WINDOWS
MACOS
ANDROID
LINUX
IOS

LE MAGAZINE DU NUMÉRIQUE

01NET

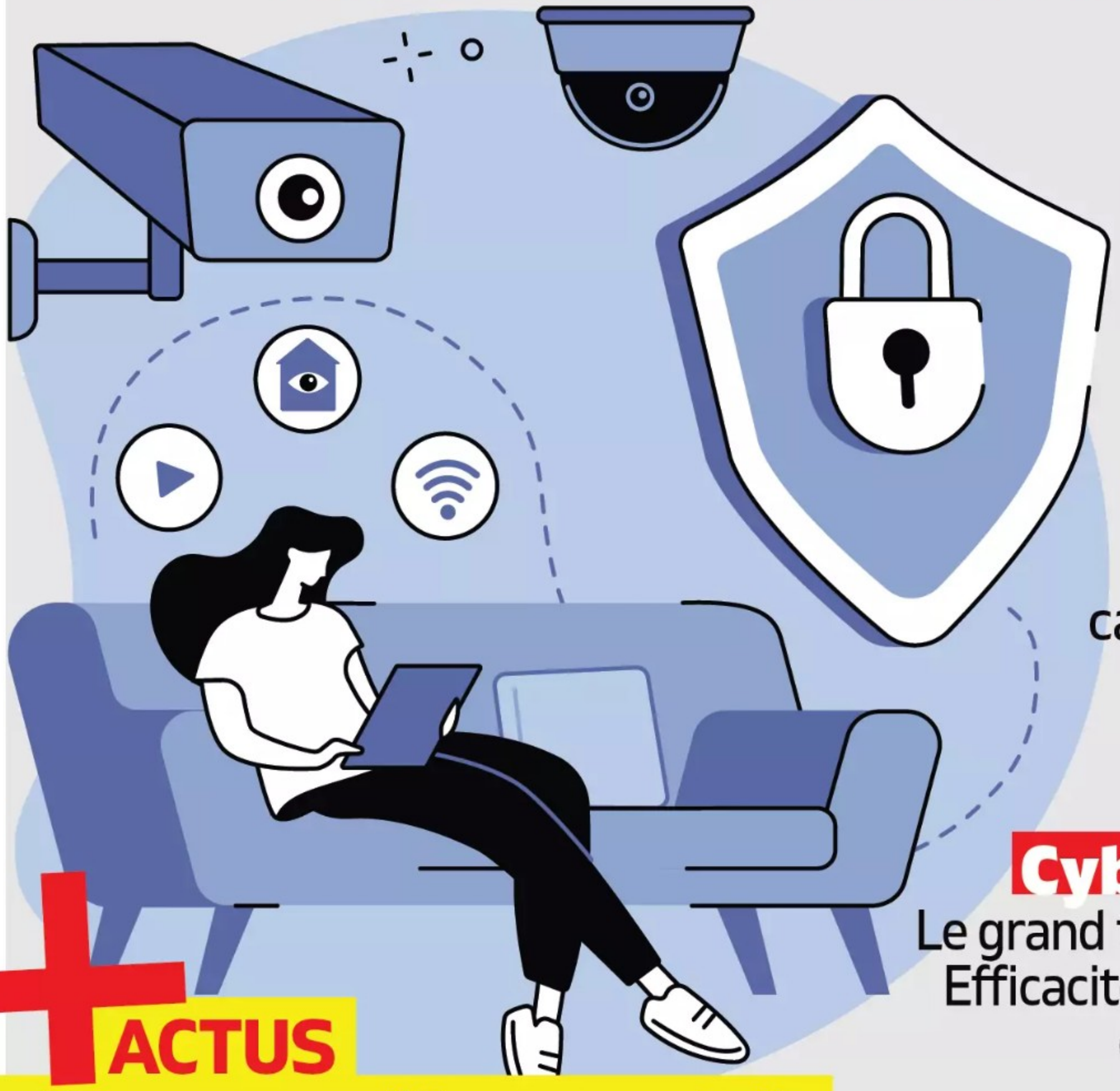
MAI-JUIN 2025 - HORS-SÉRIE 144

NUMÉRO SPÉCIAL

PROTÉGEZ-VOUS

SÉCURITÉ

VOUS N'EN FEREZ JAMAIS TROP !



Vie privée et données
Déjouez les traceurs et les arnaques

Maison
Bien choisir caméras, alarmes et détecteurs connectés

Cyberattaques
Le grand test des antivirus. Efficacité, options, tarifs… **on vous dit tout**

+ ACTUS
Processeurs : l'Europe peut-elle concurrencer la Chine ?

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 - 144 H - F : 5,90 € - RD

Avez-vous bien fermé votre porte ?

Wi-Fi intégré, batterie rechargeable et fonctionnalités avancées.

Découvrez le parfait équilibre entre sécurité et praticité avec la serrure connectée Linus® L2 de Yale, récompensée pour son excellence.
Contrôlez votre porte à distance, partagez l'accès avec vos invités, suivez leurs allées et venues et programmez des routines intelligentes. Dites adieu à la perte de clés et bonjour à la tranquillité d'esprit.

N'attendez plus, adoptez-la dès aujourd'hui !

DESIGN AWARD 2025

A'DESIGN AWARD & COMPETITION WINNER 2024 GOLD

matter

En savoir plus
www.yalehome.fr

works with Google Home

works with alexa

Works with Apple Home

Works with Samsung SmartThings

VISUAL GENERATION/ISTOCKPHOTO

LA CYBERSÉCURITÉ, UN COMBAT DE TOUS LES INSTANTS

Nos vies numériques ressemblent à une forteresse assiégée. Ordinateurs, mobiles, tablettes et objets connectés, rien n'échappe à l'œil avide des cybercriminels, entre virus, ransomwares, phishing et traqueurs. Et il ne s'agit pas seulement d'une question d'argent : notre identité numérique, nos souvenirs, nos habitudes de consommation et parfois même nos relations sociales sont des cibles de choix. Il suffit d'un clic malheureux sur un lien frauduleux ou d'une mise à jour reportée pour que le ver s'infiltre dans le fruit. Or, face à ces menaces, le grand public peine à suivre le rythme effréné des attaques. Pourquoi ? Parce que la cybersécurité est une discipline exigeante, qui demande une vigilance permanente et un minimum de connaissances techniques. Pourtant, des outils existent pour éviter de se transformer en proie facile.

HEUREUSEMENT, IL N'EST PAS NÉCESSAIRE D'ÊTRE UN EXPERT pour se prémunir des menaces numériques. Antivirus, VPN, gestionnaires de mots de passe, authentification à multiples facteurs constituent autant de boucliers susceptibles de nous prémunir des attaques numériques. Encore faut-il les adopter. Trop d'usagers continuent d'utiliser *123456* comme mot de passe et d'ignorer les alertes de mises à jour émises par leurs appareils. Il est urgent d'intégrer la cybersécurité dans notre quotidien, au même titre que boucler sa ceinture en voiture ou verrouiller sa porte en quittant son domicile. Car derrière chaque faille exploitée, il y a un utilisateur qui n'a pas pris les précautions nécessaires. La sensibilisation est donc la clé. Méfiez-vous des réseaux Wifi publics, ne cliquez pas sur des pièges grossiers et activez toutes les options de protection disponibles. Autant de gestes qui feront toute la différence.

SI LE NUMÉRIQUE NOUS EXPOSE À DES RISQUES, il génère aussi des solutions efficaces pour nous protéger dans le «vrai monde». Les objets connectés ne sont pas seulement des failles potentielles, ce sont aussi des outils de sécurité redoutables lorsqu'ils sont bien configurés. Caméras de surveillance intérieures et extérieures, capteurs d'ouverture de porte, détecteurs de fumée intelligents : il n'a jamais été aussi simple et abordable de transformer son domicile en citadelle high-tech. Mais attention, cette défense ne doit pas devenir une faiblesse. Trop souvent, ces dispositifs sont laissés sans grande protection. Accessibles via des mots de passe élémentaires ou mal paramétrés, ces dispositifs deviennent alors de fragiles portes d'entrée menant vers le réseau domestique et les données personnelles. Un comble pour des appareils censés sécuriser le domicile ! Avec le risque que les consommateurs se détournent d'outils au motif qu'ils pourraient devenir des espions au service de pirates, alors même qu'il suffit de les choisir avec soin – en fuyant les matériels sans marque à prix cassé vendus sur Ali Express ou Temu – et en prenant le temps d'activer les options de sécurité prévues par les constructeurs. ● **LA RÉDACTION**

sommaire

HORS SÉRIE #144 MAI-JUIN 2025

ACTUALITÉS

P. 22 CHOISIR

MARCELO TRAD/ISTOCKPHOTO

P. 42

COMPRENDRE

P. 58

MAÎTRISER

42 **DONNÉES PERSONNELLES**
Reprenez le contrôle

DEAGREEZ/ISTOCKPHOTO

50 **GRANDS TRAVAUX**
Échappez aux traceurs

DRAFTER123/ISTOCKPHOTO

PAS À PAS

58 **RÉSEAU PERSONNEL**
Stockez vos fichiers dans votre propre cloud

DA-KUK/ISTOCKPHOTO

CYANO66/ISTOCKPHOTO

68 **GRANDS TRAVAUX**
À la recherche des documents perdus

PAS À PAS

COUVERTURE : VISUAL GENERATION/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 8
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, Théo Brajard, Olivier Brault, Patrick Bertholet, Stéphane Joly, Thierry Lavanant, Sandrine Liger, David Namias, Veditеam.

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 newsletter) 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)

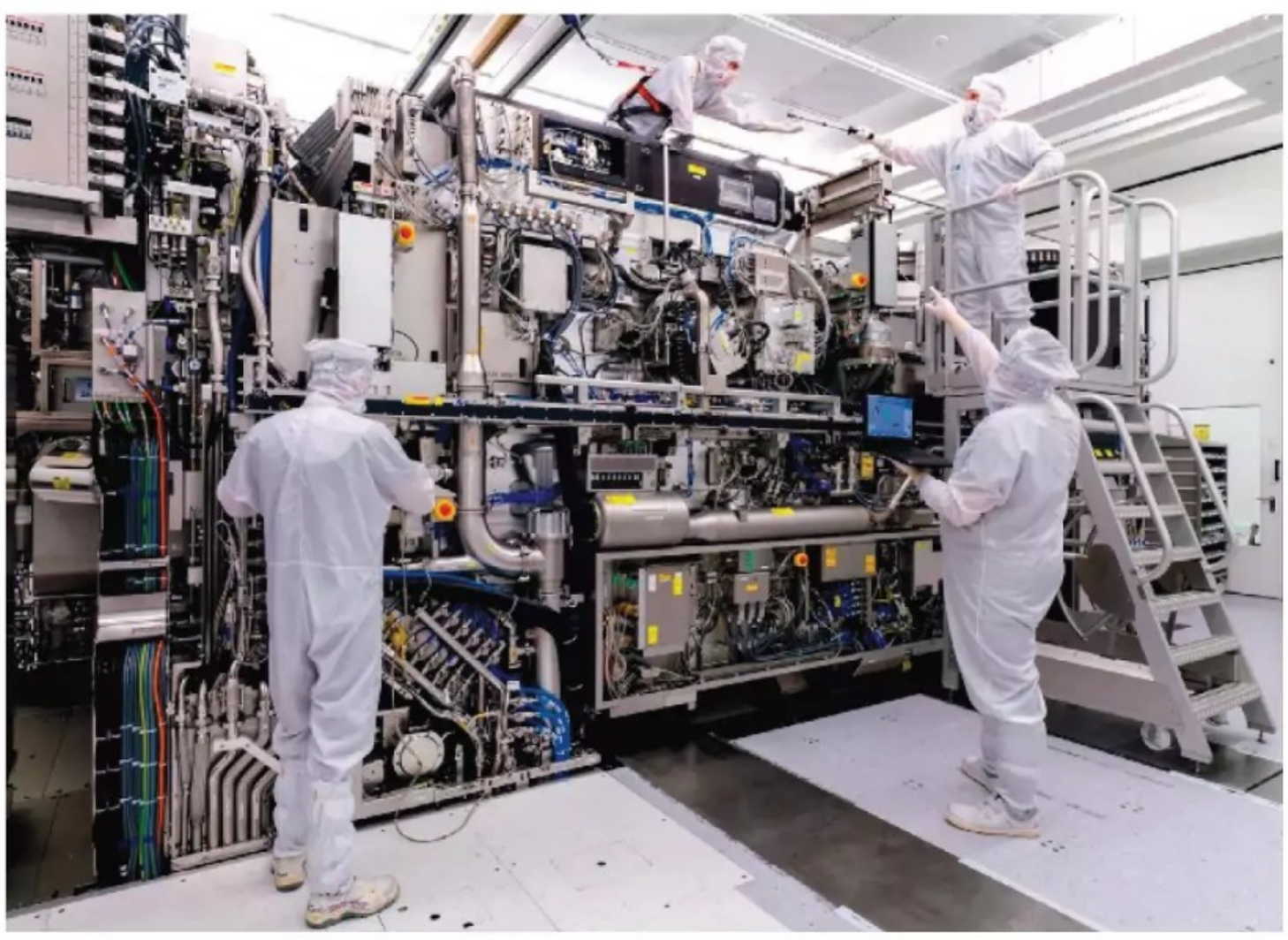
Les prix affichés dans nos pages sont donnés à titre indicatif.
Une réaction, une question ? courrier01@01netlemag.com

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

LE FAIT MARQUANT

PUCES ÉLECTRONIQUES : L'EUROPE PEUT-ELLE REFAIRE SON RETARD ?

Dans la bataille mondiale des semi-conducteurs, la France et l'Europe rêvent de souveraineté. Et pour réduire sa dépendance technologique face aux géants asiatiques, notre continent ne manque pas d'atouts.



ASML

Depuis des décennies, l'industrie des semi-conducteurs est dominée par quelques puissances, principalement asiatiques et américaines. Taïwan et la Corée du Sud dominent aujourd'hui le marché mondial, concentrant plus de la moitié de la production mondiale grâce notamment à TSMC, Mediatek et Samsung. La situation a conduit l'Union européenne – mais aussi le Japon et les États-Unis – à lancer un plan de reconquête technologique ambitieux. Les chiffres sont sans appel : l'Europe ne représente actuellement que 9 % du marché mondial des semi-conducteurs, une place en déclin constant pour un continent qui a pourtant vu naître l'un des pionniers de cette industrie avec Philips Semi-conducteurs. L'objectif fixé par Bruxelles est de passer à 20 % d'ici 2030, un défi jugé complexe par les experts malgré de réels atouts.

Des champions européens

L'Europe héberge en effet deux acteurs essentiels de la filière : le britannique ARM, à l'origine de l'architecture du même nom et qui monnaye à prix d'or ses licences auprès de Qualcomm, Samsung, Google et Apple, et ASML, entreprise néerlandaise fondée par Philips dans les années quatre-vingt, devenue le leader mondial des équipements de lithographie. Ses machines de gravure Extrême Ultraviolet, dont certaines valent jusqu'à 350 millions d'euros l'unité, sont indispensables à la production des puces hautes performances et font le succès de TSMC. Si le prix des équipements et des usines servant à la fabrication des processeurs de dernière génération profite à la trésorerie d'ASML, il constitue un sérieux frein à la relocalisation des usines de semi-conducteurs.

Des projets coûteux

Le budget des trois usines que TSMC s'apprête à implanter en Arizona afin de produire des puces 4nm et 2 nm aux États-Unis devrait ainsi dépasser 60 milliards d'euros ! Les chiffres sont presque aussi affolants pour des puces moins évoluées. Le projet de méga usine lancé par STMicroelectronics, le principal acteur européen du secteur, en atteste. Le coût estimé du site installé à Crolles, près de Grenoble, et qui fabriquera des composants gravés en 22 nm destinés à l'automobile et aux objets connectés atteint 7,5 milliards d'euros. Pour assouvir ses rêves de souveraineté, l'Europe va devoir investir massivement – à l'image du Japon qui a lancé un projet titanesque avec une usine capable de rivaliser avec TSMC en matière de gravure ultrafine à 30 milliards d'euros – et convaincre les industriels d'embrasser sa vision. Un pari loin d'être gagné. Intel, plongé dans une crise profonde, vient ainsi d'acter la suspension de ses implantations en Pologne et en Allemagne. La route promet d'être longue… ●

CONSOMMATION DURABLE

Pourquoi un nouvel indice de réparabilité ?

Depuis le 8 avril, un nouvel indicateur de durabilité vient aider les consommateurs dans leurs achats. Contrairement à l'ancien indice de réparabilité qui se concentrait principalement sur les possibilités de réparation, le nouveau dispositif intègre des critères portant sur **l'usure, la qualité de fabrication et la résistance des appareils après plusieurs années d'utilisation**. Dans un premier temps, l'indice concerne seulement les téléviseurs et les lave-linge.

La 6G se prépare en France

L'Hexagone est en pointe des télécommunications avec le projet européen Hermès. Piloté par une équipe de chercheurs bordelais, le programme a pour objectif le développement d'une **puce 6G offrant des débits 10 à 100 fois supérieurs à la 5G,** tout en consommant jusqu'à 20 fois moins d'énergie.

Clap de fin pour Skype

Né en 2003 en Estonie, le service de messagerie instantané a tiré sa révérence le 5 mai. Racheté par Microsoft en 2011 pour 8,5 milliards de dollars, **Skype a compté jusqu'à 1,3 milliard d'utilisateurs.**

APPLE

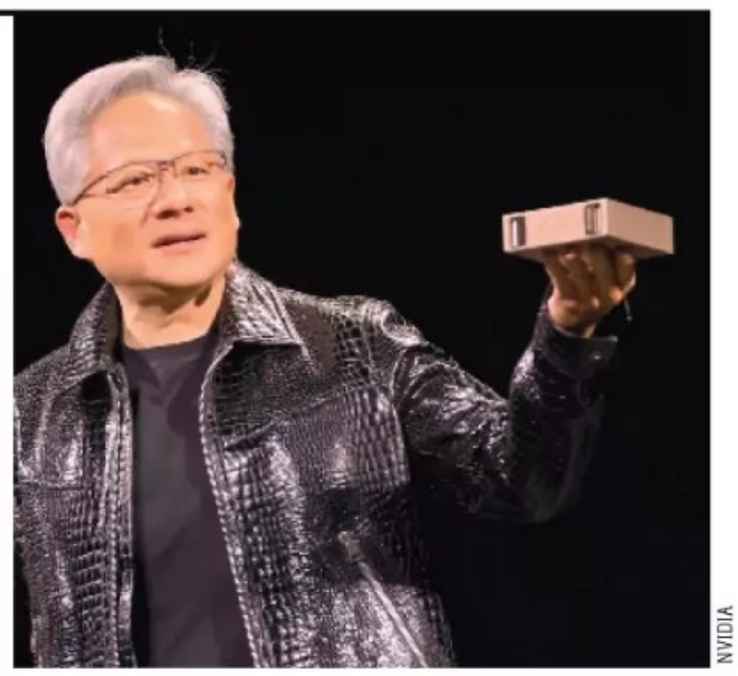
SMARTPHONE

CE CHER IPHONE 16E

L'iPhone SE est mort, vive iPhone 16e ! Plus cher que son prédécesseur (à partir de 719 € contre moins de 600 €), **le nouveau venu monte en gamme**, adoptant un grand écran Oled bord à bord de 6,1 pouces, une prise USB-C, la reconnaissance faciale Face ID et la puce A18. Apparue avec les iPhone 16, celle-ci permet de profiter des fonctions IA d'Apple Intelligence.

INTELLIGENCE ARTIFICIELLE

NVIDIA INVENTE LE MINI SUPERCALCULATEUR !



NVIDIA

Nvidia frappe un grand coup avec son Project DIGITS, un concept d'ordinateur personnel surpuissant pour l'IA destiné aux développeurs et chercheurs en IA. Sous ses airs de mini PC ordinaire, il intègre une puce GB10 Grace Blackwell conçue en partenariat avec MediaTek, l'un des principaux fabricants de SoC pour les téléphones Android. Ce circuit gravé en 3 nm combine un GPU utilisant l'architecture Blackwell inaugurée sur les cartes graphiques GeForce RTX 50 et un CPU ARM doté de 20 cœurs d'exécution. À l'image du modèle Ascent GX10 dévoilé par Asus, les futurs ordinateurs basés sur la plateforme DIGITS accueilleront au moins 128 Mo de mémoire unifiée et seront en mesure de **faire fonctionner en local de grands modèles d'IA comptant jusqu'à 200 milliards de paramètres**, et même 400 milliards en connectant deux unités ! Le tarif devrait débuter à 3 000 € environ, un prix élevé, qu'il convient toutefois de mettre en perspective avec les coûts de location d'infrastructures cloud.

DÉMARCHES

La carte Vitale s'invite dans les mobiles

Après la carte nationale d'identité et le permis de conduire, la carte Vitale se glisse dans nos téléphones.

La nouvelle appli de l'Assurance maladie est désormais disponible sur tout le territoire. Les assurés peuvent y importer la version dématérialisée de leur carte Vitale. L'opération requiert l'appli France Identité et la carte nationale d'identité électronique. Les médecins et pharmaciens peuvent la lire en scannant le QR Code présent dans l'appli ou via un terminal sans contact.

MICROSOFT

Word et Excel en version gratuite

Microsoft teste depuis le début de l'année, aux États-Unis, une version gratuite de sa suite bureautique pour Windows. Les utilisateurs qui rejoignent le **programme bêta doivent composer avec l'affichage de bandeaux publicitaires** dans Word et Excel et l'absence de certaines fonctions, comme l'enregistrement des documents en local (il faut utiliser OneDrive).

XIAOMI

SMARTPHONE

LE XIAOMI 15 ULTRA MISE SUR LA PHOTO

Le porte-étendard du géant chinois Xiaomi entend bousculer la concurrence dans le domaine de la photo. Il affiche ses ambitions avec son imposant bloc de capteurs – dont un téléobjectif périscopique x4,3 – et la présence du logo Leica, à l'origine des optiques. Les résultats impressionnent même en basse luminosité. **Le tarif aussi : 1 500 euros.**

DÉFENSE

L'IA SUR LE PIED DE GUERRE

Au moment où l'Europe renforce ses budgets militaires, la Direction générale de l'armement a passé commande à l'entreprise KNDS pour la modernisation de cent chars Leclerc.
Le blindé lourd de l'armée française accueillera des équipements de combat collaboratif, une tourelle téléopérée et un brouilleur contre les engins explosifs improvisés. Il inaugurera par ailleurs le système de visée Paseo, conçu par Safran, qui utilise l'intelligence artificielle pour détecter et identifier automatiquement les menaces, et ainsi accélérer la prise de décision.
bit.ly/4cyup2x

KNDS

WINDEV® 2025

Nouveau IA Générative de code

DÉVELOPPEZ 10 FOIS PLUS VITE

WINDOWS - LINUX - WEB - SAAS - IOS - ANDROID
AGL DEVOPS - CODE SOURCE UNIQUE
TOUT EN FRANÇAIS (+US+ES)

À PARTIR DE 45€HT PAR MOIS

VU À LA TV EN 2025

TF1

WWW.PCSOFT.FR
info@pcsoft.fr
+(33) 4 67.032.032

SANTÉ CONNECTÉE

Mesure de glycémie, attention ça pique !

Les autorités sanitaires nationales mettent en garde contre les dispositifs de mesure de la glycémie par contact de la peau.

Les montres ou bagues connectées prétendant évaluer le taux de glycémie **présentent un réel danger en raison de leur manque de fiabilité** alertent l'Agence nationale de sécurité du médicament et la Direction générale de la concurrence, de la consommation et de la répression des fraudes. Les deux organismes rappellent que ces capteurs ne peuvent en aucun cas se substituer aux glucomètres médicaux utilisés par les patients souffrant de diabète, basés sur le prélèvement et l'analyse d'une goutte de sang.

PKVITALITY

Canal+, la 4K en option

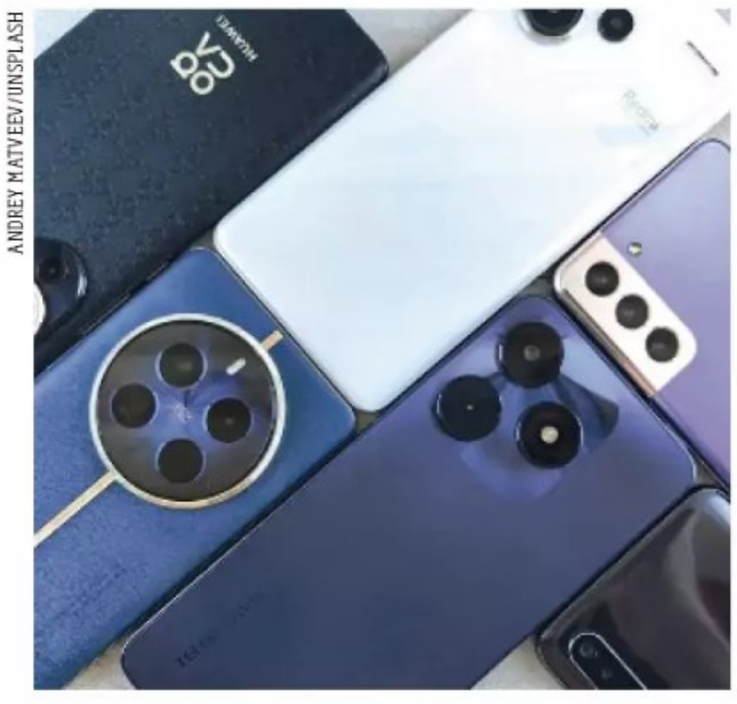
Depuis quelques semaines, les clients Canal + sans engagement via leur Freebox ne bénéficient plus du mode 4K HDR par défaut. Il leur faut désormais souscrire **une option à 5 € par mois** qui comprend, outre les contenus 4K, l'accès aux programmes en HDR et Dolby Atmos.

Apple Intelligence débarque en France

Disponible depuis le 31 mars, iOS 18.4 marque l'arrivée d'Apple Intelligence en Europe. Les utilisateurs français disposant d'un **iPhone 16 ou d'un modèle Pro et Pro Max** de la génération précédente peuvent ainsi profiter de fonctions et outils gérés par l'intelligence artificielle.

SMARTPHONES

DES MOBILES ANDROID AUSSI DURABLES QUE L'IPHONE


ANDREY MATVEEV/UNSPLASH

Le téléphone d'Apple justifie son tarif élevé par sa capacité à défier le temps. Ainsi, six ans après son lancement, le vénérable iPhone XR peut profiter d'iOS 18 au même titre que les récents iPhone 16 ! Un sacré avantage par rapport aux téléphones Android qui doivent attendre de longs mois avant de disposer des mises à jour du système. Quand ils ne sont pas tout bonnement bloqués sur leur version initiale d'Android. **Le rapport de force tend toutefois à s'équilibrer.** Google propose ainsi sept ans de mise à jour système depuis le Pixel 8, imité depuis cette année par Samsung et Honor sur les Galaxy S25, Galaxy Flip 6 et Galaxy Fold 6 pour l'un, sur les Magic Pro 7 et Magic V pour l'autre. La tendance devrait s'étendre aux autres marques puisque Qualcomm, en partenariat avec Google, promet de faciliter la vie des fabricants en assurant huit ans de mises à jour du noyau commun d'Android pour les appareils équipés de sa puce Snapdragon 8 Gen 3.

MSI

PORTABLES

MSI SORT LE GRAND JEU

Taillés pour les fans de jeux vidéo et d'IA, les portables 2025 de MSI associent les derniers processeurs AMD et Intel et les versions mobiles des puces graphiques GeForce RTX 50 de Nvidia. Des monstres de puissance, dont le tarif dépasse pour certains les 3 000 €. Pour ce prix, GeForce RTX 5090 et AMD Ryzen 9 9955HX3D ou Intel Core Ultra 9 285HX sont de la partie.

EN CHIFFRES

LES FRANÇAIS ET L'IA GÉNÉRATIVE

Les Français s'intéressent aux assistants IA, nous apprend une récente étude Ipsos.

88 %

des Français interrogés ont **entendu parler des outils d'IA générative.**

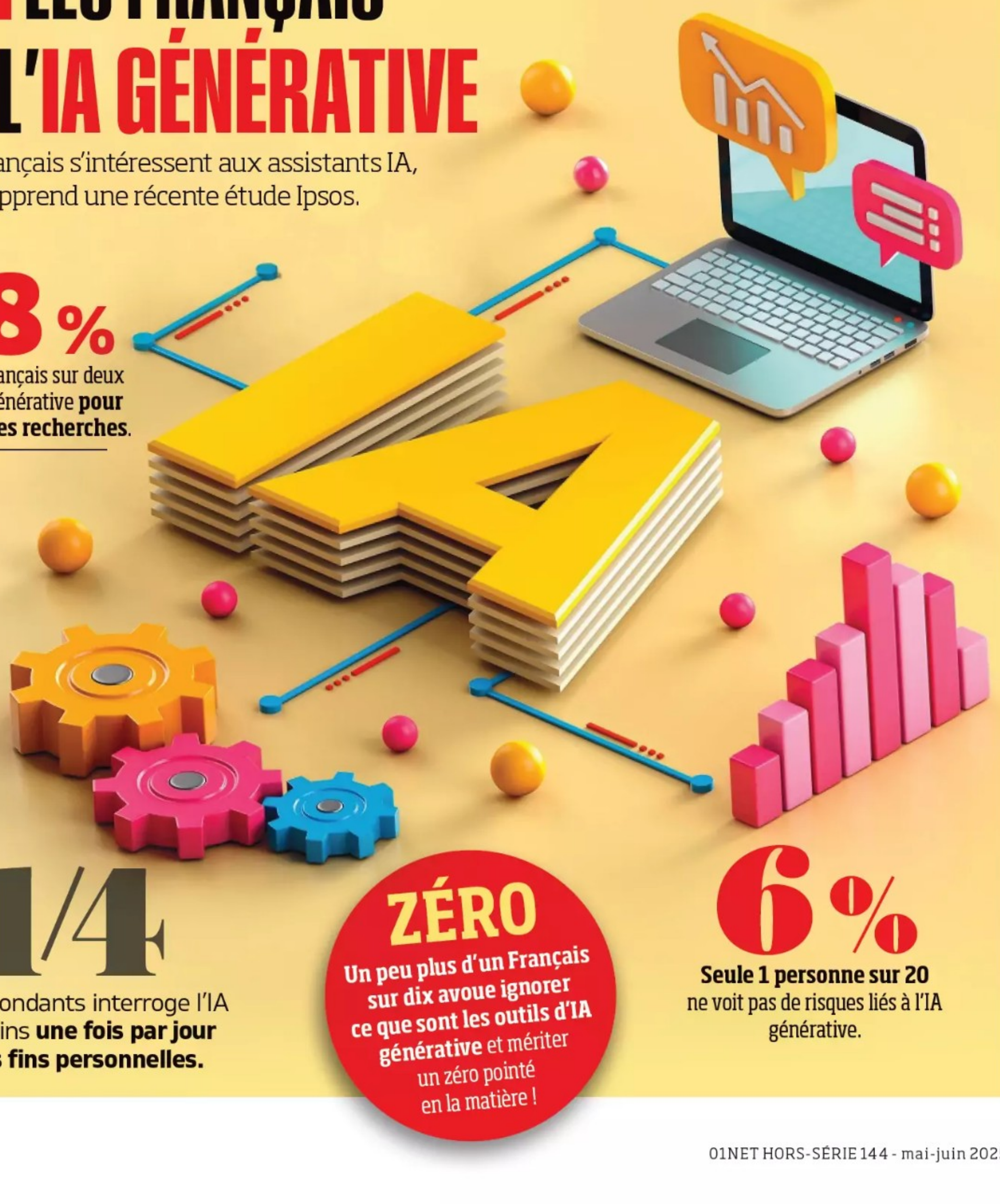
18-24 ans **L'adoption de l'IA générative** est avant tout l'affaire des jeunes générations, puisque 74 % des 18-24 ans utilisent ces outils, contre 17 % pour les 60-75 ans.

1 sur 2

Pour 49 % des sondés, le principal risque lié à l'utilisation des IA génératives **réside dans la création et la propagation de fake news.**

48 %

Près d'un Français sur deux utilise l'IA générative **pour effectuer des recherches**.



