N° 112 Septembre - Octobre 2019

01NET PRATIQUE

DES TECHNOLOGIES ET DES HOMMES

SPÉCIAL SÉCURITÉ INFORMATIQUE

- Protégez votre ordinateur
- Préservez vos données
- Sécurisez votre box

90 PAGES DE TUTORIELS

Belgique : 5,80 € - Luxembourg : 5,80 € - DOM S : 6,70 € - DOM A : 7 € - TOM S : 785 CFP - Maroc : 62 DH - Tunisie : 7,30 TND - Suisse : 9,90 FS - Canada S : 9,90 $ CAD - Portugal : 6,60 €

M 05458 - 112H - F: 5,50 € - RD

01NET HORS-SÉRIE PRATIQUE N° 112 SEPTEMBRE OCTOBRE 2019

01NET HORS-SÉRIE

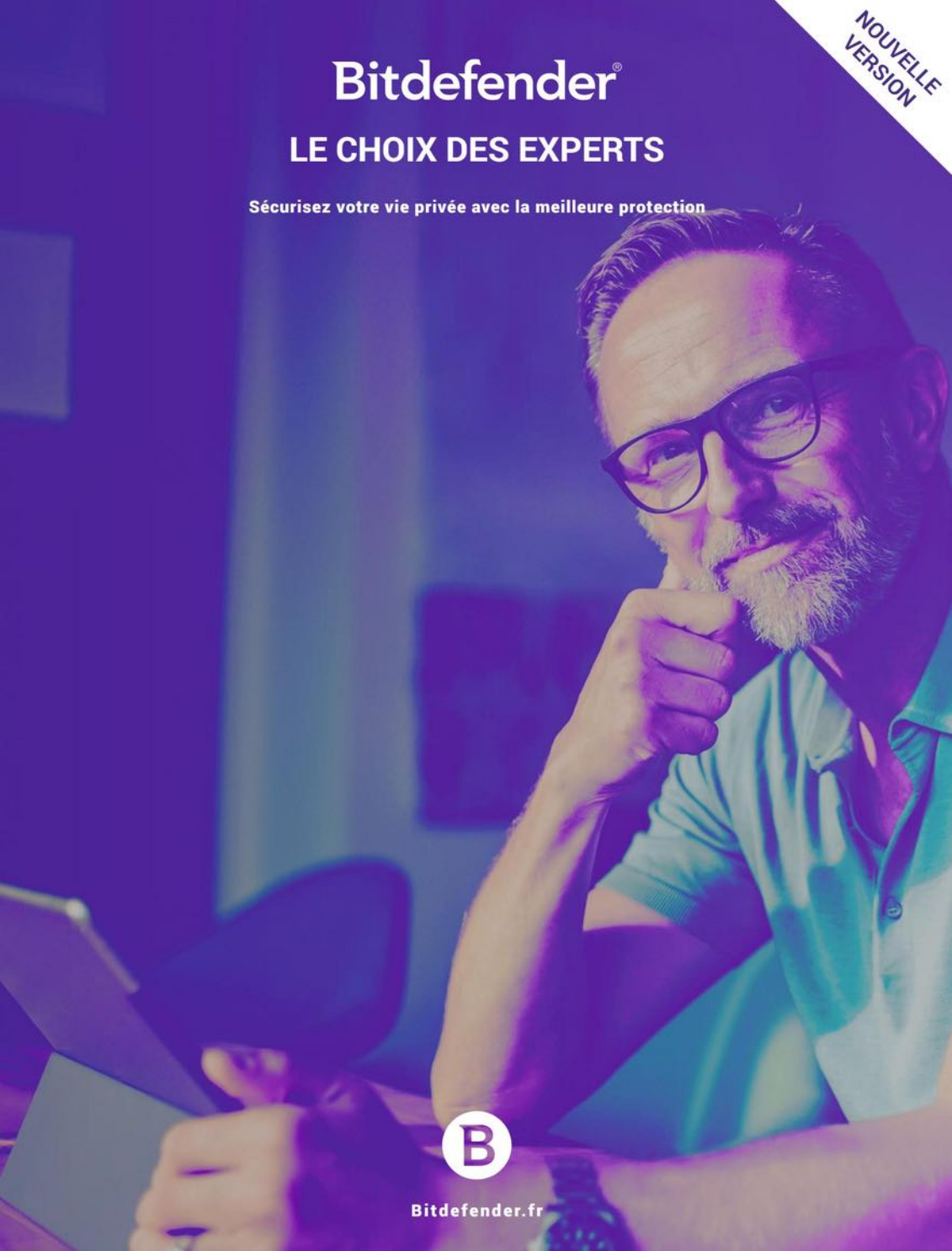
SPÉCIAL SÉCURITÉ INFORMATIQUE

NOUVELLE VERSION

Bitdefender®

LE CHOIX DES EXPERTS

Sécurisez votre vie privée avec la meilleure protection



Bitdefender.fr

UNE BATAILLE DE GAGNÉE, MAIS LA GUERRE N'EST PAS FINIE

Retadup. Ce nom sonne comme un désherbant à la composition chimique suffisamment nocive pour détruire tout sur son passage. La réalité n'est pas si éloignée. Il s'agit d'un ver informatique aux pouvoirs tout aussi dévastateurs, que les gendarmes français du C3N, le Centre de lutte contre les criminalités numériques, ont réussi à neutraliser n août. Le monstre avait infecté près de 900000 PC à travers le monde (essentiellement en Amérique latine). Objectif ? Créer un botnet, un réseau de machines « zombies » à la solde des pirates. Sans que leurs propriétaires n'en aient conscience, la puissance de calcul des ordinateurs était exploitée pour le minage de cryptomonnaie, mais pas seulement. La prise de contrôle à distance pouvait aussi conduire des attaques concertées vers des serveurs cibles a n de les rendre inutilisables. Alertés par l'éditeur d'antivirus Avast au printemps dernier, les cybergendarmes ont réussi à mettre la main sur le centre de contrôle des pirates basé en Île-de-France et à désinfecter l'intégralité des machines zombie, dont un millier se trouvaient dans l'Hexagone. Ouf !

Retadup vient ainsi s'ajouter à la longue liste des virus et autres rançongiciels (ransomwares) qui sévissent depuis les débuts de la micro et contre lesquels du bon sens, une bonne hygiène numérique et une protection antivirale efficace peuvent suffire. C'est ce que nous vous détaillons dans ce 112e hors-série. Suivez nos conseils et votre ordinateur restera à l'abri des mauvaises surprises.●

01NET

CAMPUS ALTICE
2, rue du Général Alain de Boissieu
75015 Paris

DIRECTRICE DE LA PUBLICATION
Jacqueline Galante

ABONNEMENTS
Tél. : 01 70 37 31 74 (du lundi au vendredi de 9 h 00 à 18 h 00)
abonnement.01net@groupe-gli.com
www.kiosque01.fr
1 an, soit 22 numéros
France : 59 euros TTC (TVA 2,10 % incluse)
France Étudiant : 49 euros TTC (TVA 2,10 % incluse) sur justificatif d'une carte d'étudiant en cours de validité
France avec 6 hors-séries : 79 euros TTC (TVA 2,10 % incluse)
Suisse : www.edigroup.ch
Belgique : www.edigroup.be
Autres pays : www.kiosque01.fr

Pour joindre votre correspondant, faites précéder les quatre chiffres entre parenthèses de 01 87 25

COORDINATEUR DE CE NUMÉRO
Fabrice Brochain (88 30)
fbrochain@groupelexpress.fr

RÉDACTEUR EN CHEF
Amaury Mestre de Laroque
amestredelaroque@groupelexpress.fr

SECRÉTAIRE GÉNÉRALE DE LA RÉDACTION
Christelle Denis (88 43)
cdenis@groupelexpress.fr

DIRECTEUR ARTISTIQUE
Jean-Paul Chantrieux (88 27)
jpchantrieux@groupelexpress.fr

RÉDACTION ET RÉALISATION
Alchimie Médias
www.alchimiemedias.com

ONT COLLABORÉ À CE NUMÉRO
Sandrine Liger (88 24)
sliger@groupelexpress.fr
Georges Prétat (88 26)
gpretat@groupelexpress.fr

PUBLICITÉ
Altice Media Publicité
DIRECTEUR COMMERCIAL PÔLE NEWS CULTURE
Pierre-Étienne Musson (85 60)
DIRECTEUR DE CLIENTÈLE
Olivier Denis (89 52)
RESPONSABLE COORDINATION INTERNATIONALE
Lydie Gerard (86 54)

Imprimé en France par Maury
45330 Malesherbes Cedex
SERVICE DES VENTES (réservé aux dépositaires et marchands de journaux)
A Juste Titres La Roseraie B1,
20, traverse de la Buzine 13011 Marseille
Tél. : 04 88 15 12 47

Audience mesurée par AUDIPRESSE

01NET est édité par la société 01net Mag
PRÉSIDENT 2BCG média, représenté par Jacqueline Galante
SAS au capital de 10 000 euros
SIÈGE SOCIAL 2, rue du Général Alain de Boissieu 75015 Paris
RCS : 799 351 341
Code APE : 5813Z
Siret : 799 351 341 00034
Principal actionnaire : 2BCG média

Commission paritaire
0316 K 78311 - ISSN 2266-7989
Dépôt légal : à parution
Distribution : Transports Presse

Magazine imprimé sur du papier certifié PEFC (sauf encarts). Origine du papier : Italie. Taux de fibres recyclées : 0 %. Eutrophisation. Ptot : 0.094 kg/tonne. Le papier est issu de forêts gérées durablement et de sources contrôlées. pefc-france.org

PEFC 10-31-1282 / Certifié PEFC

ILLUSTRATION DE COUVERTURE : ISTOCK

Tous les prix mentionnés dans les pages de ce hors-série sont donnés à titre indicatif.

Sommaire

Hors-Série N° 2

ORDINATEUR

06 **Protégez votre ordinateur des virus et des malwares**
09 Finissez-en avec les malwares
10 Protégez-vous en mode intégral
12 Reprenez le contrôle d'un PC infecté
13 Gardez votre PC et votre antivirus à jour
13 Faites un bilan sécurité à l'aide d'un antivirus en ligne
14 Verrouillez Windows à double tour
15 Bouclez l'accès à votre PC avec une simple clé USB
15 Vérifiez si vos identifiants ont été piratés
16 Comblez les failles de sécurité
17 Débarrassez-vous d'une mise à jour instable
17 Réparez ou réinstallez Windows après une attaque
18 Redonnez vie à un PC mis à genoux par un virus
19 Testez l'intégrité de votre PC avec Security Analyser
19 Enregistrez une image saine de votre PC
20 Protégez Ubuntu et vos données des virus
20 Empêchez Ubuntu de collecter vos données
21 Épargnez un PC Ubuntu des cyberattaques
21 Anticipez les pannes éventuelles
22 Ne laissez pas votre Mac sans protection
23 Dressez un rempart contre les malwares
23 Placez votre Mac sous sécurité renforcée
24 Créez une clé USB d'installation de Mojave
25 Sécurisez à fond votre compte utilisateur
25 Restaurez et modifiez le mot de passe Apple ID
26 Déplacez-vous sereinement avec votre MacBook
27 Gérez l'accès aux données et ressources de votre Mac
27 Chiffrez les fichiers avec FileVault
28 Sauvegardez le contenu de votre Mac
29 Gardez macOS, les applis et les pilotes à jour

