous les espaces numériques, **à commencer par les sites de vente en ligne** très fréquentés et les services de paiement internationaux.

DÉCELEZ LES ARNAQUES SUR LEBONCOIN

Le site de petites annonces entre particuliers ne renferme pas seulement des offres émanant de personnes bienveillantes. Méfiez-vous des trop bonnes affaires, des descriptifs bourrés de fautes d'orthographe et des photos de produits récupérées sur internet. Refusez de payer via le service Western Union, très populaire en Afrique. Préférez la remise en direct et les règlements utilisant le service de paiement intégré du site. Si vous vendez un article, méfiez-vous des réponses par mail ou par SMS qui interviennent quelques secondes après la publication de l'annonce. Afin de sécuriser les transactions, connectez-vous avec votre compte Leboncoin sur un navigateur à jour et faites affaire avec des profils « recommandés ».

NE VOUS TROMPEZ PAS DE PAYPAL

Quand vous réglez un achat en ligne par ce moyen de paiement, vous devez prendre quelques précautions. Si le message du vendeur indique une adresse mail ne se terminant pas par @paypal.fr, il s'agit d'une escroquerie. Si l'acheteur indique vous avoir réglé, vérifiez aussitôt votre compte PayPal. Ne cliquez sur aucun lien ou pièce jointe provenant prétendument de PayPal, cet organisme n'en envoie jamais. En vous connectant au service de paiement, vérifiez que l'adresse affichée est bien https://www.paypal.com. Pointez sur le cadenas ou le bouclier pour vous assurer que la page est sécurisée. Si vous recevez un mail frauduleux, transférez-le à l'adresse **phishing@paypal.fr**.



INTERCEPTEZ LES SMS ET MMS FRAUDULEUX

Les arnaques fleurissent également sur les téléphones. Vous pouvez limiter les risques en utilisant une application de messagerie sécurisée comme Messages de Google (bit.ly/3NT3TVs). Celle-ci intègre un module antispam fonctionnant en temps réel (touchez votre avatar, puis **Paramètres de l'application Messages**, **Protection contre le spam**). L'appli facilite aussi le blocage et le signalement des numéros frauduleux. Il suffit pour cela de le sélectionner, d'effleurer les points en haut à droite de l'écran et d'appuyer sur **Bloquer**. Si vous pensez qu'il s'agit de spam, cochez la case idoine et validez avec **OK**.

NE SOYEZ PLUS IMPORTUNÉ PAR LES APPELS INDÉSIRABLES

Bien que la loi se soit récemment durcie en matière de démarchage téléphonique, ce fléau perdure. Pour y mettre fin, installez l'application Orange Téléphone (bit.ly/44whGsc). Puis faites-en l'appli par défaut pour passer et recevoir des appels via le menu **Applications** des paramètres du téléphone. Activez l'antispam en déployant le volet d'options de l'appli. Touchez **Paramétrer les blocages** et activez les curseurs **Comme indésirable** et **Comme démarchage**. Vous pouvez aider la communauté en signalant les numéros malveillants que vous recevez et bloquer une plage de numéros (premiers chiffres).

PAS À PAS EXPRESS

ARRÊTEZ LE DÉMARCHAGE TÉLÉPHONIQUE AVEC BLOCTEL

Ce service gouvernemental, soutenu par la Direction générale de la concurrence, de la consommation et de la répression des fraudes, analyse les signalements des consommateurs et sanctionne les sociétés qui ne respectent pas la loi.

01. Créez un compte Bloctel

Rejoignez le site Bloctel (bit.ly/43zXpRb) et cliquez sur **Créer son compte**. Remplissez le formulaire d'adhésion, définissez un mot de passe fort (la mention **Fiable** doit s'afficher en vert) et cliquez sur **Valider le formulaire**.

02. Identifiez-vous

Confirmez la création du compte en ouvrant le lien Bloctel reçu par mail. Pointez ensuite sur **Se connecter** en haut à droite. Entrez vos identifiants et validez avec **Connexion**. Vous pouvez désormais dénoncer les démarchages abusifs.

03. Déposez un signalement

Actionnez le bouton **Signaler un démarchage abusif** et suivez la procédure en saisissant les infos demandées (numéro de l'appelant, son objet, etc.) Vérifiez l'exactitude des données et validez.

ÉTAPE 3

DÉJOUEZ LES TRUCAGES DE L'IA

L'intelligence artificielle permet de créer de fausses pages web, des mails d'hameçonnage parfaits et de faux avis. Il reste toutefois possible de ne pas tomber dans le panneau.

astuce 1

REPÉREZ LES COURRIELS INDÉSIRABLES

Bien que la plupart des messageries disposent d'armes contre le phishing, il arrive que des courriels frauduleux passent à travers les mailles du filet. Avant de cliquer sur un lien, vérifiez l'adresse de l'expéditeur qui doit se terminer par le nom de la société de livraison (noreply@notif-colissimo-laposte.info par exemple) et non par @gmail.com. Il est parfois impossible de visualiser l'adresse de l'envoyeur en cliquant dessus, preuve supplémentaire de l'escroquerie. Repérez également les éventuelles fautes d'orthographe et demandez-vous si vous êtes bien en attente d'un colis. En cas de doute, copiez le numéro de suivi et soumettez-le au moteur de *tracking* de l'expéditeur (La Poste, Relais Colis, DHL, DPD, etc.) ou à un site de suivi universel comme Parcelsapp.com/fr.

astuce 2

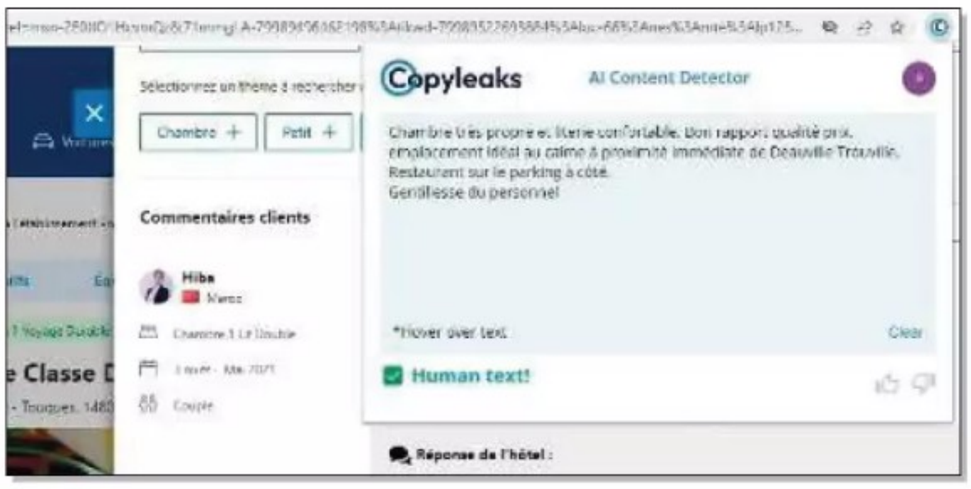
DÉJOUEZ LES PIÈGES TÉLÉPHONIQUES

L'intelligence artificielle est un outil supplémentaire au service des escrocs. Ces derniers peuvent l'utiliser pour générer des voix artificielles vous demandant, par exemple, de valider les identifiants de votre compte en banque de toute urgence. Soyez attentif aux pauses non naturelles, aux sonorités parfois étranges voire déformées. Bien évidemment, ne communiquez jamais d'informations personnelles par téléphone, et moins encore à un inconnu. L'application Téléphone de Google (bit.ly/3XYv1qE) se propose de bloquer les spams vocaux. Appuyez sur les points en haut à droite de la page d'accueil, puis sur **Paramètres**, **Numéro de l'appelant et spam** et activez les curseurs associés à ce filtre.

astuce 3

INSTALLEZ UNE EXTENSION ANTI-PHISHING

Les pirates détournent les services des IA pour générer des messages frauduleux, de fausses URL et des sites web d'hameçonnage difficilement repérables. Vous pouvez réduire votre exposition à ces menaces en dotant les navigateurs Chrome et Edge de l'extension Criminal IP (bit.ly/4dmwmxG). Une fois sur la page du module, cliquez sur **Ajouter à**..., puis sur l'icône **Extensions** à droite de la barre d'adresse. Pointez sur **Criminal IP**, **Sign in with Google** et suivez la procédure de création de compte gratuit. Vérifiez ensuite si le site web que vous visitez semble être du phishing. Cliquez sur l'icône **Criminal IP** à droite de la barre d'adresse pour connaître le niveau de risque du site : « *safe* » (sûr), « *unknown* » (inconnu)...



astuce 4

NE VOUS LAISSEZ PAS ABUSER PAR DE FAUX AVIS

L'IA peut aussi être détournée pour rédiger de faux témoignages de consommateurs vantant les mérites d'un produit ou d'un service frauduleux. Il existe une extension capable de repérer ces avis et de vous dire s'il s'agit d'un texte rédigé par un humain ou une IA comme ChatGPT, Bard T5, Jasper... Visitez la page AI Content Detector (bit.ly/3Dm7Pco) et procédez à l'installation du module sur Chrome ou Edge. Créez un compte gratuit avec vos identifiants Google, puis cliquez sur l'icône **Extension**. Épinglez le raccourci du module à la barre d'adresse. Pour vérifier un avis, copiez-le dans la zone de saisie **AI Content Detector** et pointez sur **Did a human write this?** pour afficher le verdict. La mention **Human text** indique qu'une IA ne se cache pas derrière le commentaire.

Détectez les contenus générés par l'intelligence artificielle

Les escrocs utilisent des outils de création de vidéos reposant sur des modèles d'IA pour induire en erreur les internautes. Une observation ne suffit pas toujours à déceler des incohérences. Faute de signes flagrants, soumettez le visuel suspect aux algorithmes d'Attestiv (bit.ly/3Y4xEIa). Créez un compte pour bénéficier de la période d'essai gratuite de trente jours. Pointez sur le lien de vérification reçu par mail et identifiez-vous. Téléversez le fichier douteux ou indiquez son URL, puis cliquez sur le bouton **Scan video**. Patientez quelques minutes - le délai de réponse est plus ou moins long selon la durée de la séquence à étudier. Au terme de l'analyse, déroulez la page **Scan results** pour découvrir la note de confiance attribuée au fichier (plus la valeur est basse, mieux c'est).

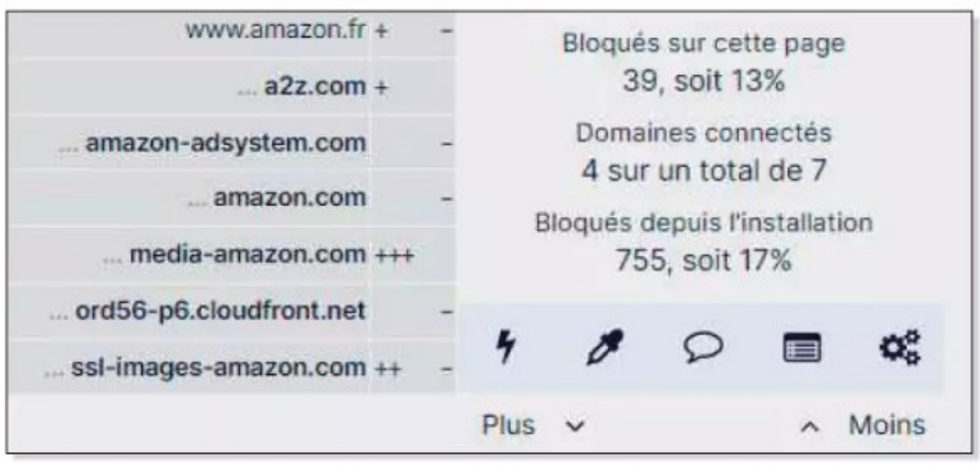
DIFFICULTÉ
MODÉRÉE
TEMPS
20 MIN
DOMAINE
NAVIGATEURS

FILTREZ INTERNET AVEC UBLOCK ORIGIN

Logiciels espions, sites malveillants, tentatives d'hameçonnage, publicités en rafale... naviguer sur le web n'est pas de tout repos. L'extension de navigateur uBlock Origin s'érige en cerbère et protège vos arrières.

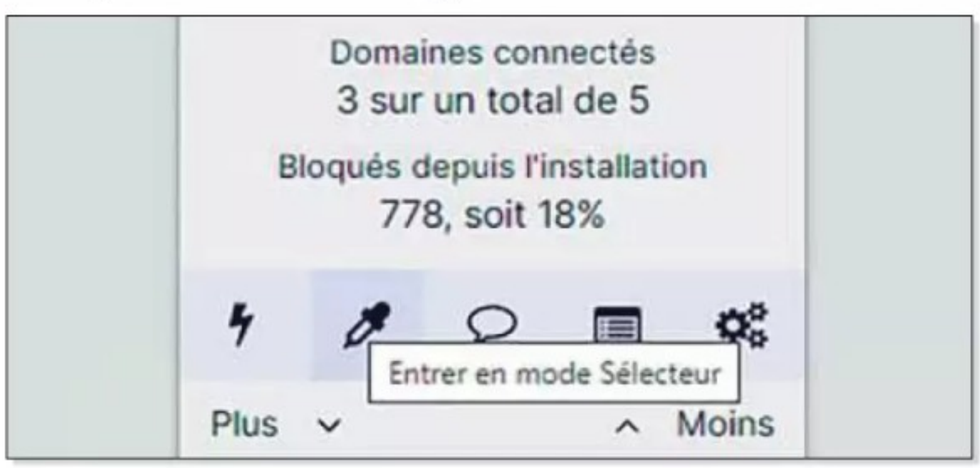
1 ACCÉDEZ AU TABLEAU DE BORD

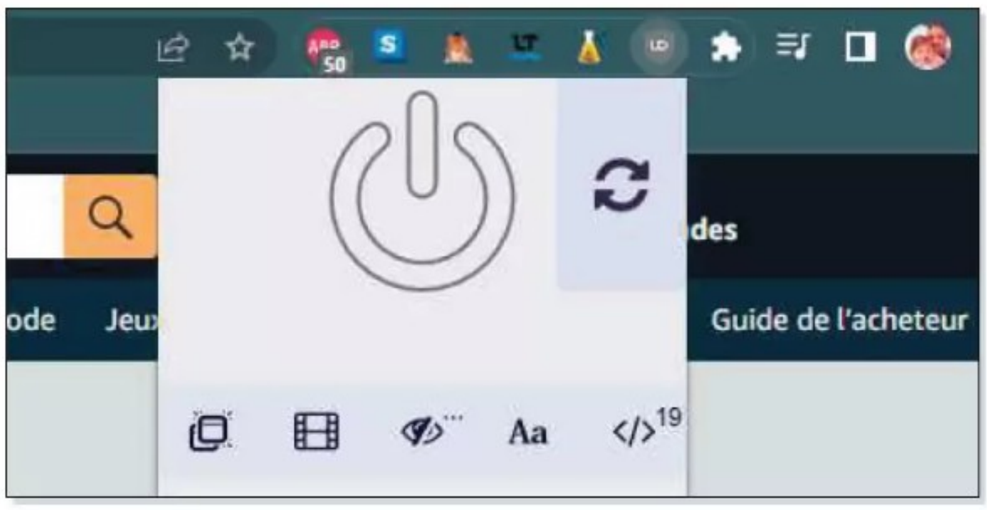
Rendez-vous dans le Web Store de Chrome (accessible à tous les navigateurs Chromium comme Brave ou Vivaldi) ou dans la boutique applicative d'**Edge**. Recherchez le module additionnel **uBlock Origin** et pointez sur **Installation**. La surveillance démarre aussitôt la procédure terminée. Épinglez un raccourci vers l'extension à droite de la barre d'adresse pour accéder rapidement aux options supplémentaires. Cliquez sur l'icône **uBlock,** puis sur **Plus** de façon à faire apparaître les outils disponibles, mais aussi la liste des capteurs d'activités et des éléments malveillants interceptés par l'application. Pointez sur l'intitulé **Moins** pour revenir à un affichage plus synthétique.



2 RETIREZ DES ÉLÉMENTS PRÉCIS D'UN SITE

Le bloqueur de publicités est activé par défaut. Il risque de faire doublon avec d'autres extensions concurrentes déjà présentes sur votre ordinateur, comme AdblockPlus. Nos tests n'ont pas laissé apparaître de conflits entre ces outils, aussi, n'hésitez pas à les conserver. Cliquez sur l'icône **uBlock** et une fois sur **Plus** pour dévoiler une barre d'outils. Le mode **Zappeur** sert à désactiver un composant potentiellement dangereux du site où vous vous trouvez. L'option **Sélecteur** fait de même, mais en créant une règle duplicable sur d'autres pages. Pointez de nouveau sur **Plus** pour découvrir une nouvelle barre d'outils et profiter de fonctions supplémentaires.





3 DÉSACTIVEZ LE MODULE EN CAS DE BESOIN

Ces icônes ont pour objet de bloquer les bannières publicitaires de type pop-up et d'empêcher la lecture et le chargement des médias de grande taille. À l'usage, **uBlock Origin** intercepte assez d'éléments par défaut pour qu'il s'avère inutile de solliciter ces options, sinon quand vous visitez des sites douteux, proposant par exemple de télécharger des films ou des jeux. Il se révèle a contrario parfois nécessaire de suspendre **uBlock**, qui peut empêcher l'accès à certains contenus. Il suffit alors de cliquer sur l'icône bleue tout en appuyant sur la touche **Ctrl**. L'extension est ainsi désactivée sur la page en cours.

4 MODIFIEZ LES FILTRES DE BLOCAGE

Cliquez sur l'icône **Ouvrir le tableau de bord** en bas à droite et sélectionnez **Liste de filtres**. Vous pouvez ajouter des annuaires de référence pour améliorer le niveau de sécurité. Sachez toutefois que plus vous activez de listes et plus l'extension utilise de ressource mémoire. À vous de trouver le juste compromis. Bien que le navigateur et l'antivirus installé sur votre PC surveillent déjà la navigation, pointez sur **Domaines malveillants** et cochez les modes **Phishing URL Blocklist** et **PUP Domains Blocklist**. Faites de même dans la section **Nuisances**. Testez différents sites pour évaluer la façon dont les réglages pèsent sur la vitesse de navigation et l'affichage des pages.

NOUVEAU la croisière cybersécurité de 01NET

COUP DE CŒUR
EN MÉDITERRANÉE

Du 22 au 25 octobre 2025
avec l'équipe 01NET à bord

Embarquez sur le **Costa Favolosa******

4 JOURS / 3 NUITS

À partir de **695 €*/personne** au départ de Marseille
« Tout compris » (pension complète, animations, boissons…)

PENDANT VOTRE TRAVERSÉE,
DES ATELIERS PRATIQUES
+ DES CONFÉRENCES
ANIMÉES PAR DES EXPERTS
DE 01NET MAGAZINE

RENSEIGNEMENTS
Tél. : +33 (0)1 84 76 22 35
Email : experiences@mycomm.fr
BROCHURE SUR DEMANDE

MYCOMM. Experiences

*base cabine intérieure, occupation double, sous réserve de disponibilité.

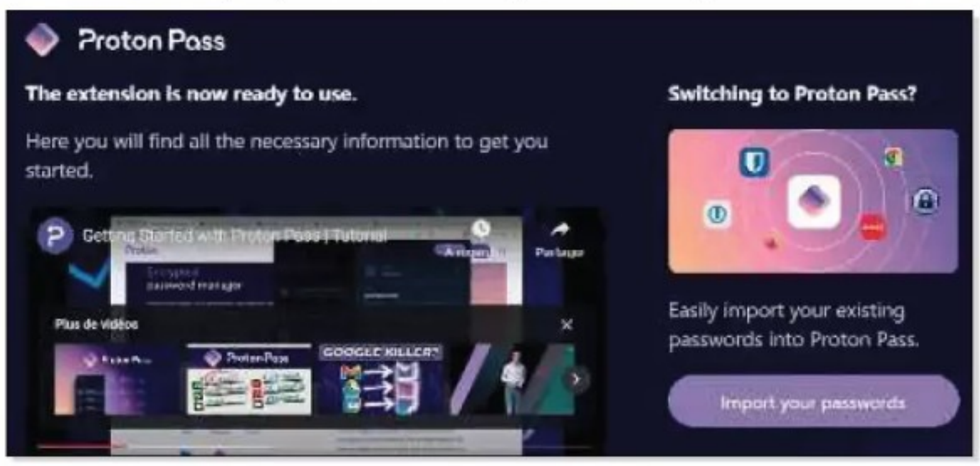
DIFFICULTÉ
MODÉRÉE
TEMPS
60 MIN
DOMAINE
IDENTIFIANTS

CONFIEZ VOS IDENTIFIANTS À PROTON PASS

Proton complète sa galerie de services **avec un gestionnaire de mots de passe sécurisé hébergé sur des serveurs européens.** Il mémorise aussi votre carte bancaire et protège toutes les notes que vous lui confiez.

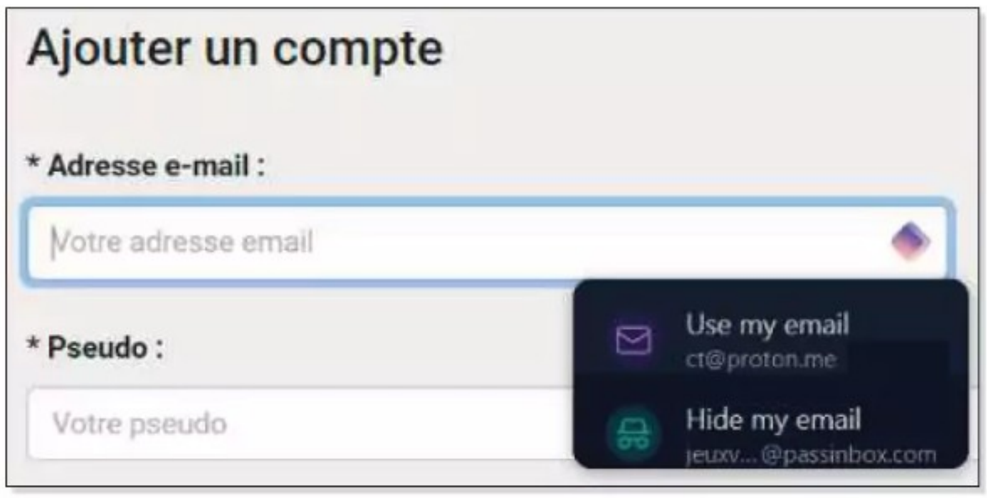
1 INSTALLEZ PROTON PASS

Allez sur la page du service (urlz.fr/mJI9). Dans la section **Installez une application de navigateur**, choisissez le vôtre (Chrome, Edge, Firefox, Brave). Connectez-vous à votre compte. Épinglez le raccourci vers l'extension Proton Pass à droite de la barre d'adresse. Cliquez sur cette icône, sur **Sign In** si vous disposez d'un compte ou sur **Create a Proton account** pour vous inscrire. Choisissez ensuite **Import your passwords** et sélectionnez l'utilitaire ou le navigateur qui abrite vos mots de passe. Actionnez le bouton **How do I export my data from** pour savoir comment créer un fichier.CSV, un format utilisé par les tableurs et adopté par Proton Pass pour l'échange de données.



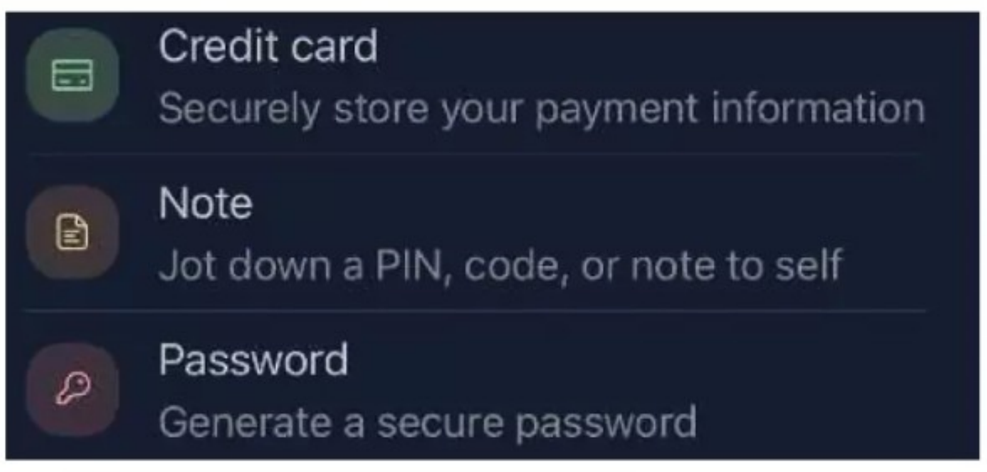
2 IMPORTEZ VOS MOTS DE PASSE

Effectuez un glisser-déposer du fichier.CSV dans la zone d'échange de Proton Pass et cliquez sur **Import**. Choisissez le coffre-fort cible (Personal, par exemple) et validez avec **Proceed**. Déployez le volet **Proton Pass** depuis le raccourci de la barre d'adresse, pointez sur **Open Navigation** (l'icône formée de trois barres horizontales en haut à gauche), **Settings**, **Security**. Cochez le mode **Auto-lock Proton pass** et définissez le code pin qui protégera l'accès à vos mots de passe et sera exigé à chaque nouvelle session de navigation. Il suffit de fermer le navigateur internet pour verrouiller Proton Pass.



3 MÉMORISEZ DES IDENTIFIANTS DE CONNEXION

Arrivé sur une page proposant un formulaire d'identification, le logo Proton apparaît avec le nombre de mots de passe enregistrés pour le service. Cliquez et choisissez un compte pour compléter automatiquement les informations d'authentification. Rendez-vous sur un site sur lequel vous n'êtes pas encore inscrit. Cliquez sur l'icône **Proton** dans le champ **Adresse e-mail**. Indiquez une adresse ou laissez Proton Pass générer un alias, afin de vous prémunir contre la revente ou du piratage de fichiers clients. Cliquez sur l'icône **Proton** dans **Mot de passe** et définissez un code secret. Validez l'inscription.