1/4

des répondants interroge l'IA au moins **une fois par jour à des fins personnelles.**

ZÉRO

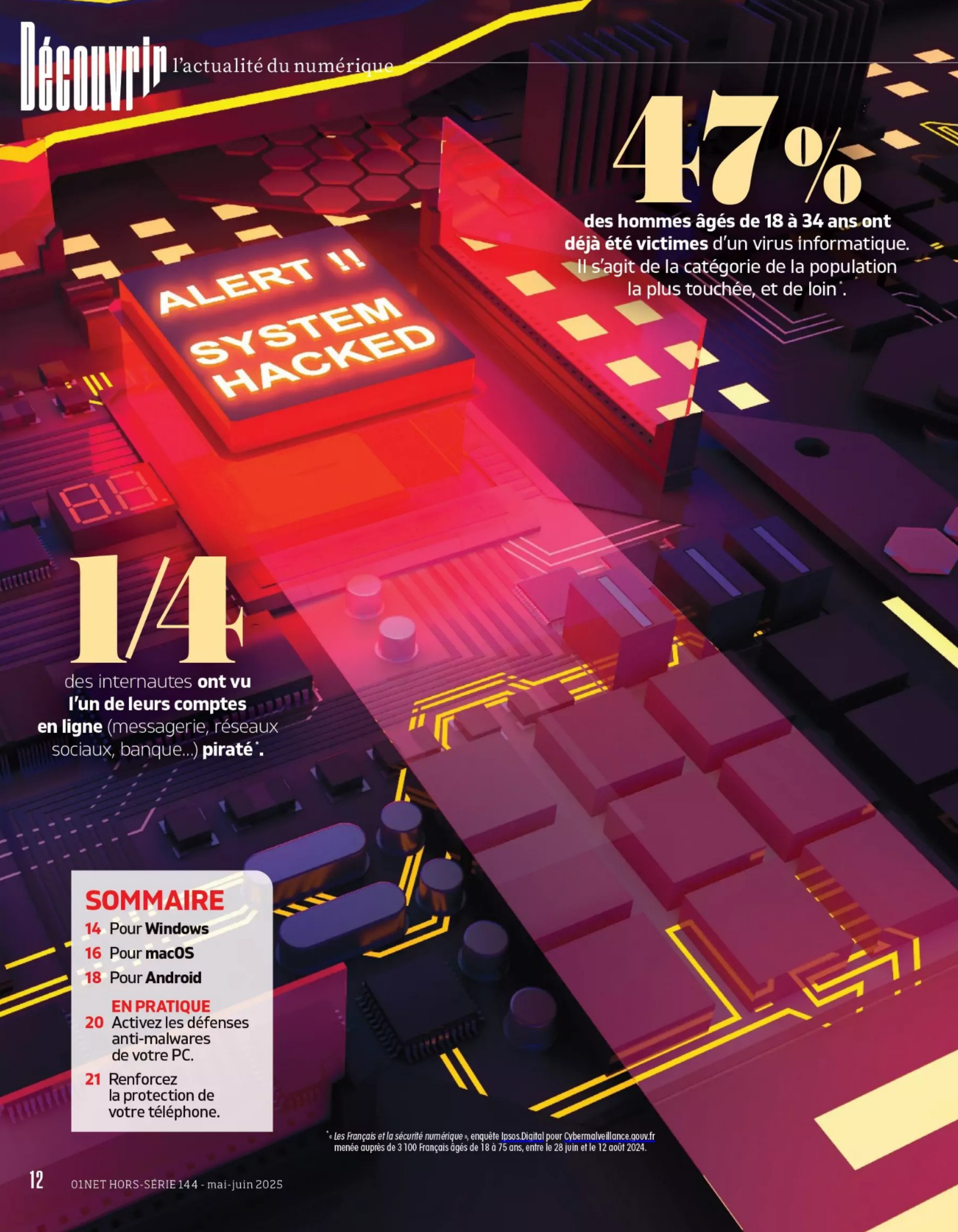
Un peu plus d'un Français sur dix avoue ignorer ce que sont les outils d'IA générative et mériter un zéro pointé en la matière !

6 %

Seule 1 personne sur 20 ne voit pas de risques liés à l'IA générative.

Source : enquête Ipsos pour CESI École d'ingénieurs, « *L'usage de l'intelligence artificielle par les Français* », février 2025.

ALEX SECRET/ISTOCKPHOTO



47 %

des hommes âgés de 18 à 34 ans ont déjà été victimes d'un virus informatique. Il s'agit de la catégorie de la population la plus touchée, et de loin*.

1/4

des internautes **ont vu l'un de leurs comptes en ligne** (messagerie, réseaux sociaux, banque…) **piraté***.

SOMMAIRE

* « *Les Français et la sécurité numérique* », enquête Ipsos.Digital pour Cybermalveillance.gouv.fr menée auprès de 3 100 Français âgés de 18 à 75 ans, entre le 28 juin et le 12 août 2024.

OSELOTE/ISTOCKPHOTO

PC, MAC, SMARTPHONES

LES MEILLEURES SUITES ANTIVIRUS 2025

La cybersécurité n'est plus une option. Car la menace vise désormais tous nos appareils, du smartphone à l'ordinateur en passant par les objets connectés.

Imaginez-vous un instant perdre l'accès à votre compte bancaire, être dépossédé de vos économies à cause d'un faux lien ou encore voir vos échanges privés exposés publiquement. Ces scénarios, autrefois rares, sont devenus monnaie courante. En 2023, les forces de sécurité intérieure ont enregistré 278 770 infractions liées au numérique*, soit une hausse de 40 % en cinq ans. 59 % d'entre elles relevaient d'atteintes aux biens, telles que des escroqueries et arnaques en ligne, et 34,5 % d'atteintes aux personnes, de la diffusion de contenus pédopornographiques au cyberharcèlement.

Depuis l'apparition des premiers virus informatiques, dans les années 1980, les cyberattaques ont bien changé. Aujourd'hui, elles prennent des formes multiples et sophistiquées, comme les rançongiciels (qui bloquent l'accès à des données jusqu'au paiement d'une rançon) ou le *smishing* (contraction des mots SMS et *phishing*), qui désigne le vol de données sensibles (numéros de cartes bancaires, identifiants, etc.) par l'envoi de messages sur le téléphone de la victime, l'expéditeur se faisant souvent passer pour une entité légitime. Face à cette évolution, une seule conclusion s'impose : en plus d'une sensibilisation accrue à ces menaces, il est indispensable de se protéger efficacement. C'est-à-dire de se prémunir contre les virus, c'est la base, mais aussi idéalement de se camoufler derrière le paravent d'un réseau privé virtuel (VPN), tout en préservant les enfants à l'aide d'un contrôle parental. De même faut-il réduire les risques liés au « facteur humain » en confiant la gestion de ses mots de passe à un outil ad hoc.

Des solutions clés en main

Il y a alors deux façons de procéder. La première consiste à sélectionner séparément un outil pour faire face à chaque menace, soit : un pare-feu, un antivirus, un filtre anti-*malwares* (logiciels malveillants), une protection des paiements en ligne, un VPN, un système antispam pour protéger sa messagerie, une solution de contrôle parental et une autre pour gérer les mots de passe. La seconde option revient à s'en remettre à une suite de sécurité qui comprend tout ou partie de ces briques de protection. Ce sont ces solutions que nous avons choisi ici de comparer en nous appuyant sur les tests rigoureux du laboratoire indépendant AV-Test, et en prenant en compte la présence d'une solution VPN, de protection parentale ou de gestion des mots de passe. Mais entendons-nous bien, le problème n'est pas tellement de tomber sur un mauvais antivirus. Tous font, globalement, parfaitement l'affaire. Non, la difficulté est aujourd'hui de se protéger sur tous les fronts. ■■■

11 SUITES DE SÉCURITÉ POUR WINDOWS

Aujourd'hui, une suite de sécurité ne peut plus se contenter d'un pare-feu et d'un antivirus. Un contrôle parental, un gestionnaire de

LOGICIEL / CARACTÉRISTIQUES		KASPERSKY PLUS	ESET HOME SECURITY ULTIMATE	MCAFEE TOTAL PROTECTION	F-SECURE TOTAL	BITDEFENDER TOTAL SECURITY
Site internet		bit.ly/4j08h7x	bit.ly/3WA13tP	bit.ly/4ØvAkj2	bit.ly/3PRf7LJ	bit.ly/4hmsQps
Protection contre les logiciels malveillants *		6/6	6/6	6/6	6/6	6/6
Impact sur les performances du PC *		6/6	6/6	6/6	5,5/6	5,5/6
Capacité à ne pas alerter inutilement *		6/6	6/6	5,5/6	6/6	6/6
VPN		OUI	OUI	OUI	OUI	OUI (200 Mo/jour) **
Contrôle parental		OUI	OUI	OUI VERSION FAMILIALE	OUI	OUI VERSION FAMILY
Gestionnaire de mots de passe		OUI	OUI	OUI	OUI	OUI
Prix annuel pour 1 appareil	PREMIÈRE ANNÉE	30 €	—	—	70 €	—
	DEUXIÈME ANNÉE	55 €				
Prix annuel pour 5 appareils	PREMIÈRE ANNÉE	40 €	120 €	40 €	100 €	50 €
	DEUXIÈME ANNÉE	80 €		110 €		95 €
VERDICT		9,5/10	9/10	9/10	9/10	9/10
NOTRE AVIS		Banni pour les fonctionnaires aux Pays-Bas ou aux États-Unis, l'antivirus russe n'en reste pas moins LA référence pour les particuliers.	Eset vient concurrencer les grands noms du secteur avec une suite complète et efficace. Mais pas la moins chère.	Pour AV-Test, cet antivirus excelle auprès des particuliers avec son faible impact sur les performances de Windows.	Un léger impact sur les performances empêche F-Secure de se hisser parmi les tout meilleurs.	Solution la plus saluée par AV-Test pour les entreprises, Bitdefender pêche seulement par son léger impact sur les performances des PC des particuliers.

▪▪▪ Un premier constat s'impose à nous : aucun des antivirus passés au crible d'AV-Test, sous Windows 10 et 11, macOS ou Android, n'a failli. Tous parviennent, à quelques exceptions près, à bloquer les attaques simulées par le laboratoire indépendant. Pourtant, dans le détail, tous ne se valent pas. Il existe des différences d'approche. Bitdefender et Kaspersky excellent, par exemple, dans l'exercice qui consiste à bloquer les vulnérabilités dites « *zero day* ». Le terme fait référence à une faille n'ayant pas encore été découverte par le développeur d'un programme, mais potentiellement exploitée par des personnes malveillantes. L'expression reflète l'urgence de la situation, car le développeur n'a eu aucun jour (zéro) pour déployer un correctif. Un autre point différenciant concerne l'utilisation de l'intelligence artificielle pour détecter de nouvelles menaces.

L'IA peut s'alerter d'anomalies et couper court à des attaques non encore répertoriées.

L'intelligence artificielle contre les malwares

Habituellement, lorsqu'un *malware* est découvert, les éditeurs d'antivirus analysent son code et en tirent une signature, qu'ils ajoutent à une base de données. Quand la suite de sécurité scanne les fichiers ou les processus en cours d'exécution, toute correspondance indique qu'une menace est présente. Si ce système jouit d'une grande précision et s'avère très fiable, il ne saurait, en revanche, reconnaître un programme malveillant qui n'est pas catalogué. C'est là que l'IA entre en jeu. En

mots de passe et un VPN sont des briques de sécurité indispensables.

AVAST ONE BASIC	NORTON 360	G DATA TOTAL SECURITY	AVIRA INTERNET SECURITY	MICROSOFT DEFENDER ANTIVIRUS	AVG INTERNET SECURITY
bit.ly/4aHZKig	bit.ly/4hw1zkz	bit.ly/4hBJ3Hv	bit.ly/42NaqKD	bit.ly/4h09lFD	bit.ly/4jtvo75
6/6	6/6	6/6	6/6	6/6	6/6
6/6	5,5/6	6/6	6/6	6/6	6/6
6/6	6/6	6/6	6/6	6/6	6/6
OUI (5 Go/semaine)**	OUI	OUI (+30 €)	NON	NON	NON
NON	OUI VERSION DELUXE	OUI	NON	OUI	NON
OUI	OUI	OUI	OUI	NON	NON
Gratuit	**30 €** VERSION STANDARD **75 €** VERSION STANDARD	**50 €**	**27 €** **55 €**	**Inclus avec Windows 11**	**35 €** **73 €**
57 € VERSION SILVER **115 €** VERSION SILVER	**35 €** VERSION DELUXE **105 €** VERSION DELUXE	**82 €**	**75 €**	**99 €** MICROSOFT 365 PERSONNEL	**60 €** 10 APPAREILS **94 €** 10 APPAREILS
8,5/10	**8,5/10**	**8,5/10**	**8/10**	**8/10**	**7/10**
Malgré l'absence de contrôle parental et le VPN limité, la version gratuite assure bien plus que l'essentiel. La version payante est chère.	Malgré son impact sur les performances du PC, Norton 360 demeure, avec son excellent VPN, une référence. Très complet.	Dommage que le VPN ne soit pas inclu dans le prix de base. Il coûte 30 € par an si acheté en même temps que la suite, ou le double !	Efficace, mais l'absence de contrôle parental et de VPN nous pousse à conseiller d'autres produits plus complets.	Si l'antivirus de Windows disposait d'un gestionnaire de mots de passe, il pourrait se suffire à lui-même. À compléter avec le VPN de Edge.	Dépourvu de gestionnaire de mots de passe, de contrôle parental et de VPN, ce dernier étant vendu à part 60 € par an. Dommage…

* Scores AV-Test publiés au mois d'octobre 2024 pour Windows 11. ** Illimité dès la version premium.

LE POINT MÉTHODO

Pour tout ce qui concerne la protection sous Windows 11, nous nous sommes appuyés sur le laboratoire AV-Test. Ses scores (dont certaines valeurs non incluses dans ce tableau) comptent pour 70 % de notre note verdict. Afin de compléter notre moyenne pondérée, nous avons compté pour 15 % la présence d'un VPN, pour 10 % celle d'un gestionnaire de mots de passe et pour 5 % le contrôle parental. Le prix de la solution joue aussi sur le classement.

surveillant en temps réel les actions des fichiers ou des programmes, comme certaines modifications non autorisées ou l'accès à des données sensibles, elle peut s'alerter de manière proactive d'anomalies et couper court à des attaques non encore répertoriées. Pour distinguer les programmes malveillants des programmes légitimes, et bloquer autant que faire se peut les premiers, l'IA s'entraîne sur de gigantesques ensembles de données qu'elle traite au moyen du « *machine learning* », autrement dit des algorithmes d'apprentissage automatique. La suite Norton 360, entre autres, met à profit ces techniques avancées.

La bourse ou les données ?

Un autre sujet d'inquiétude est celui des rançongiciels, dont de nombreux hôpitaux ont fait les (très gros) frais ces dernières années. Les particuliers ne sont pas épargnés, loin de là. L'inoculation suit toujours les mêmes scénarios : ouverture d'une pièce jointe malveillante dans un mail, clic sur un mauvais lien… Le but est d'installer un *malware* qui, en arrière-plan, va chiffrer tout ou partie des données, rendant leur ouverture future impossible à qui ne détient pas la fameuse clé. Le détenteur de cette dernière étant, bien entendu, le pirate informatique. Pire, certains rançongiciels savent se propager à d'autres appareils connectés au même réseau. À la perte de ses photos de famille et de ses documents personnels s'ajoute un stress important. Et il n'est nullement garanti qu'en payant la rançon exigée – quelques centaines, voire milliers d'euros –, l'accès à ces précieuses données soit restitué. Heureusement, là encore, la technologie vient limiter les dégâts de ce qui reste, au départ, ■■■

9 SUITES DE SÉCURITÉ POUR MACOS

À l'heure des rançongiciels et des *malwares*, les appareils d'Apple ne peuvent plus se contenter d'un pare-feu et d'un antivirus.

LOGICIEL / CARACTÉRISTIQUES		NORTON 360	KASPERSKY PREMIUM	BITDEFENDER TOTAL SECURITY	AVAST ONE BASIC
Site internet		bit.ly/4hw1zkz	bit.ly/3PQMjmy	bit.ly/4hmsQps	bit.ly/4autj6J
Protection contre les logiciels malveillants*		6/6	6/6	6/6	6/6
Impact sur les performances du Mac*		6/6	6/6	6/6	6/6
Capacité à ne pas alerter inutilement*		6/6	6/6	6/6	6/6
VPN		OUI	OUI	OUI (200 Mo/jour)**	OUI (5 Go/semaine)**
Contrôle parental		OUI VERSION DELUXE	OUI	OUI VERSION FAMILY	NON
Gestionnaire de mots de passe		OUI	OUI	OUI	OUI
Prix annuel pour 1 appareil	PREMIÈRE ANNÉE	30 € VERSION STANDARD	40 €	—	Gratuit
	DEUXIÈME ANNÉE	75 € VERSION STANDARD	80 €		
Prix annuel pour 5 appareils	PREMIÈRE ANNÉE	35 € VERSION DELUXE	55 €	50 €	57 € VERSION SILVER
	DEUXIÈME ANNÉE	105 € VERSION DELUXE	100 €	95 €	115 € VERSION SILVER
NOTE GLOBALE		10/10	9,5/10	9/10	8,5/10
NOTRE AVIS		Norton 360 l'emporte grâce à un léger avantage tarifaire sur la suite de Kaspersky.	L'antivirus russe, bien que déconseillé par certains États européens, reste l'un des meilleurs auprès des particuliers.	Très bonne et très complète. Dommage que le VPN soit très limité dans la version de base.	L'absence de contrôle parental pénalise Avast. On regrette le tarif plutôt élevé des versions premiums.

■■■ une erreur humaine. Selon AV-Test, les suites de sécurité de ce comparatif s'en sortent globalement très bien, avec une mention spéciale, sous Windows, pour Bitdefender, Eset, McAfee et Microsoft Defender, qui ont stoppé tous les rançongiciels qui leur ont été soumis en décembre 2024. Plus embêtant, Avira n'a, lui, pas réussi à bloquer deux attaques sur les dix scénarios testés. Point de panique, cependant, si vous êtes équipé de cette solution. Il n'y a vraiment pas péril en la demeure et le niveau de protection globale reste très élevé. D'ailleurs, AV-Test lui octroie tout de même sa note maximale sous Windows (100 % de protection contre les attaques « *zero day* » et les logiciels malveillants les plus répandus). C'est plutôt sous macOS et Android qu'il s'avère moins efficace (avec un score de protection de « seulement » 99,5 % et 99,9 % respectivement).

Un VPN augmente la sécurité en ligne en dissimulant votre adresse IP.

Naviguez heureux, naviguez caché

Si nous avons aussi choisi d'intégrer à notre comparatif le VPN, ce n'est pas parce que nous avons des choses à cacher, mais bien parce que cet outil est devenu réellement indispensable. Le principe est de créer une connexion chiffrée entre votre appareil et un serveur distant. Outre le fait de faire croire à un service, par exemple de vidéo à la demande, que l'on se trouve aux États-Unis alors que l'on est en France, ce type de logiciel ou d'application augmente la sécurité en ligne en dissimulant son adresse IP. Mais comment s'équiper ? D'abord, certains sont accessibles gratuitement, tels Hide.me, Proton VPN, TunnelBear ou celui intégré au navigateur internet Opera. Le

F-SECURE TOTAL	TOTALAV TOTAL SECURITY	AVIRA INTERNET SECURITY	AVG INTERNET SECURITY	INTEGO MAC PREMIUM BUNDLE X9
bit.ly/3PRf7LJ	bit.ly/3WA2TKU	bit.ly/3Eb4L6F	bit.ly/3PRrnM8	bit.ly/4hbj89P
6/6	5,5/6	5,5/6	6/6	5/6
6/6	6/6	6/6	6/6	6/6
6/6	6/6	6/6	6/6	6/6
OUI	OUI	NON	NON	NON
OUI	NON	NON	NON	OUI
OUI	OUI	OUI	NON	NON
70 €	—	27 €	35 €	70 €
		55 €	73 €	85 €
100 €	49 € 8 APPAREILS	75 €	60 € 10 APPAREILS	120 €
	149 € 8 APPAREILS		94 € 10 APPAREILS	147 €
8,5/10	7,5/10	7/10	7/10	6/10
Une très bonne suite, mais qui monnaye plus cher ses services. Sans tarif préférentiel la première année.	Quelques fausses alertes de l'antivirus et l'absence de contrôle parental affectent sa note. Dommage.	De petites erreurs de détection, pas de contrôle parental et un VPN très limité (500 Mo/mois) qui s'installe séparément.	Bonne suite, mais pas de VPN, de gestionnaire de mots de passe et de contrôle parental. Regrettable.	Un chouia en dessous niveau protection, mais l'interface a été conçue pour le Mac, et ça se voit. Tarif plutôt élevé.

* Scores AV-Test publiés au mois de décembre 2024, et septembre 2024 dans le cas d'Intego. ** Illimité en version premium.

LE POINT MÉTHODO

Pour tout ce qui concerne la protection sous macOS Sonoma, nous nous sommes appuyés sur le laboratoire AV-Test. Ses scores (dont certaines valeurs non incluses dans ce tableau) comptent pour 70 % de la note verdict. Afin de compléter notre moyenne pondérée, nous avons compté pour 15 % la présence d'un VPN, pour 10 % celle d'un gestionnaire de mots de passe et enfin pour 5 % le contrôle parental. Le prix de la solution joue aussi sur le classement.

problème reste qu'ils sont limités et proposent généralement des débits médiocres. Cela permet d'avancer masqué, mais au ralenti. Pour une utilisation autre que ponctuelle, on peut s'en remettre aux spécialistes que sont CyberGhost, ExpressVPN ou NordVPN. Après une période d'essai d'un mois, ils basculent sur un abonnement souvent modique, de l'ordre de quelques euros mensuels avec un engagement sur plusieurs mois, voire plusieurs années. Efficaces et rapides, nous ne pouvons que les conseiller. Dernière option : beaucoup de suites de sécurité intègrent leur propre solution de VPN. Par rapport aux logiciels spécialisés, on note un nombre inférieur de serveurs et donc de localisations possibles, ce qui, sauf besoins spécifiques, est de peu d'importance. Avec Bitdefender, Norton ou Kaspersky, la vitesse de connexion est au rendez-vous, ce qui reste essentiel. Pour une meilleure protection, tous possèdent une fonction ▪▪▪

COMMENT PAYER BEAUCOUP MOINS CHER

Si vous observez nos tableaux, vous verrez que le tarif bondit après la première année d'abonnement. Mais il existe une astuce pour payer moins cher. Tous les éditeurs sont contraints par le Code de la consommation à informer un mois avant la date anniversaire de la tacite reconduction du contrat pour permettre une éventuelle résiliation. C'est là qu'il faut agir, se rendre dans son espace client et supprimer cette tacite reconduction. Il y a alors fort à parier que vous receviez des offres avantageuses (nous l'avons vérifié avec Bitdefender et Kaspersky) pour vous convaincre de rester. Pour payer encore moins cher, vous pouvez aussi vous en remettre aux outils délivrés avec votre système d'exploitation. Windows Defender obtient ainsi la note maximale en matière de protection contre les virus. Microsoft propose également Secure Network, un VPN intégré au navigateur Edge, et Microsoft Family Safety, un système de contrôle parental pour restreindre les paiements ou le temps d'écran. Côté Mac, XProtect (anti-*malware*) et Gatekeeper (contrôle des applications) fournissent un degré minimal de protection.

9 SUITES DE SÉCURITÉ POUR ANDROID

La gratuité a encore cours au sein des suites de sécurité pour Android. Mais les versions payantes ajoutent des fonctions supplémentaires :

LOGICIEL / CARACTÉRISTIQUES		BITDEFENDER MOBILE SECURITY	F-SECURE TOTAL SECURITY & VPN	MCAFEE SECURITY : ANTIVIRUS VPN	KASPERSKY PREMIUM	ESET MOBILE SECURITY ANTIVIRUS	NORTON 360
Site internet		bit.ly/4azernC	bit.ly/4ØMLykq	bit.ly/4ØYOZVD	bit.ly/4gvNP8B	bit.ly/4aFy6m4	bit.ly/4hw1zkz
Protection contre les logiciels malveillants*		6/6	6/6	6/6	6/6	6/6	6/6
Impact sur les performances du smartphone*		6/6	6/6	6/6	6/6	6/6	6/6
Capacité à ne pas alerter inutilement*		6/6	6/6	6/6	6/6	6/6	6/6
VPN		OUI (200 Mo/jour) **	OUI	OUI	OUI	NON	OUI
Fonction antivol		OUI	OUI	OUI	OUI	OUI	NON
Prix annuel	PREMIÈRE ANNÉE	15 €	20 €	65 €	35 €	10 €	30 €
	DEUXIÈME ANNÉE	25 €			80 €		75 €
NOTE GLOBALE		10/10	9,5/10	9,5/10	9/10	9/10	9/10
NOTRE AVIS		Pour AV-Test, il s'agit de la meilleure suite Android pour les particuliers (award 2024).	Le VPN illimité est son point fort, idéal pour le streaming.	Une protection complète, mais un tarif très élevé face aux concurrents. Le VPN est illimité.	Bien qu'exclu du Play Store, Kaspersky n'en demeure pas moins recommandable selon nous.	Interface claire, protection au top et faible impact sur l'autonomie, il ne manque	Norton reste une référence aussi du côté des mobiles (même offre sous iOS). Manque

▪▪▪ « *kill switch* », qui bloque automatiquement tout le trafic internet de votre appareil si la connexion VPN est interrompue. Bon à savoir, certains services, notamment bancaires, n'apprécient pas ce type de connexions anonymisées et vous bloqueront l'accès. Il faudra désactiver votre VPN le temps de les utiliser.

Ne pas oublier le smartphone

Un peu plus d'un Français sur deux déclare avoir installé un « logiciel antivirus » sur son smartphone, d'après un sondage réalisé par Bitdefender entre décembre 2023 et janvier 2024. Un choix judicieux puisque, selon Thalès, près de 34 millions de cyberattaques ciblant des appareils mobiles ont été recensées dans le monde en 2023, dont plus de 300000 en France. Entre les mails frauduleux, les arnaques sur les réseaux sociaux et les appels indésirables, la réalité nous rappelle constamment qu'employer notre mobile expose à des risques. L'« ingénierie sociale », autrement dit la manipulation psychologique utilisée par des individus malveillants pour inciter des personnes à divulguer des informations confidentielles, joue un rôle essentiel. L'hameçonnage (*phishing*) passe ici par les messageries, mais aussi par la voix (*vishing*) et les SMS (*smishing*). Pour les malfaiteurs, la manœuvre consiste à se faire passer pour un tiers de confiance, soit le représentant d'une institution ou d'une société, soit pour un membre de la famille. Ensuite, c'est un aller simple vers l'arnaque, avec à la clé le vol de données personnelles et celui, pur et simple, de son argent. La première chose à comprendre, même si le cas moqué sur les réseaux de cette dame qui a lâché 830000 euros à un faux Brad Pitt semble paroxystique, est que cela n'arrive pas qu'aux autres. Avec le développement de l'IA générative, les vidéos d'un faux Florent Pagny (bit.ly/4qbsEbq) en témoignent. Le chanteur a dénoncé lui-même la supercherie auprès de TF1, soulignant à quel point

Plus de 300 000 cyberattaques ciblant des mobiles ont été recensées en France en 2023.

VPN plus rapide, protection des paiements en ligne...

AVAST ANTIVIRUS & SÉCURITÉ	AVG ANTIVIRUS GRATUIT	AVIRA ANTIVIRUS SECURITY
bit.ly/4ØQjDQV	bit.ly/4gvftm9	bit.ly/4ØPdjcr
6/6	6/6	6/6
6/6	6/6	6/6
6/6	6/6	5/6
OUI VERSION PREMIUM	OUI VERSION ULTIMATE	OUI (100 Mo/jour)
NON	NON	OUI
Gratuit	**Gratuit**	**Gratuit**
9/10	**9/10**	**8/10**
L'un des antivirus les plus utilisés au monde. La version avec VPN coûte 42 € la première année, puis 94 €.	Le VPN est inclus dans la version la plus chère (80 € puis 130 €/an), ainsi que l'optimisation des performances.	Si la version gratuite est bien, l'offre Phantom Pro (4,95 €/mois) ajoute un VPN illimité. Interface limpide.

* Scores AV-Test de janvier 2025. ** Illimité en version premium (70€ puis 110 €/an).

LE POINT MÉTHODO

Pour comparer les suites de sécurité qui sont dévolues aux smartphones, nous nous sommes appuyés sur les mesures d'AV-Test. Ils ne concernent que les appareils Android, puisque les iPhone répondent à une autre logique sécuritaire. Nous avons noté la protection contre les malwares à hauteur de 70 % de la note finale et ajouté 15 % pour le VPN intégré et autant pour la fonction antivol. Le prix de la solution joue aussi sur le classement.

son apparence et sa voix étaient bien imitées. En dehors d'une méfiance salutaire, les suites de sécurité peuvent donc aider. Mais si la tromperie concerne autant les possesseurs d'iPhone que de téléphones Android, il existe une grande différence de conception logicielle.

Android et iOS pas égaux

C'est une forme d'injustice ou peut-être le prix de la liberté face à l'écosystème fermé d'Apple, argueront les défenseurs d'Android. Mais c'est un fait, les iPhone sont moins susceptibles de subir des attaques virales que les autres smartphones. Plusieurs raisons expliquent cela. Premièrement, iOS recourt à un système dit de « bac à sable », où chaque application fonctionne en silo. Cela signifie qu'elle ne peut pas interagir directement avec d'autres ou accéder au système d'exploitation sans autorisation. Deuxièmement, l'App Store est très sécurisé, ce qui pourrait malgré tout changer avec l'avènement de magasins alternatifs imposé par la Commission européenne. Enfin, et surtout, Apple centralise et coordonne des mises à jour logicielles pour une gamme limitée d'appareils, les siens, et propose un suivi à très long terme. De l'autre côté, l'architecture logicielle plus ouverte d'Android, avec un Play Store moins contrôlé et une plus grande liberté dans les permissions accordées aux applications, se trouve plus souvent mise en défaut. La différence rappelle finalement celle qui existe entre Windows et un macOS naturellement mieux immunisé.

Un antivol renforcé

L'autre risque est bien sûr de se faire subtiliser son mobile. Si voler un iPhone verrouillé peut sembler vain puisque le malfaiteur se retrouvera avec une « brique », il peut y trouver un intérêt. On pense à la revente frauduleuse, parfois à destination de l'étranger, et à la vente pour pièces détachées. Sous iOS comme sous Android, les fonctions de localisation natives sont suffisantes. Elles permettent de géolocaliser l'appareil en temps réel, de le faire sonner à plein volume, de verrouiller l'écran et d'effacer toutes les données à distance. Pour les iPhone, un mode « Perdu » affiche en outre les coordonnées du propriétaire. Les suites de sécurité proposant une fonction antivol permettent un suivi en temps réel de l'appareil sur une carte interactive, mais aussi d'être notifié en cas de changement de carte SIM et de déclencher l'appareil photo pour espérer prendre un cliché du voleur qui essaie de déverrouiller le smartphone. Des fonctions certes inintéressantes, mais qui ne garantissent en rien le retour de son mobile chéri. ●

* D'après le « Rapport annuel sur la cybercriminalité 2024 » du Commandement du ministère de l'Intérieur dans le cyberespace.

UNE BOX POUR LES OBJETS CONNECTÉS ?

Il y a quelques années, des box spécialisées dans la sécurité des appareils connectés étaient vendues par Bitdefender et F-Secure. Alors que les objets connectés pullulent dans nos foyers et se font vecteurs de nouvelles attaques, ces appareils sont en fin de vie et indisponibles à la vente. À la place, Bitdefender préfère travailler avec l'équipementier Netgear pour intégrer dans ses routeurs ses solutions de sécurité. Pour limiter les risques, sachant que nombre de ces accessoires connectés comportent des failles de sécurité, nous conseillons, si possible, de créer un réseau Wifi réservé, distinct de celui utilisé par les ordinateurs, smartphones ou tablettes de la maison. Pour surveiller le réseau domestique, beaucoup de suites de sécurité telles que Bitdefender, Kaspersky, Norton, McAfee ou Trend Micro intègrent ce type de monitoring.

DIFFICULTÉ **MODÉRÉE** TEMPS **20 MIN** DOMAINE **SÉCURITÉ**

ACTIVEZ LES DÉFENSES ANTIMALWARES DE VOTRE PC

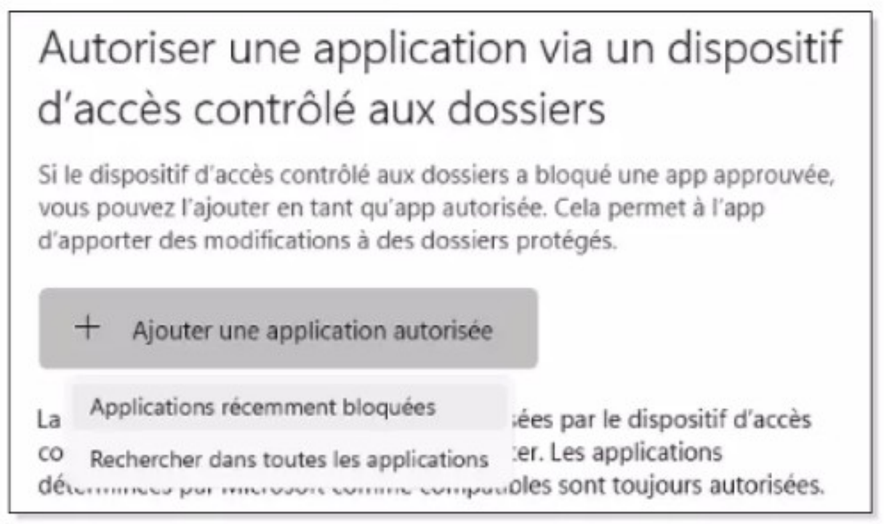
Pas question de perdre de précieuses données à cause d'un rançongiciel. Déjouez les attaques des pirates en activant les défenses antimalwares de votre ordinateur et en contrôlant l'accès à vos dossiers et applis.