MOBILE

30 **Protégez votre mobile des virus et des malwares**
32 Gardez les publicités à distance
33 Localisez votre mobile en cas de vol
33 Sécurisez le partage de connexion 4G
34 Réactivez un mobile planté
35 Bloquez les applications trop curieuses
35 Verrouillez l'accès au contenu du mobile
36 Prêtez votre téléphone sans risque
37 Évitez les logiciels espions
37 Dotez votre mobile d'une alarme antivol
38 N'exposez pas vos infos personnelles
38 Modérez la curiosité des applications
40 Comblez les failles de sécurité
41 Bloquez l'accès aux applis sensibles
41 Surveillez l'activité de votre enfant
42 Protégez l'accès à votre iPhone
42 Préparez l'iPhone avant de le prêter
43 Traitez un iPhone infecté
43 Localisez et bloquez un iPhone égaré
44 Surveillez vos dossiers cloud
45 Verrouillez l'accès à un mobile Android

RÉSEAU

46 **Protégez l'accès au réseau Wi de votre box Internet**
49 Évitez les connexions pirates
50 Encadrez les usages de vos enfants
51 Coupez le Wifi quand vous n'êtes pas là
51 Partagez le mot de passe Wifi de votre box en toute sécurité
52 Accédez à votre PC à distance sans crainte
53 Profitez des avantages du Bluetooth
53 Filtrez tout ce qui transite par votre ordi
54 Identifiez les activités suspectes
55 Paramétrez votre réseau et venez à bout des pannes
55 Gérez l'accès Wifi sur votre téléphone

INTERNET

56 **Limitez au maximum votre empreinte numérique**
59 Dites-en moins à Windows
60 Modérez la curiosité de votre navigateur
61 Surfez sans prendre aucun risque
61 Débarrassez-vous d'une barre d'outils indésirable
62 Installez et configurez un bloqueur de pubs
63 Empêchez les sites et les applis de vous géolocaliser
63 Naviguez incognito avec le VPN d'Opera
64 Restez discret grâce au mode privé
65 Évitez que Google espionne vos requêtes
66 Gérez les extensions défaillantes
67 Accédez aux options cachées des navigateurs
68 Passez à la double activation
69 Analysez les fichiers avant de les ouvrir
69 Faites le bilan de votre réputation en ligne
70 Adoptez un DNS rapide et très discret
71 Surfez incognito avec Tor Browser
71 Exercez votre droit à l'oubli numérique
72 Évitez de vous exposer sur les réseaux
74 Faites le ménage avant de céder votre PC
75 Gérez les autorisations accordées aux services

DONNÉES

76 **Échangez des chiers sans risque sur le cloud**
79 Renforcez la sécurité du cloud
80 Entretenez votre disque dur
81 Chiffrez vos documents
81 Affichez l'historique des connexions USB
82 Comment retrouver un mot de passe oublié
82 Cachez les applis et les documents
83 Évitez l'exécution de fichiers stockés sur une clé USB
83 Confiez vos codes d'accès à un navigateur
84 Gardez vos mots de passe à l'abri
85 Échangez des fichiers sans les exposer dans le cloud
85 Limitez l'exposition des fichiers partagés
86 Sécurisez les accès à un NAS
87 Bloquez l'accès aux supports de stockage USB
87 Rendez vos fichiers inaccessibles
88 Envoyez des fichiers en mode hypersécurisé
89 Empêchez que l'on exploite le contenu de votre iPhone
89 Restaurez des fichiers effacés par erreur

COMMUNIQUER

90 **Identi ez et déjouez les tentatives d'hameçonnage**
92 Chiffrez vos documents avant de les envoyer
93 Échangez des mails chiffrés avec Tutanota
93 Utilisez une adresse de courrier électronique éphémère
94 Déjouez les tentatives de piratage du compte Gmail
94 Testez la sécurité de votre boîte de réception
95 Échappez aux oreilles des espions grâce à Telegram
95 Conversez en toute discrétion avec Torchat
96 Gardez les courriels indésirables à distance
97 Filtrez les appels et les messages
97 Envoyez des mails confidentiels avec Gmail
98 Confiez vos mails à un postier épris de sécurité
98 Communiquez en toute sécurité avec Mail

MATERIEL.NET
Informatique & High-Tech

DÉCOUVREZ LE PC

★ BACK TO SCHOOL ★

EN SÉRIE LIMITÉE !

- PROCESSEUR AMD RYZEN 5 3600X
- NVIDIA GEFORCE RTX 2080
- 16 GO DDR4 BALLISTIX
- SSD 480 GO NVME CORSAIR + HDD 1 TO

À PARTIR DE

1549,90€

1ER FABRICANT DE PC
EN FRANCE

CONSEILS D'EXPERTS

REMBOURSEMENT DE LA DIFFÉRENCE

30 JOURS POUR CHANGER D'AVIS

SAV 100% NANTAIS

www.materiel.net

Modèle présenté : PC Cardinal (offre dans la limite des 40 premières pièces commandées sans OS et 160 pièces avec OS)
Retrouvez toutes nos conditions sur notre site internet https://www.materiel.net/n4601/fabricant-pc-numero-un/.
Conformément à l'article L.121-21 du Code de la consommation, le consommateur dispose d'un délai de 14 (quatorze) jours pour exercer son droit de rétractation.
MATERIEL.NET BP 64505 Grandchamp des Fontaines - 44245 La Chapelle sur Erdre Cedex.

DIFFICULTÉ MODÉRÉE TEMPS 1 H DOMAINE ANTIVIRUS

PROTÉGEZ VOTRE ORDINATEUR DES VIRUS ET DES MALWARES

Des millions de programmes malveillants apparaissent chaque année. De plus en plus sophistiqués, ils prennent vos données en otage ou s'attaquent à vos informations confidentielles. Se protéger n'est pas une option ! Installé sur tous les PC, Windows Defender veille au grain.

La sécurité des données et réseaux ne se conçoit pas comme la protection de votre domicile. Vous n'êtes pas observé par un cybercriminel décidé à rentrer dans votre machine. Les attaques sont plus complexes, globales, et facilitées par le nombre croissant d'objets connectés. Selon une étude commandée par Qualitel (association pour la qualité de l'habitat) parue en 2018, 30 % des logements récents recourent à au moins deux services connectés (vidéosurveillance, gestion du chauffage, etc.). Autant de portes d'entrée pour introduire un malware dans vos réseaux.

Ces intrusions n'ont pas pour unique but d'anéantir ou de voler vos données. Certaines se contentent d'exploiter la puissance de calcul de votre ordi – pour miner les cryptomonnaies par exemple – ou votre connexion Internet pour créer un réseau maillé d'ampleur à des ns criminelles. Conscient de la menace, Microsoft n'a cessé d'améliorer son application antivirus. Windows Defender protège les PC équipés de Windows 10. Une présence qui ne doit pas toutefois vous empêcher de rester vigilant. Les techniques telles que le phishing ou les ransomwares comptent en effet sur la crédulité des utilisateurs pour s'installer et s'activer. Un clic sur un lien et le mal est fait !●

Boîte à outils

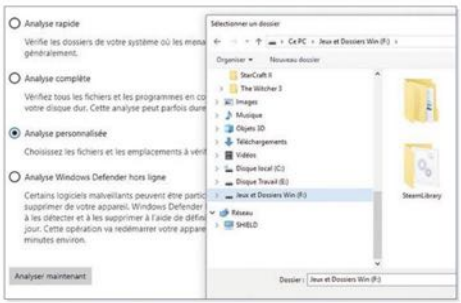
Pour ce pas à pas, nous avons utilisé

Ordinateur fixe ou portable sous Windows 10

Windows Defender

1 LANCEZ LE SERVICE DE SÉCURITÉ WINDOWS

La suite de sécurité de Microsoft s'active dès la mise en service d'un nouveau PC, à moins que le constructeur n'ait choisi d'y implanter un autre logiciel antivirus. Si une alerte de sécurité s'affiche dans le panneau des notifications, allez dans les Paramètres de Windows, accessibles depuis le menu **Démarrer**, puis cliquez sur **Mise à jour et sécurité, Sécurité Windows**. Vérifiez que les différentes options sont précédées d'une coche verte. Pointez ensuite sur **Ouvrir sécurité Windows** (ou accédez directement à cette page en tapant l'intitulé **Sécurité Windows** dans la zone de recherche du menu **Démarrer**). Ouvrez la rubrique **Protection contre les virus et menaces** de façon à afficher les options et les réglages de l'analyse antivirus.



2 CIBLEZ ET APPROFONDISSEZ LA RECHERCHE DE VIRUS

Windows effectue régulièrement des analyses rapides, dont le compte rendu apparaît sous **Menace actuelle**. Cliquez dans cette section sur **Options d'analyse**. S'il s'agit de votre premier passage, cochez **Analyse complète** et lancez la vérification avec **Analyser maintenant**. Cette opération minutieuse peut durer plusieurs dizaines de minutes. Vous pouvez aussi cibler les dossiers qui accueillent des fichiers que vous téléchargez ainsi que les emplacements associés aux derniers logiciels installés. Pointez sur **Analyse personnalisée**, **Analyser maintenant**. Désignez les répertoires à surveiller et validez avec **Sélectionner un dossier**. Procédez de même pour diagnostiquer les disques durs externes.

3 EFFECTUEZ UNE ANALYSE HORS LIGNE

Certains malwares se lancent avant même le démarrage de Windows et deviennent très difficiles à détecter. C'est pourquoi il est nécessaire de se montrer proactif. Toujours dans les options de l'application de sécurité de Windows 10, cliquez sur **Analyse Windows Defender hors ligne**. Fermez les programmes en cours d'exécution et enregistrez votre travail. Pointez ensuite sur **Analyser maintenant**. Le redémarrage du PC est suivi d'une phase de vérification au cours de laquelle les éventuels logiciels malveillants sont identifiés et placés en quarantaine. Accédez ensuite à Windows et retournez dans la section **Sécurité Windows**, **Protection contre les virus et menaces** des paramètres.

4 OPTIMISEZ LES SYSTÈMES DE PROTECTION

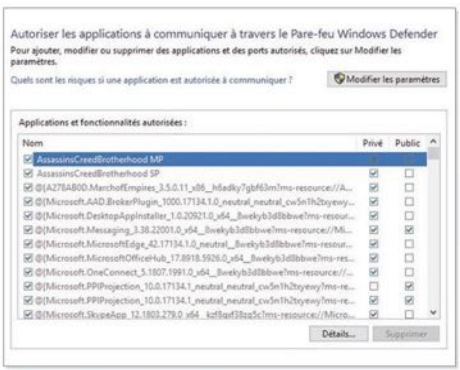
Cliquez sur **Gérer les paramètres** dans **Paramètres de protection contre les virus et menaces**. Les sections **Protections en temps réel** et **Protection dans le cloud** doivent être réglées sur **Activé**. L'envoi automatique d'un échantillon n'est pas indispensable, d'autant plus que Microsoft en profite pour collecter quelques informations vous concernant. Nous recommandons toutefois de laisser cette option activée afin de contribuer à l'éradication des nouvelles menaces. Dans **Exclusions**, cliquez sur **Ajouter ou supprimer des exclusions** puis **Ajouter une exclusion** si vous souhaitez écarter un fichier ou un dossier de l'analyse. Vous pouvez aussi exclure des formats de fichiers que vous jugez sans danger.