4 RETROUVEZ VOS CLÉS SUR UN MOBILE

Installez l'application mobile Proton Pass depuis le Play Store Android ou l'App Store Apple. Entrez vos identifiants Proton, conditionnez l'accès à l'application à la saisie d'un code PIN ou choisissez d'utiliser le dispositif biométrique de l'appareil. Touchez ensuite l'icône **Profile** en bas à droite de l'écran. Rendez-vous ensuite dans **Settings** et indiquez votre navigateur internet sous **Default browser**. Le contenu du coffre-fort est ainsi synchronisé sur tous vos appareils et vous retrouvez sur chacun d'eux vos mots de passe, alias, numéros de cartes de crédit et Notes. Appuyez sur **Password** pour générer des mots de passe complexes comptant jusqu'à 64 caractères.

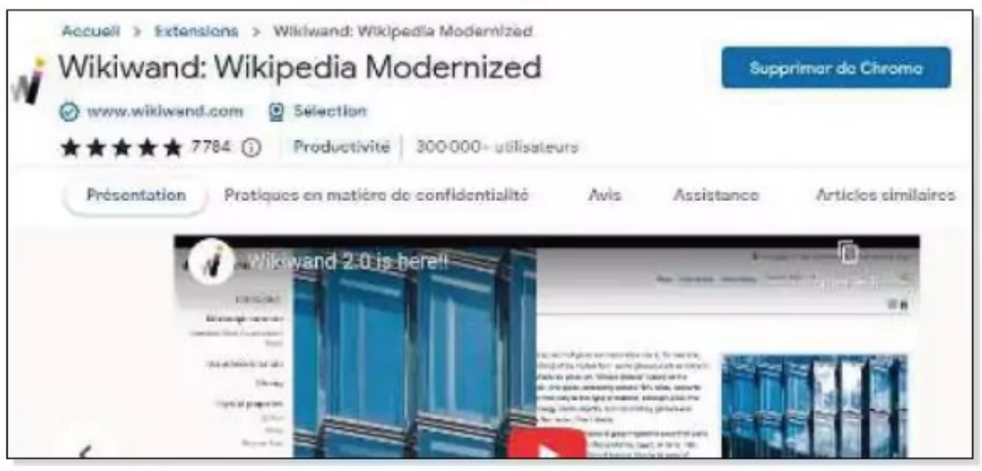
DIFFICULTÉ
MODÉRÉE
TEMPS
20 MIN
DOMAINE
NAVIGATEURS

LIMITEZ-VOUS AUX EXTENSIONS INDISPENSABLES

Tout comme votre système ne doit pas être chargé d'applications dont vous n'avez pas l'usage, **votre navigateur ne doit pas entasser les modules** au risque de laisser des failles à disposition des pirates.

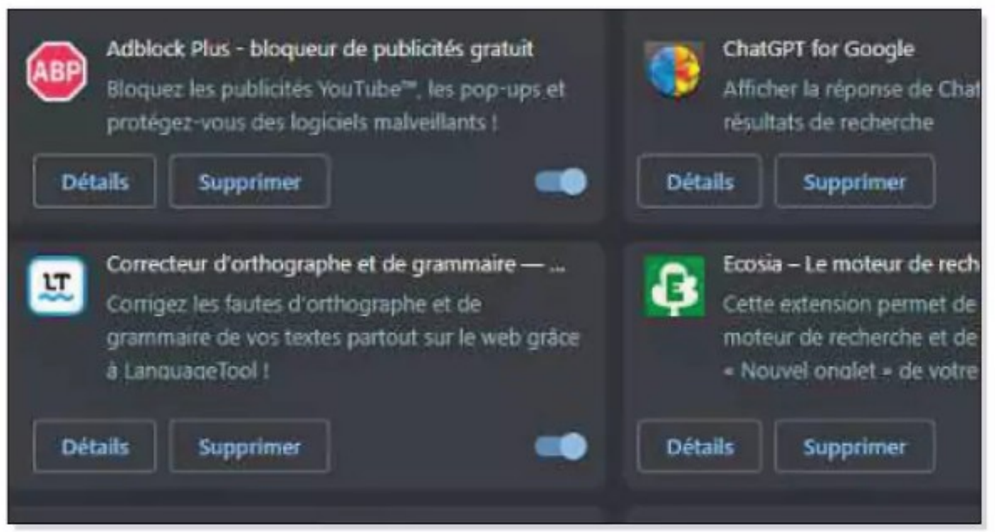
1 LIMITEZ, ANALYSEZ, AFFICHEZ, CONTRÔLEZ

Pour commencer, n'installez jamais d'extension en dehors des marchés propres à chaque navigateur (Chrome Web Store, Module complémentaire Edge…), sachant qu'il faut de toute façon rester méfiant, car même ces derniers ne garantissent pas une totale innocuité. Sur votre store, regardez toujours la note d'une extension, le nombre de votants et d'utilisateurs. N'hésitez pas à taper le nom du développeur dans une barre de recherche afin de vérifier s'il a créé d'autres applications, et avec quel succès. Évitez les extensions aux promesses trop alléchantes ou qui donnent l'impression de faire gagner du temps, mais, au mieux, alourdissent le navigateur.



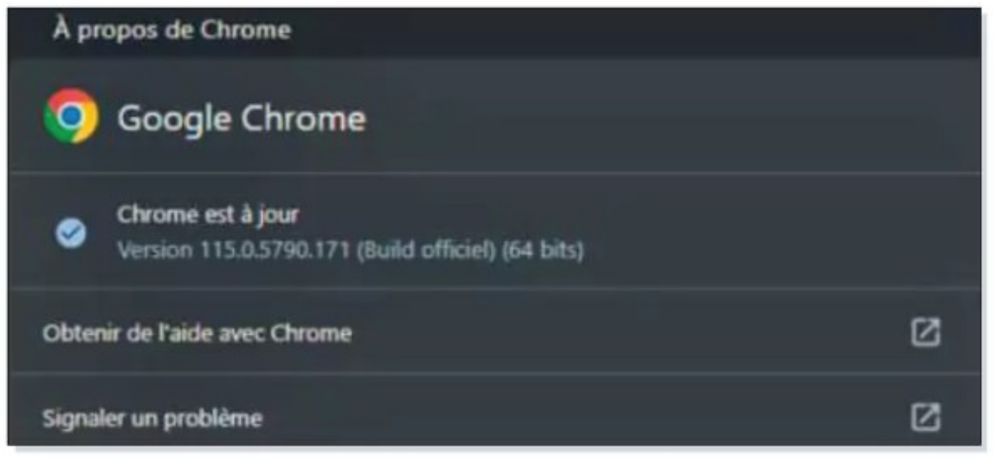
2 EXAMINEZ LES AUTORISATIONS

Sur Chrome comme sur Edge, cliquez à droite de la barre d'adresse sur l'engrenage, l'icône des trois points, puis **Afficher les autorisations Web**. Sur Firefox, effectuez un clic droit sur **Gérer l'extension** puis **Permission**. Observez ensuite toutes les autorisations que s'est octroyées l'application, s'il y en a trop ou que ce n'est pas cohérent avec le but de l'extension, cela doit vous mettre la puce à l'oreille. Si vous avez des doutes, mais n'avez pas encore désinstallé les extensions concernées, utilisez une fenêtre de navigation privée (**Ctrl+Maj+N** sur Chrome et Edge, **Ctrl+Maj+P** sur Firefox). Ainsi, elles seront désactivées sauf celles qui vous auront demandé l'autorisation à l'installation.



3 DÉSACTIVEZ ET DÉSINSTALLEZ LES EXTENSIONS DOUTEUSES

Sur Chrome et Edge, cliquez sur le puzzle puis **Gérer les extensions** ; sur Firefox, exécutez un clic gauche sur le puzzle. Commencez par la désactiver en passant le curseur à gauche. Vous la rendez inopérante et cela vous laisse le temps de vérifier sa légitimité sur les stores et dans votre navigateur. Cliquez sur **Détails** et **Afficher sur le Chrome Web Store** ou **dans le store des modules complémentaires** selon votre navigateur pour retourner sur la page. Contrôlez de nouveau la note et les appréciations. Si vous n'êtes pas en confiance, aucune hésitation, retour dans le navigateur, page des extensions et **Supprimer**.



4 VÉRIFIEZ LES MISES À JOUR

Voici venir la phrase clé que vous lisez au moins une fois par numéro : mettez à jour ! Si un problème se produit lorsque vous êtes sur internet, mettez à jour notre navigateur et faites-en de même avec votre antivirus puisqu'il est capable de détecter des extensions frauduleuses ou sinon les dommages causés dans votre PC. Certaines extensions ne font « que » lire vos cookies ou installer un traqueur pour encore davantage cibler la publicité. Rien de douloureux pour l'utilisateur si ce n'est une entaille dans la protection de la vie privée. Un antivirus saura le déceler, mais le plus efficace reste de ne pas installer une extension qui ne vous sera pas pleinement utile.

DIFFICULTÉ VARIABLE
TEMPS VARIABLE
DOMAINE SYSTÈME

APPRENEZ À BIEN PROTÉGER VOTRE PC SANS DÉPENSER UN EURO

Si vos données sont indéniablement précieuses, leur sécurité n'est pas forcément une question d'argent. Bien utilisés, Microsoft Defender et les antivirus gratuits s'avèrent d'efficaces cerbères.

Quand il s'agit des menaces cyber, la méconnaissance du grand public en matière de nouvelles technologies contribue à installer un climat anxiogène. Difficile il est vrai de ne pas s'inquiéter devant l'annonce de failles de sécurité affectant des millions d'ordinateurs, de rançongiciels bloquant les hôpitaux ou de données dérobées mises aux enchères sur le darknet. Cet environnement constitue un terreau fertile pour les éditeurs et leurs solutions de sécurité capables d'intercepter virus et logiciels malveillants, mais aussi de protéger les fichiers et les informations personnelles hébergées sur un PC ou un téléphone. Si ces outils démontrent une réelle efficacité, comme en attestent les rapports publiés par le laboratoire indépendant AV-Test, ils ont un coût non négligeable. Accessibles le plus souvent via un abonnement, les suites de sécurité nécessitent de mettre la main à la poche tous les ans. Après une première annuité à un tarif préférentiel (de 40 à 90 € selon les applications, le nombre d'appareils couverts et les modules intégrés), le prix s'envole au moment du renouvellement. L'abonnement à Norton 360 premium passe ainsi de 40 à 110 euros après douze mois.

ET POURQUOI PAS DES OUTILS GRATUITS? Si la prudence suffit à se prémunir du hameçonnage, des arnaques au faux support technique et au chantage à la webcam, les applications de protection s'avèrent indispensable concernant les virus, malwares, ransomwares, le détournement des données personnelles et le piratage des comptes en ligne. Rien ne remplace l'expertise d'un expert ! À condition d'éviter les comportements à risque, un PC sous Windows 10 ou 11 régulièrement mis à jour et protégé par Microsoft Defender présente une faible vulnérabilité aux attaques cyber. Rien n'interdit néanmoins de compliquer encore la tâche des pirates en adoptant des outils complémentaires et gratuits assurant la surveillance des mails entrants, le signalement des mots de passe compromis ou le masquage de votre adresse IP lorsque vous naviguez sur internet. ●

PESHKOV/ISTOCKPHOTO

BOÎTE À OUTILS POUR CE PAS À PAS, NOUS AVONS UTILISÉ LES ÉLÉMENTS SUIVANTS

PC

Connexion internet

- Avast
- AOEMI Backupper
- Bitwarden
- Malwarebytes
- Navigateur Brave
- Proton VPN

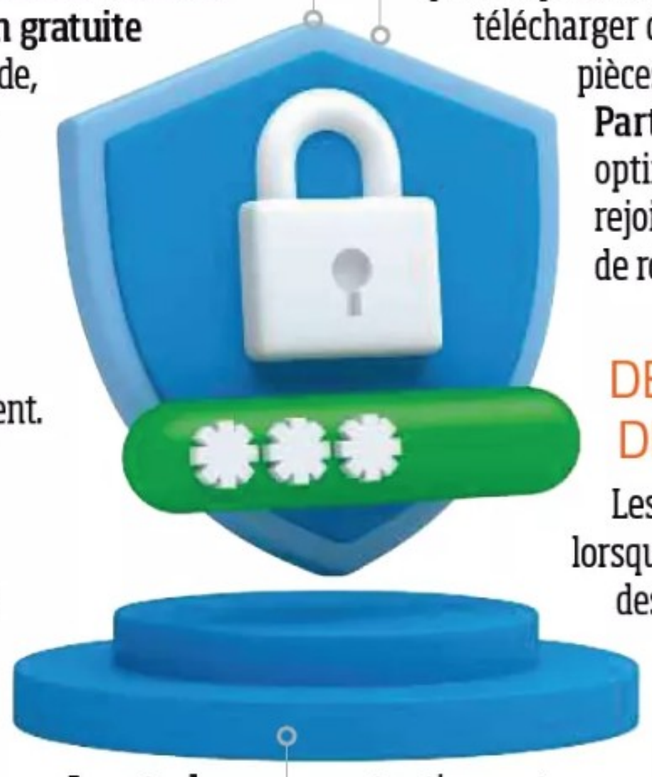
ÉTAPE 1

NE LAISSEZ AUCUN RÉPIT AUX VIRUS

Si l'on parle davantage des rançongiciels, les autres types de programmes malveillants n'ont pas disparu des radars pour autant. Voici comment vous en protéger.

DÉPLOYEZ L'ANTIVIRUS ET LE PARE-FEU **AVAST**

Avant de télécharger la version gratuite d'Avast (bit.ly/46LJPfg), prenez soin de supprimer l'ancien antivirus de votre PC. Durant l'installation, décochez les cases relatives au navigateur Avast Secure Browser et cliquez sur **Personnaliser**. Activez le pare-feu pour remplacer celui de Windows qui, par défaut, ne bloque pas automatiquement les connexions sortantes. Puis pointez sur **Continuer avec la version gratuite** et **Exécuter la première analyse**. À ce stade, un message vous informe de la connexion à un nouveau réseau, confirmant que le pare-feu joue son rôle. Cliquez sur **Afficher les résultats de l'analyse**. Passez votre réseau en revue en allant sur **Analyser tous les appareils**, **Oui**, **Continuer**. Les appareils sécurisés s'affichent. Avast vous invite par la suite à ajuster les options de sécurité du PC. Cliquez sur **Protection**, **Analyse antivirus**, puis sur l'icône en forme d'engrenage. Positionnez le curseur sur le mode **Haute sensibilité**. Cochez **Rechercher des outils** et **Suivre les liens du système pendant l'analyse**. Poursuivez l'optimisation en explorant le menu **Agents de sécurité**. Cliquez sur l'engrenage et cochez l'option **Activer le mode renforcé**. Passez au menu **Agent anti-ransomware** et choisissez **Mode strict** et **Sécuriser tous les fichiers des dossiers protégés**. Si les fausses alertes ont tendance à se multiplier, revenez au **Mode smart**.



ÉLOIGNEZ LES LOGICIELS MALVEILLANTS AVEC **MALWAREBYTES**

Ce programme (bit.ly/41dwivv) s'avère un parfait complément à Avast. Il évite les chevaux de Troie, l'hameçonnage, les logiciels espions et publicitaires. Gardez à l'esprit que l'offre gratuite qui s'active au terme de la période d'essai de la version complète n'assure pas la surveillance en temps réel du PC. Il vous incombe donc de lancer une analyse périodiquement, au moins une fois par semaine si vous avez l'habitude de télécharger des contenus sur le web ou si vous recevez de nombreuses pièces jointes. Une fois le programme installé, choisissez l'option **Particuliers** et cliquez sur **Ignorer pour le moment**. Pour optimiser la protection, pointez sur l'icône des paramètres, rejoignez l'onglet **Sécurité** et activez les curseurs de recherche de rootkits et de protection contre la force brute.

DEVENEZ ANONYME DERRIÈRE **PROTON VPN**

Les VPN (réseaux privés virtuels) masquent votre adresse IP lorsque vous visitez des sites web, protégeant vos données privées des regards indiscrets. Les solutions gratuites se comptent cependant sur les doigts d'une main. Parmi celles-ci, le Suisse Proton VPN (bit.ly/4a6nYC2) propose un service sans quotas de données. Procédez à l'installation du module, puis créez et activez votre compte. Au démarrage de l'application, vous n'êtes pas protégé. Il convient de cliquer sur **Connexion rapide** pour y remédier (Avast devrait émettre une notification vous informant de la connexion à un nouveau réseau). Proton VPN vous localise par défaut aux Pays-Bas, mais vous pouvez opter pour une adresse virtuelle aux États-Unis ou au Japon. Renforcez l'anonymat en pointant sur **Arrêt d'urgence (kill switch)** et choisissez **Arrêt d'urgence activé**.

PAS À PAS EXPRESS

AIDEZ-VOUS DES OUTILS AVANCÉS D'AVAST

La version gratuite de l'antivirus propose des options que nombre de concurrents réservent à leurs offres payantes, à l'image de **la surveillance de votre adresse mail et de la vérification des mises à jour de vos logiciels**.

01. Surveillez votre adresse mail

Placez-vous sur l'onglet **Confidentialité** et cliquez sur **Alertes piratage**, **Protéger mes comptes**. Si vous ne l'avez pas déjà fait, connectez-vous à Avast avec votre compte Google ou Apple afin de veiller sur vos identifiants.

02. Gardez vos programmes à jour

Sécurité oblige, les logiciels installés sur votre PC doivent profiter des correctifs régulièrement publiés par les éditeurs. Avast veille à ce que ce soit le cas. Pointez sur **Performances**, **Software Updater**, puis sur **Tout mettre à jour**.

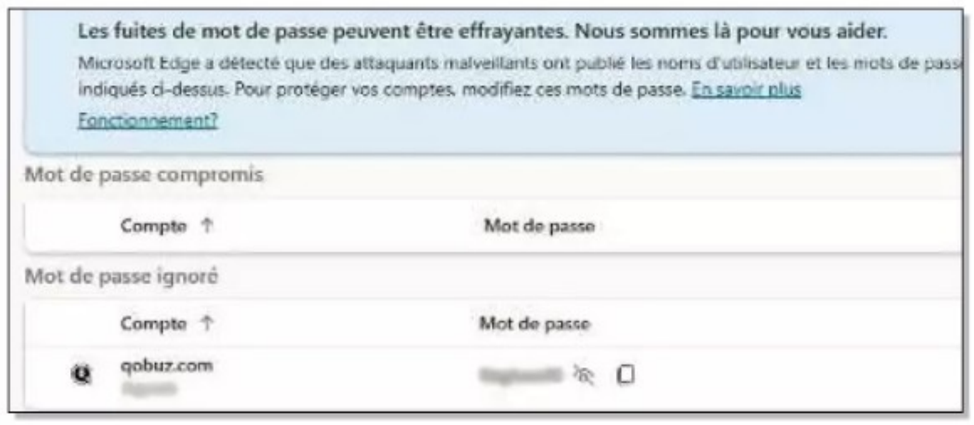
03. Travaillez sans être dérangé

Avast peut suspendre les notifications lorsqu'une application est utilisée en mode plein écran. Pointez sur **Performances**, **Mode ne pas déranger**, **Ajouter une application**, puis sur l'icône en forme d'engrenage pour paramétrer la fonction.

ÉTAPE 2

PRÉSERVEZ VOS IDENTIFIANTS ET VOTRE VIE PRIVÉE

Piratage des réseaux sociaux, accès aux données bancaires, usurpation d'identité, utiliser des mots de passe insuffisamment sûrs peut avoir de funestes conséquences.



1 EXPLOITEZ LE GESTIONNAIRE DE MOTS DE PASSE D'EDGE

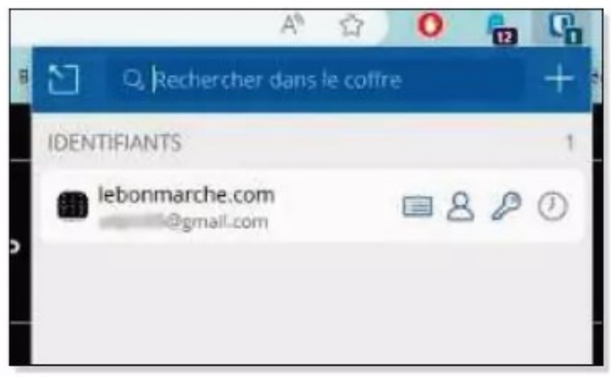
Il existe deux manières de mettre ses mots de passe à l'abri. La première, et la plus simple, s'appuie sur les outils intégrés à Chrome, Edge et Firefox. Le navigateur de Microsoft dispose depuis peu d'un portefeuille assurant la sécurité des données personnelles. L'accès à ce module s'opère depuis le menu **Paramètres, Profils**. Identifiez-vous avec votre compte Microsoft, puis cliquez sur **Ouvrir le portefeuille, Mots de passe** et **Paramètres associés**. Activez les six options proposées dans le menu **Mots de passe, Plus de paramètres** à l'aide des différents curseurs. Edge mémorise automatiquement les données saisies pour vous connecter aux sites web requérant des identifiants. Vérifiez si un mot de passe n'a pas été compromis en cliquant sur le bouton **Divulguées**. Si c'est le cas, changez-en sans tarder.

2 GÉNÉREZ DES CODES SÉCURISÉS

L'un des intérêts des gestionnaires de mots de passe comme celui d'Edge consiste à vérifier si vos combinaisons secrètes sont assez complexes pour ne pas être craquées rapidement. Vérifiez-le dans le portefeuille du navigateur en cliquant sur l'onglet **Faible** de la section **Mots de passe**. Pointez sur l'option **Modifier le mot de passe** des sites jugés peu sécurisés et définissez des codes plus complexes. Le navigateur de Microsoft se propose de vous aider dans cette entreprise : opérez un clic droit sur le champ de saisie et choisissez **Suggérer un mot de passe fort**. Enregistrez les modifications en cliquant sur le bouton **Mettre à jour**. Assurez-vous également qu'un même mot de passe n'est pas associé à trop de sites ou services en pointant sur l'onglet **Réutilisé**. Remplacez les doublons.

3 ABRITEZ VOTRE VIE NUMÉRIQUE AVEC BITWARDEN

Cette application (bit.ly/467YGjy) est née d'un projet open source. Elle propose une formule gratuite qui limite le nombre d'appareils pouvant être synchronisés et le volume de mots de passe qu'elle génère. Commencez par installer la version Free (**Get started today**) de Bitwarden sur votre PC. Créez ensuite un compte en prenant soin de définir une clé de sécurité principale renforcée afin de protéger l'accès à la bibliothèque d'identifiants. Confirmez l'inscription, puis greffez l'extension à votre navigateur internet en pointant sur vos initiales en haut à droite de la page d'accueil du service et sur **Télécharger les applications**. Désignez votre navigateur dans la section **Web Browser Extensions**.



4 NAVIGUEZ INCOGNITO À L'AIDE DE BRAVE

À la différence de Chrome ou Edge, le navigateur Brave (bit.ly/3Rg98jC) intègre des outils de blocage des traceurs publicitaires, des logiciels malveillants et d'hameçonnage. Lors de l'installation du programme, décochez les deux options d'amélioration du navigateur. Prenez ensuite le temps d'ajuster les réglages de sécurité en pointant sur l'icône en forme d'engrenage présent au bas de la page **Nouvel onglet**. Accédez au menu **Protections**. Positionnez le blocage des pisteurs et annonces sur **Agressif**, les connexions HTTPS sur **Strict**. Activez le blocage des scripts, puis ouvrez le menu **Confidentialité et sécurité**. Décochez l'envoi d'un signal quotidien à Brave avant de lancer une analyse de sécurité afin de détecter les éventuelles violations de données.

Sécurité et télétravail, les bons réflexes à adopter

Si vous utilisez votre PC pour travailler depuis un réseau Wifi, faites attention à ce qu'il ne puisse pas être piraté. À la maison, cliquez sur l'icône Wifi à droite de la barre des tâches et sur la flèche **Gérer les connexions Wi-Fi**. Le nom de votre réseau doit s'accompagner de la mention « *connecté et sécurisé* » et arbore un cadenas. Personnalisez les options de sécurité en pointant sur le **i** (pour **Propriété**), puis sur **Réseau public (recommandé)**. Si vous vous connectez depuis un réseau inconnu, demandez un audit de sécurité à Avast avant d'y échanger des données. Effectuez un clic droit sur l'icône du point d'accès dans la barre des tâches et lancez Avast. Dans le menu **Protection**, accédez à la section **Inspecteur réseau** et procédez à l'analyse.

ÉTAPE 3

SURVEILLEZ LES FAILLES DU SYSTÈME

Sans mise à jour de Windows, des applications, des pilotes de périphérique et du navigateur, vous vous exposez à des problèmes que votre antivirus ne suffira pas forcément à combler.

1 AJOUTEZ DES EXTENSIONS DE SÉCURITÉ AU NAVIGATEUR

Les malwares peuvent infecter votre PC par le biais des navigateurs. Pour éviter les pubs et les barres d'outils et de recherche indésirables, nous vous invitons à lui associer des extensions spécialisées dans le filtrage de contenus. AdBlock (bit.ly/3Rch2uq) chasse ainsi les réclames et les pop-up qui fleurissent sur les sites. Le module complémentaire Ghostery (bit.ly/488la5x) veille pour sa part sur votre vie privée en contrariant le fonctionnement des outils d'analyse web, des publicités, des mouchards et autres traceurs. Adoptez enfin l'extension Smart HTTPS (bit.ly/41gbbZM) afin de ne pas croiser la route de sites et de pages non sécurisés, et le module complémentaire d'Avast (bit.ly/486JaGØ).

2 NE PASSEZ PAS À CÔTÉ DES PILOTES DE VOS APPLIS

Parmi les conseils de sécurité distillés par Microsoft, la mise à jour périodique des logiciels figure en bonne place. Les éditeurs publient régulièrement des correctifs destinés à combler les failles de sécurité identifiées par les utilisateurs et les bêta-testeurs. Accédez notamment au menu **Performances** de l'antivirus Avast et pointez sur le bouton **Software Updater**. Installez ensuite la version gratuite du programme Driver Booster d'IObit (bit.ly/41fWMwq), spécialisé dans la recherche et la récupération des mises à jour de pilotes. Pointez sur **Analyser** et cochez l'option **Obsolètes** en haut à gauche. Cliquez sur **Mettre à jour** pour télécharger et installer les versions récentes des pilotes.