1 DÉJOUEZ LES RANSOMWARES

Depuis le Bureau, cliquez sur la flèche de la barre des tâches pour afficher les icônes cachées, puis sur l'icône **Sécurité Windows**. Sélectionnez l'onglet **Protection contre les virus et les menaces** et, dans la section **Protection contre les ransomwares**, pointez sur **Gérer la protection les ransomwares**. Passez le curseur sous l'intitulé **Dispositif d'accès contrôlé aux dossiers** en position **Activé**. Les applications inconnues ou que vous n'avez pas encore approuvées ne peuvent désormais plus accéder aux dossiers Documents, Images, Vidéos, Musique et Favoris de votre compte Windows et de OneDrive, et encore moins les modifier.

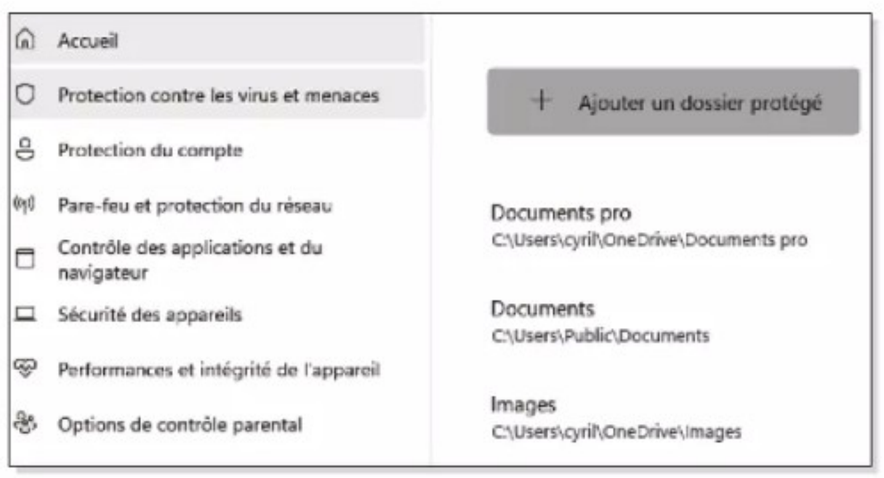
2 CRÉEZ UNE LISTE BLANCHE D'APPLICATIONS

Attention, ce type de protection empêche l'écriture d'une application tierce dans les dossiers sécurisés par Windows Defender. Le message d'erreur n'est pas toujours clair. Par exemple, un jeu peut refuser d'enregistrer une sauvegarde s'effectuant dans le dossier Mes documents sans prévenir qu'il n'a pas accès à cet emplacement. Sous l'intitulé **Dispositif d'accès contrôlé aux dossiers**, pointez sur **Autoriser une app via un dispositif d'accès contrôlé aux dossiers** puis sur le bouton **+ Ajouter une application autorisée**. Pointez sur **Applications récemment bloquées** pour redonner accès aux emplacements sécurisés à un logiciel. Si vous ne trouvez pas le programme dans la liste, utilisez la commande **Rechercher dans toutes les applications**.



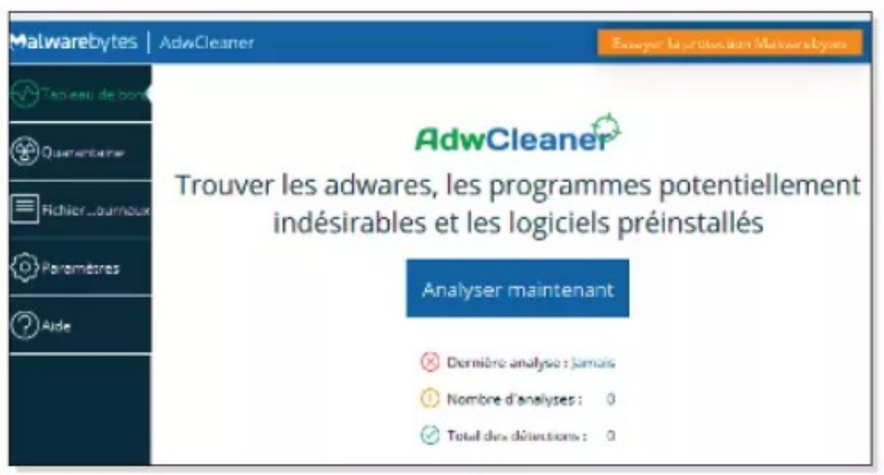
3 AJOUTEZ UN DOSSIER À PROTÉGER

Notez qu'il est possible de sélectionner le dossier C:\Programmes pour ajouter vos logiciels à la liste des applications autorisées à écrire dans les dossiers protégés. Vous pouvez compléter la liste des emplacements à sécuriser. Depuis la page **Protection contre les ransomwares**, cliquez cette fois sur **Dossiers protégés**, puis sur le bouton **+ Ajouter un dossier protégé**. Désignez le répertoire ou le disque où se trouvent des documents importants. Toutes ces précautions ne doivent pas empêcher d'effectuer une sauvegarde régulière des fichiers qui vous sont précieux. Si vous utilisez un disque dur externe, ne le laissez pas constamment connecté à l'ordinateur. Il doit être isolé afin de le protéger en cas d'attaque.



4 ANALYSEZ VOTRE SYSTÈME AVEC ADWCLEANER

Deux sécurités valant mieux qu'une, rendez-vous sur le site bit.ly/3XewBox et enclenchez le bouton **Téléchargement gratuit**. Le programme AdwCleaner ne nécessite pas d'installation. Lancez-le en effectuant un double-clic sur son fichier exécutable, puis pointez sur **Analyser maintenant**, de façon à lancer une recherche de logiciels malveillants sur l'ordinateur. Si un fichier dont l'innocuité ne fait aucun doute déclenche une alerte, on parle de faux positif. Cliquez alors sur **Paramètres**, **Exclusions**, **Ajoutez une exclusion** et désignez l'élément à exclure de l'analyse. Comme toute application portable, AdwCleaner peut être utilisé depuis une clé USB de dépannage.



DIFFICULTÉ **MODÉRÉE** TEMPS **15 MIN** DOMAINE **SÉCURITÉ**

RENFORCEZ LA PROTECTION DE VOTRE TÉLÉPHONE

Protéger son mobile n'est pas une option. C'est une nécessité absolue pour éviter d'exposer votre vie privée et vos données sensibles aux regards indiscrets. Démonstration.

1 VERROUILLEZ L'ACCÈS

Vous aviez renoncé à l'écran de verrouillage de peur d'oublier votre code d'accès ? Alors optez pour d'autres modes de protection plus adaptés. Dans les paramètres d'Android, activez la rubrique **Mot de passe et sécurité**. Vous pouvez opter pour un dispositif d'identification biométrique comme la reconnaissance faciale, si votre mobile dispose d'une caméra compatible, ou le déverrouillage par empreinte digitale.

2 COMPARTIMENTEZ LES DONNÉES

Si vous avez l'habitude de prêter votre téléphone, ne prenez pas le risque que l'emprunteur consulte vos infos personnelles. Anticipez en définissant un profil au périmètre restreint, destiné à vos enfants ou amis, en plus de votre compte utilisateur. Dans **Paramètres**, **Utilisateurs et Comptes**, activez le mode **Plusieurs Utilisateurs**. Appuyez ensuite sur **Ajouter utilisateur** et configurez le nouvel espace.

3 LIMITEZ LA SAISIE SEMI-AUTO

Désactiver le mode de saisie automatique de Google oblige à solliciter davantage votre mémoire quand un mot de passe est exigé. En contrepartie, une personne mal intentionnée ne sera pas en mesure d'accéder à des services en ligne sensibles ou d'effectuer des achats à votre place. Dans le champ de recherche des paramètres d'Android, tapez le mot **semi-automatique**. Actionnez le curseur pour désactiver la fonction.

4 EFFECTUEZ UN CHECK-UP

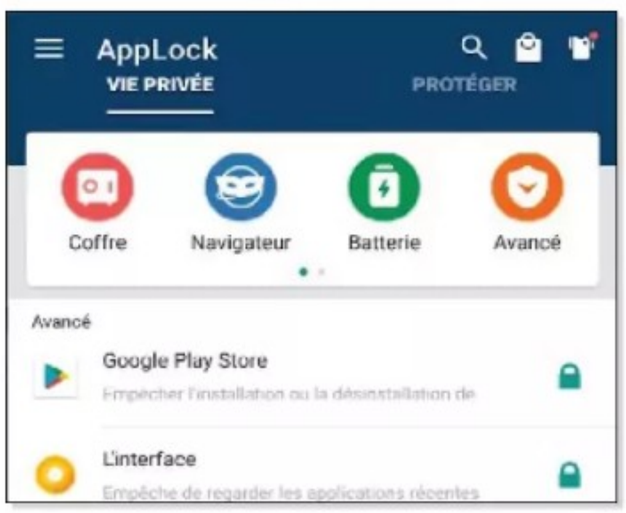
Dans le champ de recherche des **Paramètres** d'Android, saisissez cette fois **check**. Parcourez les résultats et intéressez-vous aux commandes **Check-Up Sécurité** et **Check-Up confidentialité**. Exécutez-les au moins une fois par mois de façon à évaluer la santé globale du téléphone et de votre compte Google. En cas d'anomalie, Android vous suggère des actions de nature à combler les failles de sécurité.

5 ACTIVEZ LA GÉOLOCALISATION

L'outil de géolocalisation de Google ne sert pas seulement à savoir où se trouve votre téléphone en cas de perte ou de vol. Il permet de le verrouiller et d'en effacer le contenu à distance. Activez-le dans les **Paramètres**, en pointant sur **Localiser mon Appareil**, dans la section Google. En cas de besoin, connectez-vous à la page bit.ly/3Re35gf, entrez vos identifiants Google et prenez les mesures qui s'imposent.

6 BLOQUEZ LES APPLICATIONS

Téléchargez AppLock (bit.ly/3x687EP) sur le Play Store. Cette application conditionne l'accès aux applis et aux photos sensibles à la saisie d'un code. Définissez ce dernier, puis verrouillez les contenus de votre choix (réseaux sociaux, messagerie, etc.). Quelqu'un connaissant le code PIN de votre smartphone ne pourra donc pas afficher le contenu des applis.



MAISON CONNECTÉE

NE LAISSEZ AUCUNE CHANCE AUX CAMBRIOLEURS

Plus besoin d'un gros budget pour se protéger des voleurs. Même les ménages peu fortunés peuvent garder un œil sur la maison grâce à des systèmes d'alarme faciles à installer. Mieux, les services de télésurveillance sont désormais accessibles à partir de dix euros par mois et sans engagement.

SOMMAIRE

218 700

cambriolages en 2024

recensés par les services **de police et de gendarmerie.**

Source : Service statistique ministériel de la Sécurité intérieure, mars 2025.

MARCELO TRADYSTOCKPHOTO

SERVICES AVEC ABONNEMENT

LA PROTECTION D'UN VIGILE À DOMICILE (OU PRESQUE)

Une alarme ne peut empêcher un voleur motivé de passer à l'action. Rien ne remplace l'intervention des forces de l'ordre, déclenchée par un service de surveillance.

Si la pandémie du coronavirus avait contribué à une baisse spectaculaire des cambriolages en France, les monte-en-l'air n'ont pas tardé à reprendre du service. Le nombre de délits de ce type a augmenté de 3 % depuis 2022, selon les statistiques du ministère de l'Intérieur. Le niveau reste toutefois inférieur à celui d'avant la crise sanitaire. 218 700 foyers français ont ainsi été victimes d'un cambriolage en 2024, contre 231 900 en 2019. Ce chiffre pourrait toutefois se stabiliser, voire baisser, grâce la démocratisation des systèmes d'alarme et des services de télésurveillance, qui ne sont plus réservés aux propriétaires de villas cossues. Pour quelques dizaines d'euros, caméras Wifi et détecteurs de mouvement permettent de garder un œil sur la maison à distance, de jour comme de nuit. Les foyers ont aussi accès à des solutions plus complètes, comprenant un matériel de détection et les services d'une société spécialisée, qui préviendra les forces de l'ordre en cas d'effraction. En France, le marché est dominé par Verisure et Homiris. Mais ces géants, actifs depuis une trentaine d'années, sont concurrencés par de nouveaux acteurs qui proposent souvent une offre de qualité pour un bien meilleur prix. C'est le cas des firmes françaises Somfy et Altratech (Diagral).

Les télécoms mis à profit

Cependant, la concurrence la plus redoutable pour les Verisure et autres Homiris est peut-être celle des fournisseurs d'accès à internet, qui proposent presque tous une offre de télésurveillance complète. Orange a lancé une solution « Maison protégée » dès 2019, suivi par Free et SFR en 2022. Plus exactement, la firme de Xavier Niel propose le service de télésurveillance de Qiara, une entreprise fondée par un ex-cadre de Free, Alexis Bidinot. « *Le marché de la télésurveillance est verrouillé depuis plusieurs années par un petit nombre d'acteurs, ce qui n'est pas bon pour l'innovation et la transparence des prix* », estime ce dernier. L'offre Qiara Protect comprend ainsi, pour seulement 20 euros par mois, la télésurveillance 24h/24, 7j/7 par la société Sotel, basée près de Toulouse, ainsi qu'une sirène, une caméra, un clavier, un détecteur de mouvement et un détecteur d'ouverture de porte. Et elle n'est pas réservée aux abonnés

Free (qiara.co/protect). Tandis que chez Verisure, il en coûtera à partir de 1400 euros hors taxes pour la mise en service et l'installation du système d'alarme de base, pour une maison, sans compter la télésurveillance à 49,90 euros par mois.

Choisir une solution de sécurité sur le seul critère du prix n'est toutefois pas une bonne idée, surtout pour les grands logements. D'un opérateur à l'autre, la quantité de matériels fournis (caméras, détecteurs de mouvement ou d'ouverture, badges de désactivation…) varie fortement, tout comme le niveau d'assistance. Ici, les spécialistes tels que Verisure ou IMA Protect surpassent les offres de Free ou de Somfy grâce à leur réseau de centres de télésurveillance et leur réactivité en cas de pépin. « *Nous avons plus de 250 agents sur trois sites en France qui se relaient 24h/24 et 7j/7 pour prendre en moins de dix secondes les signaux d'alarme urgents et appeler les forces de l'ordre ou les secours*, détaille Jérôme Gorges, le directeur marketing de Verisure, qui ne craint pas la concurrence. *Le marché de la sécurité est en croissance et encore sous-pénétré en France. Il a donc toujours attiré de nombreux concurrents. Beaucoup ont essayé et sont ressortis du marché après quelques années. Chez Verisure, nous protégeons cinq millions de foyers en Europe depuis plus de trente-cinq ans* ».●

IMA PROTECT

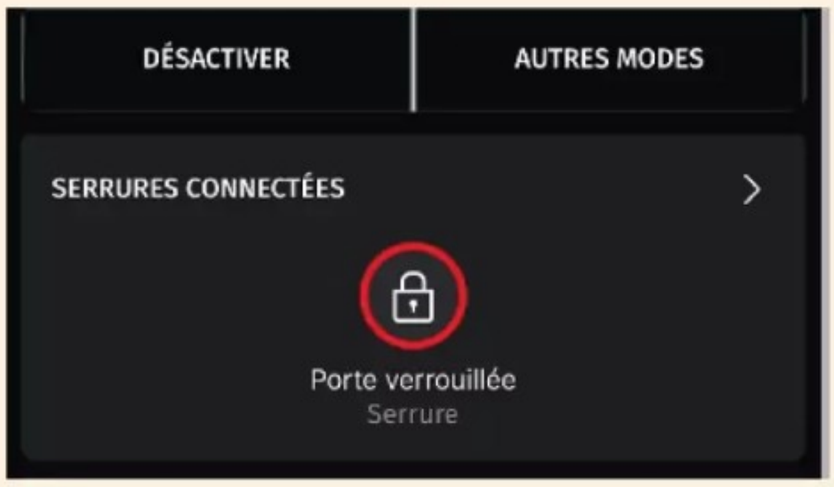
PAS À PAS EXPRESS

UNE SERRURE RELIÉE À LA TÉLÉSURVEILLANCE

Pour une protection dès la porte d'entrée, Verisure propose une **serrure connectée** à l'alarme et à la centrale de surveillance (bit.ly/42batxT).

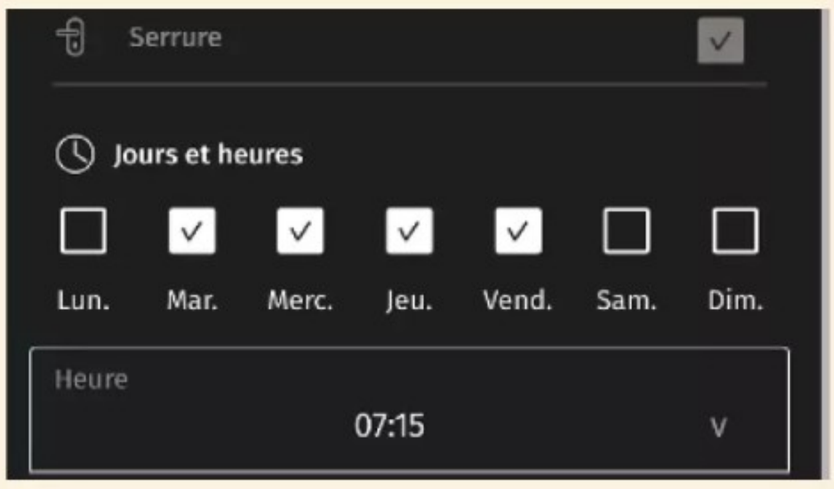
01. DISCRÈTE MAIS À L'AFFÛT DES ALERTES

Dotée de **capteurs de vibrations et de chocs**, cette serrure connectée détecte les tentatives de perçage, crochetage ou coups sur la porte. Et lance l'alerte !



02. CONTRÔLE À DISTANCE DEPUIS L'APPLI

À l'image de l'alarme, la serrure se pilote depuis le mobile. Pratique pour laisser entrer un proche ou un artisan, même si vous êtes au travail ou en vacances.



03. AUTOMATISATION DU VERROUILLAGE

Il est possible de programmer le verrouillage de la serrure selon un planning, ou après une durée précise qui suit la fermeture de la porte. Idéal pour la cave ou le garage.

MACROSTORE/ISTOCKPHOTO

10 SERVICES DE TÉLÉSURVEILLANCE

Matériel, prestations, frais d'abonnement et d'installation... Nous comparons les offres

	OFFRE PROPOSÉE	VERISURE INITIALE	IMA PROTECT TÉLÉSURVEILLANCE TOUT INCLUS	SOMFY PROTECT	SECTOR ALARM ALARME MAISON
	CARACTÉRISTIQUES				
	ABONNEMENT MENSUEL / ENGAGEMENT	59,90 € / 12 mois	37,50 € / 12 mois	10 € / Sans	37,90 € / 12 mois
	MATÉRIEL	INCLUS	INCLUS	350 €	À partir de 800 €
	INSTALLATION PAR L'ENTREPRISE	À partir de 1 400 € (HT)	100 €	NON	OUI (sans frais)
SERVICES	Prestataire	—	—	SOTEL	—
	Télésurveillance 7j/7, 24h/24	OUI	OUI	OUI	OUI
	Application mobile	ANDROID/IOS	ANDROID/IOS	ANDROID/IOS	ANDROID/IOS
	Alertes sur smartphone	OUI	OUI	OUI	OUI
	Intervention d'un agent	OUI	OUI	OUI	OUI
	Appel aux forces de l'ordre sur ligne prioritaire	OUI	OUI	OUI	OUI
	Certification NF A2P	OUI	OUI	NON	NON
	Certification APSAD *	P3	P5	P5 (PRESTATAIRE)	P3
MATÉRIEL FOURNI	Centrale d'alarme	OUI	OUI	OUI	OUI
	Caméra vidéo	1	NON	EN OPTION	NON
	Sirène	1	1	1	1
	Détecteur d'ouverture	1	1	1	1
	Détecteur de mouvement	1	1	1	1
	Détecteur de fumée	EN OPTION	OUI	EN OPTION	OUI
	Clavier ou télécommande	1	1	EN OPTION	1
	Badges de désactivation	3	2	1	3
	Batterie de secours	OUI	OUI	OUI	OUI
	Connexion de secours	GSM ET SIGFOX	GSM	EN OPTION LoRa, 3 €/mois	GSM
NOTES	Richesse de l'offre matérielle	★★★★★	★★★★☆	★★★★½	★★★★☆
	Richesse des services	★★★★★	★★★★★	★★★½☆	★★★★★
	Rapport qualité/prix	★★★☆☆	★★★★☆	★★★★★	★★★☆☆
	Verdict	★★★★½	★★★★½	★★★★½	★★★★☆
	NOTRE AVIS	Une offre complète et fiable, réputée auprès des assureurs et des forces de l'ordre. Mais gare aux tarifs.	Une formule « tout-en-un » de grande qualité, conçue par un spécialiste de l'assistance.	La solution Somfy combine un matériel efficace et un service de télésurveillance sans engagement à bon prix. Mais il faut tout installer.	Une offre proche de celle de Verisure, avec un matériel performant, une installation et un service très pro, mais cher.

* L'APSAD est une certification d'entreprise de sûreté et de sécurité validée par les pouvoirs publics. Elle comprend trois niveaux, P2, P3 et P5, ce dernier étant le plus élevé.

** Non communiqué.

À LA LOUPE

de télésurveillance de base pour une maison.

HOMIRIS (EPS) FORMULE SÉRÉNITÉ	ORANGE MAISON PROTÉGÉE	NEXECUR FORMULE INTÉGRALE	QIARA PROTECT	KIWATCH SÉRÉNITÉ ABSOLUE	SFR MAISON SÉCURISÉE
40 € / 12 mois	**24 €** / 12 mois	**29,90 €** / 12 mois	**20 €** / Sans	**29,90 €** / Sans	**15 €** / Sans
INCLUS	**INCLUS**	**INCLUS**	**INCLUS**	**INCLUS**	**121 €**
OUI (sans frais)	**OUI** (sans frais)	**OUI** (sans frais)	**NON**	**NON**	**NON**
—	PROTECTLINE	—	SOTEL	SCUTUM	EUROP ASSISTANCE
OUI	OUI	OUI	OUI	OUI	NON
ANDROID/IOS	ANDROID/IOS	ANDROID/IOS	ANDROID/IOS	ANDROID/IOS	ANDROID/IOS
OUI	OUI	OUI	OUI	OUI	OUI
OUI	OUI	EN OPTION	NON	OUI	SUR DEMANDE
OUI	OUI	OUI	OUI	OUI	NON
OUI	OUI	OUI	NON	OUI	NC**
P5	P3 (PRESTATAIRE)	P3	P5 (PRESTATAIRE)	P3 (PRESTATAIRE)	NC**
OUI	OUI	OUI	NON	OUI	OUI
NON	EN OPTION	EN OPTION	1	1	1
1	1	1	1	1	EN OPTION
4	2	1	1	1	2
4	3	1	1	2	1
EN OPTION	NON	OUI	NON	EN OPTION	NON
2	1	1	1	1	EN OPTION
NON	4	4	NON	1	EN OPTION
OUI	OUI	OUI	OUI	OUI	OUI
EN OPTION GSM, 3 €/mois	GSM	GSM	SIGFOX	GSM	GSM
★★★★☆	★★★☆☆	★★★☆☆	★★★☆☆	★★★☆☆	★★½☆☆
★★★★☆	★★★★★	★★★½☆	★★★½☆	★★★☆☆	★★★☆☆
★★★★☆	★★★½☆	★★★★☆	★★★★☆	★★★☆☆	★★★☆☆
★★★★☆	★★★★☆	★★★½☆	★★★½☆	★★★☆☆	★★★☆☆
Un matériel complet et fiable, un haut niveau de service, l'offre du groupe EPS vaut bien son prix. Pas de facturation du matériel.	Une offre solide et sérieuse, sans facturation du matériel. Télésurveilllance assurée en partenariat avec Groupama.	Une solution sérieuse et pas trop chère, gérée par le Crédit Agricole. Dommage que l'envoi d'un agent de sécurité soit en option.	On aime la simplicité d'installation du matériel. Dommage que le gardiennage ne soit pas inclus dans la télésurveillance.	La solution la plus complète (et la plus chère) de Kiwatch, avec un vrai système d'alarme. Les autres formules n'intègrent qu'une caméra.	La nouvelle offre de télésurveillance de SFR n'est pas trop chère, mais moins complète que celles de Somfy ou de Qiara.

KITS PRÊTS À L'EMPLOI

6 SYSTÈMES D'ALARME EFFICACES À

Les alarmes à installer soi-même assurent une bonne dissuasion contre les intrus, même sans télésurveillance, et se complètent facilement selon les besoins, en caméras, détecteurs de fumée…

Si la télésurveillance est accessible à presque tous les ménages, l'idée d'accueillir un espion à la maison peut rebuter. Moins intrusifs, les systèmes d'autosurveillance représentent une solution intéressante pour garder un œil sur la maison sans rogner sur sa vie privée, grâce à des modules de détection connectés et une application pour smartphone. Leur installation est simple et rapide, du moins avec les kits de base conçus pour l'intérieur de l'habitation. La majorité intègre une petite centrale reliée à la box du foyer en Ethernet ou en Wifi et de deux à six détecteurs de choc, d'ouverture ou de mouvement, ces derniers pouvant capturer des photos ou de courtes vidéos.

Parmi les nombreux kits du marché, nous avons un faible pour ceux de Somfy, qui propose un énorme catalogue de systèmes et de modules optionnels conçus pour l'intérieur et l'extérieur de l'habitation (détecteurs, sirènes, caméras…). Plus chers, les systèmes Diagral de l'entreprise Altratech se démarquent par leur double système de communication radio (433 et 868 MHz), censé fournir une plus large portée que le Wifi, le Bluetooth ou le protocole Zigbee. Les kits de Diagral sont aussi

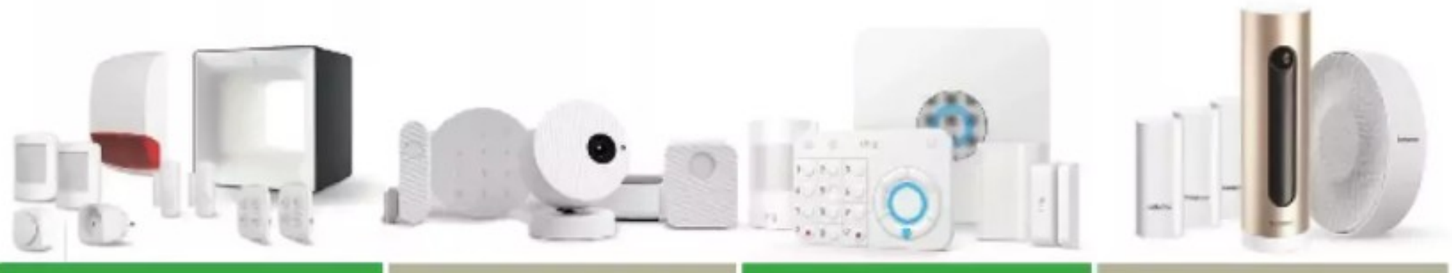
SOMFY

	NOM DU PRODUIT	SOMFY HOME ALARM ESSENTIAL	YALE ALARME INTELLIGENTE STARTER KIT
	CARACTÉRISTIQUES		
	PRIX	460 €	260 €
	Service de télésurveillance	EN OPTION Sotel, 10 €/mois	NON
MATÉRIEL FOURNI	Centrale d'alarme	OUI	OUI
	Caméra vidéo	EN OPTION	EN OPTION
	Sirène	1	1
	Détecteur d'ouverture	3	1
	Détecteur de mouvement	1	1
	Détecteur de fumée	EN OPTION	EN OPTION
	Clavier ou télécommande	EN OPTION	1
	Badge de désactivation	2	1
CARACTÉRISTIQUES	Application mobile	Android/iOS	Android/iOS
	Connectivité	Wifi 2,4 GHz, radio 835 MHz, LPWAN	Radio 868 Mhz, Wifi, Bluetooth
	Connexion de secours	EN OPTION	NON
	Batterie de secours	OUI	NON
	Garantie	5 ANS	2 ANS
NOTES	Richesse de l'offre matérielle	★★★★☆	★★★★☆
	Richesse des services	★★★½☆	★★★½☆
	Rapport qualité/prix	★★★★★	★★★★★
	Verdict	★★★★½	★★★★½
	NOTRE AVIS	Ce kit de base de Somfy s'étend grâce à l'énorme catalogue de modules en option. On aime aussi la télésurveillance à 10 € par mois, sans engagement.	Facile à utiliser et à installer, cette alarme est évolutive, grâce à la gamme de produits complémentaires. On aime aussi la connectivité avec les assistants vocaux.

L'ACCÈS PAR CODE

reste une option pratique avec de jeunes enfants : pas de crainte de perdre son badge ou ses clés.

INSTALLER SOI-MÊME



LEXMAN SYSTÈME D'ALARME SANS FIL CONNECTÉ	QIARA BASIC	RING ALARM - S	NETATMO SYSTÈME D'ALARME VIDÉO INTELLIGENT
350 €	250 €	180 €	260 €
NON	NON	NON	NON
OUI	NON	OUI	NON
EN OPTION	1	EN OPTION	1
2	1	1	1
2	1	1	3
2	1	1	NON
NON	NON	NON	NON
2	1	1	NON
NON	NON	NON	NON
Android/iOS	Android/iOS	Android/iOS	Android/iOS
Wifi, Zigbee	Wifi 2,4 GHz, radio 835 MHz, Sigfox	Wifi, Ethernet, Z-Wave	Wifi, Bluetooth, radio
NON	SIGFOX	EN OPTION	NON
EN OPTION	OUI	OUI	NON
2 ANS	2 ANS	2 ANS	2 ANS
★★★★☆	★★★☆☆	★★★☆☆	★★½☆☆
★★½☆☆	★★★½☆	★★★☆☆	★★½☆☆
★★★☆☆	★★★★☆	★★★☆☆	★★½☆☆
★★★½☆	★★★☆☆	★★½☆☆	★★½☆☆
Leroy-Merlin réussit un bon produit avec son kit d'alarme Lexman, simple à installer et bien pourvu en capteurs. Mais pas d'option de télésurveillance.	Un bon kit de base pour protéger la maison, facile à gérer soi-même. L'offre matérielle est assez pauvre pour l'instant, mais devrait vite s'étoffer.	La marque d'Amazon signe un bon kit pour un appartement ou une petite maison, très facile à gérer avec un mobile. Pas de télésurveillance.	Très élégant, mais d'une faible portée et pauvre en capteurs, convient surtout aux petits appartements. Pas d'option de télésurveillance.

★★★★★ EXCELLENT ★★★★☆ TRÈS BON ★★★☆☆ BON ★★☆☆☆ PASSABLE ★☆☆☆☆ MÉDIOCRE

certifiés NF A2P, un standard de qualité très sévère qui atteste de la résistance de l'alarme aux tentatives de brouillage électronique, de désactivation ou d'arrachage. Si la majorité des équipements grand public n'affichent pas ce niveau technique, ils sont généralement équipés d'un système d'alimentation sur piles ou batterie en cas de coupure de courant, ainsi que d'une connexion de secours GSM, radio LoRa ou Sigfox pour suppléer une panne de Wifi. Attention, celle-ci n'est parfois proposée qu'en option, comme chez Somfy ou Ring.

Une caméra souvent en option

À savoir aussi, de nombreux kits de démarrage n'intègrent aucune caméra vidéo et ne peuvent donc produire une vue en temps réel sur un téléphone. Dans notre sélection, seuls Qiara et Netatmo assurent cette prestation, la caméra devant être choisie en option chez les autres constructeurs. En revanche, tous les kits intègrent des sirènes d'intérieur (plus un modèle d'extérieur dans le kit Lexman de Leroy-Merlin) conçues pour perturber les voleurs grâce à une sonnerie de plus de cent décibels. Bien entendu, les alertes sont aussi notifiées par l'appli mobile afin que l'utilisateur puisse vérifier la nature du problème et solliciter des secours. Attention ici aux appels intempestifs aux forces de l'ordre déclenchés par un matériel défectueux ou mal installé. Un appel injustifié peut être sanctionné par une amende de 450 euros (art. L613-6 du Code de la sécurité intérieure).

Pour autant, l'utilité des systèmes d'alarme est reconnue par les autorités, bien qu'elle ne soit pas mesurée dans les chiffres officiels. « *L'installation de dispositifs d'alarme relève du domaine privé. Nous ne comptabilisons donc pas le nombre de systèmes installés et nous ne réalisons pas de statistiques sur le sujet*, explique le service d'information et des relations publiques de la Gendarmerie (SIRPAG). *Néanmoins, la gendarmerie recommande auprès des particuliers, des entreprises, des collectivités et des mairies l'installation de tels dispositifs pour dissuader et prévenir les cambriolages.* »●

MILJAN ŽIVKOVIĆ/ISTOCKPHOTO

À LA CARTE

ÉQUIPEZ-VOUS À VOTRE RYTHME

En combinant des caméras, des serrures ou des portiers connectés selon ses besoins, il est facile de garder un œil sur la maison et d'en contrôler tous les accès.