5 PROTÉGEZ-VOUS DES RANSOMWARES

De retour dans la fenêtre **Protection contre les virus et menaces**, dans la section **Protections contre les ransomwares**, cliquez sur **Gérez la protection contre les Ransomwares**. Basculez l'option **Dispositif d'accès contrôlé aux dossiers** sur **Activé** et pointez sur **Dossiers protégés**, **Ajouter un dossier protégé**. Sélectionnez les emplacements qui abritent, par exemple, vos photos ou des documents importants afin que les applications suspectes ne puissent en modifier le contenu sans votre autorisation et la saisie de votre mot de passe Windows. Les éléments ainsi protégés sont à l'abri de l'action des ransomwares. Pour faire bonne mesure, sauvegardez régulièrement vos données sur une unité de stockage externe.

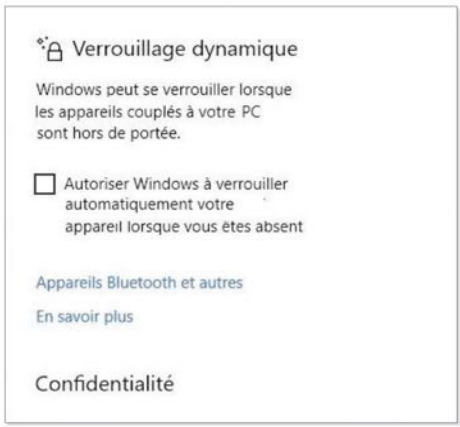
6 RENFORCER LE FILTRE SMARTSCREEN

Dans le volet gauche de Windows Defender, cliquez à présent sur **Contrôle des applications et du navigateur**. Les paramètres définis ici dépendent de vos habitudes de navigation et si d'autres personnes peuvent accéder à l'ordinateur. Par défaut, la vérification des sites et des applications est réglée sur le mode **Avertir**. En cas de risque potentiel, vous pourrez refuser l'accès à l'appli un peu trop curieuse. Sélectionnez l'option **Refuser** si vous préférez que les logiciels et les sites non reconnus par SmartScreen soient inaccessibles. Gardez bien à l'esprit que les outils de protection Web ne concernent que le navigateur Edge de Microsoft.



7 RÉGLEZ LES OPTIONS DU PARE-FEU

Parcourez le volet de navigation de Windows Defender et ouvrez la section **Pare-feu et protection du réseau**. Par défaut, toutes les options sont activées. Nous vous déconseillons de modifier ces réglages. S'il s'avère nécessaire d'ouvrir l'accès à Internet à un programme, ou au contraire de révoquer ses autorisations, cliquez sur **Autoriser une application via le pare-feu** puis, dans la fenêtre qui apparaît, sur **Modifier les paramètres**. Profitez-en pour bloquer les logiciels supprimés du PC qui figurent toujours dans la liste.



8 VERROUILLEZ VOTRE SESSION WINDOWS

Pour décourager les intrus qui accéderaient à votre PC, cliquez sur **Protection du compte**, **Windows Hello - Gérer les options de connexions**. Dans **Options de connexion**, déroulez le menu **Demander une reconnexion après votre absence** et choisissez **Lorsque le PC sort du mode veille**, **Autorisez Windows à verrouiller auto. votre appareil lorsque vous êtes absent**.

9 RETROUVEZ UN WINDOWS SAIN

Choisissez l'onglet **Performances et intégrité de l'appareil**. La section rapport d'intégrité Windows vous informe d'une difficulté avec votre espace de stockage, une application ou un service. Si votre OS rencontre des problèmes de performance et que la mémoire est anormalement saturée, vous pouvez utiliser l'option **Redémarrage à zéro** pour retrouver une version propre de Windows. Durant la réinitialisation, tous les logiciels sont supprimés, vos fichiers personnels étant en revanche conservés.

DIFFICULTÉ AUCUNE **TEMPS** 20 MIN **DOMAINE** SÉCURITÉ

FINISSEZ-EN AVEC LES MALWARES

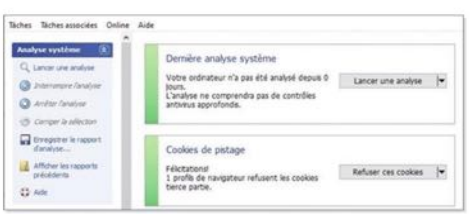
Windows Defender n'est pas infaillible. N'hésitez pas à solliciter un second avis, notamment pour contrer les logiciels malveillants. Et à ce petit jeu, Spybot Search & Destroy est sans rival.

1 INSTALLEZ SPYBOT SEARCH & DESTROY EN MODE EXPERT

Rendez-vous sur le site **bit.ly/2KhybAh** pour télécharger l'application. Lors de l'installation, Spybot Search & Destroy vous laisse le choix entre deux options : **Je veux être protégé sans avoir à m'en occuper moi-même** ou **Je veux plus de contrôle, plus de rétroaction et plus de responsabilités**. Choisissez ce second mode, car mieux vaut maintenir une certaine vigilance volontaire plutôt que tout déléguer sans comprendre. Dans la fenêtre des tâches supplémentaires, cochez toutes les cases. Choisissez ensuite de paramétrer Spybot au démarrage en cochant la case idoine.

2 LANCEZ UNE PREMIÈRE ANALYSE

Lors du lancement initial du logiciel, indiquez la langue souhaitée pour l'interface (si malgré cela, l'application ne bascule pas en français, forcez cette option dans **Outils Experts**, **Paramètres**). Cliquez ensuite sur **Afficher les détails** pour découvrir les services proposés. Commencez par pointer sur **Analyse Système**. Dans la fenêtre **Signatures absentes**, choisissez **Mise à jour** puis de nouveau **Mise à jour**. Quand les voyants sont au vert, fermez la fenêtre, revenez sur **Analyse système** et activez la commande **Lancez une analyse**. Optez pour **Corriger la sélection** pour supprimer les indésirables.



3 TRAQUEZ LES ROOTKITS

Dans le Centre de démarrage, vérifiez que le mode **Utilisateur expérimenté** (en bas à droite de la fenêtre) est bien coché de façon à accéder aux outils Experts. Cliquez sur **Recherche de Rootkit**. Sur la gauche de l'écran, choisissez **Lancer une analyse approfondie**. Sélectionnez les disques et les dossiers à vérifier et validez par **OK**. Les résultats qui apparaissent ne désignent pas forcément des éléments malveillants. Certains logiciels usent des technologies proches des rootkits pour cacher des données. En cas de doute, utilisez un antivirus ou l'analyse de hors-ligne de Windows Defender.

4 VACCINEZ VOTRE MACHINE

La vaccination empêche les logiciels malveillants d'attaquer Windows, Spybot Search & Destroy bloquant les sites contenant des indésirables, les cookies intrusifs ainsi que les extensions des navigateurs qui causent plus de dommages qu'ils ne rendent de services ! Cliquez sur **Vaccination**. Si vous détenez plusieurs comptes utilisateurs, choisissez **Vaccinez tout** et pointez sur **Vérifier le système**. Une fois l'analyse terminée, validez par **Vaccination** et attendez la fin du processus. Sur la page d'accueil de l'appli, activez le lien **Retour à la présentation**. Votre PC est dorénavant sous surveillance.

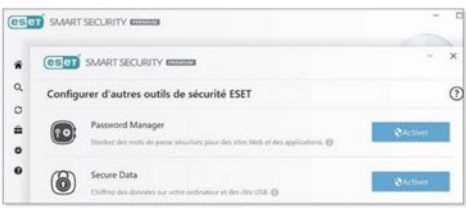
DIFFICULTÉ AUCUNE TEMPS 30 MIN DOMAINE SUITE DE SÉCURITÉ

PROTÉGEZ-VOUS EN MODE INTÉGRAL

Du côté des solutions payantes, il ne faut plus parler d'antivirus mais de suites de sécurité, capables de sécuriser mots de passe, données, transactions bancaires et tous vos appareils, PC comme mobiles.

1 INSTALLEZ ESET SMART SECURITY PREMIUM

Téléchargez la version d'essai du logiciel, pleinement fonctionnelle durant 30 jours, sur le site **bit.ly/32UAbXM** puis déroulez l'assistant d'installation (l'opération ne présente pas de piège). Si vous souhaitez tester le produit avant de l'acheter, choisissez l'option **Licence d'essai gratuit** et remplissez le formulaire d'inscription. Activez ensuite le **LiveGrid** et la **Détection des applications potentiellement indésirables**. Acceptez ou non que vos données servent à améliorer la détection des menaces, puis cliquez sur **Installer**. Au premier lancement, ESET affiche la liste complète des services proposés.

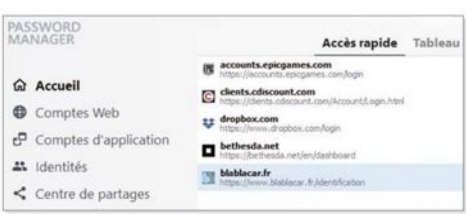


2 PARAMÉTREZ LE PASSWORD MANAGER

Si vous utilisez déjà un gestionnaire de mots de passe, cette étape est facultative. Sinon, activez le module **Password Manager** et pointez sur **Configurer maintenant**, **Créer un compte**. Indiquez votre adresse mail et définissez le mot de passe maître qui protégera l'accès à votre coffre-fort numérique (conservez précieusement ce code car il ne pourra être réinitialisé en cas de perte). Sélectionnez votre navigateur Internet pour basculer vers la fenêtre de gestion des extensions. Pour intégrer Password Manager à Google Chrome, choisissez **Ajouter à Chrome**, puis cliquez sur l'icône **ESET**.

3 CENTRALISEZ VOS MOTS DE PASSE

Une fois sur l'application, choisissez **Comptes Web**. Tous les mots de passe enregistrés dans Chrome ont été récupérés et s'affichent dans cette fenêtre. Cliquez sur l'un d'eux puis sur **Lancer** afin d'accéder au site en question. ESET remplit automatiquement le formulaire d'authentification. L'adresse est dans le même temps ajoutée au menu **Accueil** de Password Manager. Pour partir d'une copie blanche, cliquez sur **Ajouter un compte**, saisissez le nom et l'URL de la page d'identification du site, puis l'identifiant et le mot de passe de votre compte. Validez par **Ajouter**. Fermer Password Manager.



4 ACTIVEZ LE CONTRÔLE PARENTAL

Commencez par créer un profil Windows pour chacun des membres du foyer (menu **Paramètres**, **Comptes** du PC). Cliquez ensuite sur **Configuration**, **Outil de sécurité**. Activez le mode **Contrôle parental**. Pointez sur **Protégez tous les paramètres avec un mot de passe**, définissez un code secret puis indiquez le compte utilisateur qui doit être protégé et l'âge de l'enfant. Choisissez **Paramètres et contenu bloqués**. Placez-vous sur l'onglet **Catégorie** et cochez le type de contenus qui seront proscrits pour ce profil (affichage des pages et fichiers pour adulte, accès aux réseaux sociaux ou, etc.).

5 CONSULTEZ SEREINEMENT VOS COMPTES BANCAIRES

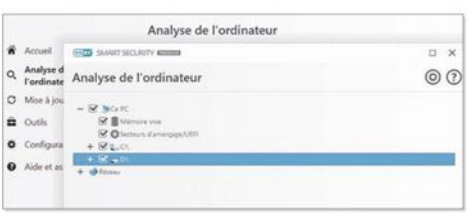
Cliquez dans l'onglet **Configuration** sur **Outil de sécurité** et pointez sur le curseur **Protection des transactions bancaires** afin d'activer la surveillance. Un raccourci est ajouté sur le Bureau de Windows. Cliquez dessus pour lancer le navigateur Internet dédié aux échanges avec votre banque. Saisissez l'URL de la page d'identification des services en ligne de l'établissement dans la barre d'adresse ou rendez-vous dans votre navigateur habituel pour cliquer sur le favori de votre banque. Le lien s'ouvre automatiquement dans le navigateur sécurisé ESET. Les échanges avec les sites de vente en ligne et les paiements peuvent également s'effectuer via ce navigateur.