3 EFFECTUEZ DES MISES À JOUR RÉGULIÈRES DE WINDOWS

Comme les applications, le système de Microsoft reçoit périodiquement des mises à jour visant à assurer la sécurité du PC. Ces correctifs sont gérés par le module Windows Update et installés automatiquement si vous avez conservé les réglages par défaut. Pour vérifier si des mises à jour sont en attente, ouvrez les paramètres (**Windows** + **I**) et pointez sur l'onglet **Windows Update**. Activez l'option **Recevez les dernières mises à jour dès qu'elles sont disponibles**. Rappelons que la fin du support technique de Windows 10, qui comprend des mises à jour de sécurité mensuelles, devrait intervenir le 14 octobre 2025. Si vous êtes passé à Windows 11, vous disposez de plus de temps, la date annoncée étant le 10 novembre 2026 pour la version 23H2.

4 FORCEZ L'ACTIVATION DE MICROSOFT DEFENDER

L'antivirus maison de Microsoft n'a pas à rougir des versions gratuites des suites de sécurité. Il se classe en milieu de peloton du classement du site AV-Test, devançant de nombreux outils payants en matière d'efficience. Windows Defender peut cohabiter avec un logiciel tiers comme Avast ou Bitdefender. Dans ce cas de figure, son mode de surveillance en temps réel se voit suspendu, laissant l'outil tiers assurer cette part du travail. Il reste toutefois possible de forcer une analyse depuis le menu contextuel de l'Explorateur de fichiers ou la page **Confidentialité et sécurité**, **Sécurité Windows**, **Protection contre les virus et menaces**, **Options de l'antivirus Microsoft Defender** des paramètres (**Windows** + **I**).

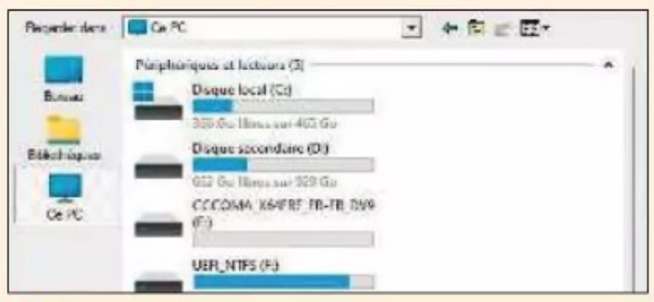
PAS À PAS EXPRESS

ANTICIPEZ LE PIRE AVEC AOMEI BACKUPPER

Aucun outil ne peut garantir une protection à 100 % contre les malwares et les rançongiciels. Assurez-vous de pouvoir **retrouver l'usage de vos fichiers en effectuant des sauvegardes régulières.**

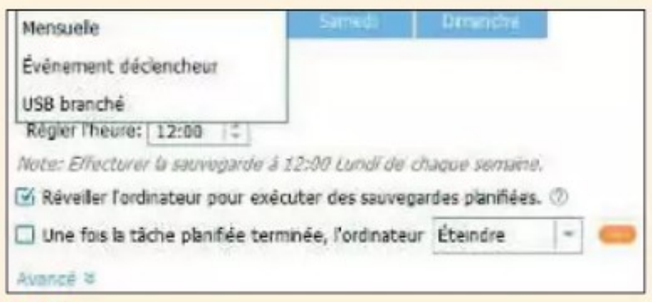
01. Installez le logiciel

AOMEI Backupper (bit.ly/3RjjUpn) effectue des sauvegardes périodiques de vos fichiers vers un périphérique de stockage ou un service cloud. Installez la version Backupper Standard, puis pointez sur **Sauvegarder** et **Sauvegarde de fichiers**.



02. Désignez un support

Cliquez sur **Ajouter un dossier**. Le plus simple consiste à sélectionner une ou plusieurs des bibliothèques personnelles de Windows. Pointez sur **Destination**, **Sélectionner un chemin local**, **Ce PC** et sélectionnez un support de stockage.



03. Planifiez la sauvegarde

Avant de lancer la sauvegarde avec le bouton **Démarrer**, rendez-vous dans le menu **Planifier**, **Activer la sauvegarde planifiée**. Réglez la fréquence et l'heure de démarrage de l'opération, cochez l'option de réveil de l'ordinateur en mode veille.

DIFFICULTÉ MODÉRÉE
TEMPS 20 MIN
DOMAINE INTERNET

IDENTIFIEZ-VOUS AVEC VOTRE SMARTPHONE

L'authentification à facteurs multiples est la seule mesure efficace pour garantir l'identité d'un utilisateur sur internet. Voici comment procéder avec Google Authenticator.

1 INSTALLEZ L'APPLI SUR VOTRE MOBILE

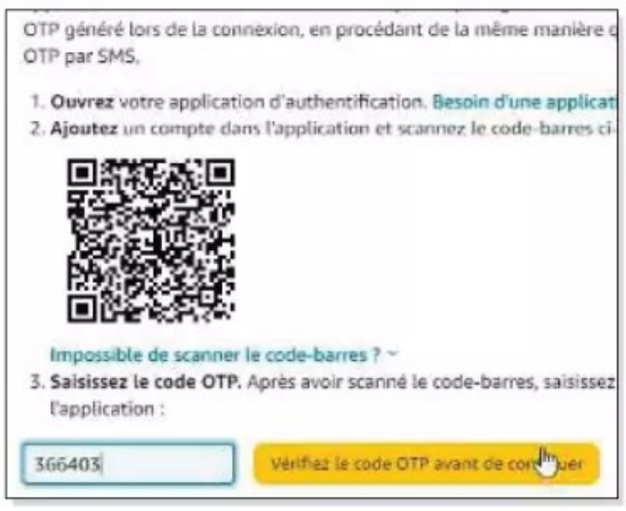
L'outil d'authentification à deux facteurs de Google constitue une alternative au service Authy et à l'Authenticator de Microsoft. Rendez-vous sur le Play Store Android (bit.ly/43CPbI9) pour l'**Installer** sur votre téléphone. Lancez l'application et touchez **Commencer**. Sélectionnez votre compte Google principal, puis actionnez **Ajouter un code**.

2 ACTIVEZ L'AUTHENTIFICATION À DEUX FACTEURS SUR VOTRE PC

Connectez-vous au service en ligne à sécuriser et affichez les paramètres du compte. Recherchez la rubrique liée à la sécurité. Dans le cas d'Amazon, cliquez sur **Connexion et sécurité** et **Modifier** à côté de **Paramètres de la vérification en deux étapes (2SV)**. Cochez l'option **Application d'authentification**. Un QR Code apparaît alors sur l'écran du PC. Revenez sur votre mobile.

3 IMPORTEZ LES COMPTES DANS GOOGLE AUTHENTICATOR

Placez-vous sur la page **Configurer votre premier compte** et touchez **Scanner un QR Code**. Autorisez l'appli à accéder à la caméra et cadrez l'image du QR Code. Un code de sécurité à six chiffres s'affiche alors dans Google Authenticator *(capture)*. Recopiez-le dans le champ **Saisissez le code OTP** du formulaire du service à sécuriser (Amazon dans notre cas). Tapez sur **Vérifier le code OTP**.



4 VALIDEZ L'ASSOCIATION

Pour finaliser l'association entre l'appli et le service en ligne, cochez l'option **Il n'est pas nécessaire d'utiliser de code OTP sur cet ordinateur** et validez d'un clic sur le bouton **J'ai compris. Activer les vérifications en deux étapes**. Répétez l'opération pour chaque service souhaité et qui propose cette option dans ses paramètres de sécurité. En cas de difficulté, reportez-vous à l'aide en ligne du service concerné.

5 SYNCHRONISEZ LES CODES 2FA ENTRE DEUX APPAREILS

Vous avez plusieurs téléphones ? Après avoir installé la version la plus récente de Google Authenticator sur tous les appareils, entamez la procédure de transfert des codes 2FA. Ouvrez Google Authenticator sur votre mobile principal. Sur la page d'accueil, touchez **Menu** dans l'angle supérieur gauche, puis les commandes **Transférer des comptes, Exporter des comptes, Continuer**.

6 SÉLECTIONNEZ ET TRANSFÉREZ DES CODES

Désignez le compte que vous entendez sécuriser avec le nouvel appareil. L'application génère un QR Code destiné à valider le transfert du code 2FA. Ouvrez Authenticator sur le mobile cible, effleurez la commande **Importer des comptes** et scannez le QR Code. Les informations sont automatiquement copiées d'un téléphone à l'autre. Une notification atteste de la réussite de l'opération.

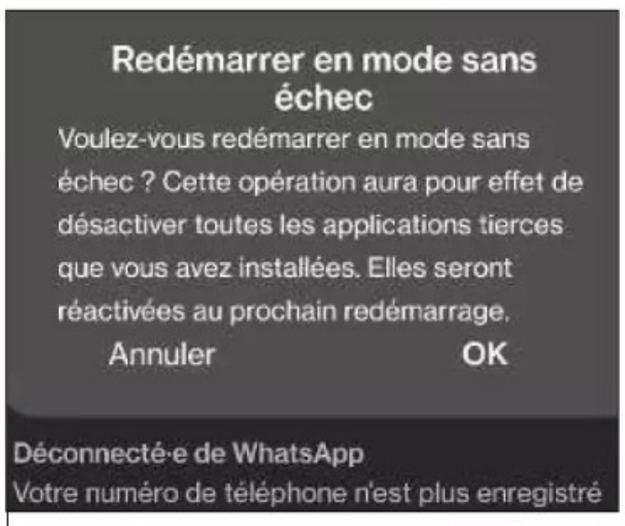
ÉLIMINEZ LES LOGICIELS ESPIONS

Sites, boutiques en ligne et pirates, tout le monde en veut à vos données. Bloquer les spywares devient dès lors crucial pour protéger votre vie privée.

DIFFICULTÉ MODÉRÉE
TEMPS 10 MIN
DOMAINE ANTIVIRUS

1 EFFECTUEZ UNE ANALYSE DU MOBILE

La batterie se décharge plus rapidement que d'habitude ? Votre téléphone ralentit inexplicablement ? Il est temps d'engager une traque des logiciels espions. Commencez par redémarrer l'appareil en mode sans échec : pressez le bouton d'alimentation jusqu'à ce que les options d'extinction apparaissent. Effectuez un appui long sur le bouton **Redémarrer** pour forcer le mode sans échec. Attendez qu'Android se lance. Accédez aux paramètres du mobile et rejoignez la page **Applications**. Parcourez la liste des applications en recherchant celles qui vous semblent inconnues. Même si elles sont légitimes, le fait que vous n'en ayez pas souvenir laisse à penser qu'elles ne vous sont pas d'une grande utilité. Effleurez l'un de ces éléments, puis actionnez la commande **Désinstaller** pour la supprimer. Redémarrez le téléphone de façon à quitter le mode sans échec. Pour compléter la recherche, retournez dans les paramètres et visitez la rubrique **Sécurité et confidentialité**. Dans **Autres paramètres de sécurité**, pointez sur **Sécurité du système**, **Autre**, **Apps gestionnaires d'appareils** et désactivez les privilèges d'administrateur des applis auxquelles vous ne faites pas confiance.



Lancez régulièrement une recherche de logiciels espions.

2 RECOUREZ À UN EXPERT VIRTUEL...

Ces vérifications manuelles peuvent être complétées par l'intervention d'un utilitaire spécialisé dans la sécurité des mobiles. Ouvrez le Play Store et installez Avast Antivirus et Sécurité (bit.ly/4401GBf). Appuyez sur le bouton **Ouvrir**, puis sur **Scan** de façon à procéder à une analyse complète du contenu de l'appareil. Attendez la fin de l'opération et prenez connaissance du diagnostic. L'application dresse un état des lieux des menaces détectées, parmi lesquelles les logiciels espions. S'il identifie un spyware, Avast Antivirus et Sécurité vous propose de l'éliminer. Appuyez sur le bouton **Supprimer** pour confirmer.

PRÉVENEZ LE VOL DE VOS APPAREILS ANDROID

Votre smartphone connaît tout de vous. Alors quand vous l'égarez ou qu'on vous le subtilise, tout s'effondre ! Mettez tout en œuvre pour le retrouver.

DIFFICULTÉ MODÉRÉE
TEMPS 15 MIN
DOMAINE GPS

1 ANTICIPEZ LA PERTE OU LE VOL DE VOTRE SMARTPHONE

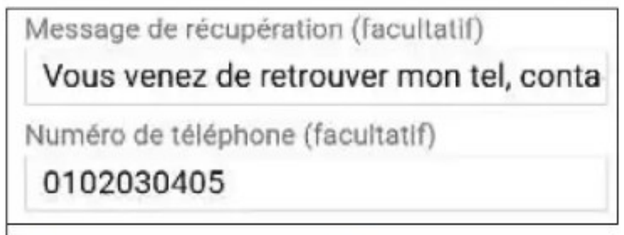
L'application Localiser mon appareil de Google évolue régulièrement pour gagner en précision et en simplicité d'utilisation. Son installation et son paramétrage constituent le préalable indispensable pour retrouver votre smartphone en cas de vol ou de perte de l'équipement. Téléchargez-la depuis le Google Play Store (bit.ly/2Wu5ryd). Pour mettre en place la localisation de votre mobile, lancez l'appli et touchez **Continuer en tant que** (suivi de votre compte Google).

2 SÉLECTIONNEZ LE TERMINAL

Si vous possédez plusieurs terminaux Android rattachés au même compte Google, ils pourront tous apparaître sur cette même interface. Si vous n'en détenez qu'un, il est reconnu instantanément. Touchez **Cet appareil**. Les informations sur votre smartphone s'affichent. Par défaut, il est identifié par sa référence produit. Effleurez l'icône symbolisant un crayon à papier pour lui attribuer un autre nom. Saisissez le nouveau nom et pressez **Renommer**.

3 PERSONNALISEZ L'APPLICATION

Touchez votre avatar en haut à droite de l'appli et, dans le volet, activez la commande **Paramètres** de l'application Localiser mon appareil. Assurez-vous que la localisation est bien activée (répétez cette vérification sur tous vos équipements), puis effectuez un test en sélectionnant la commande **Site Web Localiser mon appareil**. Votre navigateur vous amène instantanément sur le service.



Ajoutez un message à l'attention de celui qui retrouvera votre appareil.

4 TESTEZ LES FONCTIONNALITÉS

Lorsque vous êtes connecté au site Localiser mon appareil, vous visualisez la position de vos équipements sur une carte. Vous pouvez interagir avec chacun d'eux en les faisant sonner ou en les verrouillant (ou en les effaçant) à distance afin de mettre vos données privées à l'abri. Touchez **Sécuriser l'appareil** et envoyez un message ou un numéro, qui s'affichera sur l'écran du smartphone égaré, pour que la personne qui le trouve vous contacte aisément.

GÉNÉREZ DES CLÉS D'ACCÈS

Tout aussi sûres que la double authentification, **les « *passkeys* » remplacent les mots de passe** pour se connecter aux sites et services web.

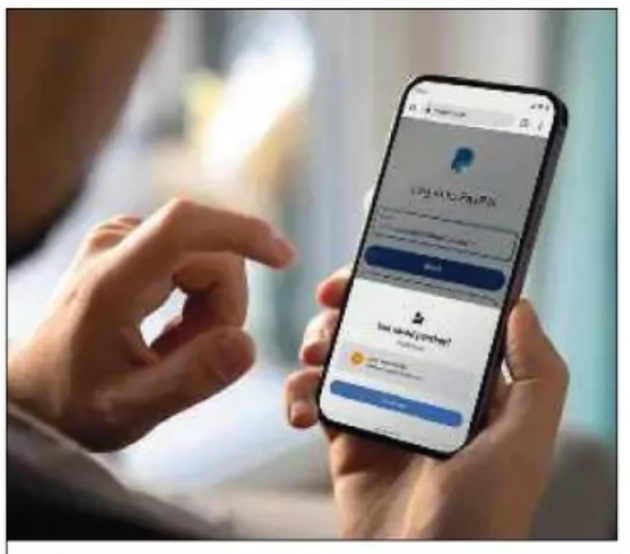
DIFFICULTÉ **MODÉRÉE**
TEMPS **10 MIN**
DOMAINE **ANDROID**

1 DÉCOUVREZ CETTE TECHNOLOGIE

Désormais implantées dans Android 14, les clés d'accès, ou *passkeys* en anglais, ont vocation à remplacer les mots de passe traditionnels pour sécuriser l'accès aux sites internet et aux applis. Elles s'appuient sur les normes Fido (Fast Identity Online), un ensemble de protocoles d'authentification ouverts et standardisés fondés sur le chiffrement à clé publique pour authentifier l'utilisateur. Ces clés d'accès apportent un niveau de sécurité bien plus élevé puisqu'elles sont stockées localement sur le mobile et non plus sur un serveur cloud. Les passkeys sont associées à votre profil biométrique (empreinte digitale, visage) ou au code de déverrouillage du téléphone, rendant l'usage des mots de passe inutile. Sachez enfin que ces clés sont dupliquées sur tous les appareils Android associés à votre compte Google.

2 METTEZ-LA EN PRATIQUE

Pour vous en servir, vous devez d'abord les activer depuis votre compte Google. Ouvrez les paramètres du mobile, rendez-vous dans **Comptes** et sélectionnez votre adresse Google. Rejoignez ensuite la section **Sécurité** et activez l'option **Utiliser les clés d'accès** sous **Comment vous connecter à Google**. Vous pouvez désormais recourir à ces clés d'accès pour vous connecter sur des sites web et aux applis compatibles. Quand vous utilisez un service en ligne ou une appli pour la première fois, vous êtes invité à appuyer sur le bouton **Créer une passkey**. Nommez le fichier et validez avec **Créer**. Deux clés sont alors générées, l'une privée, conservée en local, l'autre publique, transmise au service à l'origine de la demande.



Grâce aux passkeys, plus besoin de mémoriser de mots de passe.

ENREGISTREZ VOS MOTS DE PASSE DANS CHROME

À moins de vouloir absolument travailler votre mémoire, **le gestionnaire mis en place par le navigateur de Google** pour Android constitue votre meilleur allié.

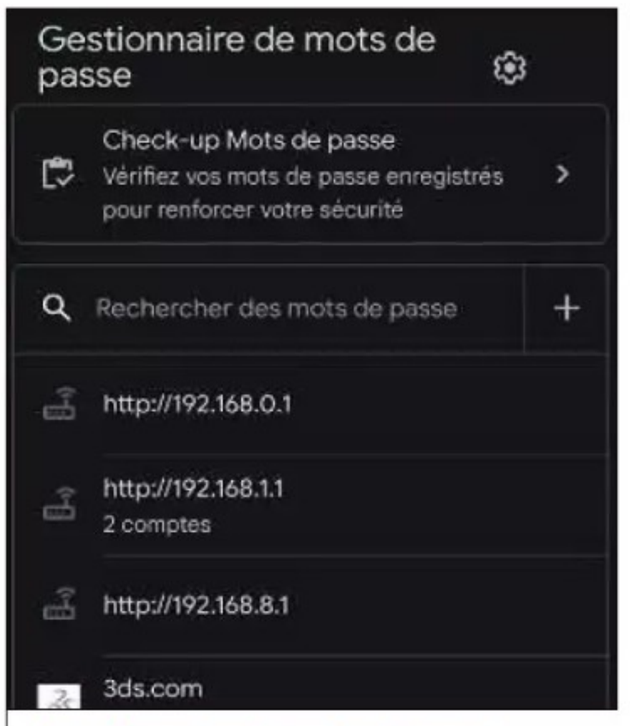
DIFFICULTÉ **MODÉRÉE**
TEMPS **10 MIN**
DOMAINE **ANDROID**

1 ENREGISTREZ AUTOMATIQUEMENT LES IDENTIFIANTS DE CONNEXION

La première étape pour gérer les mots de passe dans Chrome pour Android consiste à activer la fonction d'enregistrement automatique de ceux-ci par le navigateur. Pour ce faire, ouvrez l'appli mobile. Appuyez sur les trois points verticaux en haut à droite de l'écran, puis touchez **Paramètres**. Sous **Mots de passe**, activez le curseur **Enregistrer les mots de passe**. Dès lors, Chrome vous proposera systématiquement de mémoriser les identifiants de connexion des sites et services web auxquels vous vous inscrivez. Si vous utilisez Chrome sur d'autres appareils, prenez soin de l'associer chaque fois au même compte Google afin de synchroniser les codes d'accès définis sur ces différents outils et d'en disposer sur l'ensemble d'entre eux. L'appli comporte d'autres options intéressantes dont la suggestion de mots de passe forts, générés aléatoirement et proposés lors de l'inscription à un nouveau service en ligne.

2 VÉRIFIEZ SI L'UN D'ENTRE EUX A ÉTÉ COMPROMIS

Les identifiants sont conservés dans le cloud et en local dans des dossiers chiffrés. Ces données restent bien sûr accessibles et modifiables. Déroulez le volet de menu du navigateur et touchez **Paramètres**, **Gestionnaire de mots de passe** et **Vérifier les mots de passe**. Chrome vous indique si l'un d'entre eux a été compromis. Si c'est le cas, vous pouvez le modifier ou le supprimer. Il est aussi possible d'afficher en clair les mots de passe. Il vous suffit d'aller sur la page **Vérifier les mots de passe**, de choisir l'identifiant concerné et d'appuyer sur l'icône en forme d'œil à droite de **Mot de passe**. Il vous faut alors vous authentifier avec le code de verrouillage du téléphone pour le dévoiler.



Le gestionnaire de mots de passe de Chrome est le plus sûr remède contre les trous de mémoire.

ET TRUCS ASTUCES

ELENA SHARIPOVA/ISTOCKPHOTO

POUR Windows

SYSTÈME

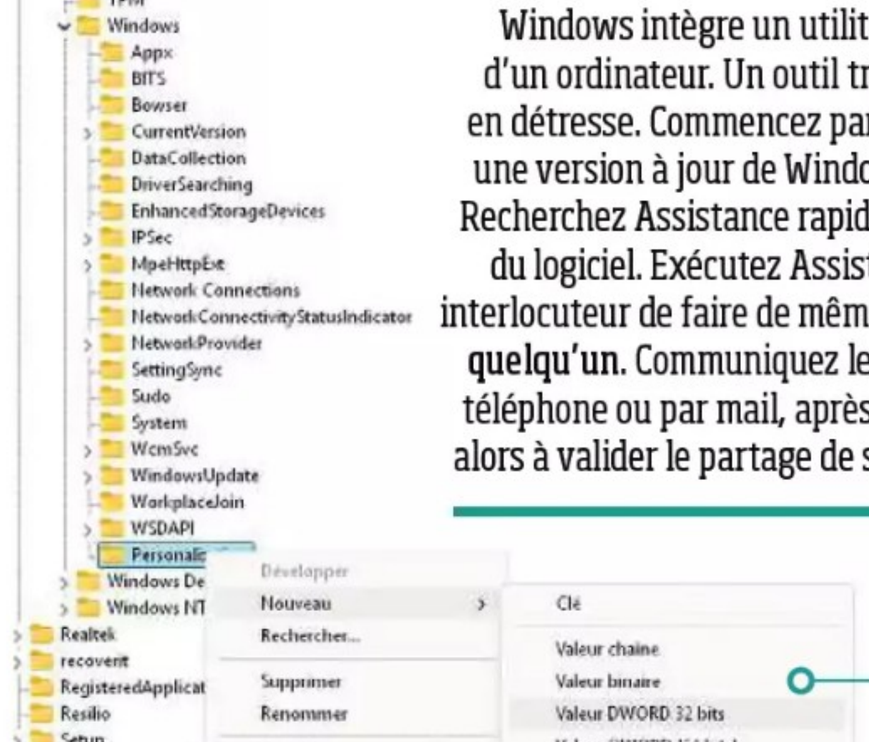
Préparez une clé d'installation à partir d'un Mac

Si une panne sérieuse rend votre PC inopérant, empêchant toute réinitialisation, et que vous n'avez qu'un Mac sous la main, voici comment créer un support d'installation amovible depuis ce dernier. Rapatriez d'abord l'image ISO de Windows 11 depuis le site de Microsoft (bit.ly/4dUH9zN). Rendez-vous ensuite sur GitHub, à la page bit.ly/3WYIlLz et pointez sur le lien **WinDiskWriter.1.3.zip** dans la section **Assets**. Affichez le dossier des téléchargements et cliquez sur **WinDiskWriter**. Dans la fenêtre de l'application, déroulez le menu **Target Device** et sélectionnez votre clé USB. Pointez sur le bouton **Choose** de la rubrique Windows Image pour indiquer l'emplacement du fichier d'installation ISO de Windows 11. Optez pour le format exFAT et lancez la copie avec **Start**.