Ils assurent un nombre incroyable de fonctions pour des prix de plus en plus bas et avec un niveau de fiabilité très correct. Des centaines d'appareils connectés, installés en quelques minutes avec un simple smartphone, facilitent aujourd'hui non seulement la surveillance, mais aussi la gestion d'une grande partie de la maison. Gestion automatisée de l'éclairage, du chauffage ou même des rideaux, tout est possible, même s'il faut encore composer avec des systèmes de communication différents selon les constructeurs. Les modules Wifi ou Bluetooth sont les plus simples à utiliser, mais accusent souvent une portée limitée et consomment beaucoup d'énergie. Ceux qui exploitent une liaison radio Zigbee – comme chez Leroy-Merlin (gamme Lexman) ou Switchbot –, exigent la mise en place d'un petit boîtier d'interface ou hub entre la box et les appareils.

Privilégier l'écosystème de produits

Pour éviter d'avoir à jongler entre différentes applications mobiles et limiter les problèmes de compatibilité, nous conseillons, autant que possible, de choisir les différents modules chez le même fabricant. Les écosystèmes de produits proposés par Konyks, TP-Link ou SwitchBot sont assez riches pour les besoins courants comme la vidéosurveillance ou l'automatisation de l'éclairage. Pour la sécurisation de la porte d'entrée, nous conseillons les excellents portiers vidéo de Ring, une filiale d'Amazon, ou les serrures connectées de Nuki. Pour les systèmes d'alarme proprement dits, Somfy mérite encore un coup de chapeau pour son offre très complète et entièrement modulaire. ●

Netatmo Caméra Intérieure Advance **250 €**

HAUTE SURVEILLANCE, GRANDE DISCRÉTION

Avec son nouveau pied, sa reconnaissance faciale améliorée et ses alertes plus intelligentes, cette caméra

LA DÉTECTION FACIALE s'affine et limite les alertes inutiles au quotidien.

8,0 SUR 10

CAMÉRA INTÉRIEURE

CAPTEUR VIDÉO 4 MP
RÉSOLUTION 2K (1 440 p)
HDR oui FORMAT paysage
ZOOM x16 MICRO oui
STOCKAGE microSD jusqu'à 32 Go (carte 8 Go classe 10 incluse)
RÉSEAU Wifi 5 (2,4-5 GHz)
DIM. 6,5 x 6,5 x 11,5 cm

POURQUOI ON EN PARLE

Dix ans après avoir lancé l'une des toutes premières caméras connectées capables de reconnaître les visages, Netatmo revient avec une version entièrement revisitée. Cette nouvelle édition conserve l'aspect cylindrique emblématique… mais gagne désormais un pied, qui lui confère un design plus stable et plus moderne. Sous cette nouvelle allure, c'est surtout une refonte logicielle qui s'opère, avec une meilleure détection des mouvements, une compatibilité renforcée et toujours la même promesse de respect total de la vie privée.

UN NOUVEAU PIED La caméra gagne en stabilité et s'installe plus facilement sur un meuble.

ON AIME

C'est la marque de fabrique de Netatmo : ici, pas de cloud imposé ni d'abonnement. Toutes les vidéos sont enregistrées en local, sur une carte microSD fournie, avec possibilité de sauvegarde sur Dropbox ou un NAS. Un positionnement rare, et bienvenu. La reconnaissance faciale, qui avait fait la réputation du modèle original, reste d'une grande efficacité : la caméra sait qui entre dans la pièce, et vous notifie uniquement en cas d'intrus. L'application est toujours aussi claire, avec des réglages fins (créneaux horaires, zones de détection, alertes personnalisées). Le tout fonctionne avec les assistants vocaux HomeKit, Alexa et Google Assistant.

ON AIME MOINS

L'évolution est surtout logicielle. Côté image, rien ne bouge : la caméra reste cantonnée au Full HD, là où la concurrence passe à la 2K, voire à la 4K. Le résultat est propre de jour, mais bruité en basse lumière, ce qui peut affecter la reconnaissance faciale. Autre limitation : l'angle de vue reste modeste, sans motorisation ni large couverture, contrairement à des modèles plus polyvalents. Enfin, l'audio bidirectionnel ne brille pas non plus : voix métalliques et puissance sonore réduite rendent les échanges peu naturels.

CE QUE L'ON EN PENSE

Plus élégante, toujours aussi respectueuse de la vie privée et dispensée d'abonnement, la nouvelle Netatmo Smart Indoor Camera reste fidèle à l'esprit de la marque. Elle ne mise pas sur la surenchère technologique, mais sur la fiabilité, la sécurité et la sobriété. ●

QUALITÉ DE FABRICATION	FONCTIONNALITÉS	PERFORMANCES	ERGONOMIE	RAPPORT QUALITÉ/PRIX
●●●●●●●●●○	●●●●●●●●○○	●●●●●●○○○○	●●●●●●●●○○	●●●●●●●●○○

NETATMO

LA PASSERELLE dispose de 16 Go de stockage et d'un emplacement pour disque dur.

LA CAMÉRA embarque un haut-parleur et un microphone.

Eufy Cam S3 Pro **à partir de 650 €**

SOUS LES YEUX DE L'IA

Ce système de vidéosurveillance extérieur s'appuie sur les algorithmes pour la détection de mouvement.

8,8 SUR 10

CAMÉRA DE SÉCURITÉ

DÉFINITION 4K (3840 x 2160 pixels)
VISION NOCTURNE oui
CHAMP DE VISION 135°
ALIMENTATION batterie (13 000 mAh)
AUTONOMIE 2 mois
CONNECTIVITÉ Wifi 4 (2,4 GHz) STOCKAGE 16 Go, emplacement disque Sata 2,5 pouces (16 To max.)
ÉTANCHÉITÉ IP67
DIMENSIONS 6,9 x 8,2 x 14,3 cm POIDS 534 g

POURQUOI ON EN PARLE

Pour Eufy, la surveillance du domicile se fait désormais en toute autonomie. Ses caméras S3 Pro (le kit de base, vendu 650 euros, en comprend deux) intègrent chacune une batterie de 13 000 milliampères et un petit panneau solaire, pour monter la garde durant des mois sans tomber à plat. Le tout sans fil pour une installation très simple.

ON AIME

Le capteur 4K des caméras produit des prises de vues détaillées y compris la nuit grâce à un traitement de l'image dopé à l'intelligence artificielle. Celui-ci parvient à restituer les couleurs d'un environnement plongé dans le noir. Les caméras sont connectées en Wifi avec la passerelle HomeBase S380. Celle-ci récupère leurs enregistrements et fait le lien avec la box internet de l'utilisateur. Ce dernier peut alors consulter les images à distance, sans frais supplémentaires. Un abonnement est néanmoins requis pour stocker les vidéos sur le cloud, pratique si le matériel subit des dommages. Ce dispositif performant s'accompagne d'une application riche en réglages. Elle permet notamment d'ajuster la sensibilité de la détection de mouvement, d'indiquer des types de cibles à surveiller (animaux, voitures, humains) ou au contraire des zones à ne pas prendre en compte.

ON AIME MOINS

La HomeBase S380 complète la détection de mouvement par une fonction de reconnaissance faciale. Celle-ci doit en principe limiter les fausses alertes, car l'utilisateur peut indiquer quels visages correspondent à des personnes de confiance pour que la caméra les ignore. Mais à plusieurs reprises durant nos tests, l'application a créé divers profils pour la même personne. Notons que la reconnaissance gagne en précision si le propriétaire lui soumet des photos prises par ses soins des visages concernés.

CE QUE L'ON EN PENSE

Ce kit contient ce qu'il faut pour laisser sa maison sous bonne garde pendant de longues périodes. Performantes, les caméras S3 Pro intègrent une détection de mouvement personnalisable et sont capables de distinguer les visages… certes avec quelques ratés. ●

QUALITÉ DE FABRICATION	FONCTIONNALITÉS	PERFORMANCES	ERGONOMIE	RAPPORT QUALITÉ/PRIX
●●●●●●●●●○	●●●●●●●●●○	●●●●●●●●●○	●●●●●●●●●○	●●●●●●●●○○

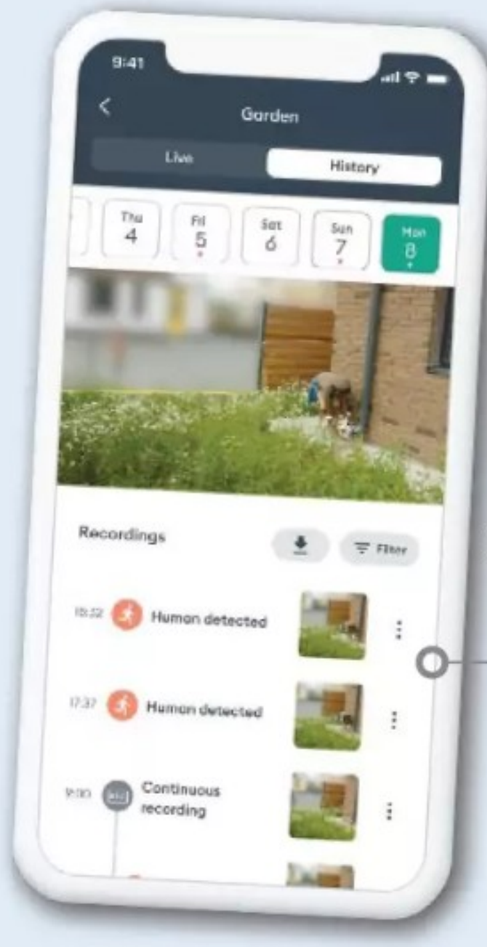
EUFY

Delta Dore Tycam Guard **350 €**

LA SURVEILLANCE DE NUIT COMME DE JOUR

Solide, cette caméra d'extérieur présente une bonne qualité d'image et une vision nocturne en couleurs d'une clarté remarquable.

UNE CARTE SD de 32 Go est fournie avec la caméra.



LE CONTRÔLE À DISTANCE s'effectue via l'appli Tydom.

7,8 SUR 10

CAMÉRA DE SÉCURITÉ

DÉFINITION Full HD, 1920 x 1080 pixels
VISION NOCTURNE oui
CHAMP DE VISION 127 °
ALIMENTATION secteur, POE
CONNECTIVITÉ Wifi 4 (2,4 GHz), Onvif
STOCKAGE carte SD (fournie, 32 Go)
ÉTANCHÉITÉ IP67
DIMENSIONS 19,1 x 7,3 x 9 cm **POIDS** 500 g

POURQUOI ON EN PARLE

Sécuriser un espace extérieur nécessite une technologie fiable et réactive. De conception française, la caméra Tycam Guard se présente comme une solution extérieure haut de gamme, pensée pour offrir une protection optimale.

ON AIME

La Tycam Guard se démarque par son solide boîtier en métal, quand d'autres sont constituées essentiellement de plastique. Elle est certifiée IP67, c'est-à-dire résistante à la poussière et aux grosses intempéries. Côté fonctionnalités, la caméra intègre une sirène de 90 décibels, un interphone directionnel et un projecteur à Led d'environ trente mètres de portée, qui assure une vision en couleurs de nuit. Pratique, le modèle peut être alimenté grâce à son adaptateur secteur (fourni), mais aussi par le biais d'une liaison réseau Power over Ethernet (POE), à l'aide du connecteur serti dans le boîtier. Le capteur vidéo, même cantonné au Full HD (1 920 x 1 080 pixels), produit une image de bonne qualité, sur un angle de vision assez large (130°) pour se passer de motorisation. Les enregistrements sont stockés sur une carte mémoire de 32 gigaoctets livrée avec l'appareil. L'installation se révèle rapide, même si elle requiert la mise en place préalable du boîtier Tycam Home, qui fait l'interface avec la box internet et gère près de 400 périphériques compatibles Zigbee. Comme la caméra, ceux-ci sont pilotés depuis l'application mobile du constructeur, intuitive et riche en réglages. Elle propose une surveillance par zones, la détection des personnes ou des véhicules et la création d'automatismes combinant divers objets connectés Zigbee, Delta Dore ou encore Philips Hue.

ON AIME MOINS

Ce qui coince, c'est le prix du hub radio (Delta Dore Box), indispensable pour exploiter la Tycam : 220 euros qui s'ajoutent à la facture déjà salée de la caméra. Dommage aussi que Delta Dore ne propose pas de service de stockage des images en ligne comme certains de ses concurrents.

CE QUE L'ON EN PENSE

Il faut un solide budget pour s'offrir cette solution de sécurité française, mais le matériel et l'appli de gestion sont de premier ordre. Il manque toutefois un service de cloud pour la sauvegarde des images. ●

QUALITÉ DE FABRICATION	FONCTIONNALITÉS	PERFORMANCES	ERGONOMIE	RAPPORT QUALITÉ/PRIX
●●●●●●●●●○	●●●●●●●○○○	●●●●●●●●○○	●●●●●●●●○○	●●●●●●●○○○

DELTA DORE

LE CLAVIER ET LA PASSERELLE DOMOTIQUE sont inclus dans un pack à 240 €.

ALIMENTÉE PAR QUATRE PILES, la serrure garantit une autonomie de six à neuf mois.

SwitchBot Lock Pro **140 €**

PLUS D'UN TOUR DANS SON APP

Commercialisée à un prix très attractif, la serrure connectée de SwitchBot n'en demeure pas moins robuste et efficace.

9,6 SUR 10

SERRURE CONNECTÉE

COMPATIBILITÉ serrure cylindre européenne, suisse, britannique **CONNECTIQUE** Bluetooth **APPLI** SwitchBot (iOS et Android) **ASSISTANTS VOCAUX** oui (avec le hub) **PILES** 4 x AA (fournies) **AUTONOMIE** de 6 à 9 mois **DIMENSIONS** 12 x 5,9 x 8,4 cm **POIDS** 435 g

POURQUOI ON EN PARLE

La marque chinoise SwitchBot complète sa gamme d'accessoires connectés avec cette serrure dont le premier atout est d'être moins chère que ses concurrentes.

ON AIME

Malgré son prix serré, la serrure connectée Lock Pro n'a rien d'un produit d'entrée de gamme. En partie constituée d'un alliage d'aluminium et de magnésium, elle se révèle non seulement bien finie mais aussi robuste. Par ailleurs, livrée avec différents adaptateurs, elle s'ajuste à tout type de canon, et son couple moteur garantit son fonctionnement même sur une serrure de sécurité multipoint. Il faudra néanmoins veiller à ce que la porte concernée dispose d'un cylindre double entrée, c'est-à-dire dans lequel on peut insérer simultanément une clé de chaque côté, puisque la Lock Pro impose d'en laisser une constamment dedans. Une fois le mécanisme installé, nous avons apprécié les diverses fonctions proposées : le contrôle avec le smartphone, l'ouverture et la fermeture à distance, l'envoi d'alertes en cas d'ouverture de la porte et la création de scénarios (par exemple, pour la verrouiller automatiquement à une heure précise ou lorsque le logement se retrouve vide). Enfin, nous avons trouvé astucieuse la possibilité d'associer la Lock Pro à un clavier extérieur - vendu avec ou à part - permettant de la déverrouiller avec un code, une empreinte digitale ou une carte NFC.

ON AIME MOINS

L'achat de la Lock Pro impose aussi celui d'une passerelle domotique, en l'occurrence le Hub Mini de SwitchBot (+ 20 €). Mais il s'agit là d'une contrainte commune à toutes les marques d'objets connectés.

CE QUE L'ON EN PENSE

Robuste, facile à poser, à utiliser et proposant de nombreuses options, la Lock Pro tient toutes ses promesses. Une nouvelle fois, SwitchBot réussit à nous surprendre avec un objet connecté à l'excellent rapport qualité/prix.●

QUALITÉ DE FABRICATION	FONCTIONNALITÉS	PERFORMANCES	ERGONOMIE	RAPPORT QUALITÉ/PRIX
●●●●●●●●●●	●●●●●●●●●●	●●●●●●●●●●	●●●●●●●●○○	●●●●●●●●●●

SWITCHBOT

DIO DIOCAM-RE02-4G **150 €**

JAMAIS À COURT DE BATTERIE

QUATRE PROJECTEURS assurent une bonne détection de nuit.

8,0 SUR 10

CAMÉRA DE SÉCURITÉ

DÉFINITION Quad XGA (2 048 x 1 536 pixels) **VISION NOCTURNE** oui **CHAMP DE VISION** 120° **ALIMENTATION** panneau solaire 5 W, batterie 9 000 mAh) **AUTONOMIE** jusqu'à 3 mois sans soleil **CONNECTIVITÉ** 4G **STOCKAGE** carte SD (non fournie) **ÉTANCHÉITÉ** IP65 **DIM.** 11 x 22 x 14,5 cm **POIDS** 550 g

Voilà une caméra bien pratique pour garder un œil sur la maison, une cabane ou un chantier. Elle n'a en effet pas besoin de box Wifi ni même de prise électrique pour fonctionner. Elle transmet ses images via le réseau 4G et embarque une batterie de 9 000 milliampères qui assure jusqu'à trois mois d'autonomie. En prime, celle-ci se recharge grâce au petit panneau solaire fourni. Très autonome, la Diocam répond aussi à tous les critères d'une bonne caméra d'extérieur, avec son boîtier résistant aux intempéries, sa tête motorisée sur deux axes et son double système d'éclairage - infrarouge et lumière visible - pour la nuit. Le capteur 2K produit des images très correctes dans toutes les conditions de luminosité, enregistrables sur carte microSD (non fournie) ou visionnables en direct dans l'appli mobile. Cette dernière propose plusieurs réglages de détection de mouvement (humains uniquement, programmation horaire, activation de la sirène…) ainsi que l'orientation du capteur. Un bon ensemble, qui doit toutefois être complété par un abonnement d'accès au réseau 4G. Il faut compter de trois à cinq euros pour un volume d'un à cinq gigaoctets par mois.

CE QUE L'ON EN PENSE

Autonome avec sa connexion 4G, sa batterie et son panneau solaire, cette caméra d'extérieur remplit bien son office. Attention quand même au coût de l'abonnement. ●

QUALITÉ DE FABRICATION	FONCTIONNALITÉS	PERFORMANCES	ERGONOMIE	**RAPPORT QUALITÉ/PRIX**
●●●●●●●●○○	●●●●●●●●○○	●●●●●●●●○○	●●●●●●●●○○	●●●●●●●●○○

CHACON

SwitchBot Pan/Tilt Cam Plus 3K **80 €**

DES DÉTAILS QUI COMPTENT

EN MODE BALAYAGE, l'objectif pivote à 360° à intervalles réguliers.

8,0 SUR 10

CAMÉRA DE SURVEILLANCE

DÉFINITION 3K (2 880 x 1 620 pixels) **VISION NOCTURNE** oui **ALIMENTATION** secteur **CONNECTIVITÉ** Wifi 4 (2,4 GHz) **STOCKAGE** carte SD (non fournie) **DIMENSIONS** 7,8 x 7,8 x 10,7 cm **POIDS** 381 g

Ce n'est pas la caméra de surveillance d'intérieur la moins chère, mais son fabricant chinois cherche à la rendre unique. D'abord, par son mode de fonctionnement extrêmement discret dans l'obscurité. En plus de son capteur 3K (2 880 x 1 620 pixels), la Cam Plus est en effet équipée de Led infrarouges invisibles à l'œil nu (940 nanomètres), contrairement aux Led infrarouges utilisées par la plupart de ses concurrentes. Ce mode d'éclairage nocturne garantit des vidéos de meilleure qualité puisqu'il ne génère aucun reflet. De jour, l'objectif à large ouverture (f/1,6) laisse passer un maximum de lumière, faisant ressortir les couleurs des zones sombres. Par ailleurs, la caméra peut pivoter sur elle-même à 360 degrés horizontalement et à 115 degrés verticalement. Grâce à ses fonctions de détection et de suivi de mouvement, elle peut surveiller et enregistrer tout ce qui se passe autour d'elle, soit sur une carte microSD, soit dans le cloud (abonnement à partir de 4 €/mois). Enfin, l'appareil, pilotable à distance via une application, peut déclencher une alarme sur demande pour effrayer les visiteurs indésirables.

CE QUE L'ON EN PENSE

Facile à installer et à piloter, cette caméra tient ses promesses. On regrette seulement son extrême sensibilité, qui entraîne quelques notifications superflues. Mais il vaut mieux cela que l'inverse… ●

QUALITÉ DE FABRICATION	FONCTIONNALITÉS	PERFORMANCES	ERGONOMIE	**RAPPORT QUALITÉ/PRIX**
●●●●●●●●○○	●●●●●●●●●○	●●●●●●●●○○	●●●●●●●○○○	●●●●●●●●○○

SWITCHBOT

Yale Linus 2 230 €

LAISSEZ VOS CLÉS À LA MAISON !

Facile à installer, ce verrou connecté s'adapte à la plupart des serrures.

8,8 SUR 10

SERRURE CONNECTÉE

COMPATIBILITÉ cylindres européens **APPLI** Yale Home (iOS, Android) **CONNECTIQUE** Bluetooth 5.3, Wifi 2,4-5 GHz **ASSISTANT VOCAUX** Alexa, Google Assistant, Matter, Apple Home **ALIMENTATION** batterie rechargeable lithium-ion **AUTONOMIE MINIMUM** 6 mois **RECHARGE** câble USB-C, env. 4,5 heures **DIM.** 14,6 x 5,2 x 4,6 cm **POIDS** 662 g

L'OUVERTURE DE LA PORTE se commande via l'appli, en Bluetooth ou à distance pour faire entrer un proche.

LA BATTERIE LITHIUM-ION procure de 6 à 24 mois d'autonomie selon l'usage et le mode de communication (Bluetooth ou Wifi).

POURQUOI ON EN PARLE

Filiale du groupe suédois Assa Abloy, premier fabricant mondial de serrures, Yale propose une version améliorée de son verrou connecté. Une nouvelle génération qui s'adapte à toutes les portes, avec ou sans modification du barillet, et qui s'intègre aux principaux écosystèmes domotiques.

ON AIME

La Linus 2 est solide et cela se sent dès la sortie de la boîte. Fabriquée en acier, la serrure pèse en effet 662 grammes. L'installation a requis moins de dix minutes sur notre porte test équipée d'un cylindre européen à double entrée - si votre serrure n'est pas compatible, il suffit de lui substituer le cylindre ajustable Linus, vendu en option (env. 40 €). L'opération nécessite un peu de minutie pour ajuster le débattement gauche et droit de la serrure et s'assurer que le moteur entraîne bien la clé. Une fois la serrure associée au réseau Wifi et appairée en Bluetooth avec le téléphone, tout se passe via l'application Yale Home : l'ouverture de la porte, le paramétrage du verrouillage automatique après un délai donné ou selon la localisation de l'utilisateur, la gestion des autorisations d'accès accordés à des tiers… L'alimentation est assurée par une batterie qui assure jusqu'à six mois d'autonomie et qui se recharge à l'aide d'un câble USB et d'un chargeur de téléphone.

ON AIME MOINS

La serrure peut être associée à un clavier extérieur combinant un clavier numérique et un dispositif biométrique pour la reconnaissance d'empreintes, afin de déverrouiller la porte sans clé ni téléphone. Un accessoire très pratique qui vient toutefois alourdir la facture de… 130 euros !

CE QUE L'ON EN PENSE

Inventeur de la serrure à goupille en 1850, la maison Yale propose un verrou connecté très convaincant. Simple à installer et à configurer, accompagnée d'une application réussie, la Linus 2 est pilotable à distance en Wifi sans avoir à acheter un hub domotique. ●

OUVERTURE SANS CONTACT grâce à la carte NFC contenue dans la boîte.

QUALITÉ DE FABRICATION	FONCTIONNALITÉS	PERFORMANCES	ERGONOMIE	RAPPORT QUALITÉ/PRIX
●●●●●●●●●○	●●●●●●●●●○	●●●●●●●●●○	●●●●●●●●●○	●●●●●●●●○○

YALE

SwitchBot Water Leak Detector **22 €**

LA VIGIE DES MACHINES ET DES SALLES D'EAU

9,6 SUR 10

DÉTECTEUR DE FUITE

CONNECTIVITÉ Bluetooth, Wifi **ALERTES** sonore (jusqu'à 100 dB), vocale, mail, notification mobile
ALIMENTATION 2 piles AAA
AUTONOMIE 2 ans
ÉTANCHÉITÉ IP67
DIMENSIONS 2,9 x 3,2 x 7,8 cm

LES CAPTEURS détectent une flaque à partir de 0,5 mm d'eau.

Voici sans doute l'un des accessoires domotiques les plus pratiques que nous ayons eu l'occasion de tester : un détecteur de fuite d'eau simple mais très efficace. Placé, par exemple, sous l'arrivée ou l'évacuation d'eau d'un évier, d'un ballon d'eau chaude ou d'une machine à laver, le Water Leak Detector alerte dès qu'il décèle des gouttes ou la formation d'une flaque au sol (à partir de 0,5 mm). Il émet alors un signal sonore, dont la durée, la répétition et l'intensité sont réglables (jusqu'à 100 dB pour être entendu de loin), et envoie une notification au mobile du propriétaire à travers une liaison Bluetooth, à condition qu'il se trouve à proximité. L'appareil peut également communiquer avec une passerelle domotique SwitchBot (hub vendu séparément à partir de 35 €) pour avertir l'utilisateur même lorsqu'il est hors de son domicile. Il sera ainsi en mesure de déclencher un scénario domotique automatique. À noter enfin : le Water Leak Detector est totalement étanche à la poussière et à l'eau, et ses piles (deux AAA fournies) n'ont besoin d'être changées que tous les deux ans. Naturellement, une notification est envoyée lorsque le niveau de charge devient faible.

CE QUE L'ON EN PENSE

Cet appareil est tellement pratique qu'il est difficile de lui trouver des défauts. Cependant, pour tirer pleinement parti de sa connectivité, il est recommandé d'acheter un hub, sauf si l'on en possède déjà un. ●

QUALITÉ DE FABRICATION	FONCTIONNALITÉS	PERFORMANCES	ERGONOMIE	RAPPORT QUALITÉ/PRIX
●●●●●●●●●●	●●●●●●●●●●	●●●●●●●●●○	●●●●●●●●●○	●●●●●●●●●●

SWITCHBOT

Ring Battery Video Doorbell Pro **230 €**

LE PETIT INTERPHONE QUI VOIT TOUT

LA CAMÉRA se révèle efficace même de nuit.

8,0 SUR 10

PORTIER VIDÉO

VIDÉO HD 1536 p **VISION NOCTURNE** oui
DÉTECTION DE MOUVEMENT oui
CHAMP DE VISION 150°
BATTERIE 5 800 mAh (adaptateur secteur en option)
AUTONOMIE de 6 à 12 mois
CONNECTIVITÉ Wifi 6
DIMENSIONS 12,8 x 6,2 x 2,8 cm

Venant compléter la gamme de sonnettes connectées de la marque Ring, filiale d'Amazon, ce modèle sans fil se distingue non seulement par le fait qu'il inclut une batterie – ce qui en facilite la pose puisqu'il n'y a plus de fil à faire passer –, mais aussi par la qualité des images haute définition en plan large (150°) captées par sa caméra. Et ce, y compris dans des conditions de faible luminosité. Le micro intégré offre, lui, des conversations claires et fluides avec les visiteurs. En outre, lors de nos tests, nous avons apprécié la précision du détecteur de mouvement de la Battery Video Doorbell Pro, celui-ci pouvant être paramétré pour ne surveiller que certaines zones dans le champ de vision de sa caméra et ainsi éviter les fausses alertes. Il est par ailleurs prévu pour avertir automatiquementde la présence de colis devant la porte – on n'en attendait pas moins de la part d'Amazon ! À noter, enfin, que la sonnette Ring est assortie d'un abonnement facultatif (4 €/mois ou 40 €/an) au service Ring Protect pour stocker en ligne vidéos et photos et recevoir des notifications même en dehors du domicile.

CE QUE L'ON EN PENSE

Voilà un véritable accessoire de sécurité. Facile à installer et à utiliser, la Battery Video Doorbell Pro tient ses promesses et ne pèche que par son prix élevé. ●

QUALITÉ DE FABRICATION	FONCTIONNALITÉS	PERFORMANCES	ERGONOMIE	RAPPORT QUALITÉ/PRIX
●●●●●●●○○○	●●●●●●●●●○	●●●●●●●●●○	●●●●●●●●○○	●●●●●●●○○○

RING

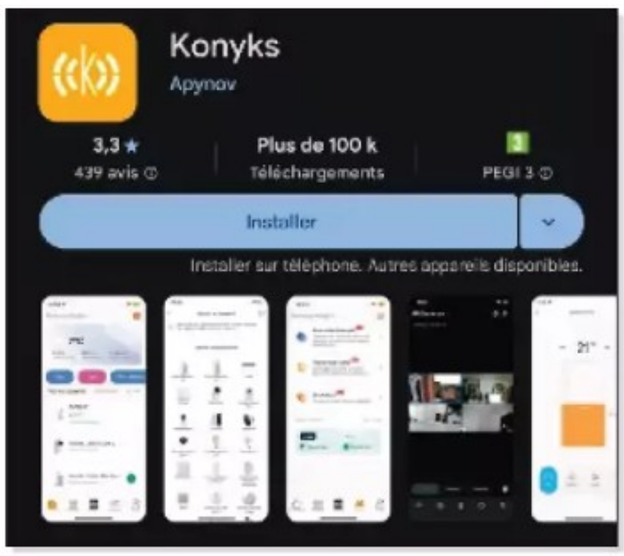
DIFFICULTÉ **MODÉRÉE** TEMPS **30 MIN** DOMAINE **MATÉRIEL**

INSTALLEZ UN KIT DE SÉCURITÉ À LA CARTE

Prévention des incendies, capteur d'intrusion, caméras intérieure et extérieure… Avec le pack Sécurité 360 de Konyks, vous pouvez vous équiper sans vous ruiner et faire évoluer l'installation au gré de vos besoins.

1 INSTALLEZ L'APPLICATION KONYKS

Ouvrez le Play Store de Google (ou l'App Store d'Apple si vous avez un iPhone). Recherchez l'application Konyks et appuyez sur **Installer**. Quittez le Play Store, déployez le volet des notifications d'Android et assurez-vous que le Bluetooth, requis pour l'appairage des appareils, et le Wifi sont activés. Vérifiez ensuite d'être bien connecté au réseau 2,4 GHz de votre box internet – la connexion des caméras et des capteurs qui constituent le pack Sécurité 360 s'avère impossible avec un réseau utilisant la bande des GHz.



2 CRÉEZ UN COMPTE

Touchez le bouton de création de compte et indiquez votre adresse mail. Ouvrez le courriel envoyé par Konyks et saisissez le code de vérification contenu dans le message. Vous devez ensuite associer un mot de passe au nouveau compte et autoriser l'application à émettre des notifications.

3 APPAIREZ LE DÉTECTEUR DE FUMÉE

Ôtez la plaque de fixation au dos du détecteur et retirez la languette en plastique située à l'avant de la batterie pour rétablir l'alimentation. Replacez le cache, puis appuyez à trois reprises sur le bouton de test placé au centre du boîtier afin d'activer le mode d'appairage. Le voyant se met à clignoter en vert rapidement. Revenez à l'application Konyks et pointez sur le bouton **Ajouter un appareil**. Attendez que le Konyks FireSafe 2 apparaisse dans la liste des appareils détectés et effleurez le bouton **Ajouter** à droite de son nom. Saisissez le mot de passe du réseau Wifi et validez avec **Suivant**, **Terminé**.

4 TESTEZ SON FONCTIONNEMENT

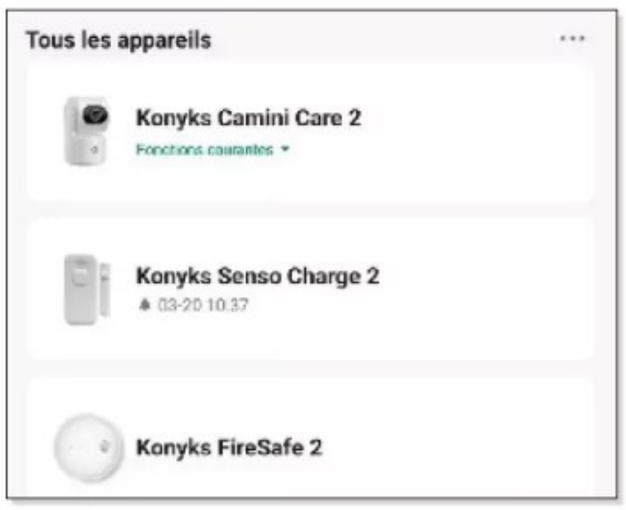
Le message **Test de notification** s'affiche à l'écran. Appuyez sur le bouton **Tester**, puis sur **L'étape suivante** et **Terminer**. Vous basculez vers la page des paramètres de l'appareil. La mention **Normal** doit figurer dans la section **État de détection de fumée**, ainsi que l'indication **Auto-test réussi** en haut de l'historique des événements. Vous pouvez à présent installer le détecteur en le fixant au plafond. Par la suite, en cas de doute sur le fonctionnement du FireSafe 2, pressez le bouton **Test** et relâchez celui-ci dès que l'appareil a émis trois séries de trois bips. Vérifiez ensuite que l'historique de l'application affiche bien le message **Auto test réussi**.