6 GARDEZ UN ŒIL SUR VOTRE APPAREIL AVEC L'OUTIL ANTIVOL

Déroulez maintenant le menu **Outils**, **Antivol** et créez un compte utilisateur. Allez ensuite sur le site **bit.ly/318L9XQ**, pointez sur **Se connecter** et tapez l'identifiant et le mot de passe de votre compte ESET. Il vous est alors demandé de créer un compte fantôme. En cas de perte ou de vol de votre ordinateur, accédez à ce même site à partir d'un autre PC ou d'une tablette. Désignez l'appareil égaré et choisissez **État** puis **Mon appareil est manquant**. ESET interdira alors l'accès à tous les comptes, hormis le compte fantôme qui sert de leurre. Dès que l'ordinateur perdu se connecte à Internet, vous le verrez dans l'onglet **Activité**.

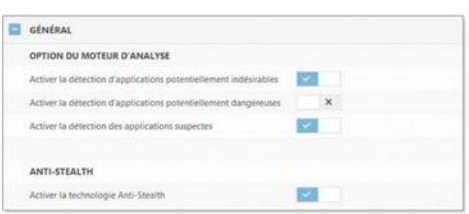
7 LANCEZ UNE ANALYSE APPROFONDIE

On aurait presque tendance à l'oublier tant il propose de fonctionnalités, mais ESET smart Security est avant tout un puissant antivirus. Cliquez sur **Analyse de l'ordinateur**, **Analyses avancées**, **Analyses personnalisées**. Sélectionnez les emplacements à vérifier (disques locaux ou externes, mémoire, zone d'amorçage, etc.) et lancez l'analyse. Testez un fichier ou un dossier en effectuant un glisser-déposer dans la fenêtre. La vérification peut s'effectuer pendant que vous utilisez votre machine. Dans le menu déroulant **Action après analyse**, choisissez l'option **Arrêt**.



8 PERSONNALISEZ LES PARAMÈTRES DE SÉCURITÉ

Dans la section **Configuration**, choisissez **Configuration avancée**. Déroulez ensuite la section **Moteur de détection**, **Générale**. Dans **Exclusion**, pointez sur **Modifier** de façon à déclarer d'éventuels faux positifs et les exclure du périmètre de l'analyse. Activez ensuite les options **Analyses des logiciels malveillants** et **Analyse en cas d'inactivité**. Déroulez le menu **Supports amovibles** et sélectionnez le mode **Analyse automatique des périphériques**. Les options d'analyses sont nombreuses et beaucoup sont activées par défaut afin d'optimiser la sécurité de votre appareil.



9 AFFINEZ LA SURVEILLANCE DES ENFANTS

Cliquez sur **Options de contrôle parental**, **Afficher les paramètres du contrôle parental**. Si la page est en anglais, cliquez sur **English** au bas de la page et sélectionnez le français. Pointez ensuite sur **Ajouter un membre de la famille**, cochez la case **Enfant** et entrez son adresse mail. Il apparaîtra dans la liste **Votre famille** après avoir cliqué sur le lien d'activation du message de confirmation. Allez sur l'onglet **Activité** pour voir les applications lancées ou les sites consultés par le nouvel utilisateur, sur **Temps d'écran** pour imposer des plages horaires pour l'utilisation de l'ordinateur.

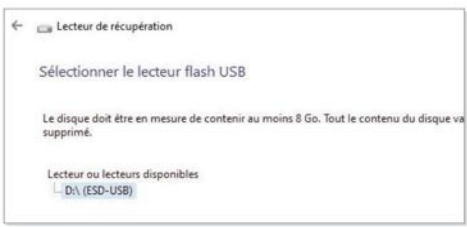
DIFFICULTÉ MODÉRÉE TEMPS 30 MIN DOMAINE SYSTÈME

REPRENEZ LE CONTRÔLE D'UN PC INFECTÉ

Quand un virus rend Windows inaccessible, vous n'avez d'autre choix que de démarrer sur une clé USB de dépannage pour restaurer le système. Procédez méthodiquement pour ne pas perdre vos fichiers.

1 CRÉEZ L'OUTIL DE RÉCUPÉRATION

Préparez le support de secours tant que votre PC fonctionne (si vous n'avez pas pris vos précautions, vous devrez accéder à un ordinateur d'emprunt pour réaliser l'opération). Munissez-vous d'une clé USB d'une capacité d'au moins 16 Go si vous utilisez Windows 64 bits, ou de 8 Go pour une configuration 32 bits. Tapez **Récupération** dans la zone de recherche de Windows, puis cliquez sur **Récupération Panneau de configuration**. Pointez sur **Créer un lecteur de récupération**. Insérez votre clé USB, cochez l'option **Sauvegarder les fichiers système sur le lecteur de récupération** et validez par **Suivant**. Désignez la clé USB et confirmez avec **Suivant** puis **Créer**.



2 MODIFIEZ LA SÉQUENCE DE DÉMARRAGE DU PC

Si l'accès à Windows est devenu impossible à cause d'un virus, il est probable que vous ne puissiez pas utiliser le mode de **Démarrage avancé** pas plus que l'option **Réinitialisation du PC** proposée dans les Paramètres de Windows (**Mise à jour et sécurité**, **Récupération**). Dans ce cas, sortez la clé de secours créée pour faire face à ce type de situations et branchez-la sur le PC. Forcez l'extinction de l'ordinateur et redémarrez la machine. Accédez au BIOS en appuyant sur la touche **Suppr** ou **F2** du clavier (la commande varie d'un PC à l'autre). Glissez la clé USB en tête de la liste ou cliquez sur **Menu de démarrage** pour sélectionner le support amovible.

3 TENTEZ DE RÉPARER WINDOWS

Choisissez d'abord la langue puis l'onglet **Dépannage**. Essayez les options **Restauration du Système** ou **Récupération de l'image système** si vous avez au préalable créé un point de restauration ou enregistré une image saine de l'environnement. Vous pouvez aussi lancer l'outil de redémarrage système pour que Windows tente une réparation. Le résultat reste toutefois improbable dans le cas d'un virus. Votre système ne démarre toujours pas ? Relancez l'outil de récupération pour revenir au menu **Choisir une option**. Optez cette fois pour la commande **Récupérer à partir d'un lecteur**.

4 RETROUVEZ VOS FICHIERS

Deux options s'offrent à vous. Dans le cas d'un virus, il est probable que différents fichiers soient infectés, en plus des composants de Windows. Il est donc préférable de choisir la méthode la plus radicale, à savoir **Nettoyer entièrement le lecteur**. L'opération efface tous les fichiers présents sur le disque dur système, mais aussi les logiciels, les paramètres et les comptes utilisateurs. Vous repartez sur des bases saines, avec un Windows tout neuf, délesté des éléments indésirables. Il vous reste à réinstaller vos applications, à synchroniser vos services Cloud et à paramétrer vos comptes mail.

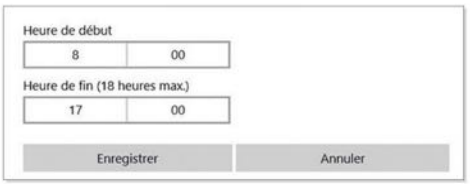
DIFFICULTÉ AUCUNE TEMPS 5 MIN DOMAINE SYSTÈME

GARDEZ VOTRE ORDINATEUR ET VOTRE ANTIVIRUS À JOUR

Microsoft publie régulièrement des correctifs destinés à combler les failles de sécurité de Windows, ainsi que des mises à jour de la base de signature de Windows Defender.

1 EMPÊCHEZ LES REDÉMARRAGES INOPPORTUNS

Dans le menu **Démarrer** de Windows, cliquez sur **Paramètres** puis **Mise à jour et sécurité**. Allez sur l'onglet **Windows Update**, cliquez sur **Modifier les heures d'activité** et indiquez une heure de début et une heure de fin afin d'empêcher Windows de redémarrer le PC durant vos horaires de travail. Validez par **Enregistrer**. Pointez sur **Options avancées** et activez **Notifications de mise à jour**. Vous serez ainsi invité à redémarrer votre PC. Si vous jugez le moment mal choisi, l'opération s'effectuera en dehors des heures indiquées.



2 DÉSINSTALLEZ UNE MISE À JOUR

Si votre PC montre des signes d'instabilité après une mise à jour, accédez à la fenêtre **Windows Update** et choisissez **Afficher l'historique des mises à jour**, **Désinstaller des mises à jour**. Rendez-vous dans la section **Microsoft Windows** et désinstallez la dernière mise à jour en date en attendant que Microsoft corrige le bug et propose un correctif. En cas de problème majeur qui empêche le bon fonctionnement de l'ordinateur, cliquez sur **Options de récupération**, **Réinitialiser ce PC** et validez par **Commencer**.

DIFFICULTÉ AUCUNE TEMPS 30 MIN DOMAINE SÉCURITÉ

FAITES UN BILAN DE SÉCURITÉ À L'AIDE D'UN ANTIVIRUS EN LIGNE

Moins complets que les suites de sécurité, les antivirus en ligne permettent toutefois de lever les doutes.

1 INSTALLEZ LE CLIENT LOCAL SUR VOTRE PC

Bitdefender, Panda, ESET ou Norton, la plupart des éditeurs d'outils antivirus proposent une solution légère basée sur le Cloud. Les bases de signature et le moteur d'analyse sont alors hébergés sur des serveurs distants et non plus sur votre ordinateur. Pour utiliser la Web app de F-Secure, ouvrez votre navigateur Internet et rendez-vous à l'adresse **bit.ly/2yuviXo**. Cliquez sur **Lancer dès maintenant**. Le service vous invite ensuite à télécharger un petit programme qui communiquera avec le logiciel distant lors de l'analyse.

2 VÉRIFIEZ VOS FICHIERS ET LA MÉMOIRE

Exécutez ce client local, puis pointez sur le bouton **Accepter et analyser**. F-Secure Online scanne vos fichiers et la mémoire vive du PC à la recherche des virus et des malwares et procède aux opérations de désinfection si nécessaire. Pour vérifier l'innocuité d'une adresse Internet ou d'un document particulier, allez sur le site **bit.ly/1hr5HS1** et glissez l'élément suspect dans la fenêtre du service VirusTotal. Ce dernier interroge alors plus de 50 moteurs de recherche pour évaluer les risques encourus.

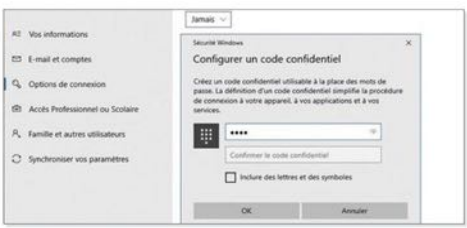
DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE IDENTIFICATION

VERROUILLEZ WINDOWS À DOUBLE TOUR

Un PC, qui plus est quand il s'agit d'un portable, ne doit pas être laissé en accès libre. Pour éviter les regards indiscrets, et le vol de données, définissez un code de verrouillage ou activez la protection biométrique si votre appareil en est équipé.