DÉMARRAGE

COURT-CIRCUITEZ L'ÉCRAN DE VERROUILLAGE

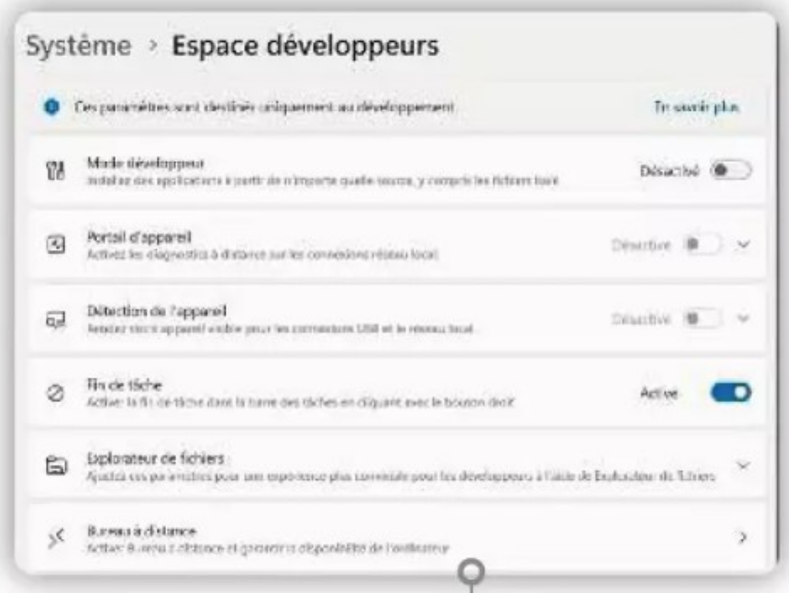
Cette manipulation ne doit être réalisée que si vous évoluez dans un environnement sécurisé où nul n'est susceptible de se pencher à votre insu sur les données de votre PC. Il s'agit en effet d'éviter l'affichage de l'écran invitant à saisir un mot de passe ou à s'identifier au moyen d'un capteur d'empreintes au démarrage de Windows ou à la sortie du mode veille. Appuyez sur les touches **Windows+R**, tapez **regedit** et validez avec **Entrée**. Déployez la branche **HKEY_LOCAL_MACHINE**, **SOFTWARE**, **Policies**, **Microsoft**, **Windows**. Faites un clic droit sur le dossier **Windows**, choisissez **Nouveau**, **Clé**. Nommez cet élément **Personalization**. Effectuez un clic droit sur cette entrée et pointez sur **Nouveau**, **Valeur DWORD (32-bit)**. Nommez cet item **NoLockScreen**, attribuez-lui la valeur **1** et enregistrez les modifications avec **OK**. Redémarrez le PC pour appliquer les réglages.



MAINTENANCE

DÉPANNEZ LE PC D'UN PROCHE... À DISTANCE

Windows intègre un utilitaire autorisant la prise de contrôle à distance d'un ordinateur. Un outil très pratique pour venir en aide à un utilisateur en détresse. Commencez par vous assurer que les deux appareils exécutent une version à jour de Windows 10 ou 11, puis allez dans le Microsoft Store. Recherchez Assistance rapide et pointez sur **Obtenir**. Autorisez l'installation du logiciel. Exécutez Assistance rapide sur votre PC et demandez à votre interlocuteur de faire de même de son côté. Cliquez ensuite sur le bouton **Aider quelqu'un**. Communiquez le code de sécurité à la personne à dépanner, par téléphone ou par mail, après avoir actionné le lien **Copier le code**. Il lui reste alors à valider le partage de son écran et à vous donner le contrôle de son PC.



SYSTÈME

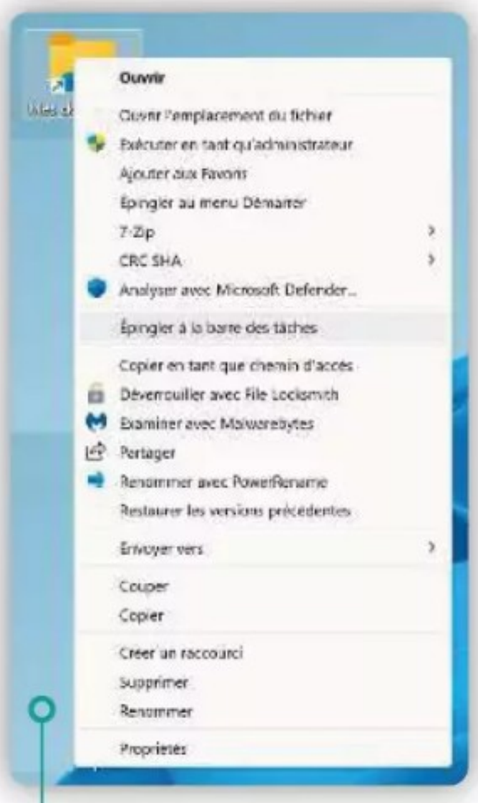
Fermez une application qui ne répond plus

Il ne suffit pas toujours de cliquer sur l'icône **X** de la barre de titre d'un programme ou sur l'option **Fermer la fenêtre** du menu contextuel pour reprendre le contrôle d'une application en souffrance. Le processus peut en effet continuer à s'exécuter en tâche de fond et empêcher le redémarrage du logiciel. La solution impose parfois le passage par le gestionnaire des tâches et l'activation de la commande **Fin de tâche**. Vous pouvez anticiper ce type de situation en ajoutant un raccourci vers cette commande dans le menu contextuel des applis. Appuyez sur les touches **Windows + I** du clavier et pointez sur l'onglet **Système**, **Espace développeurs** et sur le curseur **Fin de tâches**. Fermez les paramètres, puis effectuez un clic droit sur l'icône d'un programme en cours de fonctionnement dans la barre des tâches : une commande **Terminer la tâche** est désormais accessible.

BUREAU

ÉPINGLEZ UN DOSSIER À LA BARRE DES TÂCHES

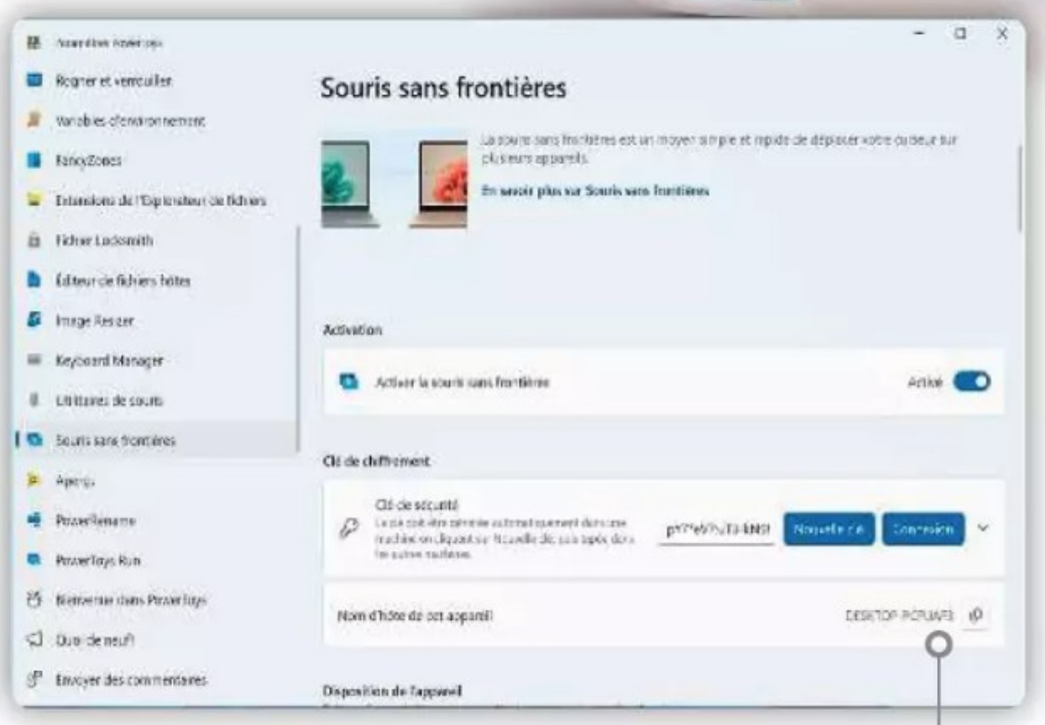
Vous avez sans doute l'habitude de placer des raccourcis vers vos dossiers personnels sur le Bureau. Mais savez-vous qu'il est possible d'épingler ces liens à la barre des tâches. Pour cela, effectuez un clic droit sur l'emplacement concerné et choisissez **Afficher d'autres options**. Pointez sur **Envoyer vers** et **Bureau (créer un raccourci)**. Revenez sur le Bureau, faites un clic droit sur l'icône du nouveau raccourci et sélectionnez **Propriétés**. Ajoutez **explorer.exe** suivi d'un espace devant le chemin du dossier dans le champ **Cible**. Validez avec **OK**. Renommez au besoin le raccourci, puis opérez un clic droit et pointez sur **Afficher d'autres options**, **Épingler à la barre des tâches**.



BUREAU

CRÉEZ UN RACCOURCI VERS UN PARAMÈTRE

Opérez un clic droit sur une zone vierge du Bureau et choisissez **Nouveau**, **Raccourci**. Dans le champ **Entrer l'emplacement de l'élément**, indiquez le lien vers la page convoitée - ***ms-settings:printers*** pour rejoindre la section **Imprimantes et scanners**, par exemple -, nommez le raccourci et validez. Sachez que la méthode fonctionne pour la plupart des options des paramètres de Windows : **ms-settings:windowsupdate** vous mène à la section relative aux mises à jour, **ms-settings:display** aux réglages de l'affichage... Vous trouverez la liste complète des commandes sur le site bit.ly/3vIAOOz.



POWERTOYS

Maniez une souris pour deux PC

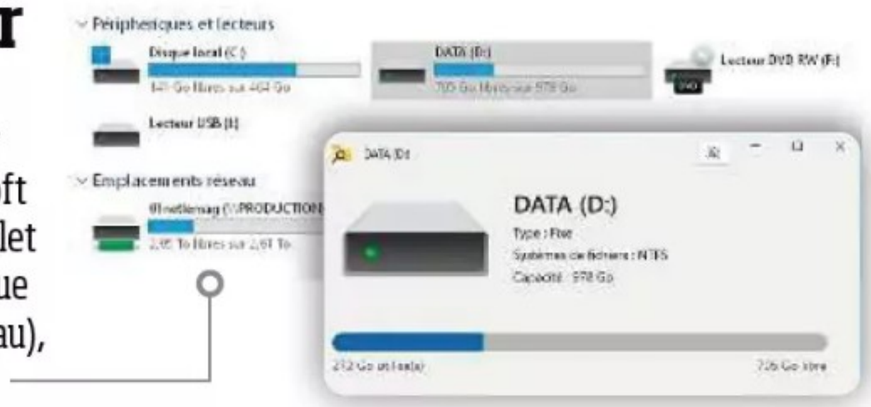
La collection d'utilitaires PowerToys propose un outil pratique si vous devez jongler entre un PC portable et un ordinateur de bureau. Plutôt que d'utiliser deux souris, Microsoft vous invite à partager le pointeur. Vérifiez que les PC sont connectés au même réseau Wifi et que les PowerToys y sont installés (l'application se télécharge depuis le Microsoft Store de Windows). Accédez à la fenêtre d'administration des PowerToys sur l'ordinateur où est branchée la souris. Pointez sur l'onglet **Souris sans frontières** et activez ce mode. Cliquez ensuite sur le bouton **Nouvelle clé** sous **Clé de sécurité**. Notez la clé qui s'affiche et le nom d'hôte de votre PC. Passez sur l'autre appareil, rejoignez la page **Souris sans frontières** pour activer le mode. Actionnez le bouton **Connexion**, entrez la clé de sécurité obtenue un peu plus tôt et le nom du PC principal. Validez avec **Connexion**.

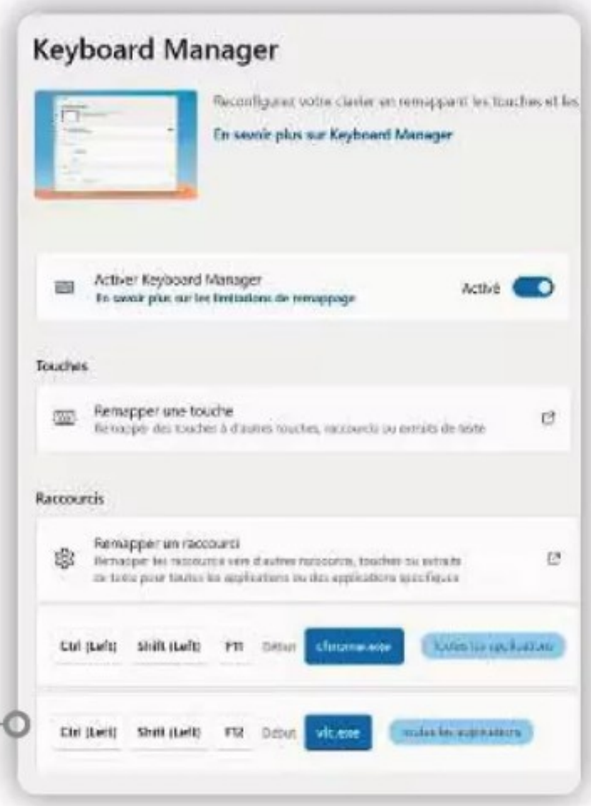
ELENA SHARIPOVA/ISTOCKPHOTO

POWERTOYS

Affichez un aperçu des propriétés d'un disque dur

Le volet de navigation de l'Explorateur de fichiers se contente d'afficher le nom et la lettre de volume des disques durs et des clés USB. Pour obtenir plus d'informations sans avoir à ouvrir les propriétés des différents volumes, installez la suite d'utilitaires PowerToys à partir du Microsoft Store. Double-cliquez sur l'icône de l'application dans la zone des notifications et pointez sur l'onglet **Aperçu**, puis **Activer Peek**. Dans l'Explorateur de fichiers, cliquez sur **Ce PC**, sélectionnez un disque et pressez les touches **Ctrl** + **Espace**. Une fenêtre précisant le type de support (fixe, amovible, réseau), le format de fichiers (NTFS, FAT32, exFAT), la capacité, l'espace utilisé et la place restante.





POWERTOYS

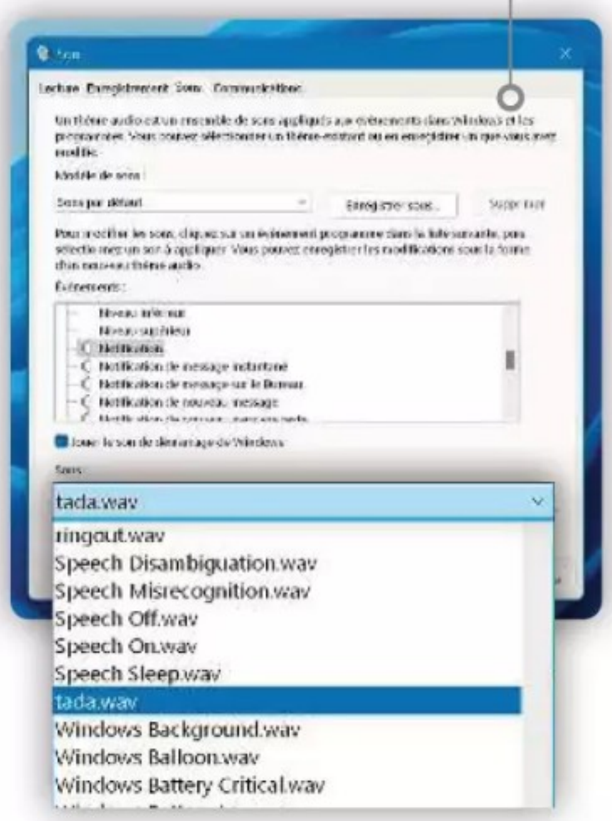
LANCEZ UNE APPLICATION VIA UN RACCOURCI CLAVIER

La collection d'utilitaires PowerToys de Microsoft autorise désormais la création de raccourcis personnalisés pour exécuter des applications ou accéder à vos pages web favorites. Installez les PowerToys depuis le Microsoft Store ou, si le programme est déjà présent sur votre PC, assurez-vous de disposer de la dernière mise à jour. Cliquez sur l'onglet **Keyboard Manager**, puis sur **Remapper un raccourci**. Pointez sur le bouton orné d'un crayon, appuyez sur les touches qui composeront le raccourci (**Ctrl+Maj+F12** dans l'exemple ci-dessus). Validez avec **OK**. Déroulez la liste **Action** et choisissez **Exécuter le programme**. Poursuivez en actionnant le bouton **Sélectionner un programme**. Recherchez le fichier exécutable du programme concerné (vlc.exe par exemple) et enregistrez le nouveau raccourci avec **OK**.

SYSTÈME

EXPLOITEZ À FOND L'OUTIL DE RECHERCHE

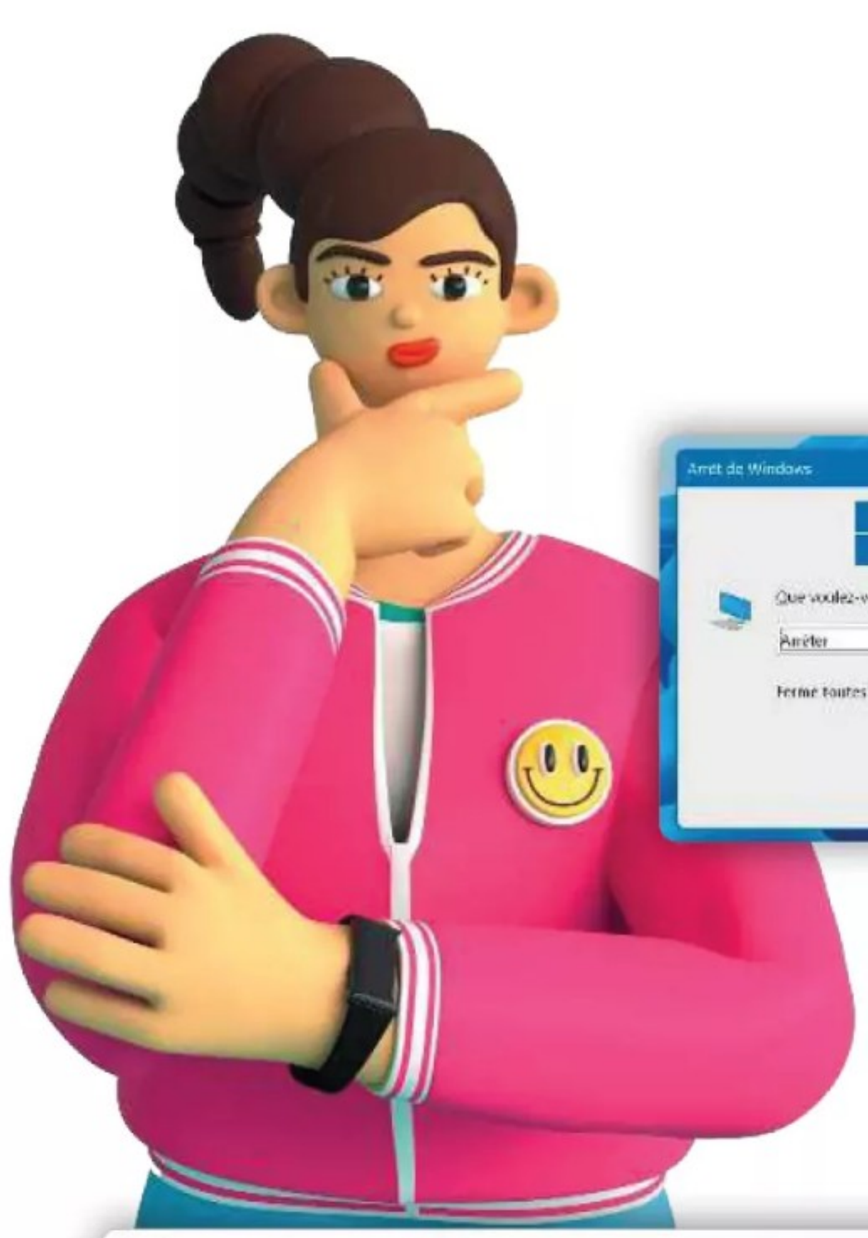
Votre PC bénéficie d'un moteur de recherche intégré capable de retrouver un document perdu aux fins fonds du disque dur. Pointez sur l'icône en forme de loupe de la barre des tâches ou cliquez dans le champ de saisie situé en haut du menu Démarrer. Saisissez votre requête, puis sélectionnez une catégorie pour restreindre le périmètre de la recherche aux documents, applications, photos… Pour ne pas limiter celle-ci aux contenus du Bureau et des bibliothèques personnelles, ouvrez les **Paramètres** et allez sur la page **Confidentialité et sécurité**, **Recherche dans Windows**. Activez le mode **Avancée** dans la section **Trouver mes fichiers**. Si vous souhaitez étendre le périmètre de la requête à votre espace OneDrive, cliquez sur les trois points en haut du volet de recherche. Choisissez **Activer la recherche sur le cloud…** et actionnez le curseur **Compte Microsoft** dans la rubrique **Recherche de contenu dans le cloud**.



SYSTÈME

Personnalisez les notifications

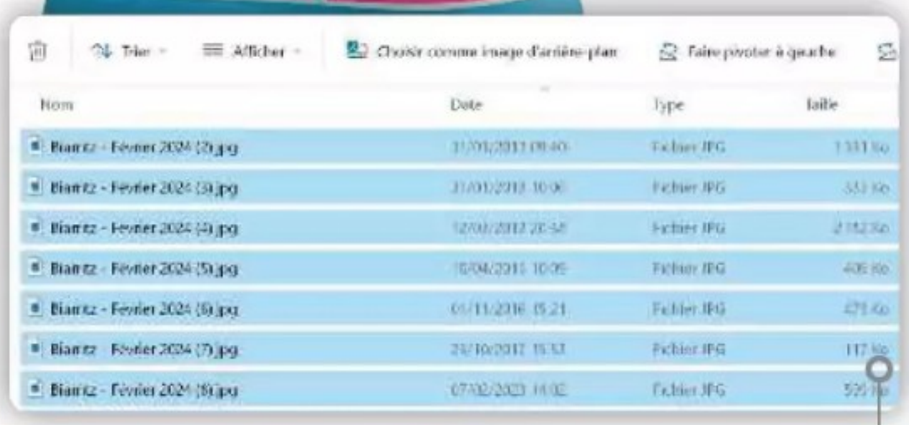
Chaque alerte émise par Windows s'accompagne d'un tintement qui peut finir par agacer à la longue ! Il est heureusement possible de modifier le son par défaut. Pour cela, saisissez **panneau** dans le champ de recherche de la barre des tâches et cliquez sur **Panneau de configuration**. Accédez à la rubrique **Matériel et audio** et pointez sur le lien **Modifier les sons système** dans la section **Sons**. Déroulez la liste **Sons** au bas de la fenêtre et sélectionnez par exemple le fichier **tada.wav**. Actionnez le bouton **Tester** pour obtenir un aperçu, puis **Appliquer** pour confirmer le nouveau réglage et **OK** pour revenir sur l'écran d'accueil du Panneau de configuration.



DÉPANNAGE

Éteignez votre PC même quand la souris est en panne

Votre pointeur sans fil ne répond plus et vous n'avez plus de piles en stock ? Pas de panique, cliquer sur le bouton **Éteindre** du menu Démarrer n'est pas la seule manière de procéder. Dans le cas où aucune application n'est ouverte sur le Bureau, appuyez sur les touches **Alt+F4**, puis **flèche bas** pour faire défiler les options de la liste **Que voulez-vous faire ?** Sélectionnez **Éteindre** et validez avec **Entrée**. Si des programmes bloquent l'opération, utilisez le raccourci **Ctrl+Alt+F4** , appuyez plusieurs fois sur la touche **Tab** de façon à placer l'icône **Démarrer** présente dans le coin droit de l'écran en surbrillance. Appuyez sur **Entrée**, choisissez **Éteindre** et validez (**Entrée**).

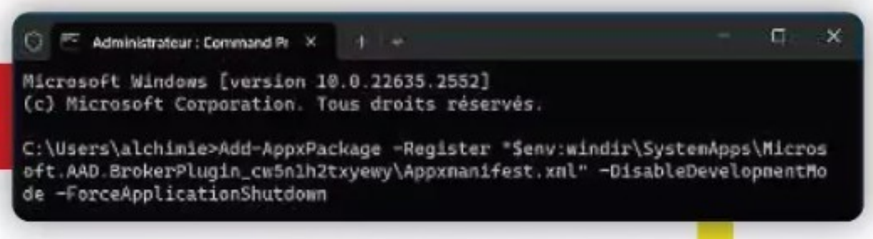


SYSTÈME

RENOMMEZ PLUSIEURS FICHIERS D'UN COUP

Les intitulés attribués par défaut lorsque vous réalisez des captures d'écran ou prenez des photos sur un téléphone ne sont guère explicites. Pour renommer rapidement une série de clichés, commencez par les regrouper dans un nouveau dossier via l'Explorateur de fichiers. Déroulez ensuite le menu **Afficher** et optez pour le mode **Détails**. Classez les images par ordre chronologique en pointant sur l'en-tête de colonne **Date**, puis appuyez sur **Ctrl+A** de façon à sélectionner tout le contenu du dossier. Appuyez sur la touche **F2**, saisissez l'intitulé de votre choix (*Biarritz - Février 2024*, dans notre cas) et validez avec **Entrée**. Windows ajoute automatiquement un suffixe de numérotation à la fin du nom des fichiers : Biarritz - Février 2024 (1), Biarritz - Février 2024 (2)...