5 AJOUTEZ LE DÉTECTEUR D'OUVERTURE

Après le dispositif de prévention des incendies, place aux systèmes anti-intrusion, à commencer par le détecteur d'ouverture des portes – si vous souhaitez sécuriser plusieurs ouvrants, il vous suffit d'acquérir d'autres modules Senso Charge 2 (20 € pièce). Chargez le boîtier principal, puis basculez l'interrupteur sur **On**. Appuyez pendant cinq secondes avec la pointe d'un stylo sur le bouton **Reset** et relâchez la pression quand le voyant se met à clignoter en rouge. Dans l'application Konyks, pointez sur l'icône + en haut à droite de l'écran, puis sur **Ajouter un appareil** et **Ajouter** à droite du nom du détecteur. Touchez **Suivant** pour l'associer au réseau Wifi et **Terminé**.

6 CALIBREZ LE SENSO CHARGE 2

Sélectionnez le détecteur dans la liste des appareils et appuyez sur **Tester** dans la fenêtre de notification. L'historique du détecteur doit afficher le message **Ouvert**. Vérifiez le bon fonctionnement du dispositif en rapprochant à trois ou quatre millimètres les deux boîtiers composant le module, puis en les écartant. Répétez l'opération. Chaque ouverture ou fermeture donne lieu à une notification et à une inscription dans l'historique du Senso Charge 2. Installez le détecteur sur la porte ou la fenêtre à sécuriser en veillant à respecter l'écartement préconisé entre les deux éléments.

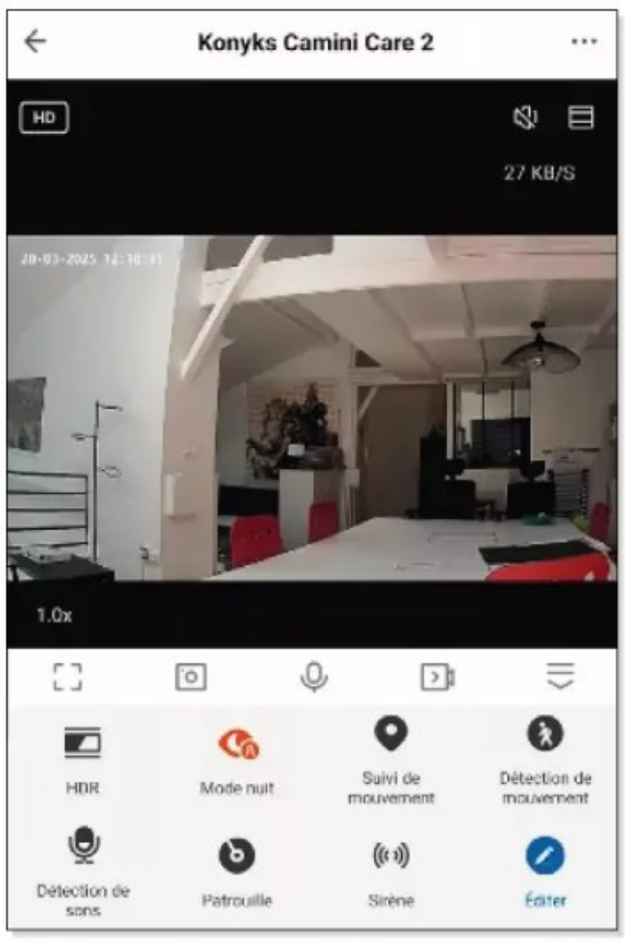


7 PRÉPAREZ LA CAMÉRA D'INTÉRIEUR

Branchez la Camini Care 2 à l'aide du chargeur secteur et du câble USB fournis. Après une courte phase d'activation marquée par l'émission d'un jingle et d'un mouvement de la caméra, ouvrez l'application Konyks. Touchez le bouton + en haut de l'écran, **Ajouter un appareil**, **Ajouter**, **Suivant** et **Terminé**. Procédez au test de notification. Une fois celui-ci mené à bien, vous arrivez sur la page de gestion du périphérique où s'affiche l'image filmée par la caméra. Effleurez l'icône représentant un haut-parleur barré pour vous assurer que le micro fonctionne et que le son est transmis au téléphone.

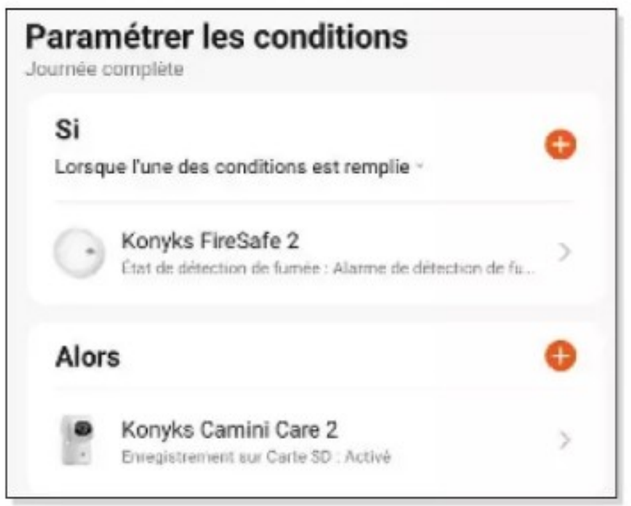
8 AJUSTEZ L'IMAGE

Installez la caméra de façon à filmer la porte d'entrée ou du salon en vous aidant de l'image qui s'affiche dans l'application. Déployez ensuite le volet d'options depuis le bas de la page pour accéder aux réglages. Vous pouvez alors activer les modes **HDR** et **Nuit**, la détection et le suivi de mouvements, la détection des bruits ou encore le mode patrouille qui indique à la caméra de balayer la pièce. Utilisez le raccourci **HD** en haut à gauche de l'écran pour régler la qualité d'image. Touchez les points en haut à droite pour découvrir l'ensemble des paramètres. L'application permet d'ajuster le contraste et la luminosité, de choisir le mode d'enregistrement (en continu ou seulement lorsqu'un événement se produit) ou encore d'activer la sirène en cas de détection d'un mouvement.



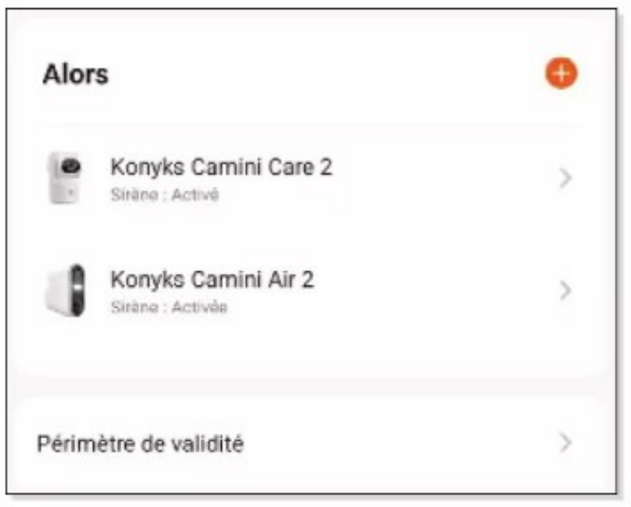
9 ACTIVEZ LA CAMÉRA EXTÉRIEURE

Commencez par connecter la Camini Air 2 au chargeur, appuyez pendant cinq secondes sur le bouton de mise en route dissimulé sous un cache, à côté de l'emplacement microSD et de la prise USB. Touchez le bouton +, **Ajouter un appareil**, **Ajouter**, **Suivant** et **Terminé**. Présentez le QR Code qui s'affiche à l'écran devant le capteur de la caméra. Appuyez sur **J'ai entendu le bip** quand vous entendez le signal sonore de validation. Fixez la caméra et orientez-la de manière à couvrir la porte d'entrée de la maison ou le portail.



10 ÉLABOREZ UN SCÉNARIO

Touchez l'onglet **Scénario** de la barre d'outils inférieure, puis le bouton **Créer une scène** et l'option **Lorsque le statut de l'appareil change**. Sélectionnez le premier périphérique concerné. Pour obtenir des images de la cuisine ou du salon en cas d'alerte incendie, choisissez le détecteur de fumée FireSafe 2 et poursuivez en choisissant **État de détection de la fumée** et **Alarme de détection de fumée**. Appuyez sur la section **Alors** et **Choisir un appareil**. Désignez la caméra intérieure chargée de la surveillance de la zone concernée et pointez sur **Activé**, **Enregistrer**, **Confirmer**.



11 DÉCLENCHEZ PLUSIEURS ACTIONS

Vous souhaitez faire retentir une alarme lorsque le détecteur d'ouverture décèle une intrusion ? Touchez **Scénario**, **Créer une scène** et **Lorsque le statut de l'appareil change**. Sélectionnez le Senso Charge 2 et **État du détecteur d'ouverture**, **Ouvert**. Pointez sur **Alors**, **Choisir un appareil** et désignez la caméra intérieure. Accédez au menu **Sirène** et cochez l'option **Activé**. Validez avec **Enregistrer**, **Suivant**. Pour faire bonne mesure, vous pouvez faire retentir également la sirène de la caméra extérieure : appuyez sur l'icône + dans la section **Alors** pour ajouter cette action au scénario. Quand vous avez fini, validez avec **Enregistrer**.

5 CONSEILS POUR ACHETER

UN DÉTECTEUR DE FUMÉE CONNECTÉ

Réussir un achat high-tech tient parfois à un détail. Voici les aspects techniques à garder en tête pour choisir un détecteur de fumée qui répondra à vos besoins.

1

LA SÉCURITÉ

VÉRIFIER LA CONFORMITÉ

Assurez-vous que le détecteur de fumée est **conforme à la norme européenne EN 14604,** qui garantit que le produit répond aux exigences de sécurité. Un détecteur non conforme peut ne pas être fiable en cas d'incendie.

2

PENSER ÉCOSYSTÈME

Si vous avez déjà un système de maison connectée (Google Home, Amazon Alexa ou Apple HomeKit), optez pour un détecteur compatible. Cela vous permettra de **gérer les alertes via votre application centrale** et d'interconnecter le détecteur avec d'autres équipements comme des caméras ou des alarmes.

ICEMAN/ISTOCKPHOTO

3

L'ENTRETIEN

VIVE LA SIMPLICITÉ !

Privilégiez un détecteur facile à installer, sans câblage, et à entretenir, avec une option pour tester régulièrement son bon fonctionnement via une application ou directement sur l'appareil. Certains modèles vous avertissent s'ils nécessitent un nettoyage.

4

L'ALARME

AUSSI SUR LE SMARTPHONE

Choisissez un modèle qui envoie des notifications instantanées sur votre smartphone en cas de détection de fumée, même lorsque vous êtes à l'extérieur. Cela vous permet de réagir vite, pour **évacuer votre domicile et contacter les pompiers.**

5

L'AUTONOMIE

AU MOINS PLUSIEURS ANNÉES

La durée de vie de la batterie est essentielle. Certaines sont remplaçables, d'autres dites de « longue durée » (dix ans). **Veillez à choisir un détecteur qui vous alerte** lorsqu'il n'a presque plus de jus.

ABONNEZ-VOUS À 01NET

LE MAGAZINE DU NUMÉRIQUE

ET RECEVEZ UN PACK DE DEUX AMPOULES LED***

Deux ampoules connectées E27 Couleurs + Blanc réglable

PHOTO NON CONTRACTUELLE

ABONNEMENT 22 NUMÉROS + LES HORS-SÉRIES + LES NEWSLETTERS + LES ÉDITIONS DIGITALES

EN CADEAU LE PACK DE 2 AMPOULES LED

89 € au lieu de ~~134,40 €~~*

Je règle en une fois par **CARTE BANCAIRE**, **je m'abonne en ligne en un clic** sur **bit.ly/ABICBAMP** ou en flashant ce **QR Code**

ou en 4 fois sans frais soit 22,25€ x4 sur **bit.ly/ABO4XAMP**

01NET DES TECHNOLOGIES ET DES HOMMES

Bulletin d'abonnement à retourner SOUS ENVELOPPE NON AFFRANCHIE à :

01net - Service abonnements - Libre réponse 43420 - 60647 Chantilly Cedex

Si je préfère parler à un conseiller client, je contacte le **01 70 37 31 74** (Numéro non surtaxé)

OUI, je souhaite m'abonner à 01NET Magazine et recevoir **les 22 prochains numéros + Les hors-série + Les newsletters et en cadeau le pack d'ampoules LED E27** au prix exceptionnel de **89 €** au lieu de **134,40 €***

Je règle par CHÈQUE

Je joins mon règlement par :

❑ Chèque bancaire à l'ordre de **01NET Magazine**

*Prix de vente au numéro. **Mention facultative. Vous êtes invité à consulter les conditions générales de vente sur bit.ly/38U8lTd avant toute souscription. Offre valable jusqu'au 31/12/2025. L'éditeur s'engage à livrer votre magazine sous un délai maximum de cinq semaines.***L'éditeur se réserve le droit de remplacer le cadeau de bienvenue par une prime équivalente en cas de rupture de stock. L'éditeur s'engage à livrer le cadeau sous un délai maximum de huit semaines. Les informations personnelles requises sont nécessaires à 01net Mag pour la mise en place et la gestion de votre abonnement. Elles pourront être cédées à des partenaires commerciaux pour une finalité de prospection commerciale sauf si vous cochez la case ci-contre ❐. Conformément à la loi « informatique et libertés » du 6 janvier 1978, vous disposez d'un droit d'accès, de rectification, de limitation, d'opposition et de suppression des données que vous avez transmises en adressant un courrier à 01net Mag.

Mes coordonnées: ☐ Mme ☐ M.

Nom : .....

Prénom : .....

Adresse : .....

Code postal : .....

Localité : .....

Téléphone portable** ____ ____ ____ ____ ____

Date de naissance** ____ ____ ____ ____ ____ ____

E-MAIL OBLIGATOIRE POUR RECEVOIR LA VERSION DIGITALE ET LES NEWSLETTERS

E-mail : ..... @ .....

J'accepte de recevoir les offres des partenaires de 01net ❑ Oui ❑ Non

Siège social : 01net Mag - 16, rue des Rasselins, 75020 Paris - SAS au capital de 10 000 € - RCS Paris 799 351 341

PAGEAMP

SOMMAIRE

DONNÉES PERSONNELLES

REPRENEZ LE CONTRÔLE

Si c'est gratuit, c'est que vous êtes le produit. La célèbre formule colle parfaitement aux applications et aux réseaux sociaux, qui pour la plupart absorbent nos données pour mieux nous cibler. Mais il est possible de retrouver un peu de liberté.

IVAN TRAIMAK/ISTOCKPHOTO

Vous ne les avez jamais rencontrés, mais ils en savent plus sur vous que certains de vos proches. Ils ne connaissent pas seulement votre nom, votre âge et votre adresse, mais aussi vos moindres déplacements, vos goûts en matière de musique ou de cinéma, vos amis ou les membres de votre famille. Ils peuvent savoir si vous vous plaisez à votre travail ou si vous vous inquiétez pour votre santé. Le tout grâce à votre smartphone, un mouchard bien plus efficace et discret qu'un détective privé. Jour après jour, il fournit une incroyable quantité d'informations à des dizaines d'entreprises, souvent situées aux États-Unis ou en Asie. La collecte est organisée par Google, Apple, Meta, Amazon, Microsoft, mais aussi par des fabricants de smartphones comme Huawei, Samsung ou Xiaomi, des éditeurs d'applis comme ByteDance (la maison mère de TikTok) et quantité d'autres acteurs moins connus.

Car les informations transmises par nos mobiles valent de l'or. Grâce à une connaissance très précise des internautes, les entreprises du web sont en mesure de leur proposer des services et des produits entièrement personnalisés par le biais de publicités ciblées. À l'image de ce spot télé des années 1980 qui visait « *la ménagère de moins de 50 ans* », les entreprises du web sont à même de cibler chaque client potentiel individuellement. Champion du genre, Google tire près de 80 % de ses revenus grâce à la pub, avec sa puissante régie Ads et son riche écosystème d'applications. La firme profite évidemment de la puissance de son moteur de recherche, le plus utilisé au monde, mais aussi de la popularité de Maps pour la navigation, de YouTube et de sa galaxie de services mobiles sous Android.

Des informations qui valent de l'or

Dans ses « *règles de confidentialité et conditions d'utilisation* », Google détaille les (très) nombreux paramètres collectés par ses soins, à commencer par les informations personnelles, c'est-à-dire celles qui se rapportent à une personne physique identifiée ou identifiable par son nom, selon la définition de la Commission nationale de l'informatique et des libertés (Cnil). Il peut s'agir d'éléments d'information directe, comme le nom et le prénom, ou indirecte, comme une photo, un identifiant ou un numéro. Google trace aussi « *le contenu que vous créez, importez ou recevez de la part d'autres personnes via [ses] services. Cela inclut par exemple les e-mails que vous écrivez ou recevez, les photos et* ■■■

▪▪▪ *vidéos que vous enregistrez, les documents et feuilles de calcul que vous créez ainsi que les commentaires que vous rédigez sur YouTube* ».Sauf que si la publicité ciblée est légale, elle n'est pas sans risque pour la vie privée et les droits des citoyens. « *De nombreux acteurs sont en mesure d'accumuler suffisamment d'informations pour créer des profils individuels très détaillés,* pointe la Cnil sur son site web. *Ces profils peuvent produire, au fil du temps, une image complète et plus ou moins exacte de votre personnalité, voire révéler des informations que vous n'aurez pas choisies d'exposer (par exemple, des données relatives à vos opinions politiques inférées à partir de l'analyse de vos lectures sur des sites d'information ou encore qui indiqueraient votre orientation sexuelle, par l'identification du genre des personnes dont vous consultez les profils sur les sites de rencontre). Plus un profil est détaillé, plus sa valeur marchande est élevée.* »

Le choc de l'affaire Cambridge Analytica

Les cas de dévoiement de la publicité ciblée ne manquent pas, l'exemple le plus célèbre étant celui de Cambridge Analytica. Après les révélations, en 2018, du lanceur d'alerte Christopher Wule, l'enquête a montré que cette société britannique avait collecté les données personnelles de 87 millions d'utilisateurs de Facebook sans leur consentement, dans le but notamment de promouvoir la candidature de Donald Trump lors de la campagne électorale américaine de 2016. Le scandale a provoqué la faillite de l'entreprise et une amende record de cinq milliards de dollars pour Facebook.

Les données de localisation, imprudemment divulguées sur les réseaux sociaux ou des applis de suivi sportif comme Strava, peuvent aussi servir à des fins indélicates ou franchement délictuelles, comme renseigner un cambrioleur à l'affût de logements vides, une personne qui chercherait à suivre son conjoint à son insu, un employeur désireux de localiser ses employés en dehors du temps de travail. Dans un régime totalitaire, les nombreuses techniques de pistage et d'identification des utilisateurs de mobiles représentent une réelle menace pour les libertés individuelles. Mais dans les pays disposant de solides protections juridiques, les techniques de traçage en ligne n'en suscitent pas moins la méfiance des associations.

Très active en France, avec de multiples plaintes portées devant la Cnil, la Quadrature du Net « *lutte pour que nos données personnelles ne soient pas considérées comme des marchandises : pour qu'aucune entreprise ou État ne puisse surveiller nos comportements et nous manipuler à des fins commerciales ou politiques, notamment en sélectionnant la publicité et les informations que nous recevons* ». L'association s'efforce notamment de faire respecter les dispositions européennes imposées aux entreprises du web par l'Union européenne. Entré en vigueur en 2018, le règlement général sur la protection des données (RGPD) est considéré comme la loi sur la protection de la vie privée la plus stricte au monde et s'applique chez les Vingt-Sept. Il impose que la collecte des données soit effectuée dans un but précis et avec le consentement de la personne concernée. Cependant, « *il est extrêmement compliqué de le faire appliquer dans une affaire transnationale impliquant plus de deux ou trois pays,* explique le juriste Romain

“Plus un profil est détaillé, plus sa valeur marchande est élevée”

Commission nationale de l'informatique et des libertés

FAIRPHONE 5 MURENA
LE MOBILE QUI NE LIVRE PAS VOS DONNÉES

Durable, réparable et respectueux de la vie privée, ce smartphone a tout pour plaire, en dehors de son prix, à partir de 600 euros. Il est le fruit d'un partenariat entre le fabricant néerlandais Fairphone et le français Murena, qui a conçu le système d'exploitation /e/OS. Pour préserver les données personnelles, l'appareil n'intègre pas les services de Google, remplacés par des logiciels libres. Il est toutefois possible d'installer manuellement Gmail, Maps ou Chrome.

Son système d'exploitation /e/OS exploite le code source d'Android 13, ouvert à tous, mais sans les services de Google. Ces derniers restent toutefois exploitables une fois téléchargés depuis l'App Lounge de Murena, qui offre presque tout le catalogue du Play Store.

La configuration, solide, comprend un écran Amoled de 6,5 pouces (16,4 cm), une puce Qualcomm QCM 6490, 8 Go de mémoire vive, 256 Go de stockage et le Wifi 6. Il est alimenté par une batterie de 4 200 mAh.

IVAN TRAIMA/ISTOCKPHOTO

Robert, de l'association de défense des droits numériques Noyb. *Même la Commission européenne reconnaît que c'est un problème.* »

Du matériel pour préserver sa vie privée

Gaël Duval, lui, propose de s'affranchir des géants du web grâce à des logiciels plus respectueux de nos données. Ce pionnier du logiciel libre a créé le système d'exploitation Linux Mandrake, devenu Mandriva, dans les années 1990, avant de se pencher sur les smartphones et de découvrir la masse effarante de données qu'ils révélaient. « *En moyenne, un iPhone ou un Android envoie près de dix mégaoctets de données par jour, de manière invisible*, explique l'informaticien de 51 ans. *Cela passe par la localisation en temps réel, les applis utilisées, l'historique de navigation, les mails… C'est quasiment toute sa vie intime qui est exposée par le biais des smartphones. Ce sont des choses que l'on n'accepterait pas pour notre courrier ou le téléphone classiques.* »

Pour en finir avec Google, Gaël Duval a fini par créer son propre système d'exploitation, baptisé /e/OS, avec son entreprise Murena. Lancé en 2020, il reprend la base d'Android, dont le code source est ouvert à tous, mais sans les services du géant américain. Exit le moteur Google Search, le navigateur Chrome, la localisation sur Maps ou les vidéos YouTube, remplacés par des programmes « libres » et sans traceurs d'activité. Ces logiciels sont préinstallés sur les smartphones proposés *(voir encadré ci-contre)* sur la boutique en ligne de l'entreprise, qui a noué un partenariat avec Fairphone, le spécialiste néerlandais des téléphones réparables et durables.

Pour les besoins de ce dossier, nous avons testé – et approuvé – le Fairphone 5 équipé du système /e/OS, assez cher (à partir de 600 € avec 128 Go) mais presque aussi agréable à utiliser qu'un mobile classique sous Android, et bien plus sobre en données personnelles. Bon point, le système de Murena reste compatible avec les applis Google, contrairement aux modèles récents de Huawei soumis aux restrictions imposées par le gouvernement américain. L'utilisateur d'un mobile Murena peut toujours utiliser Gmail ou Maps, à condition de valider la collecte des données qu'elle implique. Autrement dit, à ses risques et périls. D'autres firmes proposent des mobiles spécialement conçus pour préserver les données personnelles. Sauf qu'ils révèlent souvent hors de prix, comme le Liberty Phone du constructeur américain Purism (environ 2000 €) ou réservés aux experts de Linux comme le PinePhone Pro du hongkongais Pine64 (400 €). Plus abouti, le Volla Phone 22 (450 €) sous Linux, de l'allemand Hallo Welt, reste un peu austère pour le grand public.

Aux utilisateurs soucieux de leur vie privée, nous conseillons donc plutôt les mobiles de Murena, ou de ne rien dépenser du tout en soignant un peu leur téléphone actuel. Le pillage des données privées s'atténue sensiblement avec quelques réglages et de bonnes pratiques. Avec les mobiles sous Android, il est assez simple de réduire ses traces sur internet grâce au gestionnaire de compte intégré au système de Google. Il facilite la suppression de l'historique des sites web ou des pages YouTube visitées ou la désactivation de tout ou partie des traceurs publicitaires. Rappelons enfin que la sauvegarde de la vie privée n'est guère compatible avec une activité frénétique sur les réseaux sociaux, quels qu'ils soient. Et si vous rencontriez plus souvent vos amis dans la vraie vie, sans traceurs publicitaires ni GPS? ●

DEMANDEZ UN PEU D'INTIMITÉ À ANDROID

Les smartphones fonctionnant avec le système de Google disposent de réglages pour retrouver un minimum de confidentialité. Mais encore faut-il les activer.

GRINVALDS/ISTOCKPHOTO

1 Désactivez une application préinstallée

Il est très probable que votre smartphone ne soit pas rooté et que vous ne souhaitiez pas vous lancer dans cette opération. Dans ce cas, vous ne pourrez pas effacer les applis du système. Rien ne vous empêche néanmoins d'en suspendre le fonctionnement.

Accédez aux **Paramètres** du téléphone. Ouvrez la rubrique **Applications**, appuyez sur **Liste des applications** puis sur le nom du programme. Effleurez alors les boutons **Désactiver**, **Désactiver l'application**.

2 Neutralisez l'identifiant publicitaire

Chaque appareil Android possède un identifiant publicitaire unique qui relaie des informations relatives aux préférences et aux habitudes du propriétaire du téléphone. Pour suspendre le fonctionnement de ce dispositif de suivi, affichez l'onglet **Données et confidentialité** de votre compte Google, dans la section **Annonces personnalisées**, touchez **Mes préférences publicitaires** et choisissez la mention **Désactivé** à côté de l'intitulé **Annonces personnalisées**.

3 Renoncez aux résultats personnalisés

Google analyse vos données afin de cerner vos goûts et ainsi répondre pertinemment à vos requêtes. Si vous ne souhaitez pas exposer votre vie privée, accédez à l'onglet **Données et confidentialité** de votre compte Google. Dans la section **Résultats personnels dans la recherche**, touchez **Activé**. Décochez le curseur **Afficher les résultats personnels** pour désactiver l'option.

4 COUPEZ COURT AU SUIVI

Si vous n'en pouvez plus de vous sentir scruté sous toutes les coutures, déployez le volet des notifications du mobile et désactivez la localisation. Ainsi, ni Android ni les applis n'ont accès aux informations de la puce GPS. Une fonction à utiliser avec parcimonie, car elle entrave le fonctionnement des outils de cartographie et de navigation, comme Maps et Waze, et la bonne marche des assistants de santé.

5 Révoquez les autorisations

Quand vous installez une appli, celle-ci s'arroge le droit d'accéder à certaines ressources du téléphone – données de localisation, contenu de la mémoire, caméra ou micro. **Ces privilèges s'exercent y compris lorsque vous n'utilisez pas les applis.** Pour éviter les abus, affichez les paramètres de l'appareil, ouvrez la rubrique **Confidentialité** et touchez **Autorisation des applis**. Supprimez les droits qui ne vous semblent pas légitimes

Signal pour remplacer **Google Messages**

LA MESSAGERIE CONSEILLÉE PAR SNOWDEN

Avec son chiffrement de bout en bout, Signal est un outil hypersécurisé pour les communications écrites et les appels audio et vidéo. Mieux encore, la messagerie est disponible sur tous les supports : Android, iOS, macOS, Windows ou Linux. Et le tout gratuitement.

SIGNAL.ORG/FR

PROTON MAIL pour remplacer **Gmail**

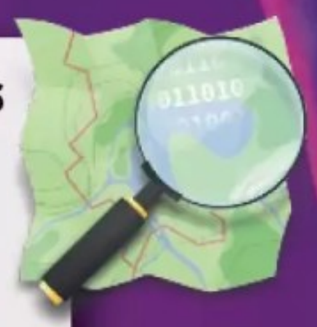
L'ARCHÉTYPE DE L'ADRESSE SÉCURISÉE

Conçu par d'anciens ingénieurs du Cern après les révélations d'Edward Snowden, ce client mail est l'un des plus sécurisés au monde. Certes, sa version gratuite comporte de nombreuses limitations, comme son gigaoctet d'espace de stockage total et ses 150 messages maximum au quotidien. Sa fonction Alias hide-my-email s'avère toutefois très intéressante quand on ne veut pas divulguer sa vraie adresse mail et que l'on a malgré tout besoin de remplir un formulaire en ligne. La version Unlimited comprend l'ensemble des services Proton, dont un VPN « haute vitesse » et 500 Go de stockage, mais s'avère assez chère (10 €/mois).

PROTON.ME/FR

DES APPLIS POUR REDEVENIR LIBRE

C'est la manière la plus simple de tromper le pistage de Google : remplacer les applications comme Gmail, Drive, Chrome ou Messages par d'autres, qui n'épient pas vos faits et gestes.



OpenStreetMap pour remplacer **Google Maps**

LE GUIDAGE SANS TRAÇAGE

Moins pratique et ergonomique que Google Maps, OSM n'en reste pas moins fonctionnel et précis. Ce service de cartographie libre constitue le cœur d'applications mobiles tierces qui utilisent ses données sans vous tracer. On trouve parmi elles Organic Maps, OsmAnd ou Geovelo pour les cyclistes.

OPENSTREETMAP.ORG

DuckDuckGo pour remplacer **Chrome**

LA VRAIE RECHERCHE ANONYME

Un moteur de recherche et un navigateur sans traceurs tiers. En clair, il ne vous suit pas, s'efforce d'empêcher les autres de le faire et ne conserve pas d'historique de votre navigation. Il indexe plus de 400 sources d'information, dont des données de Bing, Wikipédia, Sportradar... Précisons que Chrome, le navigateur de Google, ne garantit aucune forme de confidentialité même avec sa fenêtre de navigation privée, qui porte bien mal son nom. En effet, si elle évite de laisser des traces sur le terminal utilisé, elle n'a rien de privé aux yeux de son éditeur.

DUCKDUCKGO.COM

pCloud pour remplacer **Google Drive**

AVEC UN « P » COMME PRIVÉ

Ce service de stockage suisse qui stocke les données chiffrées aux États-Unis ou au Luxembourg se targue de fournir le plus haut niveau de sécurité. Pour le reste, on est séduit par la possibilité d'installer un « disque virtuel » qui s'utilise en pratique comme un support de stockage physique et par l'absence de taille maximum de fichier. La synchronisation avec vos différents appareils et les applications Android et iOS sont appréciables. Régulièrement, pCloud propose des formules de paiement à vie plutôt intéressantes. Autrement, il en coûtera une cinquantaine d'euros par an pour 500 Go de stockage.

PCLOUD.COM/FR

IVAN TRAIMAK/ISTOCK PHOTO

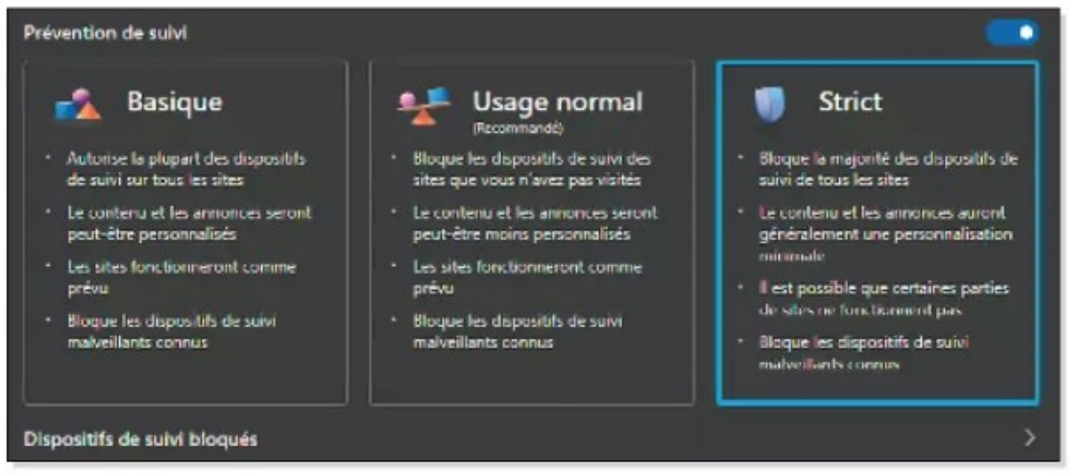
DIFFICULTÉ **MODÉRÉE** TEMPS **60 MIN** DOMAINE **NAVIGATEURS**

SURFEZ EN PAIX, SANS LAISSER DE TRACES

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

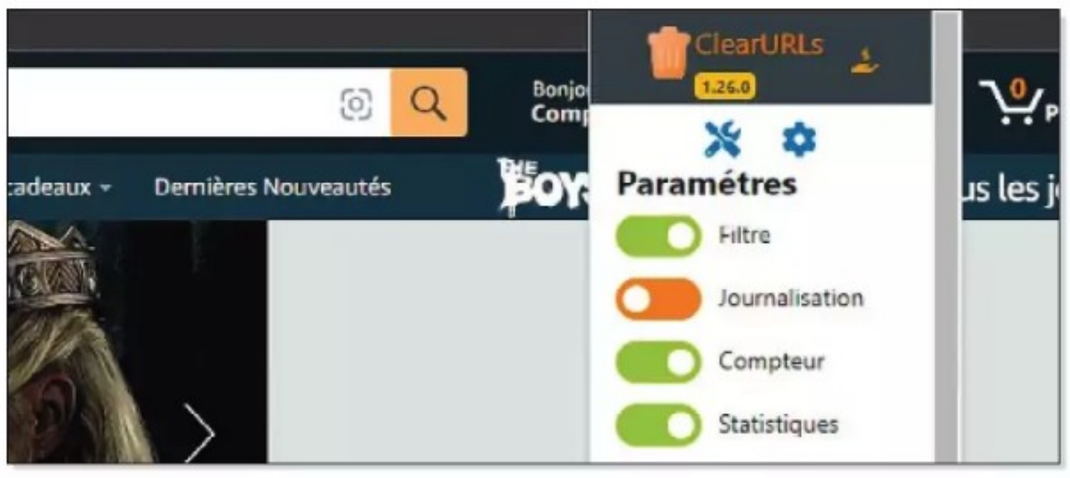
1 BLOQUEZ LE SUIVI DANS EDGE

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**.