1 INSTAUREZ UN CODE CONFIDENTIEL

Que vous soyez connecté avec votre compte Microsoft ou un profil local, prenez toutes les précautions pour empêcher que n'importe qui accède à votre PC. Appuyez sur les touches **Windows + I** et pointez sur **Comptes**, **Options de connexion**. Le dispositif le plus simple consiste à définir un code PIN. Cliquez sur le bouton **Ajouter** dans la section **Code confidentiel** et enregistrez une combinaison composée d'au moins 4 chiffres (il est possible d'utiliser des lettres et des symboles en cochant la case située sous les champs de saisie). Dans **Confidentialité**, désactivez l'option **Afficher les détails du compte** pour éviter que le code s'affiche sur la page d'identification.



2 PARAMÉTREZ LE BLOCAGE DE L'ACCÈS

Dirigez-vous ensuite vers **Écran de verrouillage** dans **Paramètres associés**, **Paramètres de l'écran de veille**. Pour que le PC bascule automatiquement en mode veille quand vous ne l'utilisez pas, ouvrez le menu **Écran de veille** et optez pour une animation. Réglez le délai d'extinction, cochez **A la reprise, demandez l'ouverture de session** et validez avec **Appliquer**. Le code PIN sera désormais exigé en sortie de veille. Si vous souhaitez activer un autre dispositif de verrouillage, revenez au menu **Comptes**, **Options de connexion** et choisissez l'une des options disponibles : un mot de passe image, par exemple, ou encore le verrouillage dynamique.

3 PASSEZ AU VERROUILLAGE BIOMÉTRIQUE

Windows 10 gère les capteurs biométriques à travers la technologie Hello. Si votre PC n'intègre pas un tel dispositif, vous pouvez y remédier en achetant un capteur d'empreintes digitales. On trouve dans les boutiques en ligne des modèles USB ultracompacts compatibles Windows Hello pour une vingtaine d'euros. Branchez-le capteur au PC et laissez Windows installer les pilotes. Appuyez sur les touches **Windows + I** et accédez à **Paramètres**, **Comptes**, **Options de connexion**, **Configurer dans Empreinte digitale**. Pointez sur **Démarrer** et suivez la procédure d'enregistrement de vos empreintes.

4 TESTEZ LA RECONNAISSANCE DU VISAGE

Windows Hello est également compatible avec la reconnaissance du visage. Vous devez pour cela disposer d'une Webcam compatible. Ces périphériques basés sur la technologie IntelliRealSense 3D d'Intel sont encore rares et ils ne sont pas donnés. Les premiers prix s'affichent à 70 € environ. Windows Hello gère aussi les dispositifs qui s'appuient sur l'analyse des yeux (pupilles, iris). Appelé Tobii 4C, le système se positionne sur le bord supérieur de l'écran, au-dessus de la webcam. Connecté en USB, il mémorise votre regard et déverrouille l'ordinateur dès que vous regardez le capteur.

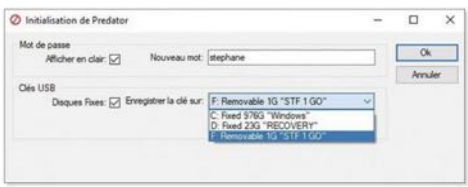
DIFFICULTÉ ÉLEVÉE TEMPS 20 MIN DOMAINE IDENTIFICATION

BOUCLEZ L'ACCÈS À VOTRE PC AVEC UNE SIMPLE CLÉ USB

L'application Predator Home Edition transforme n'importe quelle clé USB en un puissant verrou. Sans elle, il est impossible d'utiliser votre PC ni d'en voir le contenu.

1 DÉMARREZ LA SURVEILLANCE

Munissez-vous d'une clé USB dont vous n'avez plus l'usage (un modèle USB 2.0 suffit amplement). Téléchargez ensuite Predator Home Edition (**bit.ly/2LAU6FZ**) et exécutez le programme d'installation. Renseignez un mot de passe maître, puis sélectionnez le périphérique dans **Enregistrer la clé sur**. Validez avec **OK**. La surveillance débute. Retirez la clé. Après quelques secondes, une fenêtre demande de saisir le mot de passe. Si l'opération n'est pas effectuée dans un temps donné, une alarme se déclenche.



2 PARAMÉTREZ PREDATOR

Enfichez de nouveau la clé. Opérez un clic droit sur l'icône de Predator dans la zone de notification de Windows et pointez sur **Préférences**. Allez sur l'onglet **Options de base** et cochez l'option **Démarrer avec Windows**. Vous pouvez modifier le code secret depuis cette même page ou encore révoquer la clé ou définir un nouveau support amovible. Pour finir, allez sur l'onglet **Options d'alarme** pour choisir le fichier audio qui servira d'alerte et fixer le nombre de tentatives autorisées pour saisir le mot de passe.

DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE CONFIDENTIALITÉ

VÉRIFIEZ SI VOS IDENTIFIANTS ONT ÉTÉ PIRATÉS

Spybot Identity Monitor vous informe dès que quelqu'un utilise l'un de vos comptes à votre insu.

1 CONTRÔLEZ L'INTÉGRITÉ DE VOS COMPTES

Allez sur le site **bit.ly/2YnsIkK**, cliquez sur le lien de téléchargement **Standard Installer** au bas de la page puis installez l'application Spybot Identity Monitor. Celle-ci a pour fonction de vérifier si les noms et adresses mail que vous utilisez pour vous connecter aux différents services en ligne (Web marchands, banques, etc.) n'ont pas été piratés. Le logiciel s'appuie pour cela sur la base de données **have i been pwned?** (**bit.ly/2Oe4yoW**). Exécutez le programme et attendez que le résultat de l'analyse s'affiche à l'écran.

2 PASSEZ À L'ACTION !

Le diagnostic ne fait pas apparaître de violation (*breach*) ? Vos informations personnelles ne sont pas compromises. Si en revanche Spybot Identity Monitor suspecte un détournement de vos identifiants, pointez sur le résultat positif à droite pour découvrir l'adresse mail ou le pseudo piraté. Accédez alors aux comptes qui utilisent cet identifiant afin de les associer à un autre compte de messagerie (en attendant d'en reprendre le contrôle et d'écarter la menace) et de définir un nouveau mot de passe.

DIFFICULTÉ MODÉRÉE TEMPS 40 MIN DOMAINE SYSTÈME

COMBLEZ LES FAILLES DE SÉCURITÉ DE VOTRE PC

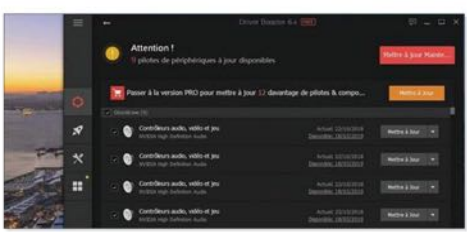
Le moindre programme compte dorénavant des millions de lignes de code. Des correctifs sont régulièrement publiés afin de corriger les erreurs et les oublis susceptibles de constituer des portes d'entrées pour les pirates. C'est pourquoi système, pilotes et applications doivent être soigneusement mis à jour.

1 ACTUALISEZ WINDOWS

N'écoutez pas les oiseaux de mauvais augure vous conseillant de ne pas mettre votre PC à jour sous prétexte qu'il fonctionnerait alors moins bien. Bien au contraire, un système, des applications et des pilotes actualisés périodiquement sont l'assurance de disposer d'un ordinateur au top de sa forme et solidement protégé contre les cybermenaces. Vérifier que Windows 10 profite des dernières mises à jour. Appuyez sur les touches **Windows + I** et cliquez sur **Mise à jour et sécurité**, **Windows Update**, **Rechercher des mises à jour**. Installez les éventuels correctifs disponibles, puis accédez aux **Options avancées** et activez les différentes options de mise à jour.

2 IDENTIFIEZ LES PILOTES OBSOLÈTES

Chaque périphérique et composant matériel est géré par un pilote. Si ces programmes ne sont pas régulièrement mis à jour, le fonctionnement et la sécurité du PC risquent d'en pâtir. L'utilitaire Driver Booster Free (**bit.ly/2KufhGp**) peut vous aider à gérer les pilotes et à les actualiser. Une fois l'application installée, cliquez sur **Analyser maintenant**. Après quelques minutes, Driver Booster indique les périphériques dont les pilotes doivent être changés. L'opération doit être effectuée manuellement pour chaque pilote. Pointez à droite sur le bouton **Mettre à jour** et validez par **OK**. La version la plus récente du driver est téléchargée et installée.



3 METTEZ VOS LOGICIELS À JOUR

Certaines de vos applications sont sans doute en place depuis un bon moment. Il existe probablement des versions plus récentes. Pour le savoir sans perdre de temps en vaines recherches, utilisez l'application Software Updater de IObit (**bit.ly/2LzsVeJ**). Celle-ci identifie les programmes présents sur le PC, évalue leur date d'ancienneté et propose le cas échéant de les actualiser. L'analyse démarre à l'ouverture du logiciel. Parcourez la liste des éléments obsolètes et cliquez sur **Mettre à jour** à droite. Quand le téléchargement et l'intégration sont achevés, redémarrez l'ordinateur.

4 OPTIMISEZ LE MICROSOFT STORE

Au même titre que les logiciels PC, les applications émanant du store de Microsoft se doivent d'être actualisées. Ouvrez la boutique en pointant sur le bouton **Démarrer** en bas à gauche de la barre des tâches, puis sur la lettre **M** dans la liste des applis. À l'ouverture, le Store indique le nombre de téléchargements et de mises à jour en attente en haut à droite de votre avatar. Lancez le téléchargement et l'installation des dernières versions disponibles en cliquant sur **Obtenir les mises à jour** ou **Tout mettre à jour**. Vous pouvez aussi opérer au cas par cas en sélectionnant chaque application.

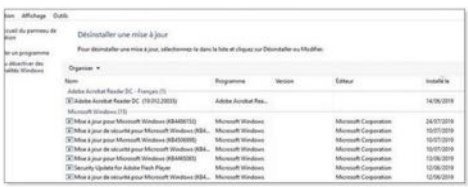
DIFFICULTÉ ÉLEVÉE TEMPS 20 MIN DOMAINE SYSTÈME

DÉBARRASSEZ-VOUS D'UNE MISE À JOUR INSTABLE

Il arrive qu'une mise à jour, loin de régler les problèmes, rende Windows instable sur certaines configurations. Un retour en arrière temporaire s'avère alors salutaire.

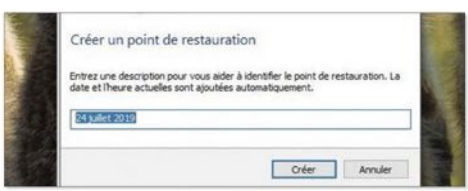
1 IDENTIFIEZ L'ÉLÉMENT RESPONSABLE DE LA SITUATION

Si vous ressentez une lenteur inhabituelle, des bugs d'affichage, voire une quasi-impossibilité à utiliser le PC après une mise à jour, ne cherchez pas plus loin l'origine de vos problèmes. Pour revenir à une configuration stable, supprimez ladite mise à jour. Activez le raccourci **Windows + I** et cliquez sur **Mise à jour et sécurité**, **Windows Update**. Pointez sur **Afficher l'historique des mises à jour**, **Désinstaller des mises à jour**. Parcourez la colonne **Installé le** pour identifier les opérations effectuées depuis le début de vos soucis.



2 CRÉEZ UN POINT DE RESTAURATION

Faites un clic droit sur la mise à jour fautive, pointez sur **Désinstaller** et redémarrez le PC. Pour vous simplifier la vie à l'avenir, enregistrez votre configuration avant chaque correctif. Tapez **Point de restauration** dans le champ de recherche de Windows 10 et suivez le lien **Créer un point de restauration**. Dans **Propriétés système**, accédez à **Configurer**, **Activer la protection du système**, **Appliquer**, **OK**, **Créer**. Indiquez la date et validez avec **Créer**. Pour rétablir la configuration, vous devrez aller dans **Restauration du système**.