BUREAUTIQUE

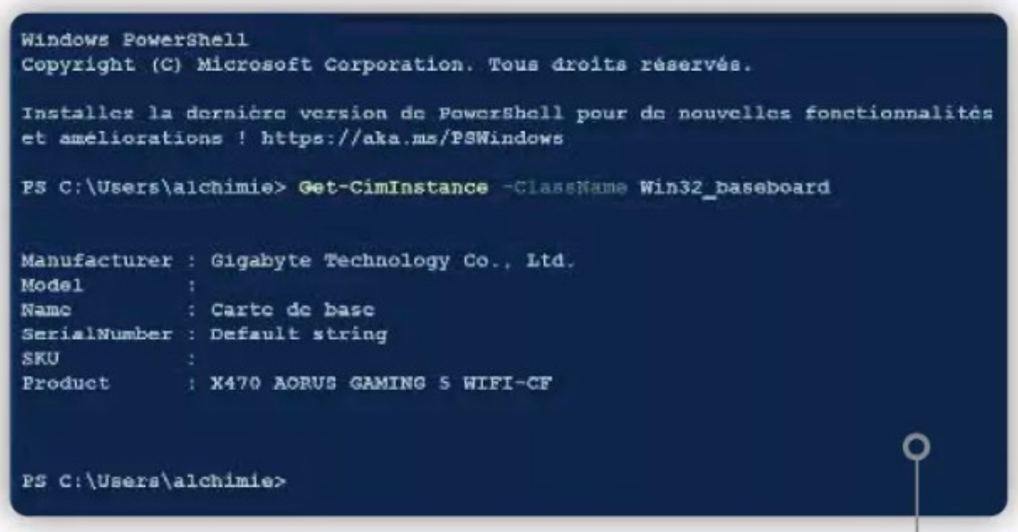


RÉTABLISSEZ LE LANCEMENT DE MICROSOFT 365

La suite bureautique connaît parfois des ratés. Un bug récent empêche d'accéder aux applications de Microsoft 365, les tentatives de lancement de Word, Excel ou PowerPoint se soldant par l'affichage du message d'erreur « *something went wrong* [1001] ». Pour résoudre ce problème, lié aux extensions Web Account Manager (WAM), ouvrez une session du Terminal de Windows 11 en mode Administrateur et exécutez les commandes suivantes :

Add-AppxPackage␣-Register␣"$env:windir\SystemApps\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\Appxmanifest.xml"␣-DisableDevelopmentMode␣-ForceApplicationShutdown

Add-AppxPackag -Register␣"$env:windir\SystemApps\Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewyAppxmanifest.xml"␣-Disable DevelopmentMode␣-ForceApplicationShutdown



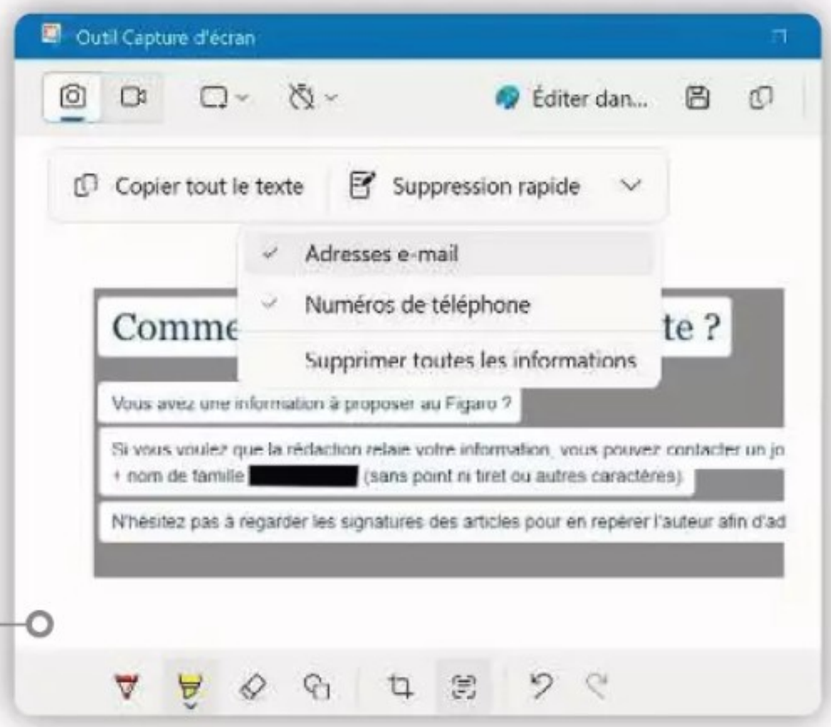
MATÉRIEL

Identifiez votre modèle de carte mère

La résolution de certains dysfonctionnements d'un PC passe par la mise à jour des pilotes ou du firmware de la carte mère. Une opération qui suppose de connaître la marque et la référence exacte de ce composant. Effectuez un clic droit sur le menu **Démarrer** de Windows et pointez sur le raccourci **PowerShell** du menu déroulant. Exécutez ensuite la commande **Get-CimInstance␣-ClassName␣Win32_baseboard** et notez les informations figurant dans les sections **Manufacturer** et **Product**. Si vous utilisez le Terminal et non PowerShell, lancez la commande **wmic␣baseboard␣get product,Manufacturer,version,serialnumber** pour afficher ces mêmes données.

ELENA SHARIPOVA/ISTOCKPHOTO

␣ Le symbole bleu représente une espace



CAPTURES D'ÉCRAN

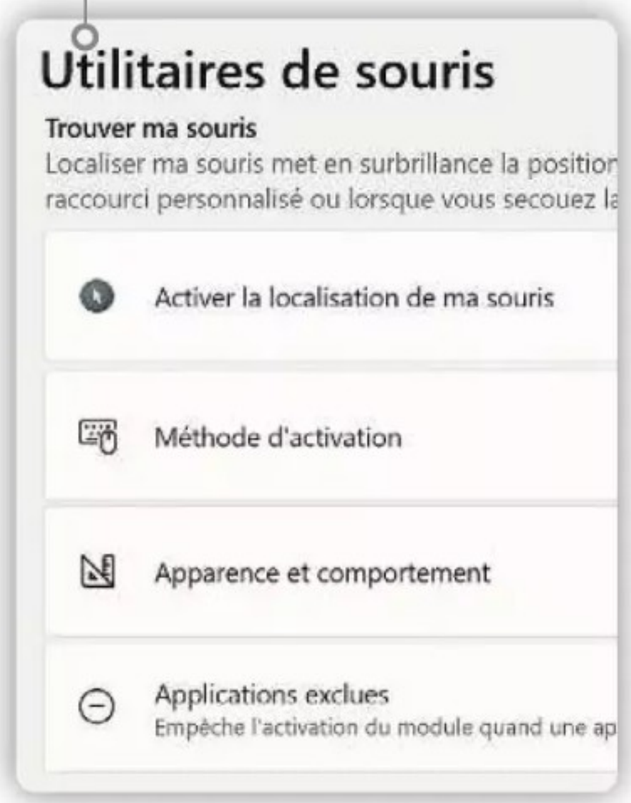
MASQUEZ ADRESSES MAIL ET NUMÉROS DE TÉLÉPHONE AUTOMATIQUEMENT

Il n'est pas forcément judicieux de partager les numéros de téléphone et les adresses mail qui apparaissent sur les captures d'écran destinées à illustrer un tutoriel ou à accompagner une réclamation auprès d'une boutique en ligne. L'application Outil Capture d'écran de Windows 11 se propose de masquer automatiquement ces informations. Une fois la capture réalisée, pointez sur l'icône **Actions de texte** au bas de la fenêtre d'édition, puis sur le bouton **Suppression rapide**. Des rectangles noirs viennent alors recouvrir les adresses mail et les numéros de téléphone.

POWERTOYS

Gardez votre pointeur en vue

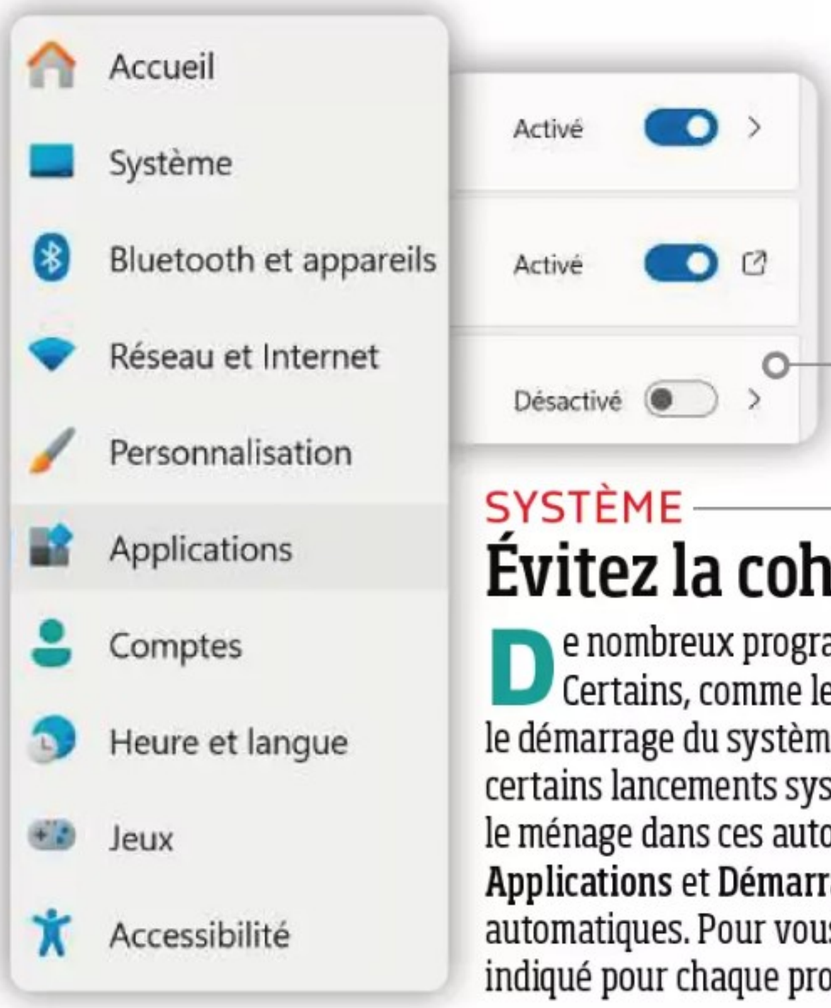
Les PowerToys intègrent des fonctions destinées à améliorer la souris. Affichez les paramètres de l'application et pointez sur l'onglet **Utilitaires de souris** pour activer les différents outils disponibles. La localisation de la souris déclenche une animation permettant d'identifier la position du curseur quand on secoue la souris ou que l'on appuie deux fois sur la touche **Ctrl**. Le mode surligneur met, lui, en surbrillance l'endroit où vous cliquez.



POWERTOYS

CONCENTREZ-VOUS SUR UNE ZONE D'UNE FENÊTRE

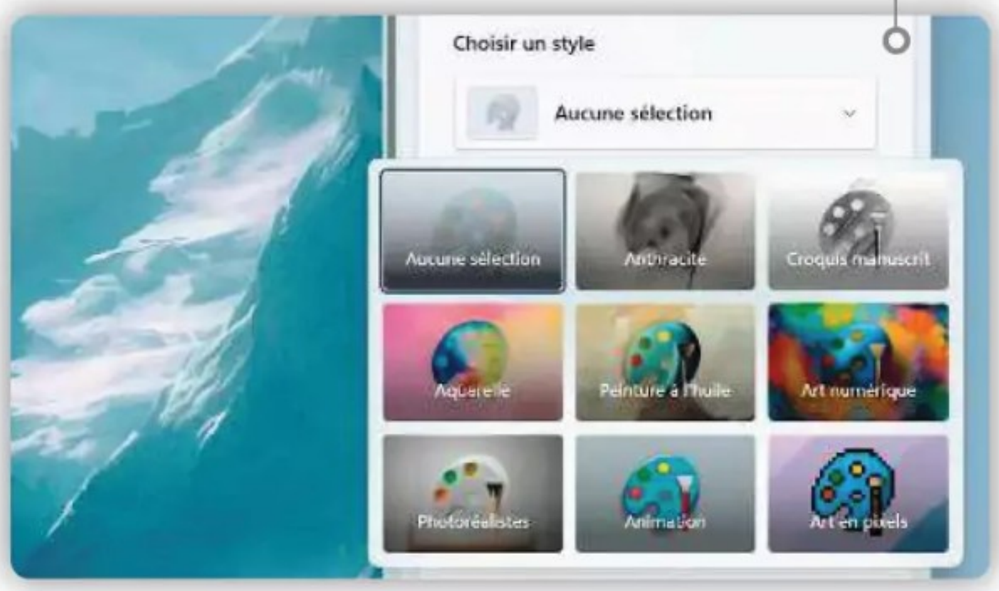
Vous n'avez pas forcément besoin de voir l'ensemble des informations contenues dans l'interface d'un programme. Les PowerToys proposent de n'afficher que la zone qui vous intéresse. Par exemple, la liste des messages reçus dans Outlook. Sur la page des paramètres des PowerToys, cliquez sur **Rogner et verrouiller** et activez le curseur. Retournez dans Outlook et appuyez sur les touches **Windows+Ctrl+Maj+T** du clavier. Délimitez la zone à conserver à l'aide de la souris. Ne fermez pas le programme concerné par l'opération. Contentez-vous de réduire la fenêtre principale de l'application dans la barre des tâches.



SYSTÈME

Évitez la cohue au démarrage

De nombreux programmes tiers gravitent autour de Windows, participant à la richesse de l'écosystème. Certains, comme les antivirus, des gestionnaires de matériels ou Microsoft Office, se lancent dès le démarrage du système d'exploitation. Si on comprend l'utilité pratique de précharger certaines applications, certains lancements systématiques sont beaucoup plus contestables et ralentissent le système. Pour faire le ménage dans ces autorisations, rendez-vous dans les **Paramètres** (touche **Windows** + **I**), puis dans **Applications** et **Démarrage**. Là, un système d'interrupteurs permet d'activer ou désactiver les lancements automatiques. Pour vous aider à faire un choix, l'impact sur l'utilisation des ressources système est indiqué pour chaque programme. Mais attention tout de même à ne pas désactiver tout et n'importe quoi.



MULTIMÉDIA

Générez des images avec l'IA dans Paint

L'intelligence artificielle envahit peu à peu Windows et ses applications. Paint s'est ainsi doté d'une nouvelle rubrique **Créateur d'image** alimentée par l'IA générative Dall-E. Rendez-vous dans cette section en pointant sur l'icône présente à droite de la barre de menu supérieur. Entrez votre demande dans le champ de saisie. Choisissez un style graphique en déroulant le menu éponyme et validez avec **Créer**. Paint propose trois variantes répondant à la requête. Sélectionnez l'une des vignettes pour afficher l'image en grand. Fermez l'aperçu, survolez la vignette avec le curseur et déroulez la liste des options en cliquant sur les points. Enregistrez le fichier.

AFFICHAGE

DESSINEZ UN BUREAU QUI N'APPARTIENT QU'À VOUS

Grâce aux options de personnalisation des couleurs de Windows, il est possible d'adapter à votre goût les bordures des fenêtres, le bouton Démarrer ou encore la barre des tâches. Ces commandes sont rassemblées dans le menu **Personnalisation**, **Couleurs** des **Paramètres**. Dans la rubrique **Choisir votre mode**, choisissez **Personnalisé**, puis le mode **clair** ou **sombre** pour Windows et les applications. Activez ensuite l'option **Effets de transparence**. Réglez la couleur d'accentuation sur **Manuel**, sélectionnez une couleur dans la palette ou définissez une teinte sur mesure en pointant sur **Afficher les couleurs**. Activez le mode **Afficher la couleur d'accentuation sur la barre de titre et les bordures de la fenêtre.**

SYSTÈME

ALLOUEZ PLUS DE PERFORMANCES AUX JEUX

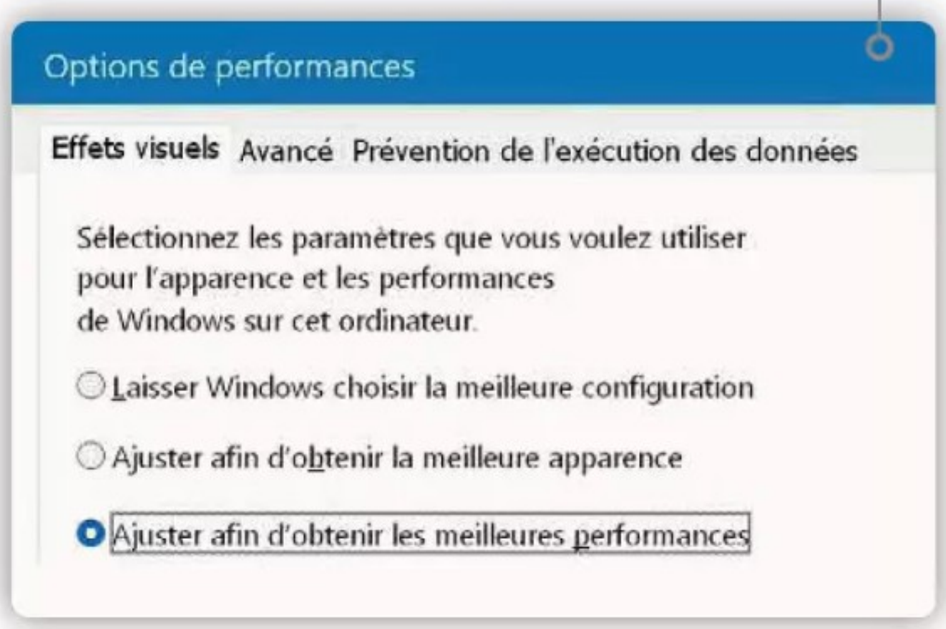
Les *gamers* sont certainement au fait de cette astuce qui maximise la puissance de l'ordinateur lors des sessions de jeu. Ce qui permet de leur allouer un maximum de ressources plutôt qu'aux autres programmes actifs. Appuyez sur les touches **Windows + I**, cliquez sur le menu **Jeux** et activez le **Mode jeu**. Dirigez-vous ensuite vers **Graphiques**. Déroulez la page vers le bas et pointez sur le nom du programme (sur le Bureau ou même dans le Microsoft Store) auquel vous jouez. Dirigez-vous vers les **Options** et cochez la case des **Performances élevées** au-dessus du nom de votre carte graphique. Validez avec **Enregistrer**. Au prochain démarrage, votre jeu devrait être plus fluide et rapide.

ACCESSIBILITÉ

Pilotez votre PC à la voix

Grâce au menu **Accessibilité**, **Voix** des paramètres du système (**Windows+I**), il est possible de dicter des commandes en français pour piloter certaines tâches sans toucher au clavier. Commencez par activer le curseur de l'accès vocal ainsi que les options associées. Cliquez sur **J'accepte**, puis configurez le microphone. La fonction **Voice access** s'active. Pointez sur l'icône en forme de micro, en haut à gauche de la fenêtre, et énoncez la commande vocale **Que puis-je dire ?** de façon à dévoiler la liste des autres commandes vocales, servant par exemple à ouvrir les applications, contrôler la souris et le clavier, sélectionner du texte ou encore interagir avec des éléments à l'écran.

ELENA SHARIPOVA/ISTOCKPHOTO



PERFORMANCES

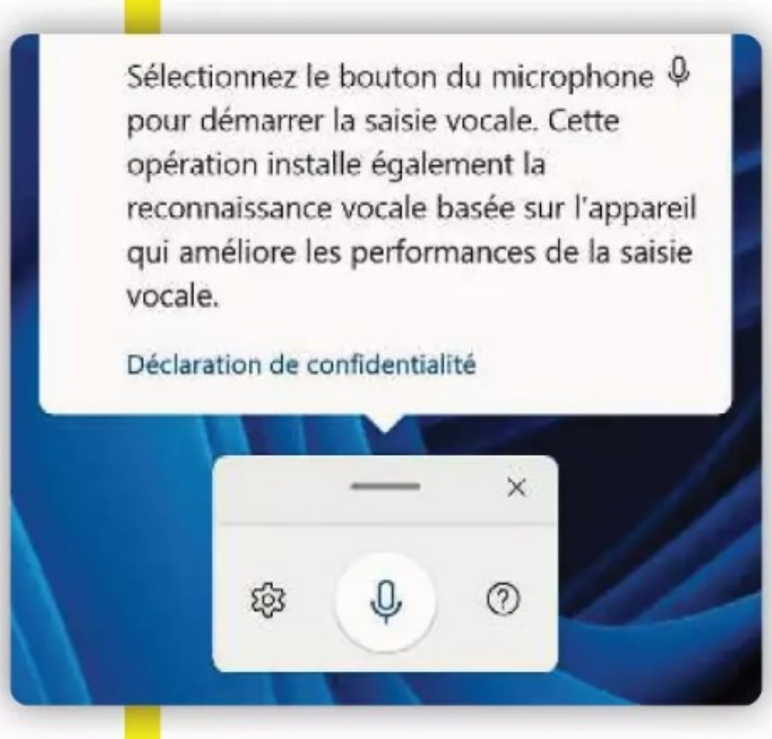
Accélérez Windows 11

Un ancien ingénieur de Microsoft faisait état de la lenteur de Windows 11, et ce, même sur des machines survitaminées. Si vous rencontrez ce type de désagréments, commencez par désactiver les effets visuels inutiles. Pour ce faire, appuyez sur les touches **Windows + R** du clavier et exécutez la commande **systempropertiesperformance**. Cochez l'option **Ajuster afin d'obtenir les meilleures performances**. Ouvrez ensuite le Gestionnaire des tâches (**Ctrl + MAJ + Échap**) et dirigez-vous vers **Applications de démarrage** à gauche de la fenêtre. Désactivez les applis qui n'ont pas besoin de se lancer à la mise en route du PC. Accédez enfin au Panneau de configuration, pointez sur **Système et sécurité**, **Options d'alimentation** et cochez **Performances élevées**.

BUREAUTIQUE

RECOUREZ À LA SAISIE VOCALE **PLUTÔT QU'AU CLAVIER**

Connectez un micro ou une webcam à votre PC. Ouvrez un fichier Word et appuyez sur les touches **Windows+H** du clavier pour afficher la fenêtre de l'application de dictée vocale. Pointez sur l'icône en forme d'engrenage et accédez aux paramètres du micro depuis **Sélectionner le microphone par défaut**. Le menu **Système**, **Son** autorise le choix du périphérique de captation et l'ajustement du volume sonore. Revenez à l'application, cliquez sur l'icône **Micro** et optez pour le mode **Écoute**. Lancez la saisie vocale. La ponctuation peut être ajoutée automatiquement en activant le curseur associé ou manuellement. Référez-vous à la liste des commandes en visitant le site bit.ly/3QtaF6e.



AFFICHAGE

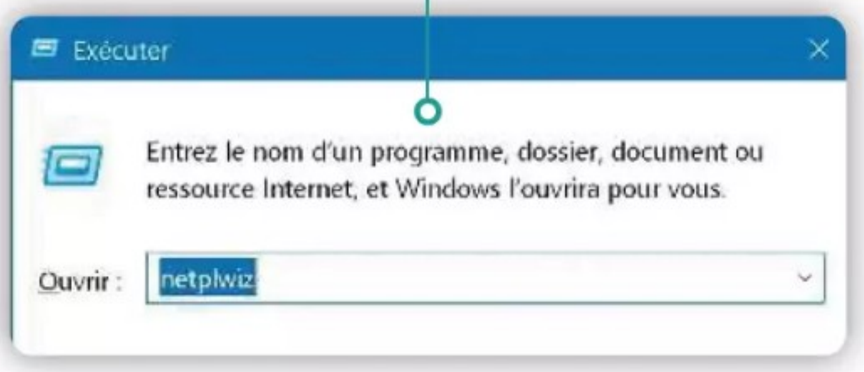
Personnalisez l'apparence du Terminal

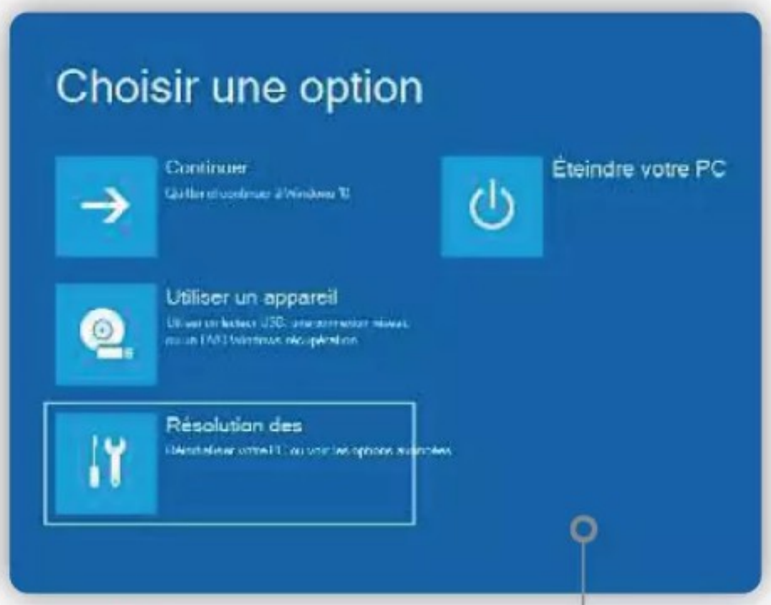
Les dernières mises à jour de Windows ont apporté une touche de modernité au Terminal, l'application servant à interagir avec le système au moyen de lignes de commande. Pour y accéder, actionnez le raccourci-clavier **Windows+X** et cliquez sur **Terminal (administrateur)**, **Oui**. Pointez sur la flèche située à droite du dernier onglet et choisissez **Paramètres**. Cette page propose de nombreuses options de personnalisation. Intéressez-vous par exemple à la section **Jeux de couleurs** en colonne de gauche et définissez la couleur d'arrière et d'avant-plan ainsi que celle du curseur. Vous disposez à cet effet de neuf modèles par défaut pouvant être adaptés à votre goût. Pensez à enregistrer les modifications.

SYSTÈME

COMMANDEZ WINDOWS VIA LA FENÊTRE EXÉCUTER

Pour donner des ordres au système, vous passez sans doute par les paramètres du PC (touches **Windows+I**) ou exécutez des commandes dans le Terminal. Il existe toutefois une troisième option : la fenêtre Exécuter. Elle s'affiche en actionnant le raccourci **Windows+R** et contient une zone de saisie. Lancez un programme en indiquant le nom du fichier exécutable (**word.exe** ou **chrome.exe**, par exemple) ou une commande système (**netplwiz** pour rejoindre les comptes utilisateurs ou **mrt** pour rechercher des virus). Vous trouverez la liste complète des commandes gérées sur le site bit.ly/3VlGMrZ. Vous pouvez aussi accéder aux dossiers système à l'aide de leur intitulé (**documents**, **downloads** ou **photos**).