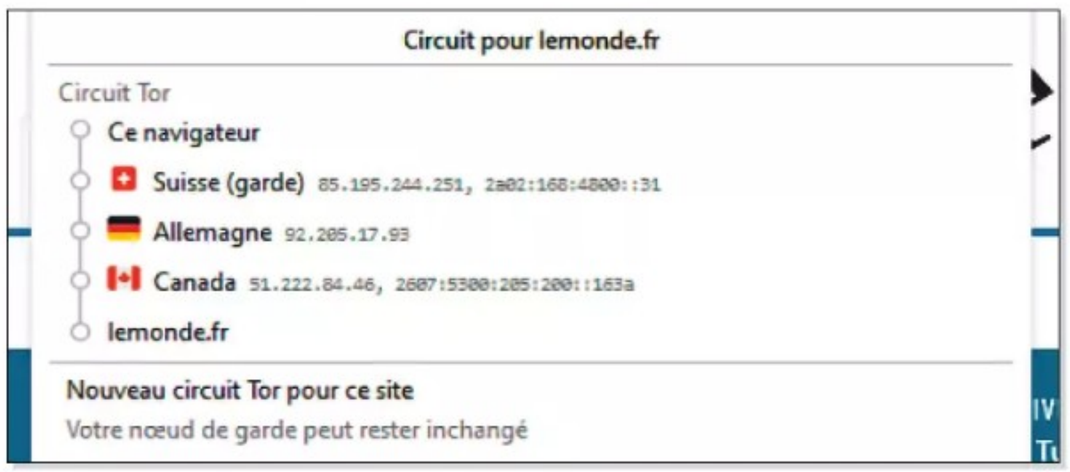
2 NETTOYEZ LES DONNÉES DE SUIVI DANS L'URL

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**.



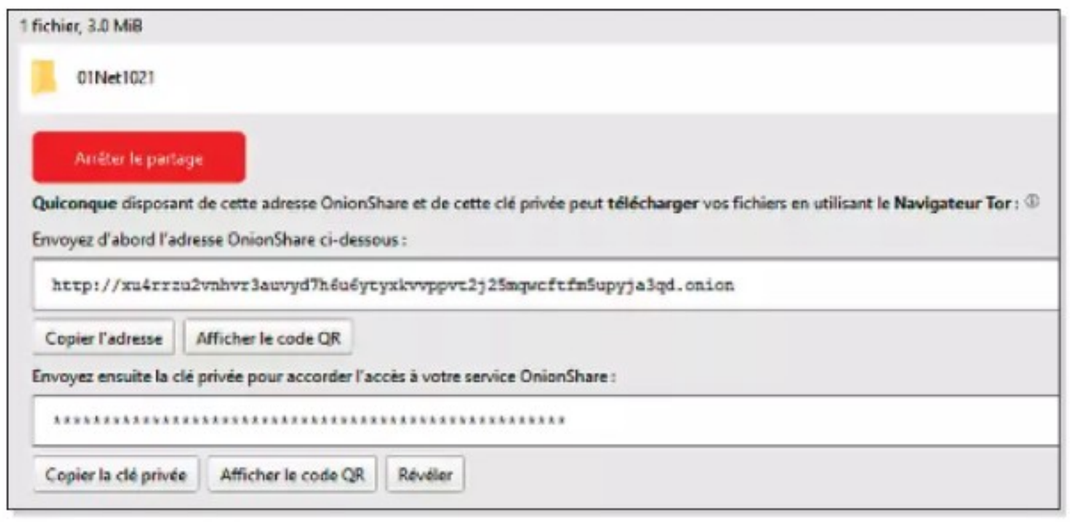
3 NAVIGUEZ AVEC TOR

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.

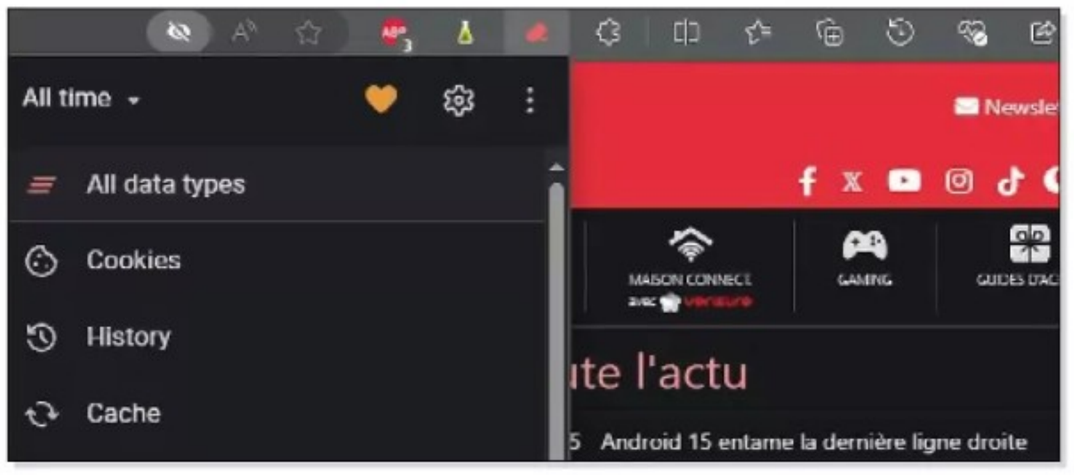


5 CHIFFREZ VOS MAILS AVEC THUNDERBIRD

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.

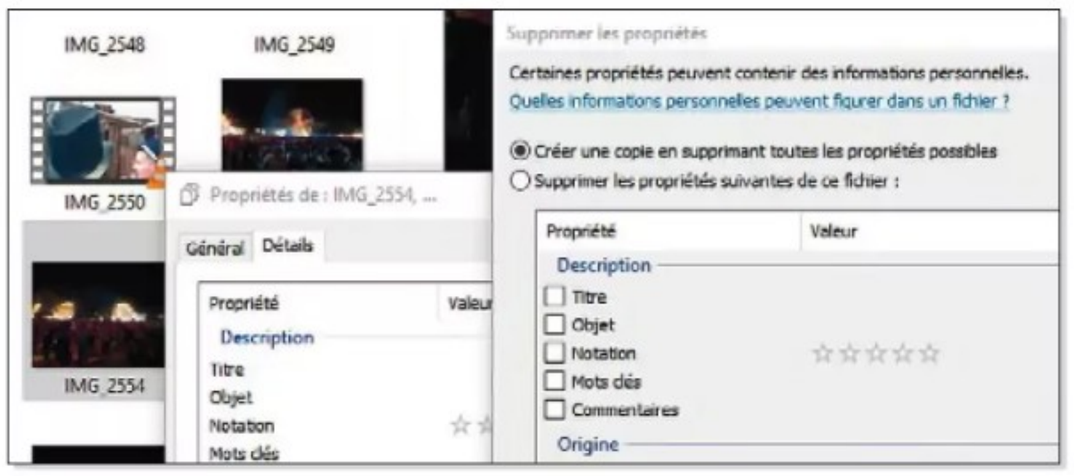
6 EFFACEZ LES DONNÉES DE VOS NAVIGATEURS EN UN CLIC

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** et **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 **MODÉRÉE**
DOMAINE **SÉCURITÉ**
TEMPS **VARIABLE**

ÉCHAPPEZ AUX TRACEURS

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.

Difficile d'échapper à l'espionnage des géants de la tech dès que l'on se connecte à internet. 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, Amazon, Meta, Apple, Microsoft… en leur assurant des revenus considérables via la vente de données privées, à partir desquels ils diffusent des publicités ciblées. Chacune de nos activités en ligne – liker un contenu sur Instagram, installer une application sur notre téléphone 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 au module anti-pistage du moteur de recherche DuckDuckGo pour mesurer l'ampleur de la collecte d'informations !

NE PAS BAISSER LES BRAS. Les tentatives de suivi sont constantes. L'espionnage se prolonge même lorsque les applications ne sont pas ouvertes. C'est le cas, par exemple, 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 numériques de plus en plus précis de ses clients. 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 de nos ordinateurs, smartphones et tablettes, ainsi qu'aux navigateurs, n'offrent pas des garanties absolues. Elles contribuent toutefois à notre tranquillité digitale. Certains utilisateurs jugeront sans doute de tels dispositifs insuffisants. La solution passera alors par l'abandon des services et outils les plus courants, qu'il s'agisse d'abandonner Windows pour Linux ou de « dégoogelisé » Android. Un choix radical, réservé aux amateurs avertis, mais qui éloigne les grandes oreilles des rois du web et de la tech. ●

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

METTEZ À PROFIT LES RÉGLAGES INTÉGRÉS À VOS 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.

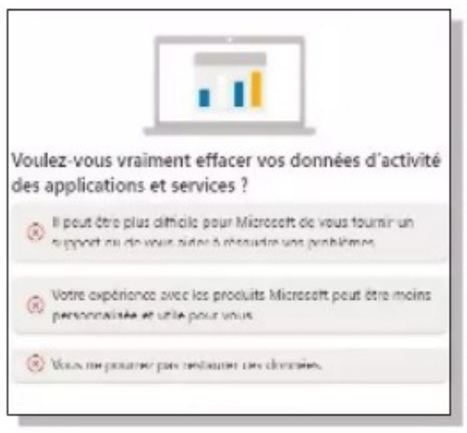
MICROSOFT

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 CHEZ 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. Désactivez les annonces personnalisées de l'iPhone
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 l'accès des applications
Sur la page **Réglages**, effectuez une requête sur le terme **Contrôle de sécurité**. Effleurez **Gérer les partages et les accès**, **Continuer**. À l'étape **Accès des apps**, cochez les applis dont vous souhaitez révoquer l'accès à votre compte Apple.

03. Supprimez l'analyse iCloud de votre Mac
Connectez-vous à votre compte Apple depuis un Mac (bit.ly/3SJRlE5). Sur 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.

DRAFTER123/ISTOCKPHOTO

ÉTAPE 2

ÉRADIQUEZ VOS DONNÉES PRIVÉES DE WINDOWS

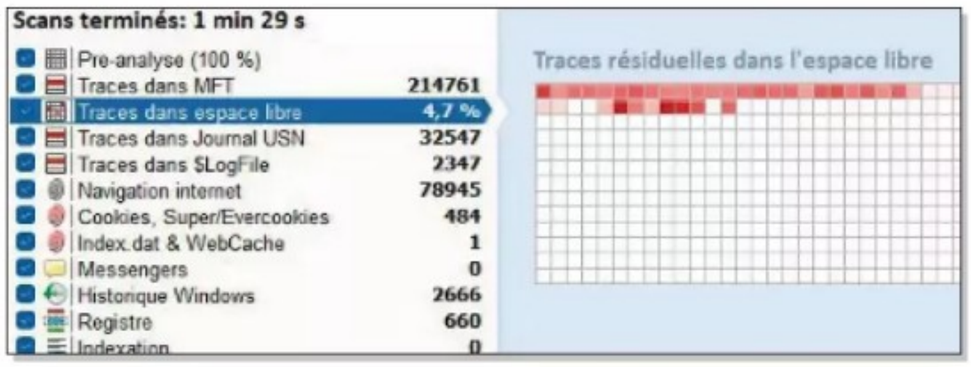
N'attendez pas que Microsoft efface l'intégralité de votre vie privée.
Pour cela, mieux vaut s'en remettre à une application tierce comme PrivaZer.

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 bureautiques** 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 l'ordinateur 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

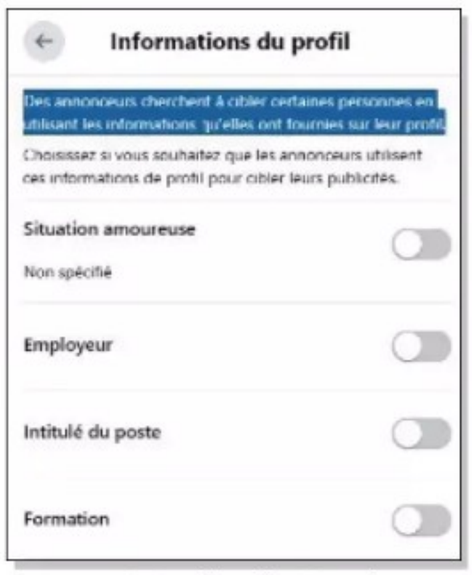
NE LAISSEZ PAS LES RÉSEAUX EXPLOITER VOTRE VIE NUMÉRIQUE

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 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 PILLER VOS DONNÉES

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

CLÔTUREZ VOS COMPTES META, GOOGLE, MICROSOFT...

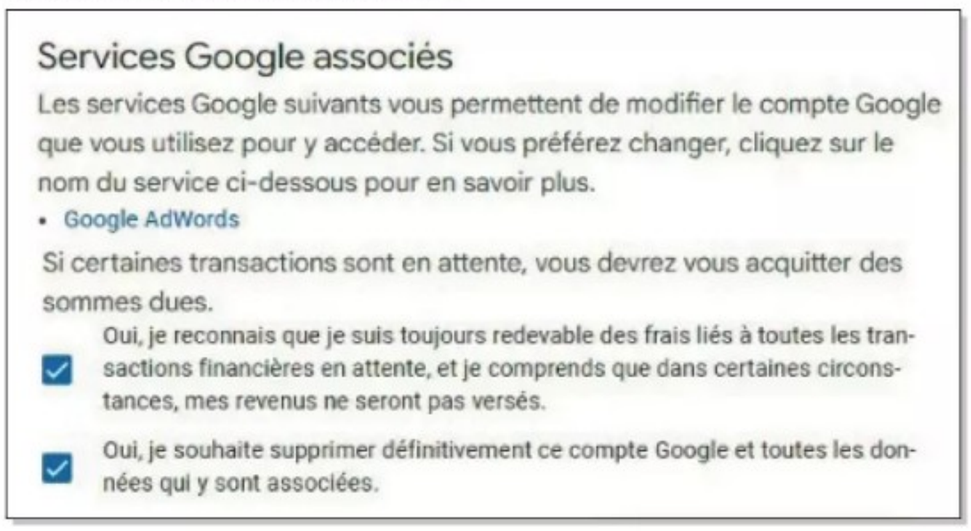
Il existe une **solution imparable à la collecte de données** : clore définitivement les comptes qui vous lient à Windows, Facebook, Instagram...

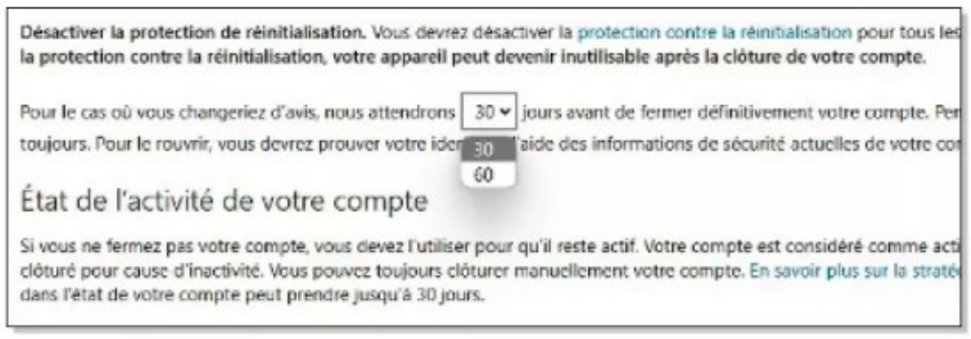
1 PRIVEZ META DE VOS DONNÉES PERSONNELLES

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 Google (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

DRESSEZ DES BARBELÉS AUTOUR DE VOS FICHIERS

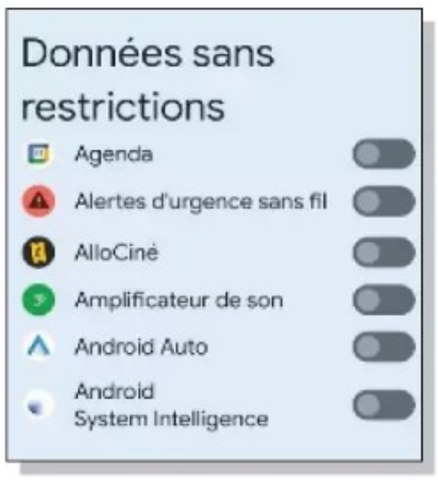
Maintenant que le nettoyage des données privées est acté, il reste à se protéger des futures tentatives de suivi. **Un jeu d'enfants avec un VPN et DuckDuckGo.**

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.

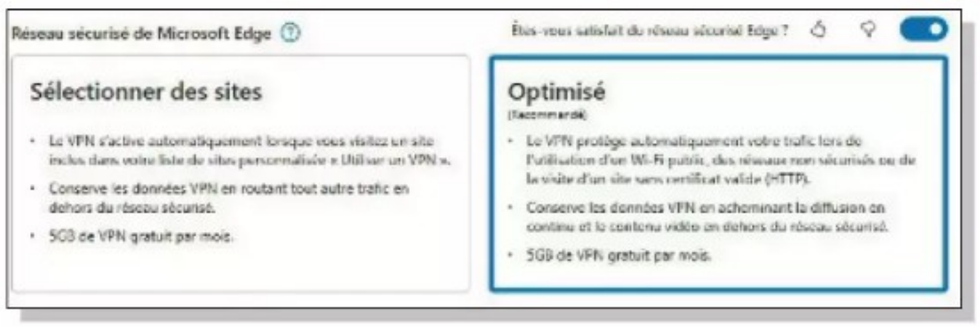
2 RÉDUISEZ L'ACTIVITÉ EN ARRIÈRE-PLAN DES APPLICATIONS

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 (MICRO, PHOTO, ETC.)

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 applis. 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 applis 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 PC et Mac, **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 vos traces d'un clic

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

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 **AUCUNE** TEMPS **20 MIN** DOMAINE **INTERNET**

IMPOSEZ VOS CONDITIONS AVEC SAFARI

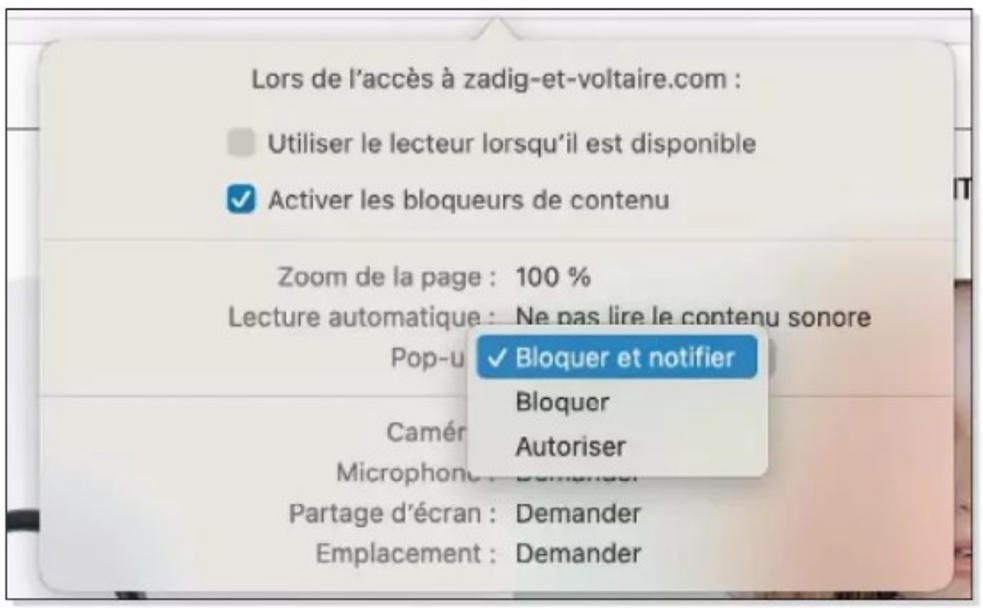
Notifications, géolocalisation, lancement automatique de vidéos… Les sollicitations ne manquent pas lorsque vous surfez. Heureusement, grâce au navigateur d'Apple, vous pouvez reprendre le contrôle.

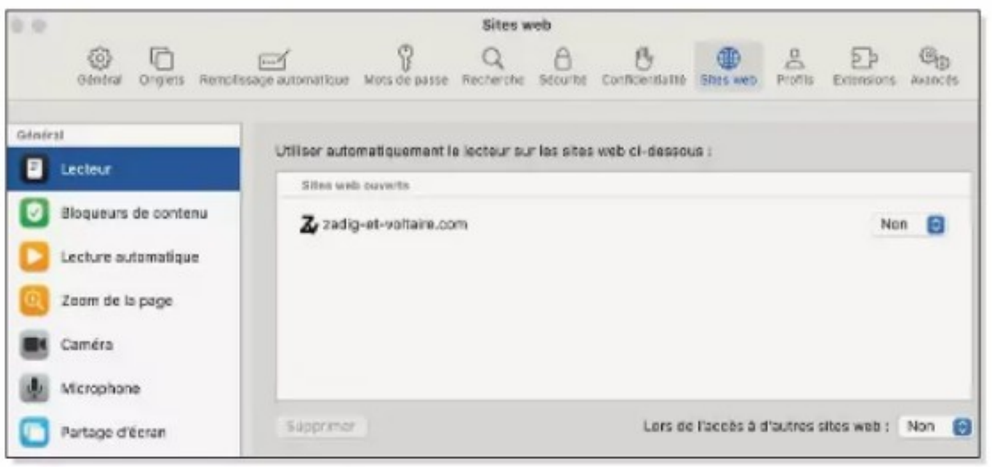
1 AFFICHEZ LES PRÉFÉRENCES

Le navigateur d'Apple vous permet de décider si vous souhaitez recevoir une notification, visionner des vidéos, télécharger du contenu, accorder l'accès à diverses fonctions de votre Mac ou afficher des fenêtres contextuelles. Pour encore plus de contrôle, il est aussi possible de définir des préférences spécifiques pour tous les sites visités. Pour choisir les réglages à appliquer au site affiché à l'écran, appuyez sur la touche **Control** du clavier et cliquez dans la barre d'adresse. Dans le menu contextuel qui s'affiche, optez pour **Réglages pour**, suivi du nom du site.

2 AJUSTEZ LES AUTORISATIONS

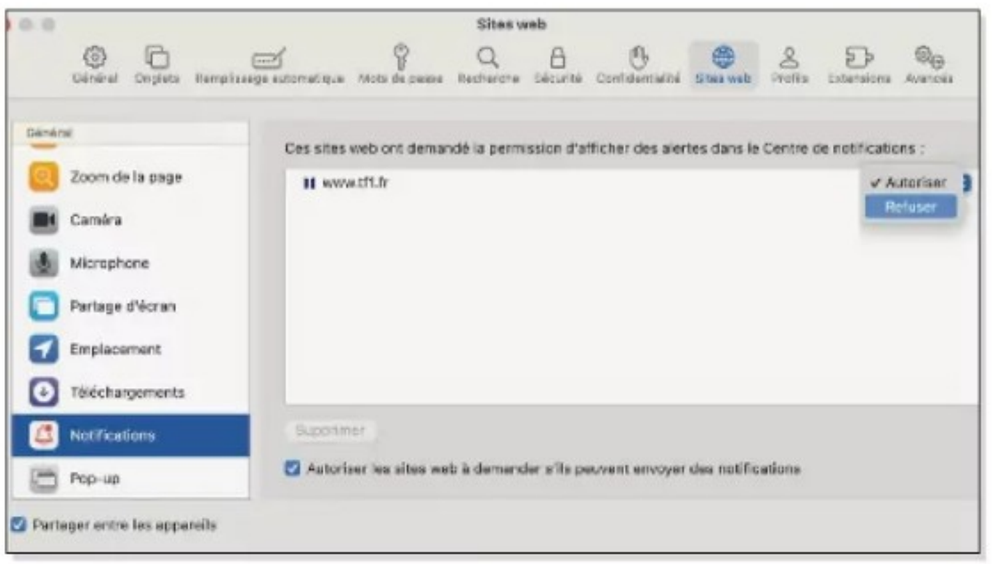
Vous pouvez maintenant définir la façon dont ce site s'affiche dans Safari. Cochez ou décochez la case **Activer les bloqueurs de contenu**, si le site conditionne l'affichage de quelques publicités à la consultation de ses pages. Intéressez-vous ensuite à l'intitulé **Zoom**. Là, cliquez sur la liste déroulante pour sélectionner le facteur d'agrandissement ou de réduction de l'affichage et l'adapter à vos besoins. Enfin, observez la ligne **Lecteur automatique**. Il s'agit ici d'autoriser ou non le lancement d'une vidéo ou d'un extrait sonore par défaut.





3 GÉNÉRALISEZ VOS RÉGLAGES

Vous avez la possibilité de dupliquer le paramétrage de l'étape précédente pour l'ensemble des sites que vous consultez. Accédez au menu déroulant **Safari** et pointez sur l'intitulé **Réglages**. Activez ensuite l'onglet **Site web** puis, dans le volet de gauche de la fenêtre, observez les différents types de fonctionnalités paramétrables. Cliquez par exemple sur **Lecture automatique**. Vous retrouvez le réglage défini précédemment. Pour le généraliser, cliquez sur la liste déroulante, située en bas à droite de la fenêtre, **Lors de l'accès à d'autres sites web** et définissez le comportement de votre choix.



4 NE VOUS LAISSEZ PAS SUBMERGER PAR LES NOTIFICATIONS

Nombre de sites internet, notamment d'actualité, émettent des notifications. Celles-ci s'affichent dans le volet du même nom et vous permettent d'accéder rapidement aux contenus qui vous intéressent. Lorsqu'elle n'est pas souhaitée, cette surabondance de notifications peut nuire à la qualité de votre expérience de navigation au quotidien. Mais rien ne vous empêche de gérer ces interventions. Restez sur l'onglet **Sites web** et, dans le volet de gauche, pointez sur la rubrique **Notifications**. Là, décochez la case **Autoriser les sites Web à demander s'ils peuvent envoyer des notifications**.

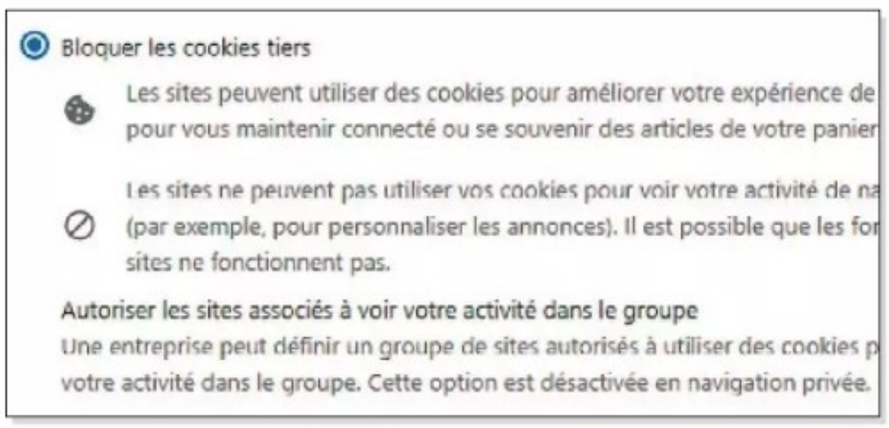
DIFFICULTÉ **MODÉRÉE** TEMPS **30 MIN** DOMAINE **NAVIGATEURS**

NE PRENEZ QUE LES (BONS) COOKIES

Se débarrasser totalement des cookies est peine perdue. Mais plutôt que de tenter un nettoyage par le vide qui pourrait pénaliser votre navigation, prenez des mesures pour réduire leur champ d'action.

1 RENDEZ-VOUS DANS LES PARAMÈTRES DE CHROME, EDGE...

Rappelons que le cookie est un fichier de quelques kilo-octets qui conserve les informations vous concernant lorsque vous naviguez sur un site. Certains sont utiles et retiennent par exemple votre panier sur un site d'achat ou vos identifiants. Mais la plupart visent à établir votre profil à partir de vos habitudes de navigation, à des fins de publicité ciblée ou de revente de fichiers clients. Il faut donc surveiller ce que vous entendez laisser comme informations. Tous les navigateurs le permettent. Sur Chrome, rendez-vous dans les **Paramètres**, **Confidentialité et sécurité** puis **Cookies tiers**. Dans Edge, allez dans les **Paramètres**, **Cookies** et **Autorisations de site**.

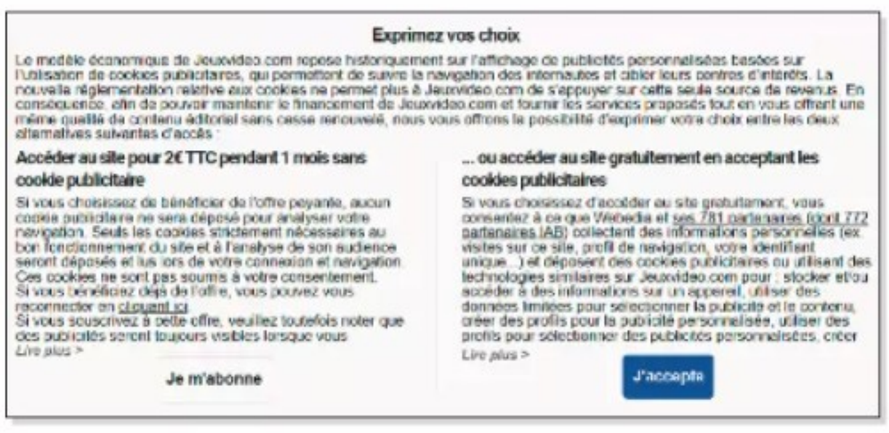


2 INTERDISEZ LE SUIVI SANS VOUS FERMER DES PORTES

Si vous empêchez les cookies en bloc, vous serez dès lors déconnecté de nombreux services. Certains moteurs de recherche internes aux sites ne fonctionneront plus, des sites marchands seront inutilisables... Pour demander aux sites de ne pas vous suivre, dans Chrome, rendez-vous à la page **Cookies tiers** et activez **Envoyer une requête « Do Not Track » avec votre trafic de navigation**. Dans Edge, accédez à **Paramètres**, **Confidentialité, Recherche et service** pour activer **Envoyer des demandes « Ne pas me suivre»**. Cliquez ensuite sur **Choisir ce qu'il faut effacer chaque fois que vous fermez le navigateur** et activez les cookies.

3 GÉREZ LES AUTORISATIONS AU CAS PAR CAS

Rien ne vous empêche de consacrer un navigateur spécifique aux recherches non tracées, en activant à la fois le VPN et le refus des cookies, auquel vous pouvez joindre un bloqueur de pubs et de pistage comme Ghostery (bit.ly/41HAmoq). Sinon, sur votre navigateur habituel, cliquez sur le cadenas situé près de la barre d'adresse puis sur **Cookies et données du site** (ou **Cookies**). Activez **Cookies actifs** et optez pour **Bloquer**. Certains sites s'opposent à ce blocage, obligeant à accepter les cookies ou à vous alléger de quelques euros. L'extension Cookie AutoDelete (bit.ly/3FlJtUq) peut vous aider à gérer les autorisations.



4 AIDEZ-VOUS DE L'EXTENSION COOKIE AUTODELETE

Une fois Cookie AutoDelete installée sur Chrome, Firefox ou Edge, cliquez sur son icône puis sur **Paramètres**. Ici, vous pouvez activer le nettoyage automatique lorsque l'onglet est fermé ou que le navigateur redémarre. Cochez **Nettoyer tous les cookies expirés** ainsi que **Activer le nettoyage pour les onglets abandonnés/non chargés**. Nous vous conseillons de vous montrer le plus restrictif possible dans un premier temps, puis d'adapter les mesures au fil de vos navigations. Ainsi, lorsqu'un site nécessite l'utilisation d'un cookie, autorisez-le en cliquant sur l'icône **Cookie AutoDelete**, **Liste blanche**. Pour terminer, dans **Options de nettoyage automatique**, réglez le délai (exprimé en secondes) et cochez l'ensemble des cases disponibles.