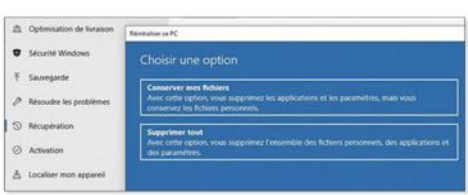
DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE SYSTÈME

RÉPAREZ OU RÉINSTALLEZ WINDOWS APRÈS UNE ATTAQUE

Un virus perturbe le fonctionnement de votre PC ? Sollicitez l'aide des outils de maintenance de Windows.

1 LANCEZ LA RÉPARATION DE WINDOWS 0

Si le virus n'a pas trop gravement endommagé le système, nous vous conseillons de tenter une simple réparation. Vous conserverez ainsi vos fichiers et vos données personnelles. Appuyez sur les touches **Windows + I** et pointez sur **Mise à jour et sécurité**, **Récupération**. Dans la section **Réinitialiser ce PC**, exécutez la commande **Commencer**, puis optez pour le mode **Conserver mes fichiers**. Si le résultat n'est pas satisfaisant, revenez sur le menu d'accueil et choisissez cette fois l'option **Supprimer tout**.



2 REPARTEZ SUR DES BASES SAINES

Si la réparation échoue à restaurer une configuration fonctionnelle, un grand ménage s'impose. Sauvegardez le contenu du disque dur dans le Cloud ou sur un support de stockage externe, puis accédez à la section **Mise à jour et sécurité**, **Récupération** des paramètres de Windows. Pointez sur **Voir comment recommencer à zéro avec une nouvelle installation de Windows** dans **Démarrage avancé**, **Oui**, **Prise en main**, **Oui**, **Suivant**. Les applications allant être supprimées s'affichent à l'écran. Cliquez sur **Démarrer** pour confirmer.

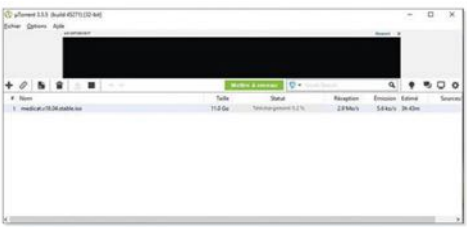
DIFFICULTÉ ÉLEVÉE TEMPS 45 MIN DOMAINE DÉPANNAGE

REDONNEZ VIE À UN PC MIS À GENOUX PAR UN VIRUS

Donnez-vous les moyens d'accéder de nouveau à votre ordinateur en préparant une clé de secours. Doté de multiples utilitaires, ce support résout la plupart des problèmes, y compris l'infection par un virus.

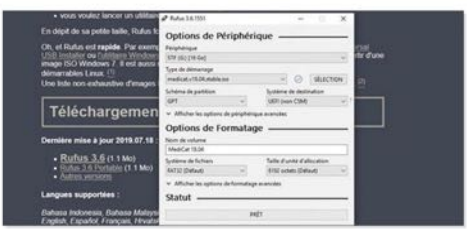
1 TÉLÉCHARGEZ L'OUTIL MEDICAT USB

Certains logiciels malveillants parviennent à bloquer l'action des antivirus et le recours aux outils en ligne. Pour vous en débarrasser, et corriger les dégâts occasionnés, tournez-vous vers Medicat. Cette trousse de secours regroupe une série d'utilitaires (antimalwares, gestionnaire de disque dur, contrôle de la mémoire, récupération des mots de passe, etc.). Medicat tient sur une clé USB. Téléchargez la version 18.04 de l'appli (**bit.ly/2Y2jj2o**) à l'aide du lien **Torrent Download** et du programme uTorrent (**bit.ly/2Y25mS5**). Préparez une clé USB de 12 Go minimum, puis récupérez le logiciel Rufus (**bit.ly/2OwcW3p**) qui servira à rendre le support bootable.



2 PRÉPAREZ LA CLÉ BOOTABLE

Une fois tous les éléments en votre possession, procédez à l'installation de l'utilitaire Rufus. Branchez ensuite la clé à un port USB et lancez Rufus. Sélectionnez le support amovible dans la liste des volumes qui s'affiche dans la section **Périphériques**. Dans **Type de démarrage**, cochez l'option **ISO**, pointez sur le bouton **Sélection** et accédez au dossier des téléchargements. Cliquez sur le fichier **medicat.v18.04.stable.iso** et validez avec **Ouvrir**. Une fois l'intégrité de l'image ISO vérifiée, la mention **Prêt** se dévoile dans la section **Statut**. Il reste à confirmer la création de la clé bootable avec **Démarrer**, **OK**. Attendez que tous les fichiers soient copiés sur la clé.

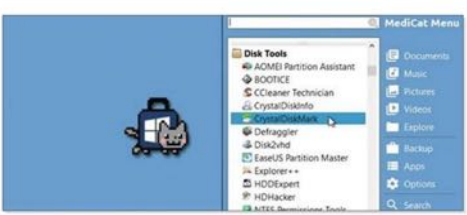


3 OUVREZ LA TROUSSE DE SECOURS

En cas de problème, branchez ce support de dépannage sur le PC endommagé. Redémarrez l'ordinateur, accédez au Bios en appuyant sur la touche **F2**, **F10**, **Echap** ou **Suppr**, et modifiez la séquence de boot en remontant la clé USB en première place de la liste. Enregistrez les modifications (**F10**, **OK**). L'ordinateur boote sur la clé qui abrite Medicat. Après quelques instants, l'écran d'accueil apparaît à l'écran. L'interface ressemble à celle de Windows 10. La navigation s'effectue à l'aide de la souris. Les différents outils sont accessibles dans la barre des tâches qui occupe le bord droit du Bureau.

4 EFFECTUEZ LES RÉPARATIONS

Cliquez sur l'intitulé **PortableApps.com**. Le menu **Medicat** se compose d'une myriade d'utilitaires classés par type (Accessibility, Disk Tools, Drivers, Graphic and Pictures, etc.). Activez **Dead Pixel Tester** pour vérifier qu'il n'existe pas de pixels morts ; **Driver Booster** pour être sûr que les pilotes sont à jour, **Smart Defrag** pour défragmenter le disque dur. Utilisez l'option **Reset User Account Passwords** pour débloquer un PC dont vous avez oublié le mot de passe ou l'icône **Malwarebytes** du Bureau pour rechercher les logiciels malveillants. Quittez Medicat en éteignant le PC et en retirant la clé USB.



DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE SYSTÈME

TESTEZ L'INTÉGRITÉ DE VOTRE PC AVEC SECURITY ANALYSER

Microsoft propose un outil d'analyse des éventuelles lacunes sécuritaires de l'ordinateur. Pratique pour repérer les failles avant qu'elles ne deviennent critiques.

1 PRÉPAREZ L'EXAMEN

Accédez à la page de rapatriement de l'outil Microsoft Baseline Security Analyzer 2.1.1 (**bit.ly/2LKBgML**). Pointez sur **Télécharger**, cochez la case **MBSASetup-x64-FR.msi** et validez par **Next**. Procédez à l'installation du programme. L'écran d'accueil apparaît, proposant d'analyser un ou plusieurs ordinateurs. Contentez-vous de votre PC en pointant sur le lien supérieur. La page suivante indique le nom de la machine ainsi que la liste des éléments qu'il convient de surveiller. Cochez la case **Configurer les ordinateurs pour Microsoft Update**.

2 PASSEZ LES FAILLES EN REVUE

Cliquez sur le bouton **Démarrer l'analyse**. La vérification débute après le téléchargement des informations de mises à jour de sécurité. Les résultats s'affichent dans un tableau où la colonne **Score** indique en rouge les failles les plus graves. Utilisez le lien **Comment corriger le problème** pour appliquer un correctif. Penchez-vous aussi sur les points précédés d'une icône orange. Il peut s'agir d'une mise à jour incomplète, d'un mot de passe trop simple ou de règles configurées à tort dans le pare-feu. Cliquez sur **OK** pour terminer.

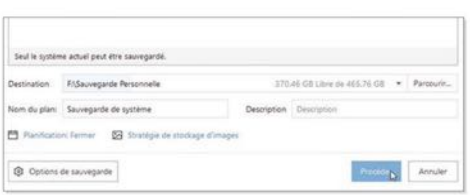
DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE SYSTÈME

ENREGISTREZ UNE IMAGE SAINE DE VOTRE ORDINATEUR

Votre PC est dans une forme éblouissante ? Faites-en une image que vous pourrez restaurer en cas de problème.

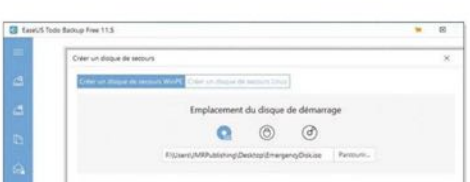
1 AJUSTEZ LES PARAMÈTRES DE L'IMAGE

Téléchargez la version gratuite de l'utilitaire EaseUS ToDo Backup (**bit.ly/2Fx8ICm**). Au cours de l'installation, refusez l'intégration du programme partenaire, puis cliquez sur **Parcourir** afin de désigner le dossier de sauvegarde par défaut. Déployez ensuite le menu latéral et indiquez le type de sauvegarde que vous souhaitez mettre en place. Une fois l'installation finalisée, pointez dans le volet de gauche sur **Sauvegarde de système**, sélectionnez la version de Windows utilisée sur votre PC et cliquez sur le bouton **Procéder**.



2 RÉALISEZ UN CLONE PARFAIT

La fonction **Sauvegarde du système** se limite aux fichiers et paramètres de votre système d'exploitation. Avec Easus Todo Backup, vous pouvez aller plus loin et réaliser un clone parfait de votre configuration. Cliquez sur le bouton **Clonage du système**. Sélectionnez les disques durs à inclure dans la sauvegarde. Pour être en mesure de restaurer l'image disque, pointez sur **Menu**, **Outils**, **Créer un disque de secours**, **Créer un disque de secours WinPE**. IL suffira de brancher le support au PC pour restaurer votre configuration.



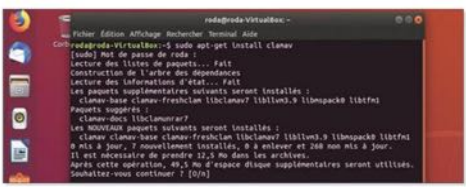
DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE SYSTÈME

PROTÉGEZ UBUNTU ET VOS DONNÉES DES VIRUS

Même s'il est moins exposé aux menaces virales que Windows, Ubuntu gagne à se doter d'un antivirus.

1 INSTALLEZ CLAMAV DEPUIS LE TERMINAL

Utilisez le raccourci clavier **Ctrl** + **Alt** + **T** de façon à ouvrir une session du Terminal. Exécutez ensuite la commande **sudo apt-get install clamav** pour implanter l'antivirus gratuit Clamav. Selon votre configuration, le mot de passe administrateur peut être exigé. Une alerte affiche l'espace disque nécessaire à l'installation. Confirmez l'opération en appuyant sur la touche **O** du clavier. Clamav veille désormais sur la sécurité de votre PC. Recherchez d'éventuelles mises à jour à l'aide de la commande **sudo freshclam**.