SYSTÈME

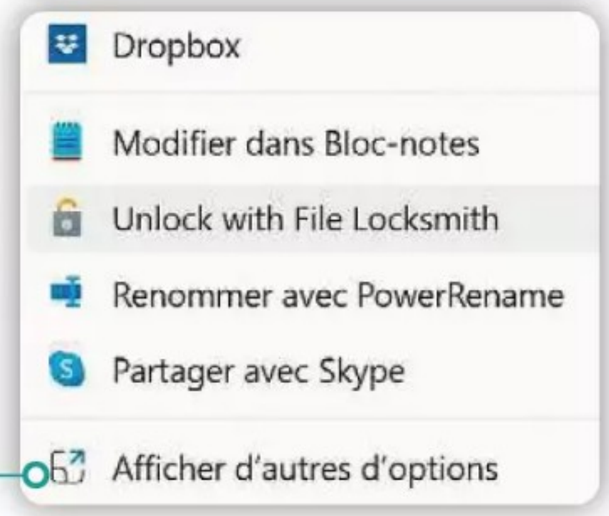
Réinstallez Windows sans gadgets inutiles

Même après sa réinstallation complète, Windows 11 comporte toujours des logiciels ou des utilitaires tiers pas forcément utiles. Il est heureusement simple de se débarrasser de Spotify, TikTok, Amazon Prime Vidéo ou d'une solution antivirus en version d'essai. Après avoir lancé l'assistant de réinstallation de Microsoft, il faut choisir **Anglais International** comme langue par défaut, puis poursuivre le processus d'installation comme d'habitude.
Si le message d'erreur « OOBREGION » apparaît, cliquez sur **Ignorer**.
À la fin de l'installation, les logiciels indésirables ont disparu. Ne reste plus qu'à restaurer le **Français (France)** en tant que langue par défaut, dans **Paramètres, Heure et langue, Langue et région, Format régional.**

POWERTOYS

REPRENEZ LE CONTRÔLE D'UN FICHIER OU D'UN DOSSIER VERROUILLÉ

Windows peut refuser de supprimer un fichier, de renommer ou déplacer un dossier quand celui-ci est utilisé par un programme ou un processus système. Le module Fichier Locksmith des PowerToys peut aider à dénouer la situation.
Une fois celui-ci activé, opérez un clic droit sur l'élément récalcitrant et pointez sur **Afficher d'autres options** et **Qu'est-ce qui utilise ce fichier ?** Parcourez la liste des processus ayant accès au document ou au dossier, sélectionnez celui qui semble être à l'origine du blocage et pointez sur **Terminer la tâche.**



SÉCURITÉ

OUVREZ L'ACCÈS À VOTRE PC À TOUTE LA FAMILLE

Les membres du groupe familial associé à un PC peuvent s'y connecter en utilisant leurs propres identifiants, dès lors que l'Administrateur a autorisé le partage. Leur avatar s'affiche en bas de l'écran de connexion. Il leur suffit de sélectionner leur compte et d'entrer leur mot de passe. Pour mettre en place le partage du PC, ouvrez les paramètres (**Windows+I**) et cliquez sur **Comptes.**
Déroulez le menu **Famille** pour découvrir les personnes dans le groupe. Choisissez un utilisateur pour voir ses privilèges, puis cliquez sur **Connexion impossible, Autoriser la connexion.** Vous pouvez lui accorder des privilèges d'administrateur avec **Changer le type de compte.**

POWERTOYS

Profitez d'autres outils et applications

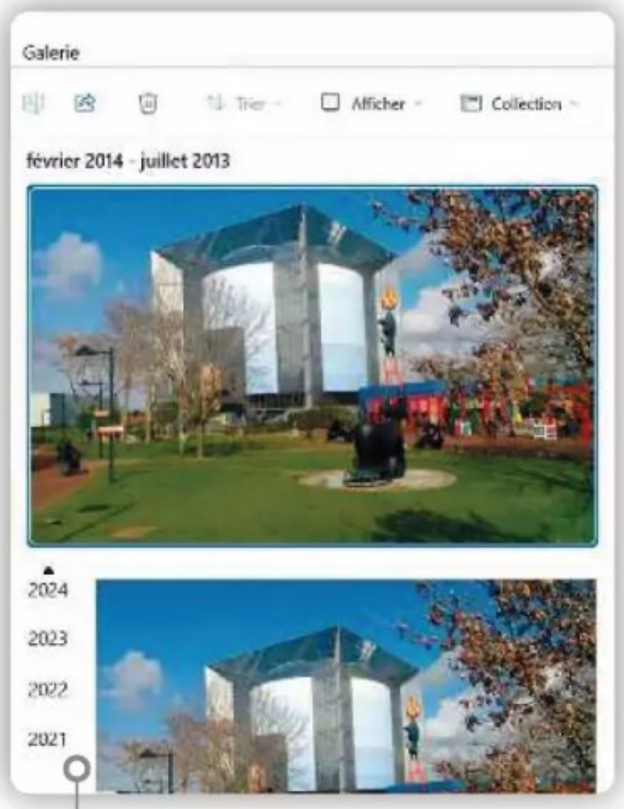
Vous trouvez qu'il manque des outils au système, comme une application capable de redimensionner vos photos, de renommer des fichiers par lots ou d'éviter que votre PC ne bascule en mode veille ? Ces fonctions, et quelques autres, existent et sont rassemblées au sein des PowerToys.
La liste des utilitaires figure en colonne gauche de la page d'accueil du programme. Pour recadrer une image, choisissez **Image Resizer** ; pour changer l'intitulé de fichiers, optez pour **PowerRename.**
Chacun de ces modules propose un résumé détaillé et des conseils de mise en œuvre.

ELENA SHARIPOVA/ISTOCKPHOTO

BUREAUTIQUE

Obtenez des polices supplémentaires

Si les polices de caractères présentes dans Word ne comblent pas vos envies créatives, amusez-vous à en installer de nouvelles depuis le site Dafont.com. Le téléchargement et l'usage des polices proposées ici sont gratuits dans le cadre d'une utilisation privée. Choisissez une fonte et pointez sur **Télécharger** à droite. Décompressez l'archive Zip, allez dans les paramètres du PC (**Windows + I**) et cliquez sur **Personnalisation, Polices, Parcourir et installer les polices.** Ouvrez le dossier que vous venez de rapatrier et sélectionnez les fichiers portant les extensions .otf et .ttf. Validez avec **Choisir des polices.** Ouvrez un document Word et cherchez les fontes dans la liste des polices de l'onglet **Accueil.**



BUREAUTIQUE

VISUALISEZ VOS IMAGES

Le gestionnaire de documents de Windows dispose d'options destinées au visionnage des photos. Ouvrez l'Explorateur de fichiers en appuyant sur les touches **Windows+E** du clavier et affichez le contenu de la bibliothèque **Images.** Les clichés apparaissent sous la forme d'une liste ou de petites icônes. Sélectionnez un élément, déployez le menu **Afficher** et choisissez **Très grandes icônes** et **Volet de visualisation.** Pointez sur l'une des vignettes de façon à en disposer dans le volet d'aperçu ancré sur la droite de la fenêtre. Utilisez les commandes de la barre d'outils pour opérer un pivotement de la photo vers la gauche ou la droite ou encore en faire l'image d'arrière-plan du Bureau.

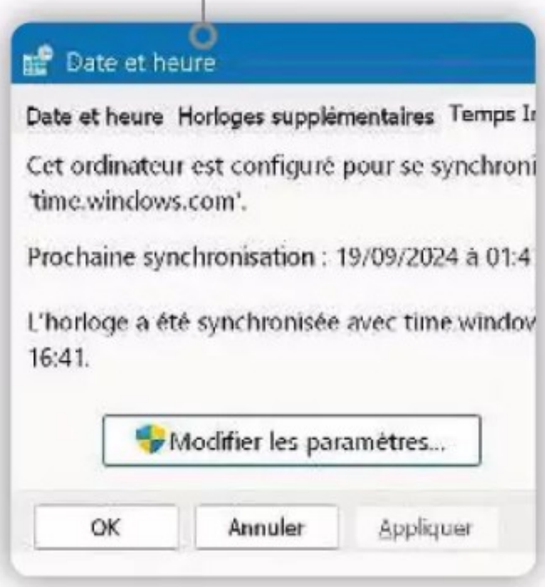
BATTERIE

RÉDUISEZ LA CONSOMMATION D'ÉNERGIE

Au fil des versions, les paramètres de Windows s'enrichissent de nouveaux menus et de commandes, à côté desquels on passe parfois! Si vous utilisez un PC portable à l'autonomie limitée (ou que vous souhaitez modérer la consommation électrique d'un PC de bureau), votre système d'exploitation prodigue conseils et astuces pour préserver l'autonomie et réduire la facture d'électricité. Appuyez sur les touches **Windows+I** du clavier et pointez sur **Système, Batterie et alimentation** et **Recommandations sur l'énergie.** Quatre opérations sont suggérées : optimiser l'efficacité énergétique, mettre en veille après x minutes, désactiver l'écran au bout de… ou désactiver l'écran de veille. Cliquez sur **Appliquer** et ajustez les réglages.

SYSTÈME

Venez à bout des problèmes d'heure

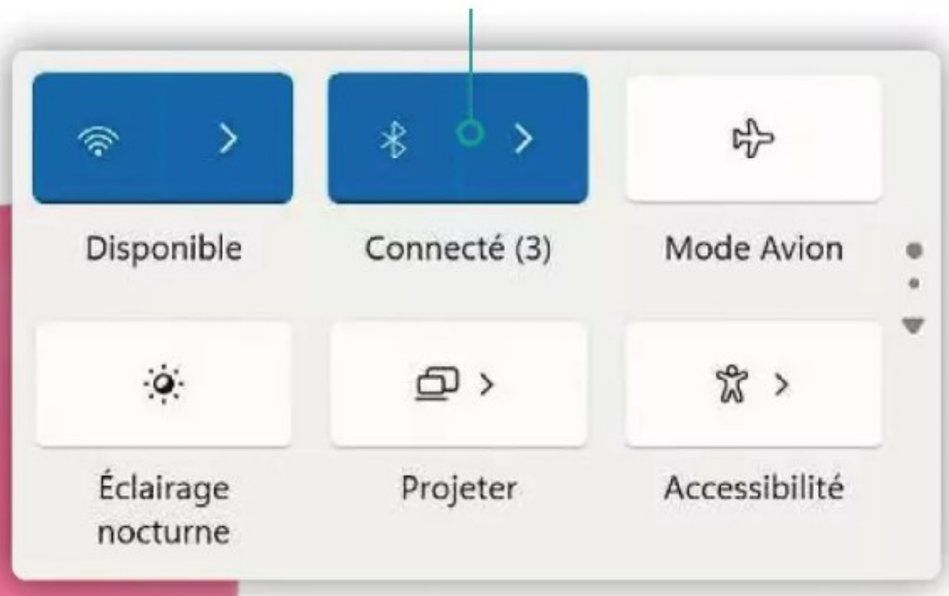


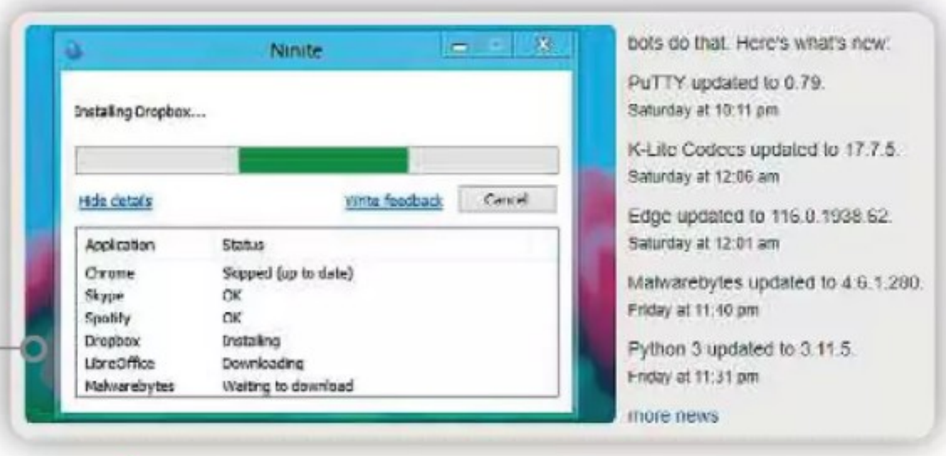
Il arrive que l'horloge Windows se trompe d'heure. Vous pouvez régler ce dysfonctionnement en ouvrant le menu **Heure et Langue, Date et heure,** puis en choisissant le bon fuseau horaire. Si le problème demeure, pointez sur **Langue et région,** déroulez le menu **Format régional** et désignez votre localisation. Une autre solution consiste à passer par la fenêtre **Date et heure** : appuyez sur les touches **Windows+R,** tapez **timedate.cpl** et validez avec **OK.** Dans l'onglet **Temps Internet,** cliquez sur **Modifier les paramètres.** Dans **Serveur,** sélectionnez **time.nist.gov,** à savoir des fuseaux horaires gérés par l'Institut national des normes et de la technologie des États-Unis. Enregistrez **les réglages avec Mettre à jour, OK.**

SYSTÈME

ADAPTEZ LES PARAMÈTRES RAPIDES

Ces raccourcis de Windows accessibles en deux ou trois clics servent à piloter des lecteurs audio comme Spotify, à modifier la luminosité et l'éclairage ou encore à lancer un partage de proximité. Ils sont également les bienvenus pour actionner les options d'accessibilité, atteindre le menu général des paramètres ou personnaliser la sortie audio. Vous pouvez épingler des liens vers les commandes que vous utilisez fréquemment en opérant un clic à l'extrême droite de la barre des tâches, sur l'icône **Volume**, puis en pointant sur l'icône en forme de crayon et sur **Ajouter**. Sélectionnez les raccourcis voulus et enregistrez les réglages à l'aide du bouton **Terminer**.





SYSTÈME

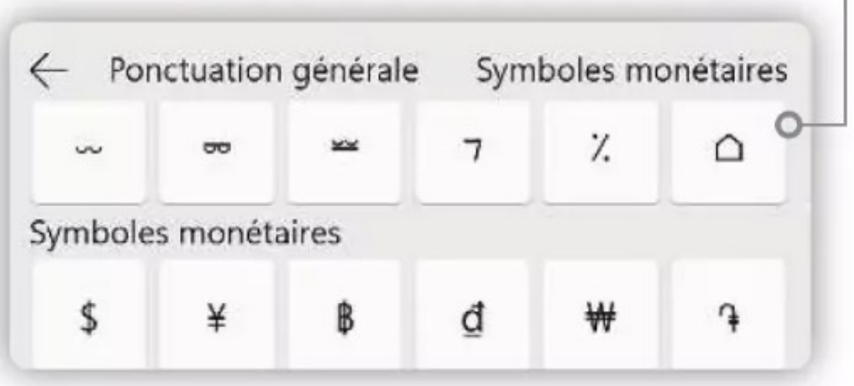
Automatisez l'installation des utilitaires avec Ninite

L'installation de programmes pour Windows sur une nouvelle machine ou un système fraîchement réinstallé peut se révéler longue et fastidieuse. Sauf si l'on confie ces tâches à Ninite. Ce service en ligne automatise l'installation de nombreux logiciels gratuits parmi les plus connus, comme les navigateurs web, les antivirus (AVG, Avast, Avira, etc.) ou les lecteurs multimédias (VLC, iTunes, etc.). Le site propose aussi divers utilitaires de compression, de traitement vidéo ou de retouche d'image. Depuis le site Ninite.com, il suffit de cocher les logiciels souhaités dans une longue liste, puis de télécharger et de lancer le fichier exécutable généré par le site. Les utilitaires sont ensuite installés en quelques minutes, avec la dernière version disponible, sans solliciter la moindre action de l'utilisateur.

BUREAUTIQUE

Ne vous trompez plus de symbole

Rien de plus rageant que de ne pas trouver précisément le bon signe de ponctuation ou le symbole exact lorsqu'on rédige un texte dans Word ou Excel. Il faut dire que tous les caractères n'apparaissent pas sur les touches du clavier. Pour résoudre ce casse-tête, appuyez sur les touches **Windows+;**. Une fenêtre contextuelle repositionnable dotée de six icônes (menu supérieur) s'affiche alors à l'écran. Pointez sur l'avant-dernier raccourci en partant de la droite, puis faites défiler les catégories à l'aide des flèches droite et gauche. Parcourez le tableau en actionnant la molette de la souris et sélectionnez le caractère convoité. Celui-ci prend place dans le document, à l'endroit où se trouvait le curseur.



PÉRIPHÉRIQUES

DÉCLENCHEZ UNE ACTION VIA LA PRISE USB

Windows est en mesure de déclencher automatiquement l'action de votre choix lorsqu'il détecte une clé USB, une liseuse ou un appareil photo. Appuyez sur les touches **Windows+I** du clavier et pointez sur **Bluetooth et appareils**, **Exécution automatique**. Après avoir activé ce curseur, déroulez le menu **Lecteur amovible**. Sélectionnez dès lors l'événement devant être systématiquement exécuté à l'insertion du matériel (ouvrir l'Explorateur de fichiers, par exemple) ou demandez l'affichage d'un menu si vous préférez décider d'une action au cas par cas. Avec un lecteur de carte mémoire, les possibilités se révèlent plus nombreuses : importation des photos, lecture d'une vidéo…

ELENA SHARIPOVA/ISTOCKPHOTO

POUR Internet

GOOGLE

RETROUVEZ MAPS DANS LES RÉSULTATS DE RECHERCHE

Vous avez sans doute remarqué, depuis quelques mois, que les résultats affichés par le moteur de recherche de Google n'affichent plus de liens renvoyant au plus célèbre des services de cartographie. L'explication tient en trois lettres : DMA, l'acronyme de *digital markets act*, le règlement européen qui entend lutter contre les ambitions monopolistiques des géants du Net. Google a sacrifié ses passerelles vers Maps afin de respecter la législation. Accédez à la page d'accueil du moteur de recherche et connectez-vous à votre compte Google. Cliquez sur votre profil en haut à droite, puis sur **Autres paramètres** et à nouveau **Autres paramètres** en colonne gauche. Pointez sur **Langue et région** et **Région pour les résultats**. Sélectionnez un pays hors de l'UE et validez avec **Confirmer**.

OFFICE ONLINE

ENREGISTREZ VOS DOCUMENTS DANS LE CLOUD

Grâce à l'option de sauvegarde automatique dans OneDrive proposée par Word, Excel et PowerPoint, vous ne risquez plus de voir des heures de travail anéanties faute d'avoir pensé à actionner la commande Enregistrer.

ÉTAPE 1 Commencez par associer l'application (Word, par exemple) à votre espace OneDrive en allant dans le menu **Fichier, Compte**. Dans la section **Services connectés**, pointez sur les intitulés **Ajouter un service, Stockage, OneDrive** et indiquez les identifiants de votre compte Microsoft.

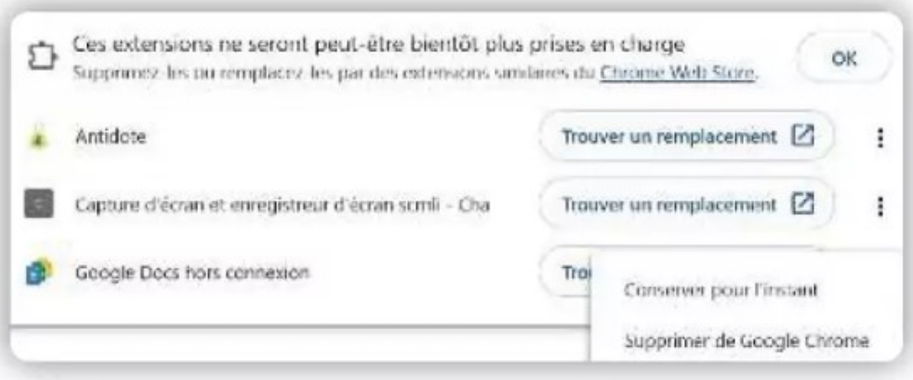
ÉTAPE 2 Revenez sur le document. Cliquez sur l'onglet **Fichiers** du ruban d'outils, puis sur **Options, Enregistrement.**

ÉTAPE 3 Activez le mode **Enregistrer automatiquement les fichiers stockés dans le cloud par défaut…**

ÉTAPE 4 Sauvegardez les réglages avec le bouton **OK.**

ÉTAPE 5 Créez un nouveau document (**Fichier, Nouveau**) et enregistrez celui-ci dans le dossier OneDrive par défaut (**Ctrl+S, OK**).

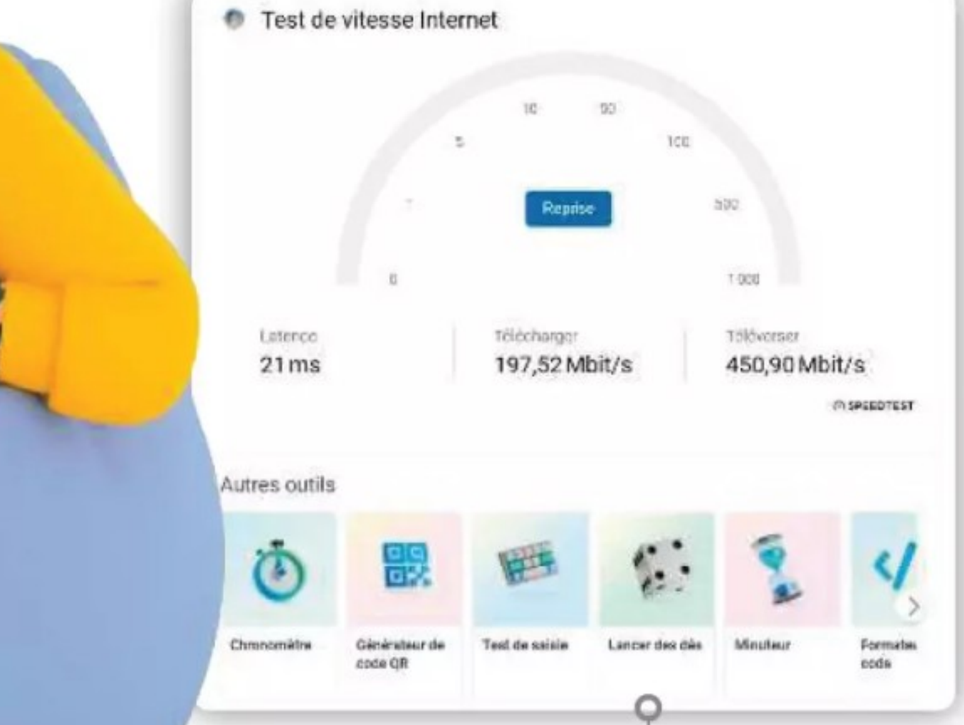
À partir de cet instant, les modifications apportées sont sauvegardées en temps réel dans le cloud. Si vous souhaitez revenir à une version antérieure du fichier après des modifications malheureuses, accédez à votre espace OneDrive depuis un navigateur internet, faites un clic droit sur le document et choisissez **Historique des versions.**



GOOGLE CHROME

Faites le ménage dans les extensions

Afin de lutter contre les bloqueurs de pubs, Google a modifié l'interface de programmation d'applications (API) pour les extensions de son navigateur. Pour les utilisateurs, cela se traduit par des modules additionnels ne fonctionnant plus. Déployez le menu de Chrome et pointez sur **Extensions, Gérer les extensions.** Le volet Contrôle de sécurité signale les extensions dangereuses désactivées par le navigateur. Cliquez sur **Supprimer** pour les effacer. La section suivante dresse la liste des modules incompatibles avec la nouvelle norme Manifest V3. Visitez le Chrome Web Store pour installer une éventuelle mise à jour. Sinon, actionnez le bouton **Trouver un remplacement** afin d'identifier une extension équivalente.



MICROSOFT EDGE

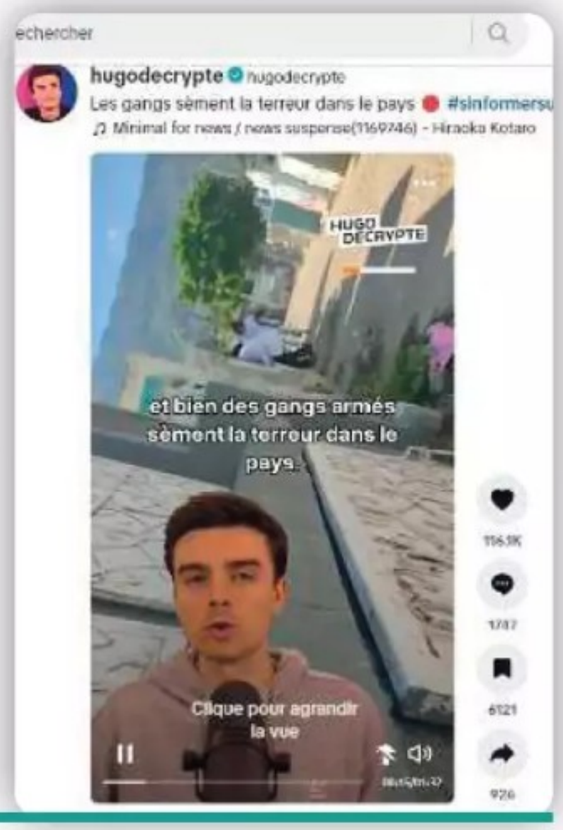
Testez la vitesse de votre connexion

Pourquoi recourir à un service tiers quand on a les outils sous la main ? Parmi ses innombrables fonctionnalités, le navigateur Edge propose un module réalisé en partenariat avec Speedtest pour mesurer les débits de la connexion internet. Pour y accéder, cliquez sur l'icône **Outils** dans la barre latérale. Faites défiler le contenu de ce volet vers le bas jusqu'à la section Test de vitesse et pointez sur le bouton **Démarrer**. Un nouvel onglet s'ouvre et les mesures commencent. Les résultats s'affichent après quelques secondes : temps de latence, vitesses de téléchargement et d'envoi. Cliquez sur le bouton **Découvrir d'autres outils** au bas du panneau pour accéder à un chronomètre, un minuteur ou encore un générateur de QR Codes. Ces modules fonctionnent sur le même principe que le test de vitesse et s'exécutent dans un bloc en haut de la page de recherche Bing.