Maîtriser

les outils du numérique

SOMMAIRE

RÉSEAU PERSONNEL

STOCKEZ VOS FICHIERS DANS VOTRE PROPRE CLOUD

Plutôt que de les confier à Google ou Dropbox, vous pouvez mettre vos données à l'abri sur votre propre espace de stockage en ligne, avec un serveur NAS.

DA-KUK/ISTOCKPHOTO

Pour une fois, on ne pourra pas vous reprocher d'avoir la tête dans les nuages. Nous allons même vous le conseiller. Afin de gérer sa vie numérique, de partager ses photos ou ses fichiers de travail, il n'y a rien de plus pratique et d'efficace que les services de stockage dans le cloud tels que Google Drive, Apple iCloud, Dropbox ou Microsoft OneDrive. Ceux-ci sont compatibles avec toutes les plateformes, très simples à utiliser et parfaitement intégrés aux systèmes d'exploitation des ordinateurs. L'ennui, c'est que la capacité de stockage des formules gratuites est particulièrement limitée, avec 5 à 15 Go pour les principaux opérateurs. Si l'on souhaite de plus gros volumes de stockage, il faut souscrire un abonnement mensuel ou annuel qui peut vite revenir assez cher. Autre inconvénient des espaces de stockage en ligne : leur pérennité n'est pas garantie. Samsung a ainsi mis fin à son cloud le 30 juin 2021 et a proposé à ses utilisateurs de migrer leurs données sur le service OneDrive de Microsoft. Un peu plus tard, à la fin 2023, le service Amazon Drive a lui aussi été fermé après plus de onze ans d'activité.

Rappelons aussi que les systèmes de cloud ne sont pas infaillibles, même ceux des géants du secteur. En septembre 2023, un bug de Google Drive a provoqué un vent de panique chez certains utilisateurs après avoir fait disparaître une partie de leurs données. Le problème a certes été résolu, et les données restaurées, mais il a écorné la réputation d'un service jusqu'ici considéré comme très fiable.

Du profilage dans les Drive

Enfin, les systèmes de cloud peuvent présenter des risques pour la confidentialité et la sécurité des informations, à la suite d'un piratage ou du fait du fournisseur lui-même. « *Google ne fouille pas dans les données, mais il peut recourir aux métadonnées, c'est-à-dire aux informations sur vos dates de connexion, sur votre activité, sur les dossiers déposés ou partagés. Ces données peuvent être utilisées pour du ciblage publicitaire, par exemple* », reconnaît Florent Della Valle, chef du service de l'expertise technologique à la Commission nationale de l'informatique et des libertés. Pour autant, l'expert ne recommande pas de quitter Google ou Apple : « *La législation américaine est considérée par l'Europe comme adéquate du point de vue de la protection des données.* » ■■■

▪▪▪ Il serait bien dommage, en effet, de se priver de services en ligne aussi pratiques. Mais il n'est pas très prudent de leur confier toute notre vie numérique. La solution, c'est de compléter les services en ligne avec un cloud personnel, un espace de stockage logé à la maison mais relié au monde extérieur grâce à internet. Et le meilleur moyen de le mettre en œuvre, c'est d'opter pour un serveur personnel ou NAS (Network Attached Storage). Il prend la forme d'un petit boîtier à relier sur la box internet du foyer, capable de stocker une grande quantité de documents bureautiques, de photos ou de films et de les mettre à disposition de tous les appareils de la maison, ordinateur, téléphone, tablette, téléviseur ou console de jeux. Plus fort, le NAS est aussi très facile à consulter à distance grâce à un simple navigateur web ou à des applis pour les mobiles Android ou Apple. En prime, ces boîtiers sont conçus pour se synchroniser avec les principaux services de stockage en ligne du marché, ce qui renforce la sécurité des données qui y sont conservées. Reste à choisir le bon modèle, selon ses besoins ou son budget, puis à installer et à configurer un cloud domestique digne des professionnels.

Un petit boîtier bien pratique

Ne vous laissez pas décourager par son drôle de nom et son allure un rien austère. On devient vite accro à ce petit boîtier-là, même si sa mise en route demande un peu de patience. S'il ressemble un peu à un gros disque dur externe, un NAS est en fait un ordinateur un brin spécial, qui n'a besoin ni d'écran ni de clavier. On l'installe et l'exploite par le biais d'une autre machine (PC, Mac, smartphone…) et d'une connexion réseau. Comme tout ordinateur, il intègre un processeur, de la mémoire vive, un système d'exploitation – dérivé de Linux – et un jeu d'applications spécifiques. Les meilleurs spécialistes des NAS s'appellent Synology, Qnap et Asustor, trois firmes de Taïwan qui proposent une vaste gamme de produits pour tous les budgets et un écosystème assez riche pour tous les besoins. Entre ces trois-là, nous avons un petit faible pour Synology, le bon choix selon nous pour bien démarrer dans le monde du NAS. Ses tarifs sont assez élevés mais nous semblent justifiés par une interface logicielle de tout premier ordre et des applis plus soignées que celles de ses concurrents Qnap et Asustor. Légèrement en retrait par rapport à ses trois rivaux, le chinois TerraMaster aligne des produits au rapport qualité/prix souvent intéressant mais qui sont moins richement dotés en logiciels.

10 NAS À PARTIR DE 155 €

Du Qnap TS-133, parfait pour une personne seule, au très performant DS-923+



MODÈLES	SYNOLOGY DS124	QNAP TS-133	QNAP TS-216G
CARACTÉRISTIQUES			
PRIX (hors disque)	155 €	160 €	300 €
Processeur	Realtek RTD1619B (4 cœurs)	ARM Cortex A55 (4 cœurs)	ARM Cortex A55 (4 cœurs)
Mémoire (DDR4)	1 Go	2 Go	4 Go
Mémoire maximale	1 Go	2 Go	4 Go
Baies de disque	1	1	2
Supports de stockage gérés	HDD, SSD	HDD, SSD	HDD, SSD
Prises réseau	1 Gbit	1 Gbit	1x 1 Gbit, 1x 2,5 Gbits
Autres prises	2 USB 3.2	USB 3.2 USB 2.0	1x USB 3.2, 2x USB 2.0
Support Raid	NON	NON	Raid 0, 1, JBOD
Système d'exploitation	DSM 7.2	QTS 5.1	QTS 5.1
Dimensions	16,6 x 7,1 x 22,4 cm	18,6 x 6,7 x 15,8 cm	165 x 102 x 220 mm
Poids (sans disque)	0,7 kg	1 kg	1,45 kg
Consommation électrique (en accès)	10,7 W	7,3 W	13,9 W

LEXIQUE

JBOD
Just a Bunch of Disks
Configuration de stockage utilisant plusieurs disques durs sans appliquer de Raid. Chaque disque est employé indépendamment, sans redondance intégrée.

RAID
Redundant Array of Inexpensive Disks
Technologie combinant plusieurs disques pour améliorer la performance (Raid 0), la redondance des données (Raid 1) ou les deux (Raid 5 et 10).

De 65 à 900 euros pour un disque

Selon les modèles, les boîtiers NAS destinés au grand public coûtent entre 180 et 800 euros environ. Le prix dépend en bonne partie du nombre de disques que le boîtier peut accueillir. Les modèles les moins chers, à moins de 200 euros, sont généralement cantonnés à un seul disque dur HDD (Hard Disk Drive) ou SSD (Solid State Drive). Entre 300 et 400 euros, on a droit à des modèles un peu plus élaborés, capables de recevoir deux ou quatre disques dans des baies amovibles. En montant en gamme, on obtient aussi un système plus nerveux et en mesure de gérer davantage d'utilisateurs ou de tâches en même temps. Le

de Synologie, idéal pour toute la famile ou une petite entreprise, cette sélection couvre tous les besoins.

 ASUSTOR AS3302T V2	 TERRAMASTER F2-423	 SYNOLOGY DS224+	 ASUSTOR AS5402T	 QNAP TS-462 4G	 ASUSTOR AS5404T	 SYNOLOGY DS-923+
285 €	**330 €**	**360 €**	**430 €**	**520 €**	**600 €**	**635 €**
Realtek RTD1619B (4 cœurs)	Intel Celeron N5095 (4 cœurs)	Intel Celeron J4125 (4 cœurs)	Intel Celeron N5105 (4 cœurs)	Intel Celeron N4505 (2 cœurs)	Intel Celeron N5105 (4 cœurs)	AMD Ryzen R1600 (2 cœurs)
2 Go	4 Go	2 Go	4 Go	4 Go	4 Go	4 Go
2 Go	32 Go	6 Go	16 Go	4 Go	16 Go	32 Go
2	2	2	2	4	4	4
HDD, SSD	HDD, SSD, M2	HDD, SSD	HDD, SSD, M2	HDD, SSD, M2	HDD, SSD, M2	HDD, SSD, M2
2,5 Gbits	2,5 Gbits (x2)	1 Gbit (x2)	2,5 Gbits (x2)	2,5 Gbits	2,5 Gbits (x2)	1 Gbit (2x)
3 USB 3.2	2 USB 3.1	2 USB 3.2	3 USB 3.2 Gen 1, HDMI	2 USB 3.2, 2 USB 2.0, HDMI	3 USB 3.2 Gen 1, HDMI	2 USB 3.2
Raid 0, 1	Raid 0, 1	Raid 0, 1, SHR	Raid 0, 1	Raid 0, 1, 5, 6, 10	Raid 0, 1, 5, 6, 10	Raid 0, 1, 5, 6, 10
ADM 4.3	TOS 6	DSM 7.2	ADM 4.3	QTS 5.1	ADM 4.3	DSM 7.2
17 x 11,4 x 23 cm	13,3 x 11,9 x 22,7 cm	16,5 x 10,8 x 23,3 cm	17 x 11,4 x 23 cm	16,5 x 17 x 22,6 cm	17 x 17,4 x 23 cm	16,6 x 19,9 x 22,3 cm
1,6 kg	2,4 kg	1,3 kg	1,7 kg	3,5 kg	2,3 kg	2,2 kg
13,1 W	22 W	14,7 W	22,9 W	32,4 W	38,3 W	35,5 W

processeur monte en puissance, et la mémoire vive grimpe à deux voire quatre gigaoctets, contre un seul pour les boîtiers d'entrée de gamme.

Mais attention, à l'exception de certains serveurs d'entrée de gamme comme le BeeStation de Synology (240 €), les NAS sont vendus nus, sans support de stockage. Il faut donc les compléter avec des HDD, des SSD ou des modules à mémoire flash (M2). L'opération, détaillée plus loin, n'a rien de sorcier, mais elle alourdit l'investissement à consentir pour monter son cloud personnel. Comptez au moins 65 euros pour un HDD de 1 To et près de 700 euros pour le monstrueux – et excellent – modèle de 24 To que Seagate nous a prêté pour nos essais (IronWolf Pro, *voir les modèles conseillés p. 62*). Les SSD sont beaucoup plus chers et bien loin d'offrir les capacités des HDD, même dans le très haut de gamme. Il faut ici débourser en moyenne 80 euros pour un modèle de 1 To et presque 900 euros pour un 8 To. Si les SSD présentent l'avantage sur les HDD de n'émettre aucun bruit et d'être à peu près insensibles aux chocs et aux vibrations, nous recommandons toutefois le choix des disques mécaniques pour leur énorme capacité de stockage. Il faut quand même vérifier leur compatibilité avec le NAS envisagé sur le site du constructeur. Et pour contrôler la fiabilité des disques eux-mêmes, on se reportera aux données régulièrement publiées par le gestionnaire de stockage en ligne Backblaze (bit.ly/46hh3o3). ...

Les SSD sont beaucoup plus chers et bien loin d'offrir les capacités des HDD.

LEXIQUE

CIFS/SMB
Common Internet File System/Server Message Block
Protocole réseau permettant le partage de fichiers et d'imprimantes entre systèmes Windows. Utilisé couramment dans les NAS pour l'accès aux fichiers.

▪▪▪ Le relatif faible prix des disques durs autorise notamment la constitution d'un cloud domestique tolérant aux pannes. L'astuce consiste à répartir les données sur les différents disques grâce à la technologie Raid, pour « *redundant array of independent disks* » (matrice redondante de disques indépendants). Pour en profiter, il faut disposer d'au moins deux disques identiques. Lorsqu'ils sont combinés en mode Raid 1, les données sont dupliquées sur les deux supports, ce qui les protège contre la défaillance de l'un des deux mais réduit la capacité de stockage à celle d'un seul disque. En Raid 0, à l'inverse, les données sont divisées en blocs et distribuées sur les disques, sans redondance. Ce système accélère la lecture et l'écriture et maximise l'espace disponible, mais toutes les données sont perdues en cas de panne de l'un des disques. Les NAS à quatre baies autorisent la création de volumes plus élaborés en Raid 5, qui octroie une capacité de stockage équivalente à celle de trois disques et une tolérance de panne de l'un d'entre eux.

Aussi pratique en local qu'à distance

Précisons toutefois que le meilleur des systèmes Raid, à la maison, reste bien moins fiable qu'un gros service de stockage en ligne comme ceux d'Amazon ou Apple. Un NAS demeure vulnérable à un dégât des eaux, à un incendie ou à un choc électrique, qui se traduira immanquablement par la perte de toutes les données. Pour un stockage vraiment sécurisé, il faut copier les données du NAS sur un autre appareil, de préférence situé à un logement différent (en suivant la stratégie 3-2-1 des pros, *lire p. 64*). Côté fonctionnalités et applications, en revanche, les bons NAS en offrent beaucoup plus que les services de stockage en ligne classiques, même les plus chers.
Partage de photos, de musique et de vidéos, gestion de caméras de surveillance, hébergement d'un site web ou d'une boutique en ligne… tout est possible, bien au-delà du simple archivage automatique de données bureautiques, et parfaitement piloté par toutes les marques. Ces NAS sont capables de gérer les documents de toute la famille, en fournissant à chacun un espace

8 DISQUES DE 500 GO À 16 TO

	Marque	Référence	Stockage	Prix
HDD	SEAGATE	IronWolf Pro	16 TO	370 €
HDD	TOSHIBA	N300	12 TO	320 €
HDD	SEAGATE	IronWolf	8 TO	190 €
HDD	WESTERN DIGITAL	WD Red Plus	4 TO	120 €
HDD	SEAGATE	BarraCuda	2 TO	65 €
SSD	SAMSUNG	870 EVO	2 TO	145 €
SSD	WESTERN DIGITAL	WD Red SA500	1 TO	100 €
SSD	CRUCIAL	BX500	500 GO	35 €

INSTALLER UN SERVEUR NAS

Non, les serveurs NAS ne sont pas réservés aux experts. Une petite heure suffit pour mettre en route son propre serveur, du moins pour les sauvegardes de base. Démonstration avec le DS224+ de Synology.

01. PLACEZ LES DISQUES DURS
La plupart des NAS sont vendus nus. Il faut donc les compléter avec un ou plusieurs disques HDD ou SSD, choisis dans la liste des modèles compatibles indiqués sur le site du constructeur. Pour notre boîtier Synology DS224+, nous avons utilisé deux disques de 4 To au format 3,5 pouces (HAT5300-4T). **Ils s'installent très facilement, et sans outil, dans des berceaux amovibles.** Ces derniers peuvent aussi accueillir des supports SSD.

05. ACTIVEZ L'ACCÈS À DISTANCE
Il faut maintenant rendre le NAS accessible depuis internet pour en faire un vrai cloud personnel. **Il suffit pour cela d'activer le service QuickConnect** de Synology, qui convertit l'adresse interne de l'appareil en un lien accessible par tout navigateur. Il faut pour cela créer un compte (gratuit) chez le constructeur. Ceux qui rechignent à confier le routage à Synology peuvent opter pour un service de serveur DNS dynamique (DDNS).

LEXIQUE

NFS
Network File System
Protocole de partage de fichiers principalement employé dans les environnements Unix/Linux. Permet aux utilisateurs d'accéder aux fichiers distants comme s'ils étaient locaux.

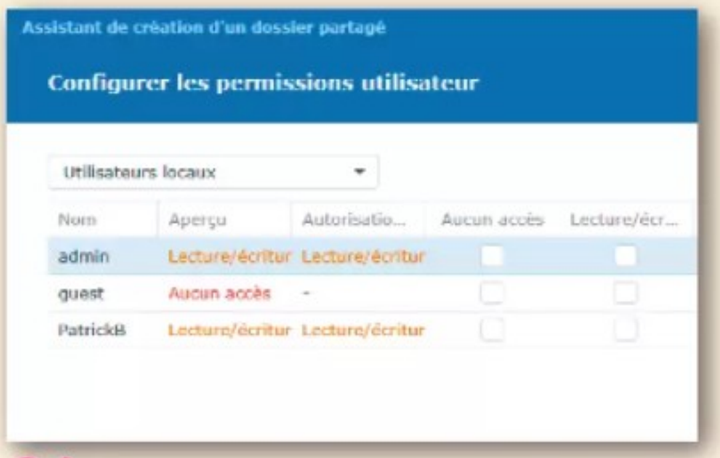
SNAPSHOT
Technique de sauvegarde instantanée d'un état du système ou d'un volume de données à un certain moment. Permet de restaurer rapidement les données en cas de perte ou de corruption.

02. LANCEZ L'INSTALLATION

Une fois le NAS relié à la box du foyer et démarré, il faut installer son système d'exploitation et régler les paramètres de base. Chez Synology, mais aussi chez Qnap ou Asustor, l'opération est à la portée de tous **grâce à un petit programme d'assistance**, qu'il suffit de lancer depuis un ordinateur relié au même réseau que le NAS. Particulièrement bien fait, celui de Synology guide l'utilisateur étape par étape. Quelques minutes suffisent, sans compétences spécifiques.

03. OUVREZ UN ESPACE DE STOCKAGE

Le programme d'installation propose ensuite la création d'un ou plusieurs espaces de stockage et le choix du niveau de protection des données. **Celui-ci dépend en partie de la configuration Raid retenue pour la composition des disques internes.** Sur le DS224+, il est possible d'opter pour le Raid 0, qui combine les capacités des deux disques mais n'autorise aucune tolérance de panne. En Raid 1, les données sont copiées sur les deux disques.



04. CRÉEZ DES COMPTES D'UTILISATEUR

L'interface du NAS est désormais accessible depuis tout ordinateur relié à la box du foyer, en entrant l'adresse locale qui lui a été attribuée à l'étape précédente. Il est ensuite très simple de **créer des dossiers et des droits d'accès pour tous les membres de la famille** (lecture seule, lecture et écriture, pas d'accès du tout…) comme sur un serveur pro. Le système propose aussi l'activation des services de fichiers en réseau courants (SMB, AFP, FTP…).

06. AJOUTEZ DES FONCTIONS AU NAS

Au-delà de la sauvegarde de données, les NAS de Synology (et de Qnap et Asustor) assurent de nombreuses fonctions grâce à des applications, presque toutes gratuites, à télécharger depuis un magasin d'applis. **Nous recommandons notamment Synology Photos (bit.ly/4kZczJE), qui sauvegarde et classe les images de tous les ordinateurs et smartphones reliés au NAS.**

07. INSTALLEZ DES LOGICIELS

Pour simplifier les opérations de sauvegarde et d'accès aux données, Synology propose des logiciels sous Windows, macOS ou Linux, à récupérer sur son site web. Pour le grand public, **les plus utiles sont Synology Photos et le client de sauvegarde automatique Synology Drive (bit.ly/4hJJAa2).** Pour les smartphones Android et Apple, Synology offre aussi toute une panoplie d'applis.

08. PROGRAMMEZ LES SAUVEGARDES

Le NAS est prêt à accueillir toutes les données. Ne reste plus qu'à **désigner les fichiers ou dossiers à mettre à l'abri** depuis les programmes Synology installés sur les différents appareils du réseau. Attention, les premières sauvegardes peuvent être très longues, notamment pour les dossiers photo et vidéo. Pour éviter les effacements involontaires de données, il faut aussi bien choisir le mode de copie.

personnel ou l'accès à des dossiers communs. La possibilité d'y accéder depuis l'extérieur du foyer, par le biais d'un navigateur web ou bien d'une application pour PC ou smartphone, se révèle aussi plutôt magique. L'établissement de la liaison à distance est bien plus simple à effectuer qu'avec un ordinateur classique, ou un serveur domestique fait maison via un logiciel comme TrueNAS *(lire p. 65)*. Les principaux fabricants proposent en effet un service d'accès à distance gratuit qui sert à retrouver le NAS relié sur la box du foyer, en lui donnant une adresse fixe et facile à retenir, accessible depuis l'extérieur. C'est ce que l'on appelle un «vservice de nom de domaine dynamique » ou DDNS. Chez Synology, Qnap et les autres, un assistant de connexion se charge de modifier automatiquement les réglages du NAS et de la box pour ouvrir les ports nécessaires à l'accès distant. Il suffit ensuite d'entrer l'adresse externe, puis son nom d'utilisateur et son mot de passe, pour accéder au NAS depuis le monde entier. Ce système facilite la synchronisation du cloud domestique avec les principaux services de stockage en ligne comme Google Drive, Dropbox ou Apple iCloud, en quelques clics. Très fort !●

LES BONNES PRATIQUES

POUR SAUVEGARDER ET PROTÉGER VOS DONNÉES

Même à la maison, la sécurité des données passe par un peu de rigueur et de méthode. Voici ce que conseillent les experts.

SISI LIU/ISTOCKPHOTO

1 Répertoriez les supports de données

Ordinateurs, téléphones, tablettes, supports de stockage externes : les fichiers importants peuvent être disséminés sur de nombreux appareils. **Prenez le temps de les identifier et de vérifier leur contenu.** C'est l'occasion de repérer les données en doublon (photos, musique, vidéos…) pour réduire le nombre de fichiers à copier et accélérer les sauvegardes.

2 Adoptez la stratégie 3-2-1

Cette méthode est recommandée par les spécialistes de la sécurité dans le cadre professionnel, mais elle est aussi le modèle à suivre pour les particuliers. Elle consiste à réaliser trois copies des données sur deux supports et de déporter l'une d'elles sur un site différent de celui des deux autres. La diversification des supports réduit le risque que tous échouent simultanément en raison d'une vulnérabilité spécifique ou d'une durée de vie limitée. La sauvegarde hors site, elle, protège les données contre les catastrophes locales telles qu'un incendie, une inondation ou un vol. La copie distante peut être placée par exemple sur un cloud en ligne ou un NAS situé dans un autre logement.

3 Renforcez vos mots de passe

Qu'elles soient stockées chez Google ou à la maison, **les données doivent être protégées par des codes d'accès plus complexes que « 123456 » ou « loulou42 » pour résister aux pirates.** La Commission nationale de l'informatique et des libertés rappelle les conseils de base sur son excellent site web. Un bon mot de passe comporte au moins douze caractères, de quatre types différents. Des majuscules, des minuscules, des chiffres et des caractères spéciaux, comme un point d'interrogation ou un symbole monétaire. Un gestionnaire de mots de passe comme 1Password.com ou Dashlane (bit.ly/4hNdN86) simplifie leur création, leur mémorisation et leur utilisation sur de multiples plateformes. Il est aussi recommandé d'activer la double authentification (code envoyé par mail ou SMS).

4 Automatisez les sauvegardes avec les bons outils

Règle numéro un de la sauvegarde : **elle doit être régulière, effectuée chaque semaine, voire chaque jour pour le télétravail ou la création numérique.** Cette tâche fastidieuse peut être en partie assurée par les systèmes de sauvegarde automatique de Windows et macOS. Mais pour choisir précisément les données à récupérer, le rythme des copies et l'emplacement de stockage, mieux vaut opter pour un bon NAS ou un logiciel spécialisé. Aomei Backupper (bit.ly/4iZEmYH) ou EaseUS Todo Backup (bit.ly/3ZCUngo) conviennent à la majorité des besoins. Pour sauvegarder une « image » complète d'un ordinateur, système d'exploitation compris, nous recommandons Acronis True Image (bit.ly/427XH3c), accessible à partir de 35 euros par an.

5 Déconnectez votre support de sauvegarde après utilisation

Dans ses recommandations aux particuliers, **le site Cybermalveillance.gouv.fr préconise de ne pas laisser un support de sauvegarde comme un disque dur externe ou une clé USB relié en permanence à un ordinateur**. En cas d'attaque informatique par un virus ou un rançonlogiciel, l'unité de sauvegarde peut être affectée par le programme malveillant. Mieux vaut donc la déconnecter ou la placer hors ligne lorsqu'elle n'est pas utilisée. Il est également recommandé de vérifier régulièrement le bon fonctionnement des supports de sauvegarde pour éviter les mauvaises surprises. Attention notamment aux clés USB !

CRÉEZ VOTRE CLOUD DOMESTIQUE AVEC UN VIEUX PC

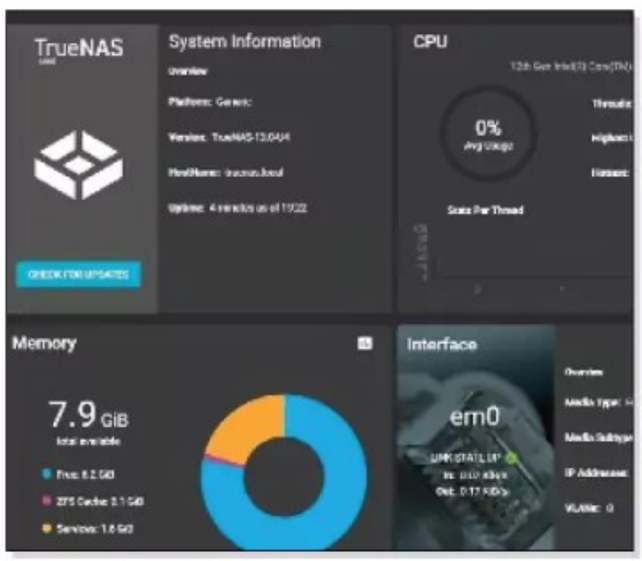
Pas de budget pour un NAS ? Recyclez donc un vieux PC au format tour ou un PC portable en serveur domestique grâce au logiciel TrueNAS, puissant et entièrement gratuit.

1 RÉUNISSEZ LE MATÉRIEL

Un petit PC au format tour est idéal pour un serveur domestique, étant facile à ouvrir pour ajouter des disques durs. TrueNAS propose en effet la création de volumes de stockage sécurisés en mode Raid, qui nécessite au minimum deux disques. Il est toutefois possible d'utiliser TrueNAS sur un PC portable équipé d'un seul support de stockage, mais il faudra alors se passer des fonctions Raid.

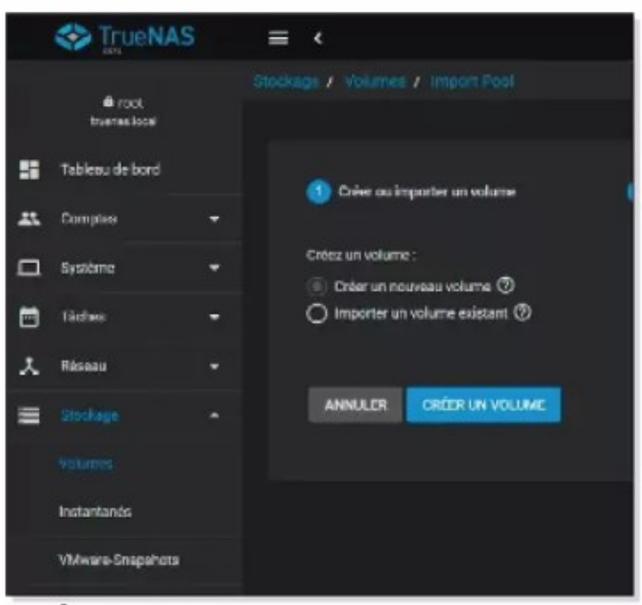
2 PRÉPAREZ L'INSTALLATION

Pour la partie logicielle, vous aurez besoin d'une clé USB d'au moins 8 Go. Téléchargez l'image disque de TrueNAS Core (bit.ly/4bXOL37), puis enregistrez-la sur une clé USB démarrable avec le logiciel gratuit Rufus (bit.ly/3YabZ2M). Branchez la clé sur le PC et forcez son démarrage prioritaire dans le Bios du PC pour lancer TrueNAS. Le PC doit être connecté au réseau du foyer par un câble Ethernet.



3 RÉCUPÉREZ L'ADRESSE DU SERVEUR

Une fois l'assistant affiché à l'écran, lancez l'installation (menu 1) puis désignez le support de stockage qui doit abriter le système. La suite ne demande qu'un nom d'utilisateur, un mot de passe et quelques options à valider. Après quelques minutes, l'interface indique l'adresse attribuée à TrueNAS par la box du foyer, par exemple 192.168.1.3. Il suffit ensuite d'entrer cette adresse dans un navigateur web, depuis un autre ordinateur, pour configurer le serveur.

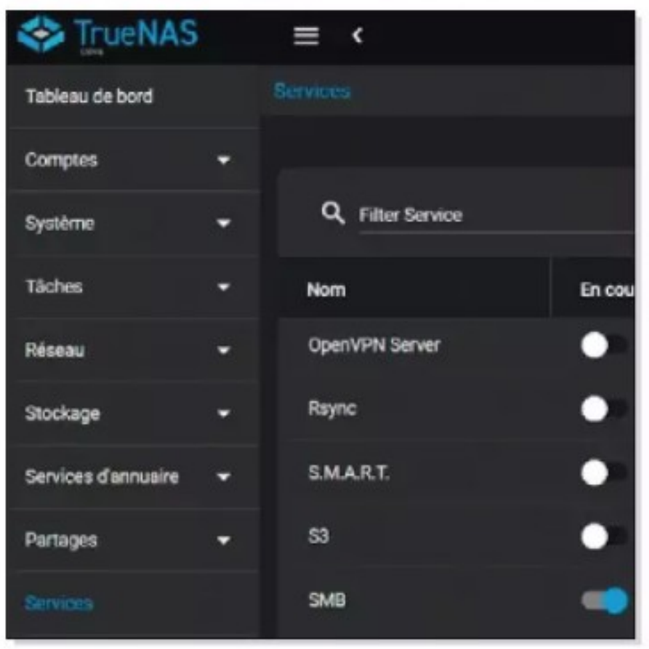


4 CRÉEZ LE VOLUME DE STOCKAGE

Les choses sérieuses commencent. Depuis le panneau d'accueil de TrueNAS, localisez le serveur (langue, fuseau horaire…) et ajustez les paramètres réseau de base (adressage DHCP ou fixe) avant de créer le volume ou « pool » de stockage et les différents dossiers partagés. Il faut ensuite définir les utilisateurs et leurs droits d'accès aux divers dossiers.

5 PARTAGEZ VOTRE NAS

Les services réseau sont activés et réglés depuis l'onglet Services, pour rendre le NAS accessible aux PC (avec le protocole Samba, ou SMB) et aux Mac (AFP) en réseau local. Sous Windows, le support de stockage partagé apparaît dans l'Explorateur de fichiers. Pour l'accès à distance, il faut disposer d'un service de redirection d'adresse IP (DynDNS) et modifier certains des ports de la box du foyer.



6 AJOUTEZ DES FONCTIONS

TrueNAS propose de nombreux plugins pour ajouter des fonctionnalités comme des serveurs médias, des outils de sauvegarde, des gestionnaires de téléchargement… Depuis l'interface principale, cliquez sur Plugins pour découvrir et installer les modules disponibles, comme le serveur multimédia Plex ou les modules Nextcloud et OwnCloud pour la synchronisation avec d'autres appareils.

DIFFICULTÉ **MODÉRÉE** TEMPS **30 MIN** DOMAINE **MESSAGERIE**

PASSEZ AU CRIBLE LES PIÈCES JOINTES SUSPECTES

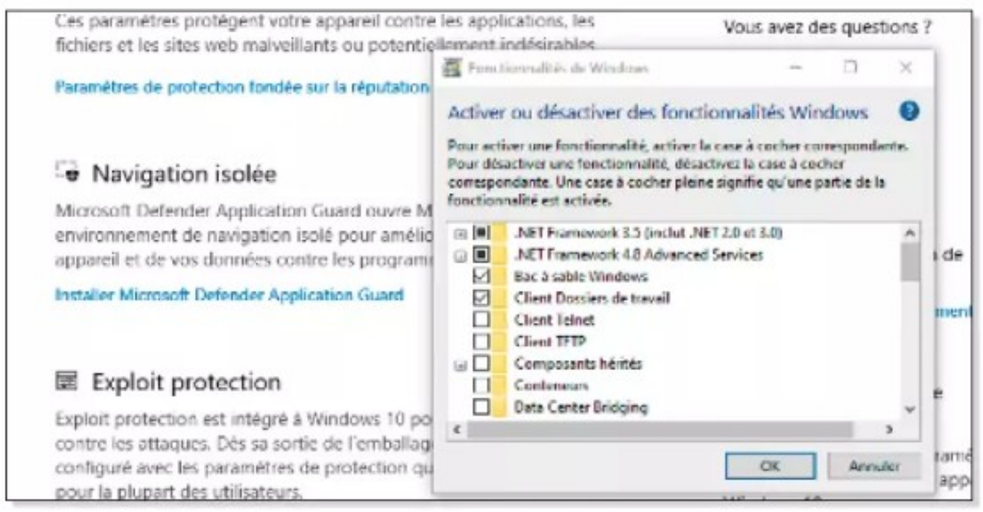
La cybercriminalité ne s'est jamais aussi bien portée. Il suffit d'une seule erreur pour faire vaciller votre système et perdre de précieux fichiers.