TIKTOK

VISIONNEZ DES VIDÉOS SANS VOUS INSCRIRE

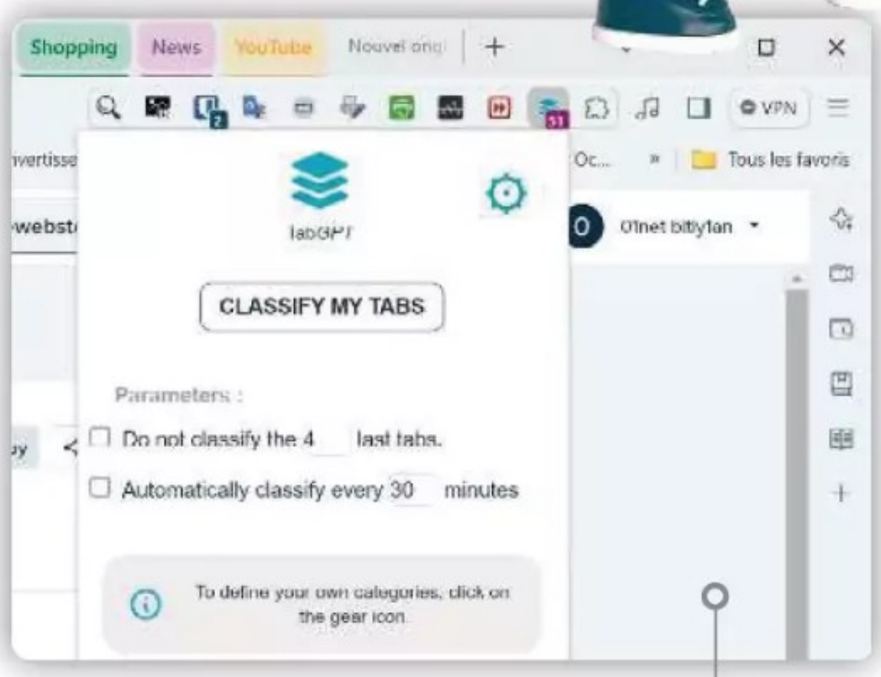
Savez-vous qu'il est possible de tester TikTok sans révéler votre identité ? Pour visionner les contenus de TikTok du réseau social sans ouvrir de compte, il convient de se connecter au service à partir d'un navigateur internet et non de l'application mobile. Lorsque la fenêtre **Connecte-toi à TikTok** s'affiche, pointez sur le lien **Continuer en tant qu'invité**, puis choisissez une vidéo dans la galerie pour en lancer la lecture. Vous avez la possibilité de partager le contenu sur les réseaux sociaux à l'aide des icônes situées en haut à droite de la fenêtre. Il arrive que la fenêtre de connexion réapparaisse de temps à autre. Cliquez sur le bouton **x** pour la fermer.



BITWARDEN

RETROUVEZ VOS MOTS DE PASSE DISPARUS

Depuis quelques jours, certains identifiants peuvent disparaître du coffre-fort du gestionnaire de mots de passe Bitwarden sans prévenir. Un lecteur nous a ainsi rapporté avoir vu son compteur passer du jour au lendemain de 698 à 99 clés ! Le phénomène est lié à une modification opérée par le service, qui fait que les mots de passe non assignés ne s'affichent plus dans le dossier **Tous les coffres** ni dans les formulaires d'identification des sites qui leur sont associés. Ils ne sont pas effacés pour autant ! Pour les restaurer, rendez-vous à l'adresse vault.bitwarden.com. Cliquez sur l'icône **App Launcher**, puis sur **Admin Console**. Rejoignez l'onglet **Collections** du volet gauche. Ouvrez la collection **Non attribué**. Sélectionnez le contenu du dossier, puis pointez sur les trois points à droite de la barre d'en-tête de la liste et optez pour **Collections**. Désignez puis choisissez une collection (**Collection par défaut** ou un dossier personnalisé).



TABGPT

Laissez l'IA mettre de l'ordre dans les onglets

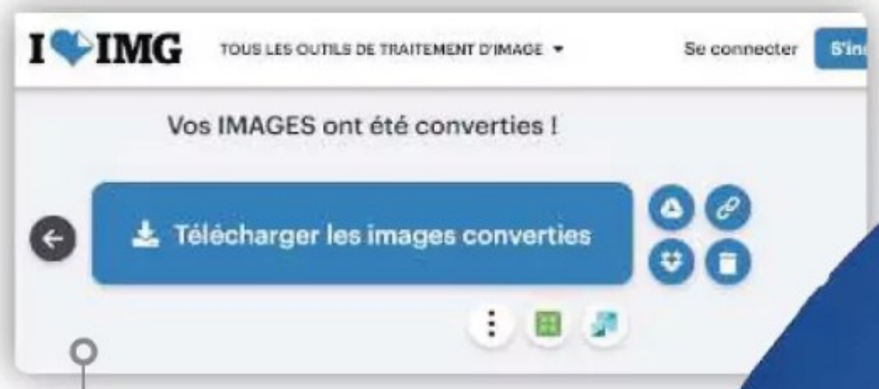
Chrome et les navigateurs utilisant le noyau Chromium (Edge, Brave, Opera, etc.) proposent d'organiser les onglets en les rangeant dans des groupes. Un dispositif très utile pour gérer des dizaines de pages sans s'y perdre. Si vous trouvez fastidieux de devoir affecter à la main les onglets aux différents groupes, confiez cette tâche à l'IA. Allez sur le Chrome Web Store et installez l'extension TabGPT (bit.ly/4aZxHKB). Faites un clic droit sur l'icône du module qui a été ajouté dans la barre d'outils de Chrome et choisissez **Épingler** pour garder le raccourci à portée de clic. Pointez sur ce dernier, puis sur le bouton **Classify my tabs**. TabGPT identifie les pages associées à l'actualité, au shopping et à YouTube, plaçant les autres sites dans un dossier Autres catégories (*Other categories*). Vous pouvez définir des groupes personnalisés en indiquant un libellé et des mots-clés.

ELENA SHARIPOVA/ISTOCKPHOTO

I LOVE IMG

Convertissez des images en ligne

Il est de plus en plus fréquent de trouver des fichiers au format WebP sur internet. Si vous ne parvenez pas à les afficher dans votre éditeur d'images, rendez-vous sur le site iloveimg.com/fr/convertir-en-jpg. Glissez la photo dans la zone **Sélectionner des images** ou pointez sur les icônes Dropbox ou Google Drive si les fichiers sont conservés dans le cloud. Cliquez sur le bouton **Convertir en jpg**, puis sur **Télécharger les images converties** pour rapatrier les clichés sur votre PC. Ce service en ligne sait traiter avec le même bonheur les contenus enregistrés en HEIC, le format d'images d'Apple.



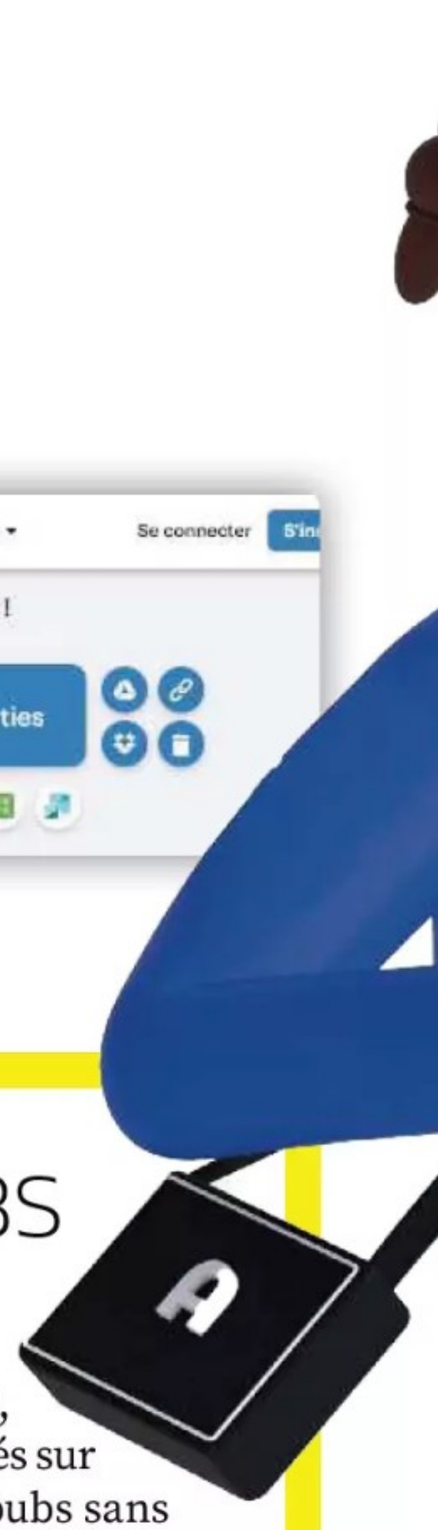
LOCALSEND

TRANSFÉREZ DES CONTENUS ENTRE TOUS VOS APPAREILS

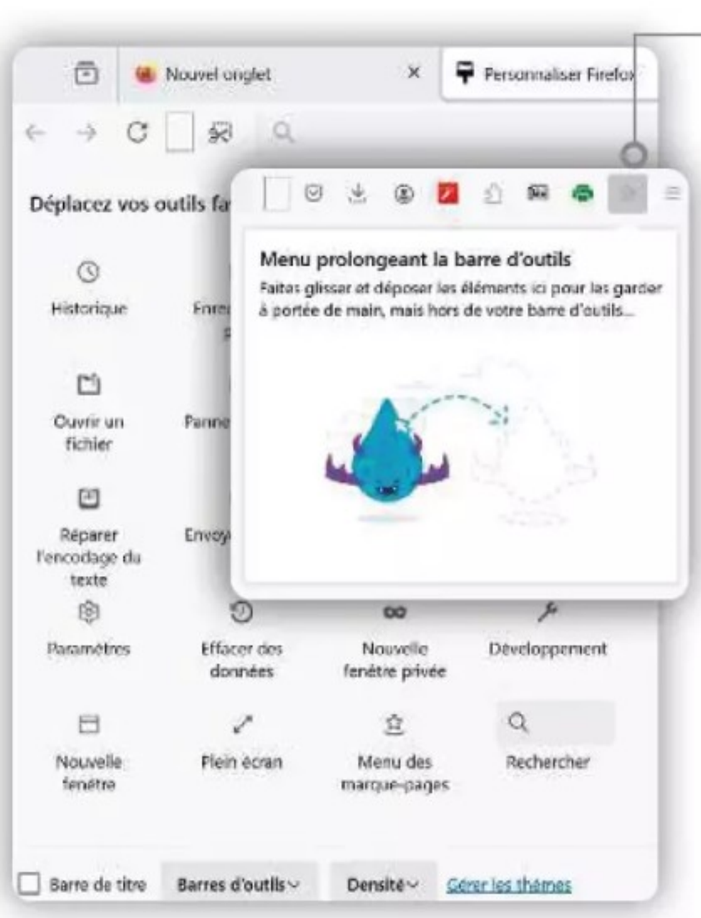
Aussi pratiques soient-ils, AirDrop et Nearby Share ne fonctionnent que dans l'univers Apple pour l'un, entre appareils Android et Windows pour l'autre. Si vous recherchez un outil universel capable de réconcilier les environnements Apple et Google, rendez-vous sur le site localsend.org. Installez LocalSend sur vos différents matériels (Android, iOS, macOS, Windows et Linux), puis ouvrez l'application sur votre iPhone et un mobile Android par exemple. Touchez l'onglet **Envoyer** sur le premier, puis **Media** si vous souhaitez transmettre une photo ou une vidéo, ou **Fichier** dans le cas d'un PDF. Sélectionnez l'élément à transmettre et désignez l'appareil cible. Allez sur ce dernier et pointez sur **Accepter**.

YOUTUBE

DÉBARRASSEZ-VOUS DES PUBS SANS RESTRICTION



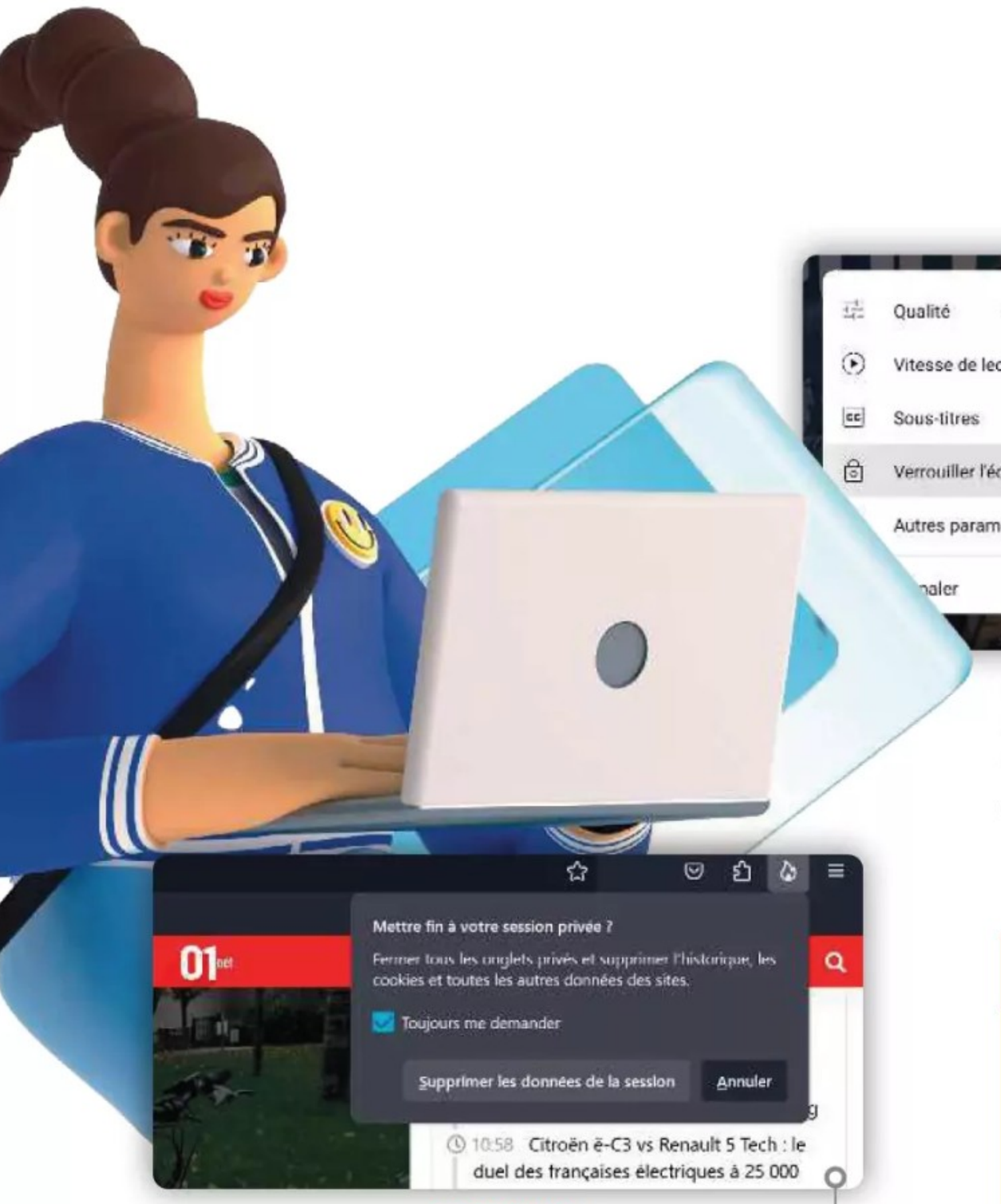
Le principal avantage de l'abonnement premium de YouTube, facturé 13 euros par mois, tient à la disparition des publicités sur la plateforme de partage de vidéos. Pour échapper aux pubs sans passer par l'offre payante, il reste néanmoins possible de faire appel à un bloqueur, malgré les restrictions adoptées par Google contre certains d'entre eux. Nous avons opté pour l'extension Music Mode, disponible pour les navigateurs Chrome (bit.ly/47GKsXD) et Firefox (mzl.la/48vnaW0). Avec le premier, cliquez sur **Ajouter à Google Chrome**, **Ajouter l'extension**. Un nouvel onglet s'ouvre afin de paramétrer le fonctionnement de l'extension. Activez le mode **Enabled by default** si vous souhaitez systématiser le blocage, puis indiquez les contenus qui seront masqués : vidéos (vous continuerez de profiter du son), miniatures des séquences (**Thumbnails**), publicités (**Ad Skipper**)…



FIREFOX

Personnalisez la barre d'outils

Utilisateur de l'excellent navigateur libre et gratuit, vous aimeriez sans doute remodeler la barre d'outils en y plaçant des raccourcis répondant à vos besoins. Pour ce faire, pointez sur les traits horizontaux en haut à droite de la fenêtre, puis sur **Outils supplémentaires** et **Personnaliser la barre d'outils**. Ce menu intègre plusieurs commandes pouvant être épinglées à la barre personnelle d'un simple glisser-déposer, puis repositionnées sur le bord droit ou gauche. Si la barre se révèle trop exiguë pour tous vos raccourcis, déplacez certains liens dans la zone située à droite de la barre d'outils. Retrouvez-les d'un clic sur la double flèche (>>) visible en haut à droite de l'écran.



YOUTUBE

Profitez des nouvelles options de lecture

Vous utilisez l'application mobile de la plateforme vidéo de Google, mais connaissez-vous ces commandes apparues lors d'une récente mise à jour ? Pour augmenter la vitesse de lecture de la vidéo que vous visionnez, appuyez durant une seconde sur l'image. La mention 2x s'affiche en haut de l'écran. Pour éviter qu'un geste intempestif ne vienne interrompre la lecture, pointez sur l'image, puis sur l'icône **Paramètres** en haut à droite et sur **Verrouiller l'écran**. Touchez l'image puis le bouton **Appuyer pour déverrouiller** afin de retrouver un fonctionnement normal.

FIREFOX

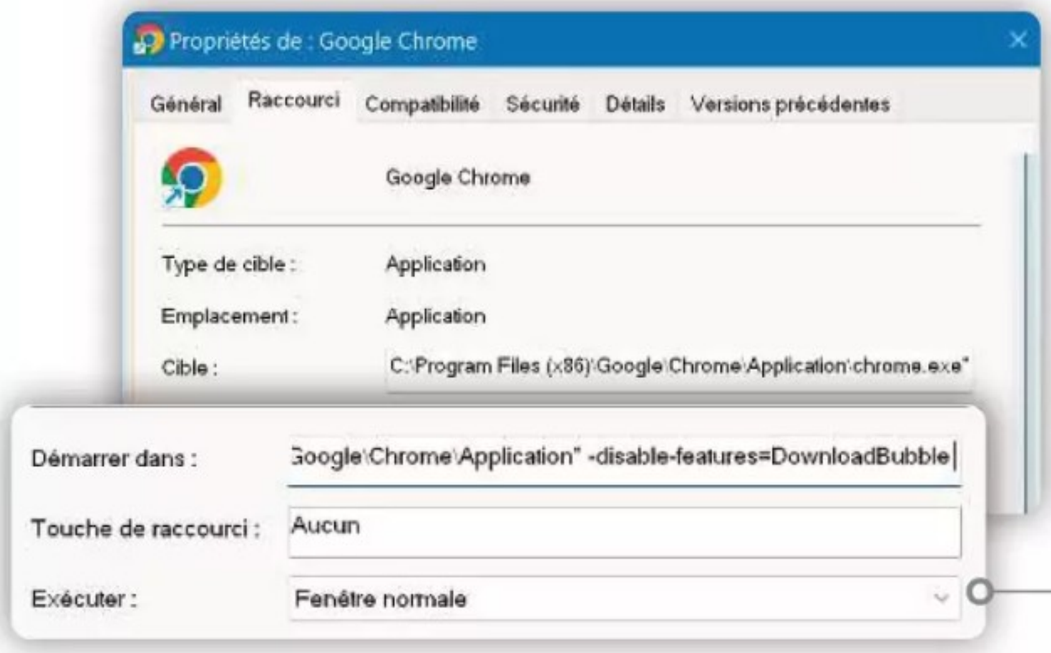
VERROUILLEZ LE MODE DE NAVIGATION PRIVÉE

Comme ses concurrents, Firefox propose de parcourir le web sans laisser de traces grâce au mode de navigation privée. L'application supprime à cet effet l'historique des pages visitées, les cookies et les données relatives aux sites affichés. Pour être certain que ce grand ménage ait bien lieu, pensez à actionner la commande **Mettre fin à la session privée** d'un clic sur l'icône en forme de flamme à droite de la barre de menu et à presser le bouton **Supprimer les données de la session**. Si ce raccourci n'apparaît pas, tapez **About:config** dans la barre d'adresse, appuyez sur la touche **Entrée** du clavier et pointez sur **Accepter le risque et poursuivre**. Lancez une recherche sur les termes **browser.private** et double-cliquez sur la ligne **browser.privatebrowsing.resetPBM.enabled** pour passer le statut sur **true**. Redémarrez Firefox.

FACEBOOK

ENTREZ DANS LE MONDE REELS

Facebook propose de regarder de courtes vidéos inspirées de TikTok et nommées « Reels ». Elles sont accessibles dans le menu principal de l'appli. Touchez les traits horizontaux en haut à droite, effleurez **Reels** et faites défiler les vidéos en effectuant une pichenette de bas en haut. Touchez l'icône **Loupe** et lancez une recherche sur un thème. Les résultats se présentent sous forme de vignettes. Pointez sur l'une d'elles pour la regarder. Si le contenu vous plaît, pressez sur les points en bas à droite, puis sur **Voir plus**. Vous pouvez aussi liker un Reel à l'aide du pouce levé ou exprimer de la tristesse, de la colère, du rire… en faisant un appui prolongé sur celui-ci et en choisissant un émoji.



CHROME

Retrouver la « bonne vieille » barre des téléchargements

Google a profité d'une récente mise à jour de son navigateur pour remplacer l'historique barre des téléchargements. L'accès aux fichiers récupérés sur le web s'opère désormais via un raccourci ajouté à la barre de menu. Si vous souhaitez revenir à l'ancien dispositif, faites un clic droit sur le raccourci de Chrome et choisissez **Propriétés**. Cliquez dans le champ **Cible**. Placez le curseur à la fin du chemin d'accès du fichier exécutable, ajoutez un espace, puis saisissez la commande **-disable-features=DownloadBubble**. Enregistrez les changements à l'aide du bouton **OK**.

ELENA SHARIPOVA/ISTOCKPHOTO

FIREFOX

Débloquez les réglages cachés

Firefox ne se livre pas entièrement au premier venu, préférant réserver certains paramètres avancés aux plus experts. Pour y accéder, tapez **about:config** dans la barre d'adresse du navigateur, pressez la touche **Entrée** et pointez sur le bouton **Accepter le risque et poursuivre** sur la page de mise en garde (*voir capture*). Il suffit ensuite d'utiliser le champ de recherche pour trouver les options qui vous intéressent. Si vous devez composer avec une liaison internet lente, désactivez l'option de chargement prédictif des pages web - qui consomme beaucoup de bande passante - en lançant une requête sur les termes **network.prefetch-next** et double-cliquez sur le résultat qui apparaît (la valeur passe de *true* à *false*).

DALL-E 3

AGRANDISSEZ LE CADRE D'UN TABLEAU CÉLÈBRE

Certaines intelligences artificielles génératives sont capables d'étendre le cadre d'une image. C'est le cas de Dall-E 3, développée par OpenAI, l'éditeur de ChatGPT. Ouvrez votre navigateur et rendez-vous sur la page bit.ly/4gUlrhQ. Pointez sur le bouton **Se connecter**, avec votre compte Google ou Apple, puis sur **Continuer**, **Activer**. Décrivez l'œuvre que vous avez en tête et soumettez la demande à Dall-E 3. Le résultat s'affiche après quelques secondes. Cliquez sur l'aperçu pour basculer en mode plein écran. Si le tableau ou la photo vous satisfait, actionnez l'icône **Télécharger** pour récupérer le fichier au format WebP.

WHATSAPP

DÉCOUVREZ LES NOUVELLES CHAÎNES

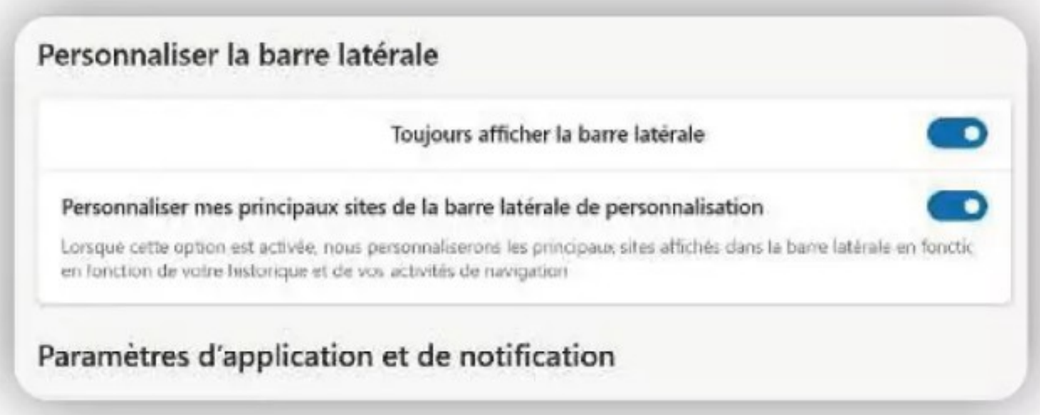
L'application de messagerie du groupe Meta a lancé progressivement, depuis l'an dernier, un nouveau canal de diffusion. Ces chaînes permettent de suivre les actualités publiées par des médias, des personnalités ou des marques, via ce qu'il est déjà possible d'envoyer sur WhatsApp (texte, photos, vidéos, *stickers*, sondages). Pour les suivre, depuis l'application, rendez-vous sur l'onglet **Actus, Trouver des chaînes**. Vous accédez alors à celles recommandées pour vous par le réseau social, mais vous pouvez rechercher celles que vous voulez via la loupe.

ELENA SHARIPOVA/ISTOCKPHOTO

TIKTOK

ACCÉLÉREZ LES VIDÉOS

Les *shorts* du réseau social chinois n'ont beau durer que quelques dizaines de secondes, cela ne va pas encore assez vite pour certains. Mais une solution existe pour ces impatients « boulotteurs » de vidéos. Pour doubler la vitesse de lecture, restez appuyé sur le côté gauche ou droit de votre écran. Vous pouvez alors toucher l'option **Vitesse de lecture** pour régler celle-ci, jusqu'au double, ou, au contraire, ralentir la vidéo jusqu'à un quart de sa vitesse normale.



EDGE

Personnalisez la barre latérale

On n'a jamais assez de raccourcis ! En plus de l'habituelle barre de favoris, le navigateur internet de Microsoft propose d'afficher une barre d'outils. Celle-ci prend place sur la droite de la fenêtre. Elle arbore une série d'icônes donnant accès à diverses applications. Ces liens ne renvoient pas vers un nouvel onglet de navigation, mais ouvrent la suite bureautique Microsoft 365, Outlook ou encore le formulaire de recherche dans un volet qui prend place à côté de la page active. Pour supprimer un élément de la barre latérale, faites un clic sur son icône et choisissez **Retirer de la barre d'appui**. Si vous souhaitez y intégrer d'autres outils, pointez sur le bouton **+**, puis lancez une recherche ou sélectionnez un service parmi les sites suggérés. Vous n'utilisez jamais la barre latérale ? Alors, cliquez sur l'engrenage présent au bas de la barre et décochez le mode **Toujours afficher**.

POUR Android

AFFICHAGE

Adaptez l'écran à la lumière

Si vous souhaitez lire dans la pénombre sans vous abîmer les yeux ni déranger personne, plusieurs possibilités s'offrent à vous. L'une consiste à réduire manuellement la luminosité depuis le panneau des actions rapides, accessible d'une pichenette de haut en bas de l'écran. La seconde solution passe par les **Paramètres**. Dans la section **Affichage**, activez le mode **Luminosité adaptative** pour assombrir l'écran dans un environnement obscur. Si la luminosité est encore trop forte, rendez-vous dans le menu **Accessibilité** et utilisez la commande **Encore moins lumineux** dans la rubrique **Affichage**. Ajustez manuellement l'intensité lumineuse pour obtenir un résultat optimal.

ALERTES

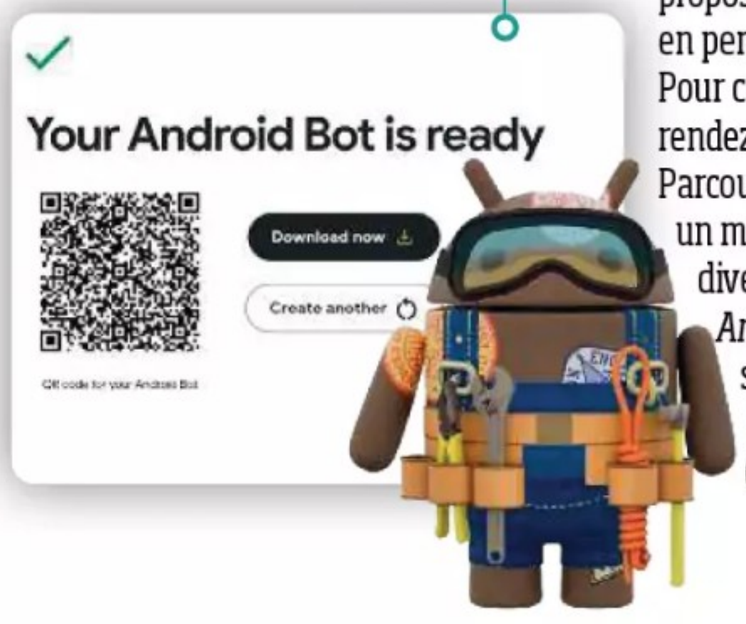
UTILISEZ LE FLASH POUR SIGNALER L'ARRIVÉE DE NOUVEAUX MESSAGES

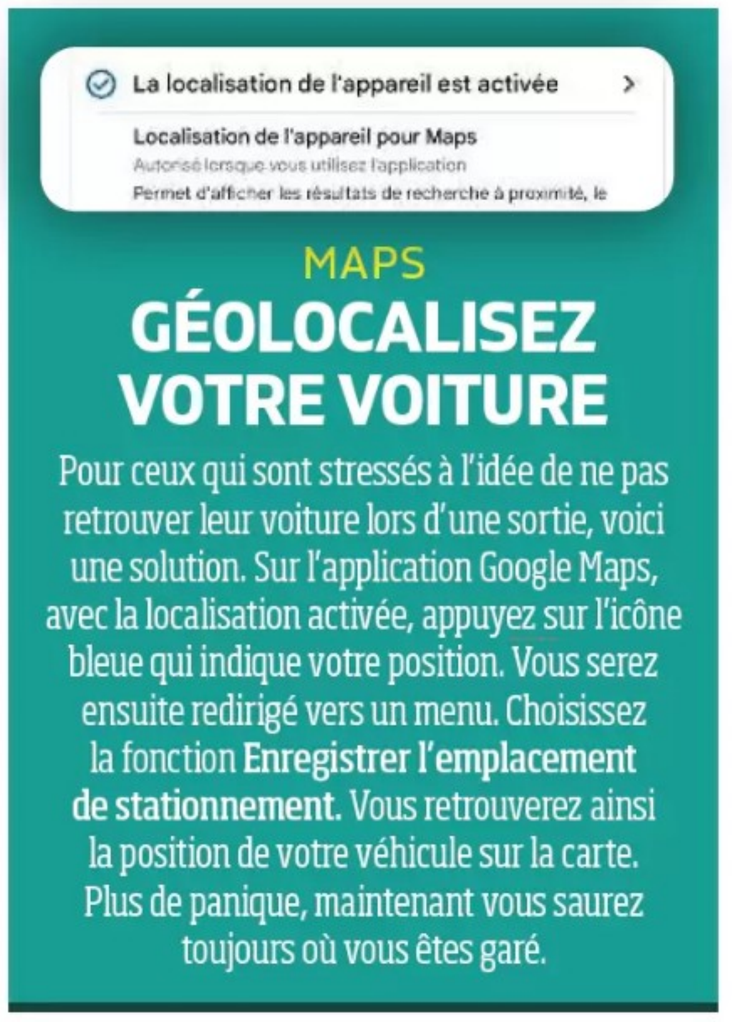
Dans le train ou en réunion, le mode silencieux est de rigueur pour ne pas importuner ses voisins avec les sonneries et les alertes audio. Android 14 propose une alternative : remplacer les sons par des signaux lumineux en utilisant le flash du téléphone. Pour activer cet outil, ouvrez les paramètres de votre appareil et rendez-vous dans la section **Accessibilité**. Descendez jusqu'à la rubrique **Audio** et touchez **Notifications lumineuses**. Activez alors les modes **Clignotement du flash** et **Clignotement de l'écran**. Vous êtes ainsi sûr de ne manquer aucune alerte, que votre mobile soit posé côté pile ou face ! Appuyez sur **Prévisualiser** afin d'obtenir un aperçu du dispositif. Sachez que vous avez la possibilité de choisir la couleur utilisée pour illuminer l'écran.

AVATAR

HABILLEZ VOTRE ROBOT

Plus qu'aux noms de pâtisseries associés jusqu'en 2019 aux générations successives du système d'exploitation mobile, le grand public identifie Android au petit robot vert affublé d'une paire d'antennes qui lui sert de logo depuis les premiers jours. Google vous propose de concevoir un avatar sur mesure en personnalisant ce petit personnage. Pour cela, ouvrez votre navigateur web et rendez-vous sur la page bit.ly/30YzztP. Parcourez les différents onglets pour choisir un modèle de robot, l'habiller et lui attribuer divers accessoires. Quand le message « *Your Android bot is ready* » apparaît, pointez sur **Download** pour télécharger le fichier au format PNG ou flashez le QR Code (depuis un PC) avec votre téléphone.





MAPS

GÉOLOCALISEZ VOTRE VOITURE

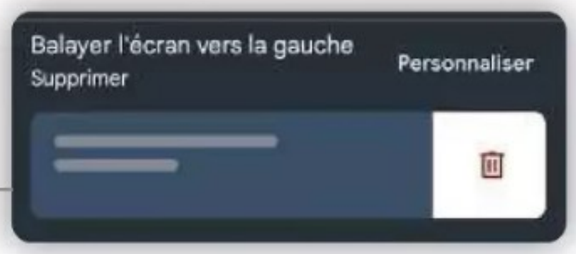
Pour ceux qui sont stressés à l'idée de ne pas retrouver leur voiture lors d'une sortie, voici une solution. Sur l'application Google Maps, avec la localisation activée, appuyez sur l'icône bleue qui indique votre position. Vous serez ensuite redirigé vers un menu. Choisissez la fonction **Enregistrer l'emplacement de stationnement.** Vous retrouverez ainsi la position de votre véhicule sur la carte. Plus de panique, maintenant vous saurez toujours où vous êtes garé.

ELENA SHARIPOVA/ISTOCKPHOTO

MESSAGES

Triez vos textos

Présente par défaut sur la plupart de nombreux téléphones Android, l'application Messages de Google aide à faire le tri dans les SMS. Il est ainsi possible d'archiver ou de supprimer un message en balayant l'écran de gauche à droite ou de droite à gauche depuis la boîte de réception.
Pour personnaliser le fonctionnement de cette option, effleurez votre avatar en haut de la page, puis touchez **Paramètres de l'application Messages, Actions de balayage**. Pointez sur la commande **Personnaliser** de la section **Balayer l'écran vers la droite** et choisissez l'action voulue (**Archiver, Supprimer, Marquer comme lu** ou **non lu, Désactiver**). Faites de même pour le raccourci **Balayer l'écran vers la gauche**.



SÉCURITÉ

ACTIVEZ LA BALISE DE DÉTRESSE

Les versions 12 et suivantes d'Android intègrent des fonctions de sécurité poussées. Parmi celles-ci, une balise de détresse propose de contacter ses proches en cas d'accident. Allez dans les paramètres de l'appareil, touchez le menu **Sécurité et urgences** et **Ouvrir Sécurité personnelle.** Pressez sur **Balise de détresse,** puis sur **Ajouter des contacts.** Indiquez le nom de la personne à joindre parmi vos contacts. Revenez en arrière et effleurez **Partager.** Le référent reçoit un message envoyé par Google afin de l'informer de son nouveau rôle. Gardez à l'esprit que l'activation de la balise entraîne de facto le partage de votre position en temps réel. L'appli propose par ailleurs un raccourci pour appeler le 112.

SYSTÈME

ACCÉLÉREZ LES RECHERCHES

Les Google Pixel et Samsung Galaxy de dernière génération proposent une nouvelle manière d'effectuer des recherches sans quitter l'application active. Vérifiez que votre téléphone est à jour en allant dans le menu **Système, Mises à jour logicielles.** Rejoignez ensuite la page **Système, Mode de navigation,** touchez l'icône en forme d'engrenage à droite de Navigation par gestes et activez le mode **Entourer pour rechercher.** Lancez une appli. Effectuez un appui long sur la poignée située en bas de l'écran. La mention **Entourer/Appuyer n'importe où pour rechercher** s'affiche. Tracez un cercle autour d'une image ou d'un mot pour interroger Google. Les résultats défilent dans le panneau déroulant inférieur.

VISIOCONFÉRENCE

TRANSFORMEZ VOTRE MOBILE EN WEBCAM

Si la caméra de votre ordinateur se fait vieille et restitue une image de piètre qualité, pourquoi ne pas lui substituer le capteur 4K de votre mobile ? L'opération peut être réalisée avec une application tierce comme DroidCam (droidcam.app) ou via les options d'Android 14. Reliez le mobile au PC avec un câble USB. Déroulez le panneau des actions rapides, ouvrez le menu **Recharge de cet appareil via USB** et cochez la case **Webcam.** Accédez au menu **Service de webcam** qui propose de basculer du capteur photo principal à la caméra selfie si vous le souhaitez ou de régler le zoom sur une échelle de 1 à 10 en écartant ou en rapprochant le pouce de l'index sur l'écran.

SÉCURITÉ

Déverrouillez sans y penser avec Extend Unlock

Taper son code pin, tracer son schéma secret ou apposer son doigt sur le lecteur d'empreintes sont autant de manières sécurisées d'ouvrir son smartphone. Mais à la longue, la manœuvre peut se révéler fastidieuse. C'est là qu'intervient Extend Unlock (ex-Smart Lock), une fonction d'Android qui déverrouille automatiquement votre terminal si et seulement si certaines conditions sont réunies. Le téléphone peut ainsi repérer qu'il se situe dans un lieu sûr (géolocalisation), si on le porte sur soi (capteurs internes) ou encore s'il se connecte à un appareil de confiance référencé comme tel (des écouteurs Bluetooth par exemple). Pour activer ces options, rendez-vous, sous Android 14, dans **Paramètres, Sécurité et confidentialité, Autres paramètres, Extend Unlock.** Sous Android 13, il faut cocher **Smart Lock** dans **Agents de confiance.**

ELENA SHARIPOVA/ISTOCKPHOTO

POUR Apple

IOS 17

Raccrochez… sans les mains !

Peu importe que vous ayez ou non les mains encombrées pour mettre fin à une communication audio ou vidéo sur l'iPhone. À défaut de pouvoir toucher l'écran, il est possible de raccrocher en sollicitant l'assistant Siri d'iOS 17. Après avoir vérifié que le mobile dispose de la dernière version du système d'exploitation, ouvrez les réglages et touchez **Siri**, **Parler à Siri**, **Dis Siri**. Déroulez ensuite le menu vers le bas et effleurez la commande **Raccrocher les appels** pour activer ce mode. Désormais, la communication s'interrompt dès que vous prononcez la formule *« Dis Siri, raccrocher »*. Pratique quand on cuisine ou que l'on conduit !

MACOS

RÉINITIALISEZ VOTRE MAC

Vous vous apprêtez à vendre votre Mac ? Vous bataillez avec de trop nombreux bugs ? C'est qu'il est temps de procéder à une réinitialisation complète. L'opération efface les documents et données personnelles et restaure les fichiers système. Avec un Mac équipé d'un processeur Intel datant de quelques années et dénué de la puce de sécurité T2, déconnectez-vous d'iTunes, iCloud et iMessage. Redémarrez en mode Récupération en appuyant sur les touches **Command + R** et choisissez l'option entraînant l'effacement des données et la réinstallation de macOS. Avec un processeur Apple Silicon ou Intel récent, déroulez le menu **Pomme** et pointez sur **Réglages système**, **Général**, **Transférer ou réinitialiser**, **Effacer contenu et réglages**. Entrez le mot de passe du compte Administrateur de l'ordinateur. Cliquez sur **Continuer**, saisissez le mot de passe de votre compte Apple ID et lancez la réinitialisation avec **Effacer tous les contenus et réglages**.

IOS

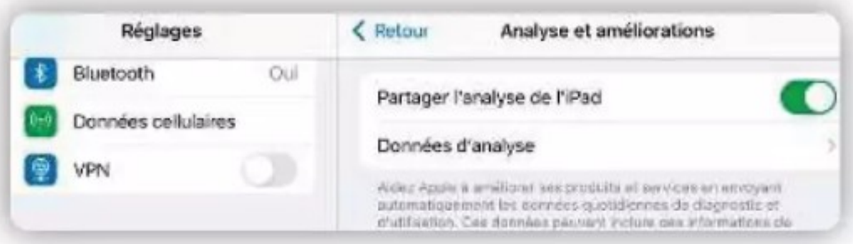
LOCALISEZ UN IPHONE, MÊME S'IL EST ÉTEINT

Quand il est hors tension, mais si sa batterie n'est pas déchargée, l'iPhone émet un signal périodique pouvant être détecté par les autres iPhone à proximité. Ces appareils servent ainsi de relais pour la géolocalisation. Vérifiez que l'option est fonctionnelle en vous rendant dans les **Réglages**. Effleurez votre nom, puis le menu **Localiser**, **Localiser mon iPhone**. Activez les curseurs associés, dont celui lié à **Réseau Localiser**. Si vous égarez votre mobile ou que vous vous le faites voler, allez sur icloud.com à partir d'un ordinateur. Connectez-vous avec vos identifiants Apple ID, puis cliquez sur **Localiser**. Sélectionnez votre appareil dans la liste pour afficher sa position sur la carte.

IOS 17

LIEZ DES MEMOJI À VOS CONTACTS

Depuis le déploiement d'iOS 17, il est possible d'apporter une touche personnelle à l'écran d'appel de vos contacts. Dans l'application Téléphone, appuyez sur **Contacts** et sélectionnez la personne concernée. Pointez sur **Modifier** en haut à droite de la fenêtre, puis sur cette même commande sous l'avatar du correspondant. Touchez le bouton **Personnaliser**, **Affiche**. Choisissez une photo en puisant parmi les Memojis ou dans votre bibliothèque d'images et validez avec **Suivant**. Effleurez le nom du contact pour ajuster la police, la couleur et la graisse des caractères. Fermez le volet d'édition et enregistrez avec **OK**, **Continuer**, **Continuer**.



IPADOS

Évaluez l'état de santé de la batterie

Activez le mode **Partager l'analyse de l'iPad** dans **Réglages**, **Confidentialité et sécurité**, **Analyse et améliorations**. Laissez le temps (quelques jours) à iPadOS de collecter des infos. Revenez sur la page **Analyse et améliorations**. Touchez **Données d'analyse**, affichez le fichier **log-aggregated** le plus récent et copiez le contenu de la fenêtre dans un éditeur de texte (Notes, Google Docs, etc.). Recherchez les lignes *Maximum CapacityPercent et CycleCount* pour découvrir la capacité max de la batterie, par rapport à son état initial, et le nombre de cycles de recharge.

ELENA SHARIPOVA/ISTOCKPHOTO

PLANS

Téléchargez des cartes pour naviguer hors ligne

Cette fonction, présente dans Google Maps depuis de nombreuses années, fait enfin son apparition sur l'iPhone. Avant de partir pour une destination privée de 4G ou de Wifi, ouvrez l'application Plans sur votre téléphone. Touchez votre avatar à côté du champ de recherche, puis **Plans hors ligne** et **Télécharger un nouveau plan**. Indiquez la ville ou la région concernée, ajustez les contours de la zone en déplaçant les poignées de sélection et validez avec **Télécharger**. Quand vous n'en avez plus besoin, retournez sur la page **Plans hors ligne**, touchez la carte de votre choix et **Supprimer le plan**.

IPAD

DÉPLOYEZ LA PROTECTION ANTIVOL

Apple n'a pas attendu 2024 pour se préoccuper de la sécurité de ses appareils. Localisation, blocage et effacement à distance sont autant de fonctions de nature à dissuader les voleurs. Depuis la sortie d'iOS 17.3, le dispositif s'enrichit d'un nouveau mode, **Protection en cas de vol de l'appareil**. Une fois celui-ci activé, le code d'accès de déverrouillage ne suffit plus pour accéder aux cartes de crédit et aux mots de passe enregistrés sur le téléphone dès lors que l'iPhone ne se trouve pas dans un lieu connu (domicile, bureau, etc.). Il faut procéder à une identification biométrique via FaceID ou TouchID. Pour mettre la fonction en œuvre, allez dans **Réglages, Face ID et code**. Tapez votre code personnel et touchez le lien **Activer la protection** sous **Protection en cas de vol de l'appareil**.

ICLOUD

FAITES DE LA PLACE SUR VOTRE MAC

Si l'espace vient à manquer dans le disque dur, exploitez les 5 Go de stockage gratuit associés à votre compte Apple. Dans le menu Pomme, pointez sur **Réglages Système** et **Général, Stockage**, puis sur l'icône **i** à droite des intitulés Applications, Documents et photos. Cliquez sur l'en-tête de la colonne **Taille** pour trier les données. Actionnez **Stocker dans iCloud** et les curseurs **Bureau et Documents, Photos**. Validez avec **Stocker dans iCloud**. Surveillez l'évolution de votre espace iCloud en tapant **iCloud Drive** dans Spotlight, puis choisissez **Ouvrir les réglages Identifiant Apple, Afficher plus d'apps**. Utilisez les curseurs pour synchroniser ou non les fichiers associés aux différentes applis.

WATCHOS

VÉRIFIEZ L'ÉTAT DE SANTÉ DE LA BATTERIE DE L'APPLE WATCH

Avec le temps, les cellules lithium-ion de la batterie de la montre connectée d'Apple se dégradent et l'autonomie baisse. Si vous rencontrez des difficultés à tenir une pleine journée sans passer par la case recharge, un remplacement de l'accumulateur est peut-être nécessaire. Pour en avoir le cœur net, appuyez sur la Digital crown, puis sur l'icône **Réglages** et sur **Batterie, État de santé de la batterie**. Si la section **Capacité maximum** affiche une valeur supérieure à 85 %, tout est en ordre et la baisse d'autonomie est liée à d'autres facteurs. Pour qu'il en aille ainsi le plus longtemps possible, activez le mode **Recharge optimisée de la batterie** sur ce même écran.

IOS

Naviguez en mode privé sur l'iPhone avec Safari

Il n'est pas nécessaire d'avoir des choses à cacher pour apprécier de parcourir le web sans risquer de voir son adresse IP et des informations personnelles utilisées à des fins commerciales. Pour utiliser ce dispositif dans le navigateur internet de l'iPhone, touchez l'icône **Onglets** au bas de l'écran, puis le bouton **Privée**. Pour revenir au mode classique, appuyez sur **Onglets, X onglets**. Il est possible de verrouiller les onglets ouverts en mode privé afin d'empêcher que l'on y accède en votre absence. Dans les réglages, pointez sur **Safari, Confidentialité et sécurité** et activez l'option **Exiger l'utilisation de Face ID pour déverrouiller la navigation privée** (ou **TouchID** sur un iPhone plus ancien).

On alloooo oooooooooo oooooonge la garantie !

Elle passe de 2 ans à 3 ans,
sur tous les produits.*
Et c'est gratuit !

SEULEMENT CHEZ

LDLC

Expert high-tech depuis 28 ans | 25 000 références sur ldlc.com | 100 boutiques à votre service

*Produits neufs vendus par LDLC, hors batteries et consommables. Plus d'info sur ldlc.com/garantie.

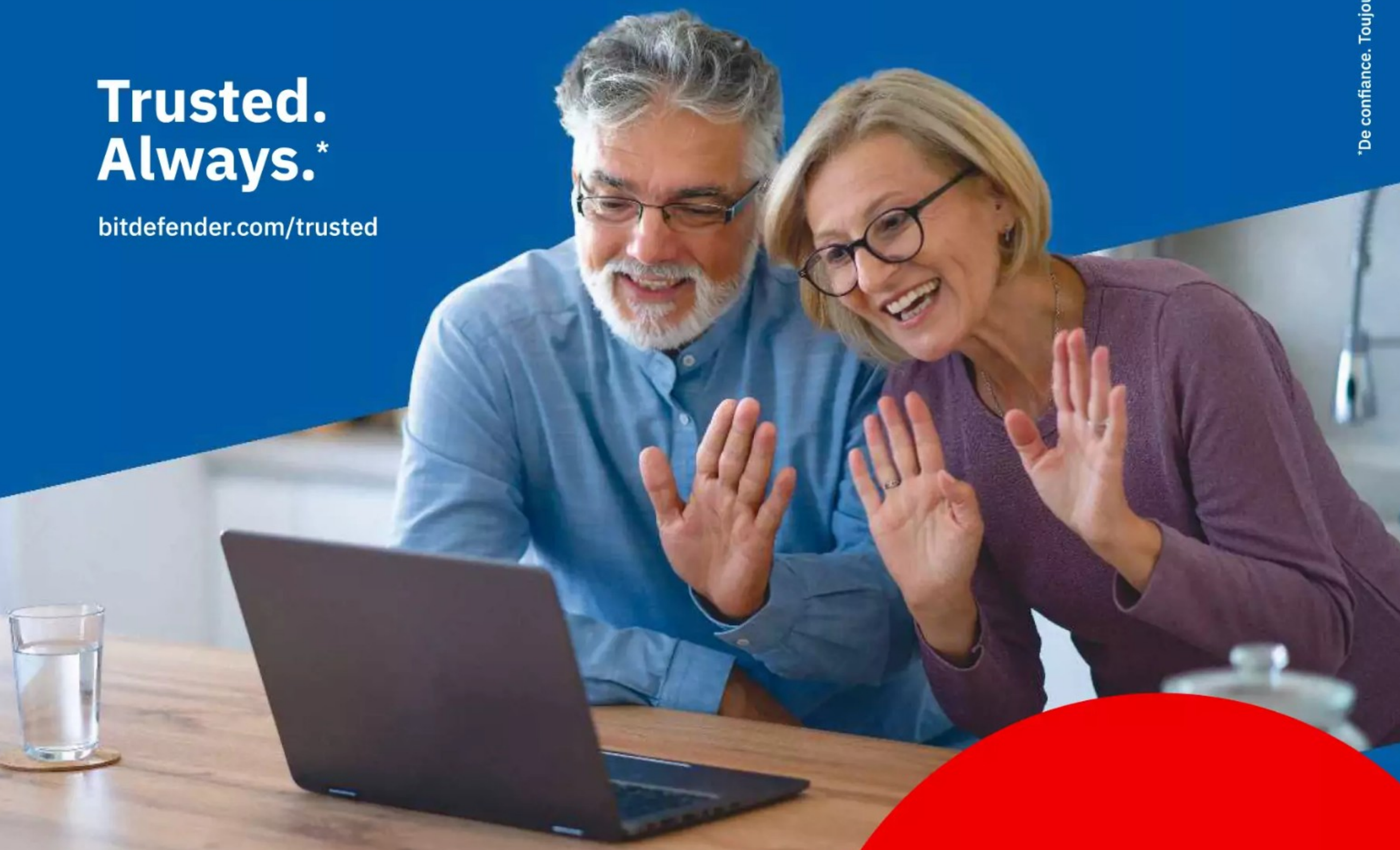
Bitdefender®

Leader Mondial
en Cybersécurité

Soyez toujours en contact.
En toute sécurité.

Trusted.
Always.*

bitdefender.com/trusted



*De confiance. Toujours.

EU
MADE IN EUROPE

Le partenaire Européen de confiance
pour protéger votre vie numérique