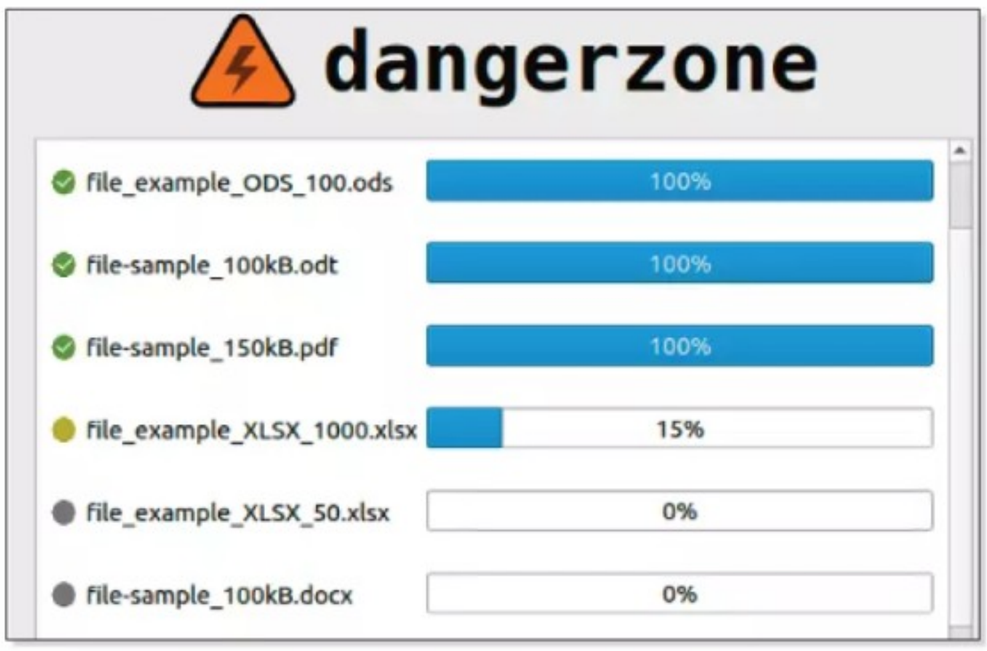
1 PROTÉGEZ VOTRE BOÎTE MAIL AVEC SÉCURITÉ WINDOWS

La protection de Microsoft se fait en amont de l'arrivée des mails dans la boîte de réception. La majorité des menaces sont envoyées dans les courriers indésirables. Dans **Sécurité Windows**, vérifiez que toutes les fonctions de **Pare-Feu et Protection du réseau** sont activées. Dans **Contrôle des applications du navigateur**, cliquez sur **Paramètres de protection fondée sur la réputation** et vérifiez là aussi que toutes les options sont activées. Smartscreen se charge de vérifier l'innocuité des pages web, dont la web app Outlook.

2 NAVIGUEZ DANS LE BAC À SABLE DE MICROSOFT

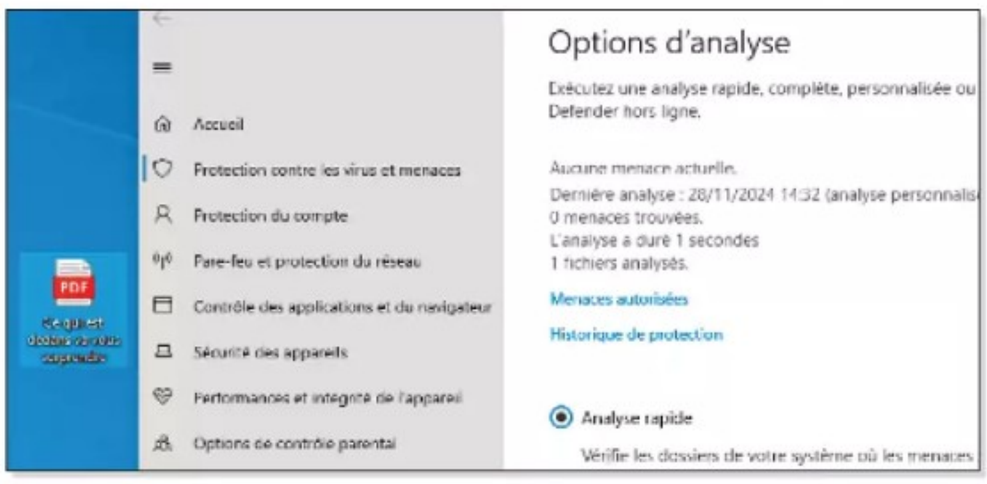
Il est aussi possible d'examiner les mails en exploitant la machine virtuelle de Microsoft Defender Application Guard. Il faut toutefois que la virtualisation soit activée dans l'UEFI et que votre appareil soit compatible. Rendez-vous dans **Windows Defender**, **Contrôle des applications et du navigateur** et, sous **Navigation isolée**, cliquez sur **Microsoft Defender Application Guard**. Cochez ensuite **Bac à sable Windows**. Une fois l'ordinateur redémarré, lancez l'application Sandbox pour naviguer et lire vos pièces jointes sans risque de contaminer votre PC. Dans le menu de Edge, cliquez sur Nouvelle fenêtre application guard pour naviguer de manière ponctuelle sur une page web isolée dans un bac à sable.





3 CONFIEZ VOS DOCUMENTS À DANGERZONE

Dangerzone converti les PDF, les images ou document Office en PDF sécurisé en exploitant le processus du bac à sable. Installez au préalable le logiciel Docker.desktop (bit.ly/4eQVJIL), puis créez un compte. Il s'agit d'un outil de conteneurisation pour les développeurs. Il est donc préférable de s'en remettre aux deux étapes précédentes si vous n'avez pas l'utilité de Docker. Une fois ce dernier installé, rendez-vous à l'adresse bit.ly/3Zp58Tq pour télécharger et installer l'application Dangerzone. Une fois celle-ci lancée, il suffit de glisser des documents dans l'appli et de cliquer sur **Convert to safe document**.



4 ADOPTEZ LES BONNES PRATIQUES

La première faille de tous les systèmes informatiques reste le facteur humain. Lorsqu'un contact envoie une pièce jointe, vérifiez d'abord la ligne **De**. Le nom de la personne que vous connaissez a pu être posé sur une autre adresse de messagerie. Si le mail contient un exécutable, effacez-le systématiquement. Pour les images ou documents Office, effectuez un clic droit dessus et optez pour l'option **Analyser avec Microsoft Defender** (ou n'importe quel autre antivirus).

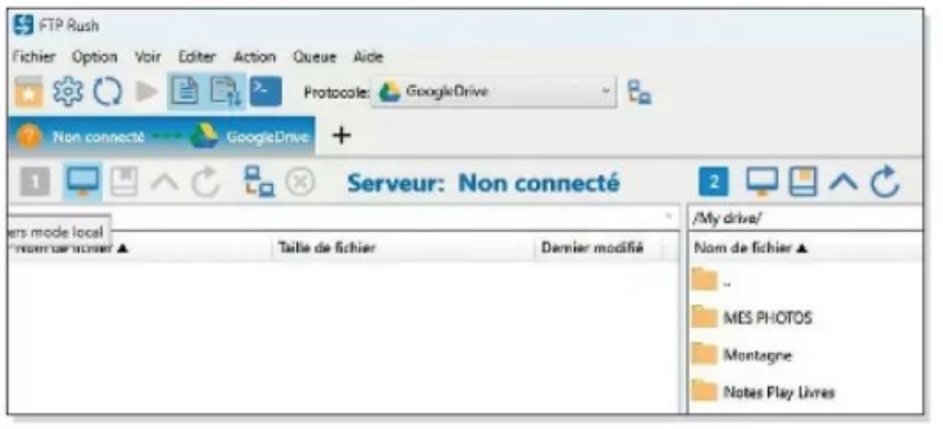
DIFFICULTÉ **MODÉRÉE** TEMPS **30 MIN** DOMAINE **CLOUD**

GARDEZ DES DOUBLES DE VOS FICHIERS

Deux ou trois précautions valent mieux qu'une. N'hésitez pas à recourir à vos comptes Microsoft et Google pour multiplier les copies de vos documents, photos et vidéos.

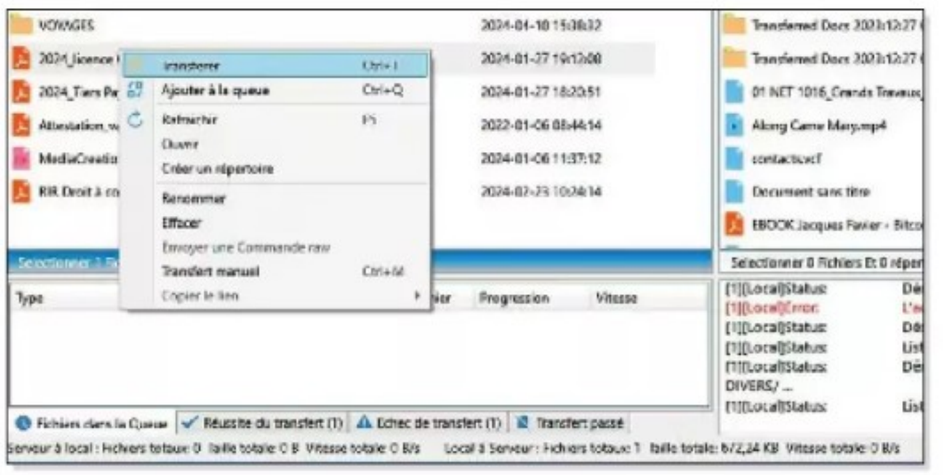
1 CONNECTEZ GOOGLE DRIVE AU SERVEUR FTP

Pour des transferts entre les services cloud ou depuis un disque dur, nous allons employer le protocole FTP. Installez et lancez l'utilitaire gratuit FTP Rush v3 (wftpserver.com/download.htm) dans sa version Windows NET Framework. 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.



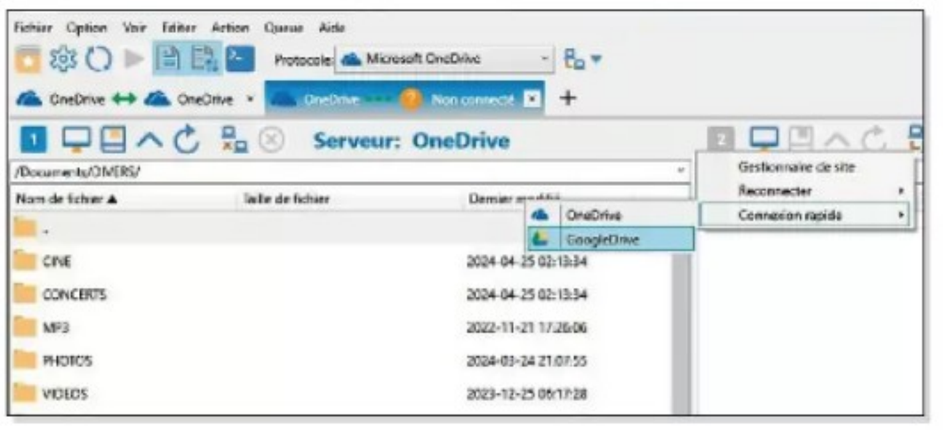
2 TRANSFÉREZ UN FICHIER DU PC VERS LE CLOUD

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.



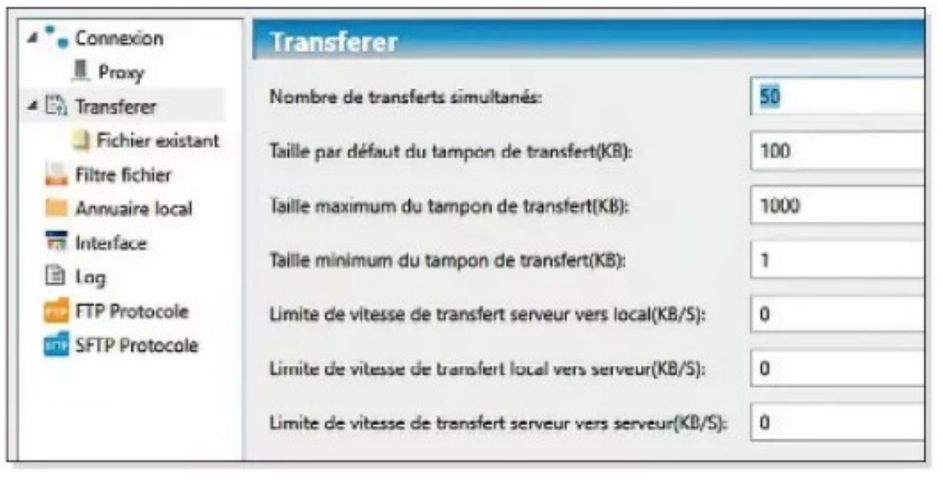
3 ÉCHANGEZ DES ÉLÉMENTS ENTRE GOOGLE DRIVE ET ONEDRIVE

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.



À LA RECHERCHE DES DOCUMENTS PERDUS

DIFFICULTÉ **VARIABLE**
TEMPS **VARIABLE**
DOMAINE **SYSTÈME**

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 hackers 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 appli 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 et/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

Smartphone Android ou iPhone

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

RÉCUPÉREZ DES FICHIERS SUR VOTRE PC

Lorsqu'un fichier disparaît de l'ordinateur, **cela ne signifie pas qu'il est définitivement perdu**. Sauf en cas de reformatage du disque dur. Il existe plusieurs méthodes, plus ou moins simples et performantes, pour le récupérer.

1 VÉRIFIEZ LE CONTENU DE 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.

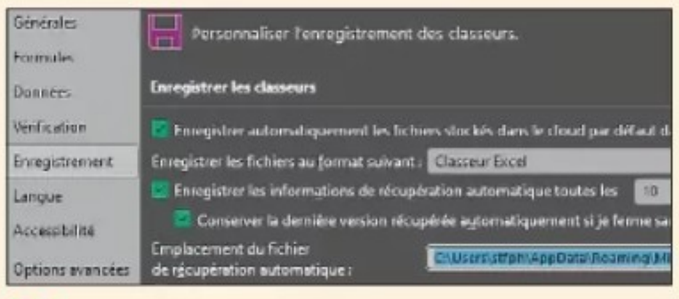
4 TENTEZ VOTRE CHANCE AVEC L'UTILITAIRE RECUVA

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

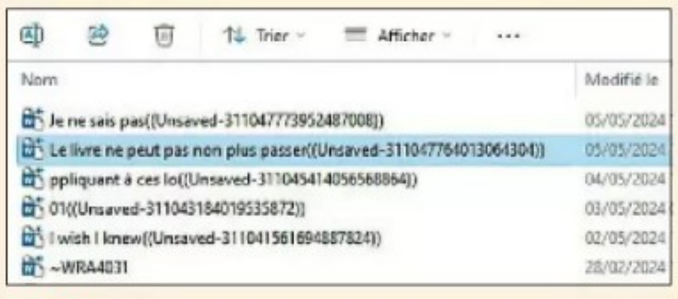
RETROUVEZ VOS DOCUMENTS OFFICE

La suite bureautique proposée par Microsoft regorge de petites astuces utiles qui permettent de **retrouver plus facilement des documents** Word, Excel ou PowerPoint égarés ou supprimés.



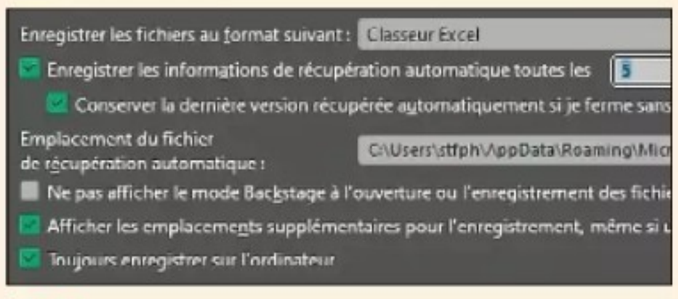
01. Repérez l'emplacement du fichier de récupération

Ouvrez 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**.

PARTEZ À LA RECHERCHE DE VOS FICHIERS SUR MAC

Fidèle à sa réputation, **Apple mise sur une interface intuitive** qui rend la recherche et la récupération de fichiers, dossiers ou applications à la fois simple et agréable.

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**.

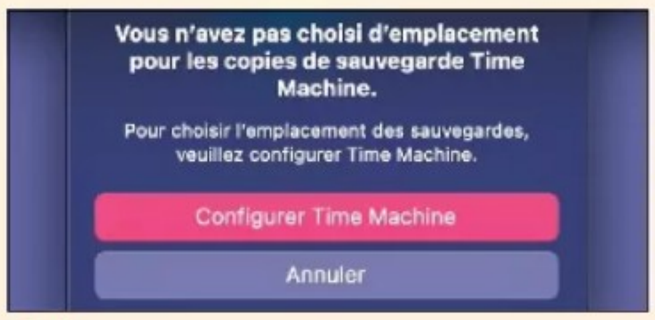
4 RECOUREZ AUX COMMANDES DU TERMINAL

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

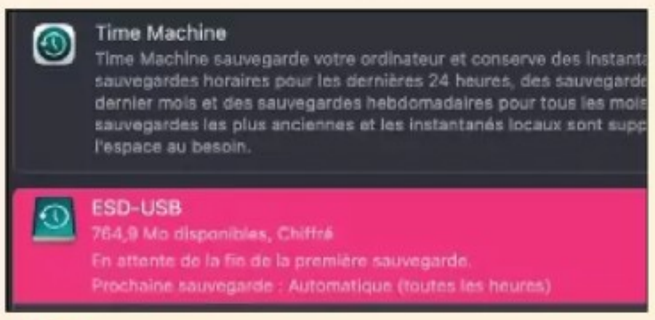
REMONTEZ LE TEMPS AVEC TIME MACHINE

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

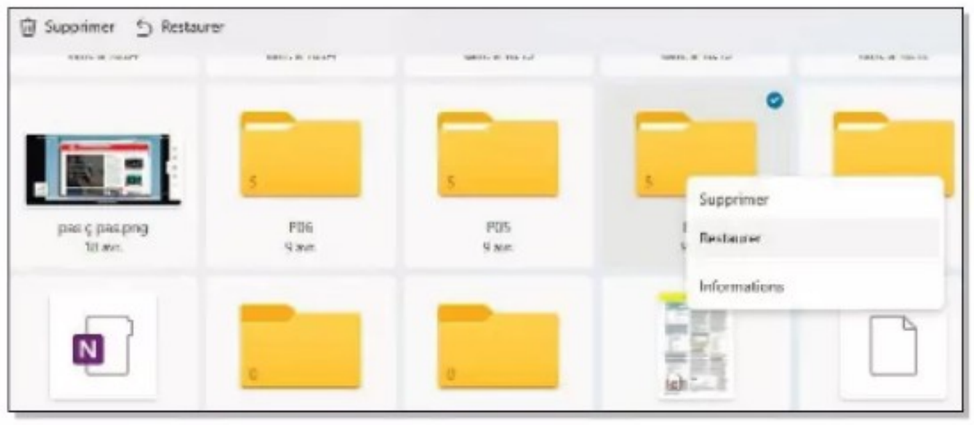
S'il existe des sauvegardes, vous pouvez y accéder à tout moment pour restaurer une version passée de votre Mac. Ouvrez de nouveau Time Machine. L'application dresse la liste des archives accessibles. Utilisez les options disponibles pour ajuster la fréquence des sauvegardes.

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 LES PROFONDEURS DU CLOUD

Les principaux services de stockage en ligne gardent un historique des modifications apportées à vos documents, ainsi qu'une sauvegarde temporaire des fichiers supprimés et placés dans la corbeille



1 EXPLOITEZ LES OPTIONS DE ONEDRIVE

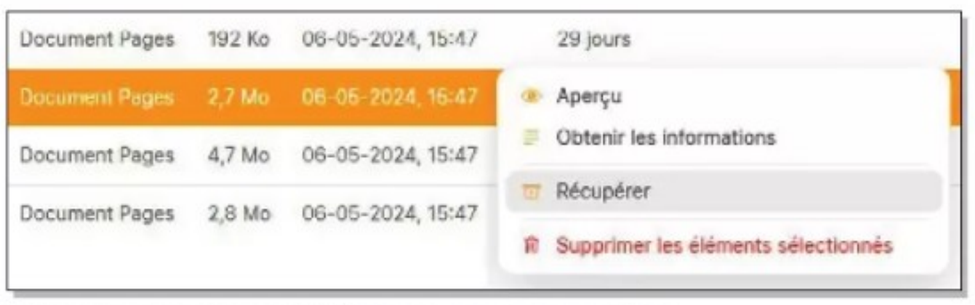
Si vous disposez d'un abonnement premium au cloud de Microsoft, OneDrive (à partir de 20 €/an), vous avez une chance supplémentaire de retrouver un fichier déposé dans la corbeille. Accédez à cette dernière en opérant un clic droit sur l'icône en forme de nuage à droite de la barre des tâches. Pointez 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.

Déterrez 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.

FOUILLEZ 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

METTEZ VOS PHOTOS ET VIDÉOS À L'ABRI DANS LE CLOUD

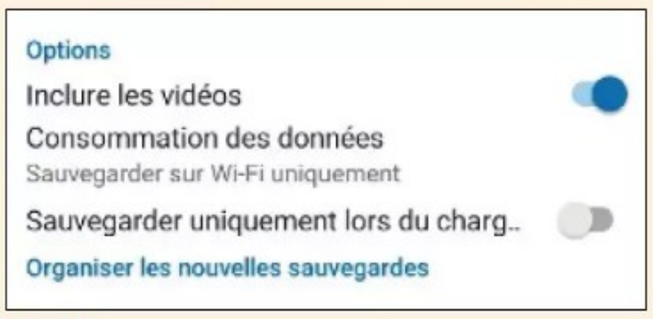
Les applications de stockage en ligne comme Dropbox ou OneDrive sont capables d'enregistrer automatiquement sur leurs serveurs les photos et vidéos que vous capturez avec l'appareil photo de votre smartphone.

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…

RÉPAREZ LES DISQUES ET CLÉS DE STOCKAGE

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.

Restaurez 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.

DIFFICULTÉ **MODÉRÉE** TEMPS **30 MIN** DOMAINE **SÉCURITÉ**

N'ÉPARPILLEZ PLUS VOS CODES AVEC AUTHENTICATOR

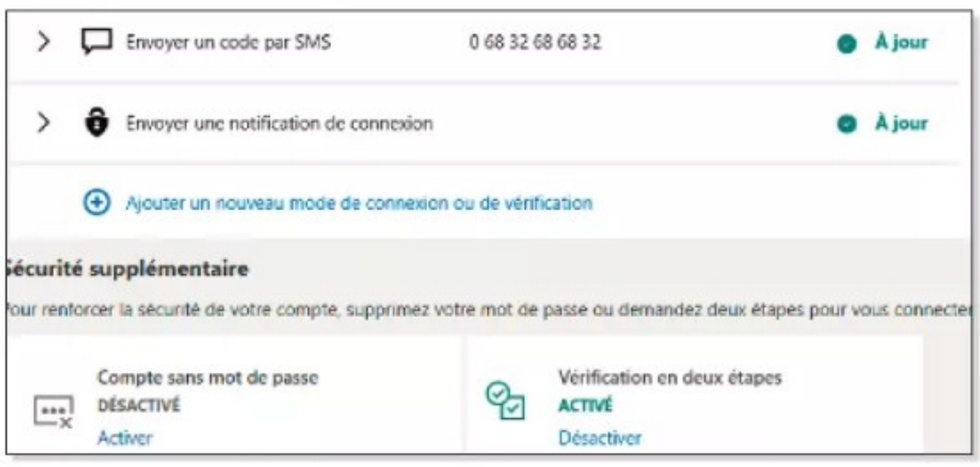
Grâce à l'application de Microsoft, vous n'avez plus à mémoriser vos identifiants et mots de passe. Les sites auxquels vous tentez d'accéder sur votre PC communiquent avec votre téléphone pour vérifier votre identité.

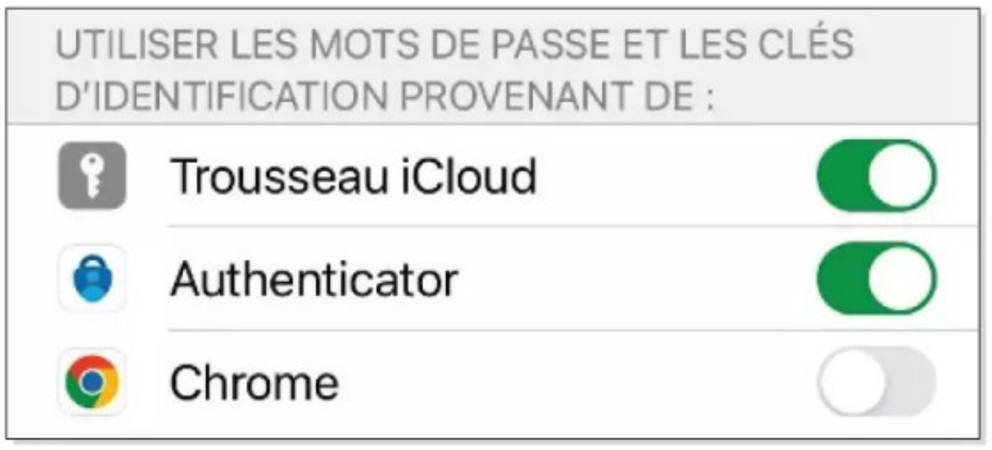
1 RÉCUPÉREZ VOS IDENTIFIANTS

Rendez-vous sur le Google Play ou l'App Store pour télécharger et installer l'application Microsoft Authenticator (bit.ly/4iGUGx5) sur votre smartphone. Au premier démarrage, vous devez fournir l'adresse mail et le mot de passe de votre compte Microsoft. Si vous utilisez le navigateur Edge, tous vos mots de passe sont automatiquement importés dans l'application. Touchez l'icône **Mots de passe** au bas de la page d'accueil d'Authenticator pour y accéder. Sélectionnez n'importe quel compte pour afficher le nom d'utilisateur et le mot de passe associés.

2 ACTIVEZ LA DOUBLE AUTHENTIFICATION

De plus en plus de sites recourent à la double authentification, qui impose d'avoir son mobile en main pour valider son identité. Rendez-vous, par exemple, sur votre compte Microsoft (account.live.com), cliquez dans la colonne de gauche sur **Sécurité** et **Gérer la façon dont je me connecte**. Dans **Sécurité supplémentaire**, sous **Vérification en deux étapes**, choisissez **Activé** et **Suivant**. Une notification est envoyée sur votre téléphone. Touchez celle-ci pour ouvrir l'application Authenticator. Votre compte Microsoft a été ajouté à la section **Authenticator**. À chaque fois que vous essaierez de vous connecter depuis un nouvel ordinateur, il vous faudra insérer le code à usage unique fourni par Authenticator.





3 IMPORTEZ VOS TROUSSEAUX

Sur votre PC, ouvrez les paramètres de Microsoft Edge (**Alt** + **F**) et sélectionnez **Mots de passe**. Cliquez sur l'icône ···, **Importer des mots de passe**. Si ces derniers sont enregistrés dans le portefeuille de Google Chrome, vous avez juste à cliquer sur **Importer**. Avec d'autres gestionnaires, exportez les données au format CSV. Pointez ensuite sur le menu déroulant **Importer depuis**, **Fichier CSV de mot de passe** et **Importer**. Les éléments importés sont synchronisés sur votre mobile. Sous Android 15, rendez-vous dans les **Paramètres**, **Mots de passe et comptes** et activez le curseur **Authenticator** sous **Fournisseurs supplémentaires** (Google utilise un Authentificator équivalent pour Chrome). Avec un iPhone (iOS 18), rendez-vous dans les **Réglages**, **Général**, **Remplissage auto. et mots de passe**.

4 VERROUILLEZ LES ACCÈS

Le lancement d'Authenticator est protégé par le verrouillage biométrique du mobile. Dans le cas d'un iPhone, par exemple, il faut donc vous identifier à l'aide de Face ID afin d'afficher le code à usage unique. Si vous prêtez votre mobile, vous pouvez ajouter une couche de sécurité supplémentaire. Dans les réglages d'iOS, touchez ainsi l'intitulé **Authenticator** et activez le curseur **Face ID** sur la droite. Ainsi, même si le téléphone est déverrouillé, il faudra lui soumettre votre visage pour débloquer l'accès aux mots de passe. Est-il utile de souligner que la session de votre PC doit aussi être verrouillée par un mot de passe solide pour que personne n'accède à vos sésames ?

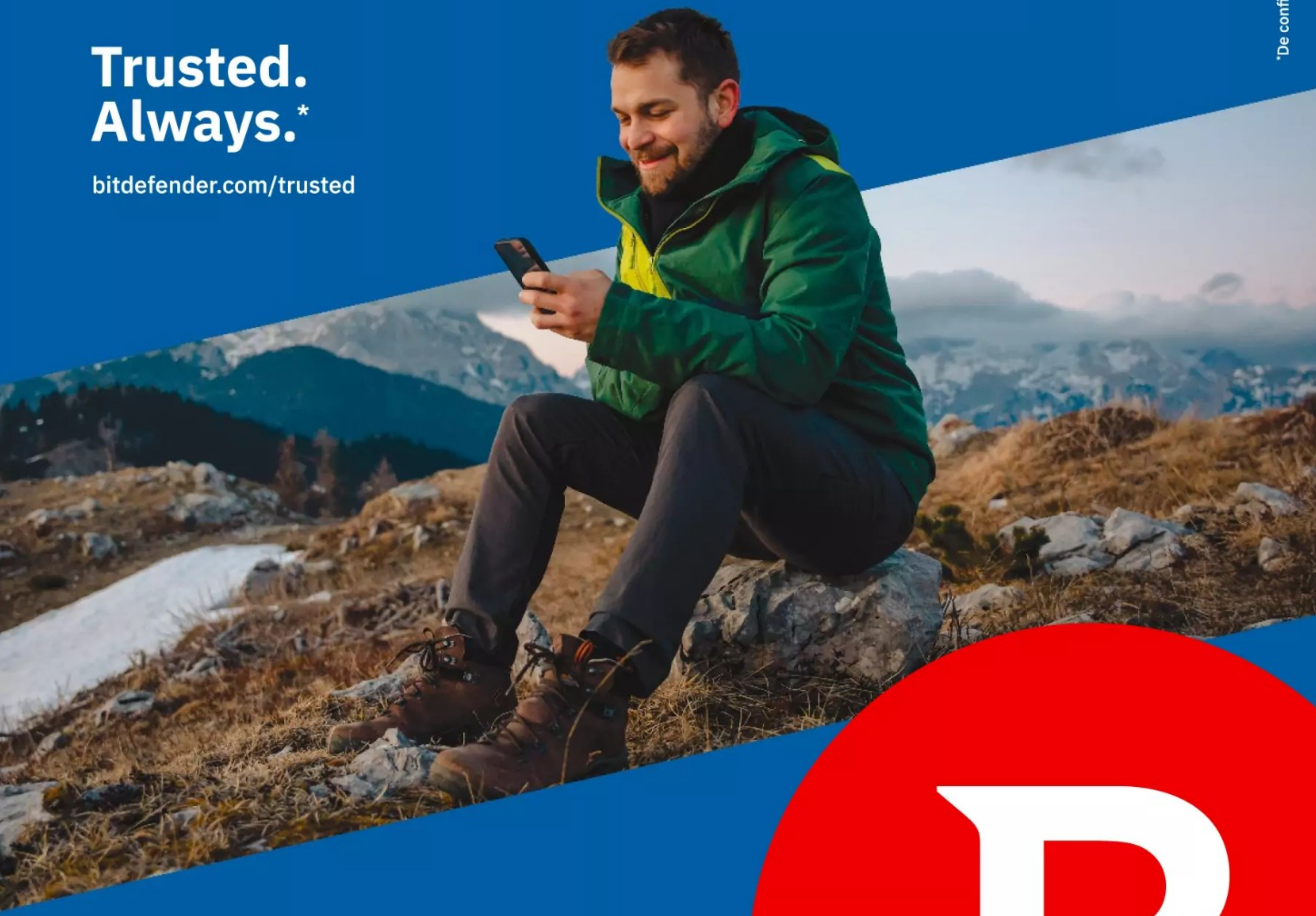
Bitdefender®

Leader Mondial
en Cybersécurité

Restez en mouvement.
En toute sécurité.

Trusted.
Always.*

bitdefender.com/trusted



*Des partenaires de confiance. Toujours.

EU
MADE IN EUROPE

Le partenaire Européen de confiance
pour protéger votre vie numérique

Avast

Protection en ligne contre les menaces les plus récentes. C'est gratuit.

Téléchargez gratuitement sur
avast.com/01net

Avast Antivirus Gratuit

- Antivirus primé
- Protection contre les escroqueries en ligne
- Facile à installer et à utiliser