2 LANCEZ UNE ANALYSE

Clamav ne propose pas d'interface graphique par défaut. Tout se déroule à partir du Terminal. Si vous souhaitez lancer une analyse du dossier Utilisateur, exécutez la commande **sudo clamscan -r /home/utilisateur**. S'il s'agit de surveiller votre Dropbox, utilisez la commande **sudo clamscan -r /home/utilisateur/Dropbox**. Vous êtes allergique aux lignes de commandes ? Dans ce cas, ouvrez le module **Logiciel Ubuntu**, puis recherchez et installez **ClamTk**, l'interface graphique développée pour l'antivirus.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE CONFIDENTIALITÉ

EMPÊCHEZ LE SYSTÈME DE COLLECTER VOS DONNÉES

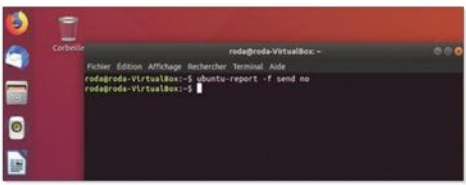
Il n'en a pas l'air et pourtant, Ubuntu, comme tous les autres OS, en sait beaucoup sur votre compte. Trop sans doute à votre goût, aussi apprenez à modérer sa curiosité.

1 DÉSACTIVEZ LES SIGNALEMENTS DE BUGS

Par défaut, l'éditeur d'Ubuntu, Canonical, collecte une foule d'informations sur votre utilisation du système. Mieux vaut toutefois prévoir des garde-fous. Désactivez par exemple l'envoi automatique de données en refusant le signalement automatique des problèmes rencontrés par les applis : accédez aux **Paramètres** d'Ubuntu, cliquez sur **Confidentialité**, **Signalement des problèmes**, **Automatique** et passez en mode **manuel**. Il vous appartient dorénavant de décider si vous souhaitez ou non transmettre les rapports de bugs.

2 VERROUILLEZ L'ENVOI DE DONNÉES

Si vous êtes du genre intransigeant, vous pouvez bloquer l'envoi des rapports à Canonical. Ouvrez une instance du Terminal (**Ctrl** + **Alt** + **T**). Tapez ensuite la commande **ubuntu-report -f send no** et validez par **Entrée**. Indiquez votre mot de passe administrateur pour appliquer la nouvelle règle. Cette commande limite l'envoi de rapports. Si certains d'entre eux venaient néanmoins à passer entre les mailles du filet, ils seraient vides de toute information. Pour revenir sur votre choix, remplacez **no** par **yes** dans la commande.



DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE SYSTÈME

ÉPARGNEZ UN PC UBUNTU DES CYBERATTAQUES

Aucun système d'exploitation ne peut prétendre être immunisé contre les conséquences des attaques menées par les cybercriminels. Le pare-feu constitue le premier rempart indispensable pour protéger votre PC.

1 ACTIVEZ LE PARE-FEU

Cliquez sur **Logiciels Ubuntu**, puis saisissez **GuFW** ou **Firewall** dans le champ **Rechercher**. Cliquez sur **Installer**, saisissez le mot de passe de votre compte administrateur et pointez sur le bouton **Lancer**. Les paramètres par défaut de GuFW sont verrouillés. Pour personnaliser le fonctionnement du pare-feu, activez le bouton **Déverrouiller** (ou **Unlock** suivant votre version). Indiquez de nouveau le mot de passe administrateur au sein de la fenêtre **S'authentifier**. Activez ensuite le curseur **État** pour mettre le firewall en service.

2 CRÉEZ DES RÈGLES DE FILTRAGE

Le filtre **Entrant** empêche les flux de données malveillants de pénétrer au cœur de votre système. Si vous venez d'activer le firewall, votre PC abrite peut-être déjà des logiciels malveillants. Il importe donc de surveiller aussi ce qui en sort. Sélectionnez **Rejeter** dans la liste déroulante, allez sur l'onglet **Règles** et pointez sur **+**. Pour autoriser une application à échanger des données avec Internet, activez l'onglet **Préconfigurée** dans la fenêtre **Ajouter une règle au pare-feu**. Déroulez la liste **Politique** et choisissez **Autoriser**.

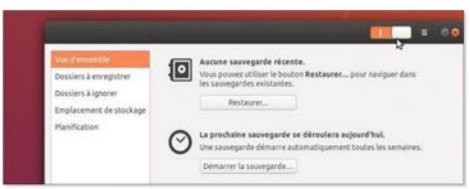
DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE SYSTÈME

ANTICIPEZ LES PANNES ÉVENTUELLES

Les plantages d'Ubuntu sont rares, mais souvent lourds de conséquences. Prenez les précautions qui s'imposent.

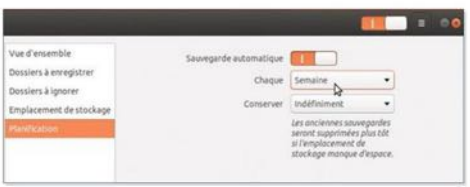
1 CONFIGUREZ LA SAUVEGARDE AVEC DÉJÀ DUP BACKUP TOOL

Cet utilitaire gratuit qui s'installe depuis le module **Logiciel Ubuntu**, accessible dans le lanceur. Saisissez le nom de l'appli dans le champ de recherche et pointez sur les boutons **Installer** puis **Lancer**. Dup affiche la rubrique **Vue d'ensemble**. À ce stade, la page est vierge. Actionnez le curseur de mise en marche de la sauvegarde automatique. Dans le volet gauche de l'interface, cliquez sur **Dossier à enregistrer** puis sur l'icône **+** au bas de l'écran. Indiquez alors les chemins d'enregistrement des dossiers à intégrer à la sauvegarde.



2 METTEZ À L'ABRI L'ESSENTIEL

Pour enregistrer une image complète de votre système, sélectionnez l'option **Autres emplacements** dans le volet gauche et cliquez sur **Ordinateur**, **Ajouter**. Excluez dans un deuxième temps les éléments inutiles en pointant sur **Dossier à ignorer**. Choisissez ensuite où seront enregistrés les fichiers dans **Emplacement de stockage** (si un PC Windows est connecté au réseau local, cliquez sur **Partage Windows**). Pour finir, activez l'onglet **Planification** et définissez la fréquence des sauvegardes et leur durée de conservation.



Le symbole bleu représente une espace

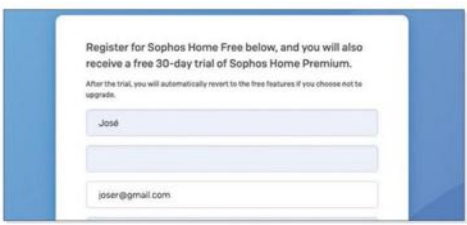
DIFFICULTÉ MODÉRÉE TEMPS 25 MIN DOMAINE SYSTÈME

NE LAISSEZ PAS VOTRE MAC SANS PROTECTION

macOS est victime de son succès. Pourtant construit sur un noyau Unix robuste, le système d'exploitation d'Apple est victime de nombreuses attaques. Le recours à un logiciel antivirus s'avère aujourd'hui recommandé pour déjouer les menaces.

1 CONFIEZ LA SURVEILLANCE À SOPHOS HOME

Sophos est un éditeur d'antivirus qui jouit d'une bonne réputation. Vous pouvez télécharger la version pour macOS de l'antivirus gratuit Sophos Home en vous rendant à l'adresse **bit.ly/2LmWxM0**. L'installation de l'application ne présente aucune difficulté. La seule formalité un peu contraignante consiste à créer un compte Sophos. Remplissez le formulaire d'inscription puis pointez sur le lien d'activation reçu par mail. Une fois le transfert achevé, ouvrez le Finder, accédez au dossier des téléchargements et décompressez l'archive ZIP obtenue. Glissez ensuite le fichier **Sophos** dans le dossier **Applications** du disque dur système.



2 ACTIVEZ LA PROTECTION EN TEMPS RÉEL

La base de signature de virus est mise à jour dès la fin de l'installation, de façon à disposer d'une protection optimale. Une notification vous informe qu'une extension système a été bloquée par macOS. Cliquez sur **Ouvrir les préférences Sécurité**, puis sur la page **Sécurité et confidentialité**, pointez sur **Autoriser**. Pour finaliser la configuration de l'antivirus, cliquez sur l'icône **Sophos** dans la barre de menus. Un volet se déploie alors et signale un défaut de sécurité. Pour faire disparaître cette alerte, actionnez le bouton **Activer** qui se trouve près de la commande **Protection en temps réel**. Sophos veille dorénavant sur votre Mac.

3 ANALYSEZ VOTRE MACHINE

Il est temps de s'assurer que vous n'êtes pas sous la menace d'un virus qui se serait infiltré avant la mise en place de Sophos. Lancez pour cela une analyse complète. Pointez sur le bouton **Sophos** dans la barre des menus, puis sur les trois points à droite du volet qui apparaît et enfin sur **Contrôle**. Activez la commande **Démarrer le contrôle** après avoir pris soin de cocher l'option **Exécuter un contrôle complet**. L'opération est méticuleuse et peut se révéler longue. Avec un disque dur de grande capacité bien rempli, plusieurs heures sont nécessaires pour mener à bien l'analyse.

4 PERSONNALISEZ LES OPTIONS DE SÉCURITÉ

Pendant que l'analyse est en cours, déployez le volet **Sophos**, déroulez le menu des options et activez la commande **Préférences**. Safari est alors automatiquement ouvert et pointe vers une interface en ligne qui dresse un état des lieux complet de la santé de votre Mac. Vous accédez aussi à la liste des options et des fonctionnalités de Sophos Home. Passez l'ensemble des onglets en revue pour ajuster le niveau de protection et l'adapter à vos usages. Pointez sur la commande **Configure** pour dévoiler les options disponibles pour chacune des rubriques (antivirus, ransomwares, malwares).

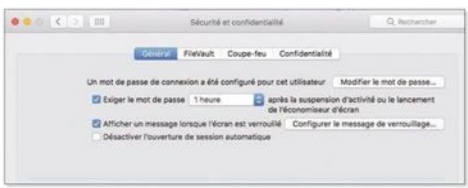
DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE ANALYSE

DRESSEZ UN REMPART CONTRE LES MALWARES

Moins virulents que les virus, les logiciels malveillants ciblent vos données personnelles et les ressources de votre ordinateur. Ne vous laissez pas envahir !

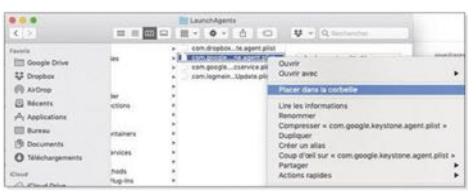
1 CONTRÔLEZ L'INSTALLATION DES PROGRAMMES

Apple se porte garant des applications qui sont disponibles sur le Mac App Store. macOS bloque en revanche l'installation des logiciels qui ne proviennent pas de sa boutique applicative. Pour y remédier, ouvrez les **Préférences Système** et pointez sur **Sécurité et confidentialité**, **Général**. Effectuez un double-clic sur le cadenas au bas de l'écran et tapez le mot de passe du compte administrateur. Cochez **App Store et développeurs identifiés** dans la section **Autoriser les applications téléchargées de**.



2 FAITES LE MÉNAGE DANS LA SÉQUENCE DE DÉMARRAGE

Si les malwares sont si dangereux, c'est qu'ils se lancent automatiquement avec macOS. Prenez l'habitude de dresser un état des lieux des programmes intégrés à la séquence de démarrage de votre Mac. Ouvrez le Finder, déroulez le menu **Aller** et sélectionnez **Aller au Dossier**. Saisissez **~/Library/LaunchAgents**. Repérez les éléments qui ne sont pas associés à un logiciel connu. Effectuez un clic droit et pointez sur **Placer dans la corbeille**. Répétez l'opération avec tous les comptes utilisateurs définis sur l'ordinateur.



DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE SYSTÈME

PLACEZ VOTRE ORDINATEUR SOUS SÉCURITÉ RENFORCÉE

Mettez à profit tous les outils de macOS pour protéger vos données et éviter les intrusions.

1 AJUSTEZ LE PARE-FEU

Affichez les **Préférences Système**. Accédez à l'onglet **Coupe-feu** de la rubrique **Sécurité et confidentialité** et assurez-vous que le firewall est activé. Si ce n'est pas le cas, cliquez sur le cadenas, identifiez-vous et mettez-le en service. Pointez ensuite sur **Options de Coupe-feu** et cochez **Bloquer toutes les connexions entrantes**. Il reste à définir des listes d'exceptions pour les activités réputées sûres. Cochez enfin **Activer le mode furtif** afin que votre Mac ne réponde pas aux sollicitations des programmes malveillants.

2 VERROUILLEZ L'ACCÈS AUX PARAMÈTRES

Parfois, les pires menaces viennent de l'intérieur. Aussi, après avoir peaufiné les paramètres de sécurité de votre Mac, il serait dommage qu'un importun ou un maladroit vienne tout remettre en cause. Pour éviter un tel désastre, revenez sur l'onglet **Général** des **Préférences de sécurité**. Pointez sur le bouton **Avancé** et cochez l'option **Exiger un mot de passe administrateur pour accéder aux préférences affectant l'ensemble du système**. Dorénavant, l'accès aux réglages sensibles sera conditionné à la saisie de votre code secret.

DIFFICULTÉ MODÉRÉE TEMPS 40 MIN DOMAINE SYSTÈME

CRÉEZ UNE CLÉ USB D'INSTALLATION DE MOJAVE

Parez à toute éventualité en préparant un support d'installation de macOS Mojave qui vous servira à remettre votre Mac d'aplomb en cas de problème. N'attendez pas d'en avoir besoin !

1 RASSEMBLEZ LES ÉLÉMENTS NÉCESSAIRES

L'opération consiste à copier les fichiers d'installation de macOS Mojave sur un support externe. Commencez par vous procurer une clé USB disposant d'une capacité d'au moins 16 Go, si possible un modèle rapide USB 3.0. Il faut ensuite en assurer le formatage. Lancez pour cela l'utilitaire de disque de macOS en saisissant *Utilitaire de disque* dans le champ de recherche Spotlight. Quand la clé est prête, téléchargez l'utilitaire Free Disk Drill (**bit.ly/2GzcxHM**). Double-cliquez sur le fichier **.DMG** copié sur votre disque dur pour installer Disk Drill. Finissez en glissant le fichier **DiskDrill.app** dans le dossier **Applications** du volume système.

2 TÉLÉCHARGEZ MACOS MOJAVE

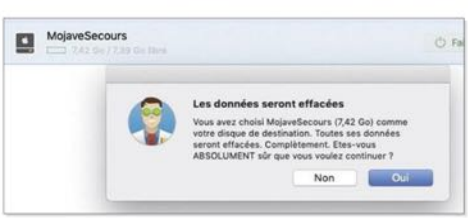
La clé USB est maintenant prête à accueillir la dernière version de macOS. Vous disposez également de l'utilitaire de transfert capable de rendre le support bootable. Il vous faut maintenant récupérer les fichiers d'installation de Mojave. Ouvrez le Mac App Store en cliquant sur l'icône de la boutique présente par défaut dans le Dock de macOS. Pointez dans le champ de recherche qui figure dans l'angle supérieur gauche de l'interface et saisissez l'intitulé **Mojave**. Cliquez sur le bouton **Obtenir** pour lancer le téléchargement de l'image disque du système d'exploitation. Ce dernier pèse un peu plus de 6 Go, aussi armez-vous de patience si vous disposez d'une connexion ADSL.

3 CONFIGUREZ LA CLÉ USB AVEC DISK DRILL

Au terme du téléchargement, insérez la clé USB préalablement formatée dans un port vierge de votre Mac. Ouvrez ensuite l'utilitaire de disque et renommez le support amovible afin de l'identifier sans l'ombre d'un doute dans Disk Drill. Lancez ce dernier et déroulez le menu **Créer un disk de démarrage**. Activez la commande **Outils d'installation OSX/MACOS**. Si le téléchargement de l'image de mac OS est terminé, Disk Drill détecte le fichier sur le disque dur et l'affiche parmi les suggestions. Sélectionnez l'image et pointez sur le bouton **Utiliser comme source**.

4 GÉREZ LA COPIE DES DONNÉES

Consultez la liste des supports de stockage identifiés par Disk Drill. Repérez votre clé USB et activez la commande **Créer un disque de démarrage** puis **Outils d'installation OSX/macOS**. Un message d'alerte vous informe que le support va à nouveau être formaté. Cliquez sur **Oui** pour passer à l'étape suivante. Il ne vous reste qu'à patienter jusqu'à la finalisation de l'opération. Le jour où vous avez besoin de restaurer macOS, éteignez le Mac avant de le remettre sous tension tout en appuyant sur la touche **Alt** du clavier. Vous pouvez alors sélectionner la clé de secours et réinstaller Mojave.



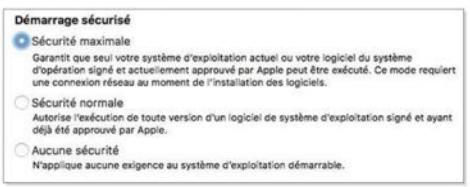
DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE SYSTÈME

SÉCURISEZ À FOND VOTRE COMPTE UTILISATEUR

L'OS d'Apple présente quelques faiblesses et de menues lacunes. Il faut ainsi protéger votre compte de façon à empêcher que ce dernier ne soit réinitialisé en mode recovery.

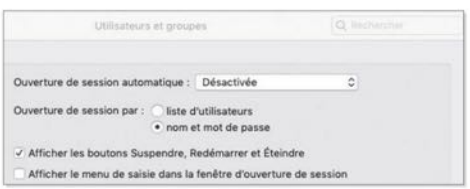
1 EXPLOITEZ LE DÉMARRAGE SÉCURISÉ

Si vous avez récemment acquis votre Mac (après novembre 2018), il est doté d'une puce T2 d'Apple. Celle-ci présente la particularité de donner accès à un démarrage sécurisé. Pour l'activer, allumez l'ordinateur en appuyant simultanément sur les touches **cmd + R**. Cliquez sur **Utilitaires**, **Utilitaire Sécurité au démarrage** et tapez le mot de passe de votre compte administrateur. Cochez **Sécurité Maximale** dans **Démarrage sécurité** et **Ne pas autoriser le démarrage à partir de supports externes** dans **Démarrage externe**.



2 DISSIMULEZ LES UTILISATEURS

Quand vous ouvrez une session sous macOS, le nom du dernier compte activé s'affiche. Seul le mot de passe est exigé. Pour renforcer la sécurité, demandez que les noms d'utilisateurs ne soient plus suggérés. Ouvrez les **Préférences système** et pointez sur **Utilisateurs et groupes**. Double-cliquez sur **Options** et identifiez-vous. Déroulez la liste **Ouverture de session automatique** et désactivez cette option. Cochez **Nom et mot de passe** dans **Ouverture de session par** et décochez **Afficher les indices de mots de passe**.



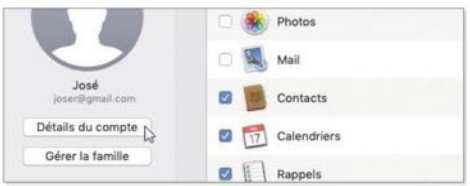
DIFFICULTÉ AUCUNE TEMPS 10 MIN DOMAINE SYSTÈME

RESTAUREZ ET MODIFIEZ LE MOT DE PASSE APPLE ID

Mieux vaut bien protéger votre compte Apple puisque celui-ci donne accès à iCloud et à vos infos personnelles.

1 RÉINITIALISEZ LE SÉSAME SUR UN MAC...

Ouvrez les **Préférences système** de macOS et cliquez sur l'icône **iCloud**. Pointez sur la commande **Détails du compte** et activez l'onglet **Sécurité** (saisissez le code de confiance à 6 chiffres qui vous est adressé si vous avez activé l'authentification à deux facteurs). Choisissez **Modifier le mot de passe**, saisissez le mot de passe du compte administrateur de votre Mac, indiquez le nouveau code secret et confirmez-le. Validez par **Modifier**. La procédure est comparable si vous effectuez l'opération à partir d'un iPhone.



2 ... OU MODIFIEZ-LE DEPUIS LE WEB

Il peut arriver que vous soyez dans l'incapacité d'accéder à votre compte Apple faute de disposer d'un iPhone ni d'un Mac. Rien n'est perdu, Apple ayant prévu une procédure applicable depuis n'importe quel ordinateur. Connectez-vous depuis un PC au site **apple.co/2Vx5yI7**. Après avoir saisi l'adresse mail associée à votre Apple ID, un assistant vous guide pas à pas dans votre démarche. Vous serez amené à répondre à quelques questions personnelles destinées à s'assurer de votre identité.

DIFFICULTÉ MODÉRÉE TEMPS 40 MIN DOMAINE SÉCURISATION

DÉPLACEZ-VOUS SEREINEMENT AVEC VOTRE MACBOOK

Un portable est par nature plus exposé qu'un ordinateur de bureau. Léger et voué à vous accompagner au cours de vos déplacements, il se vole ou se perd bien plus facilement. Quelques précautions s'imposent.

1 APPLIQUEZ DES PROTECTIONS PHYSIQUES

La première des menaces auxquelles votre MacBook est exposé lorsque vous partez en déplacement c'est évidemment le vol. Il existe heureusement des solutions efficaces pour dissuader les indélicats. Vous trouverez des adaptateurs de sécurité couplés à un câble de verrouillage en acier pour une somme comprise entre 80 € et 100 € dans les boutiques en ligne. Ces dispositifs permettent d'arrimer solidement le portable à un bureau. Évitez les solutions d'entrée de gamme qui n'offrent pas les meilleures garanties de solidité. La serrure de l'adaptateur qui se couple au boîtier du MacBook doit offrir une bonne résistance, de même que le câble en acier.

2 EMPÊCHEZ LES REGARDS INDISCRETS

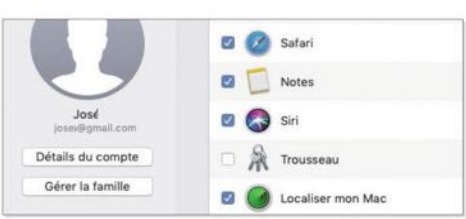
Dans le train ou un espace de coworking, il convient aussi de préserver la confidentialité des contenus affichés à l'écran de votre portable. Pour s'assurer que vos voisins ne peuvent pas lire vos mails ou vos documents de travail d'un simple regard en coin, investissez dans un filtre de polarisation à appliquer sur l'écran du MacBook. Maintenu en place par l'électricité statique, ce dispositif a un impact limité sur la qualité d'affichage (il assombrit un peu l'image) quand vous regardez l'écran de face. En revanche, pour les personnes situées à la périphérie, impossible de déchiffrer quoi que ce soit. Comptez environ 75 € pour un tel filtre.

3 VERROUILLEZ L'ACCÈS À LA MACHINE

Le pire étant toujours possible, pensez à protéger vos données. Allez dans les Préférences Système et cliquez sur **Sécurité et confidentialité**, **FileVault**. Cochez **Activer FileVault** afin de chiffrer le contenu du disque dur. Pour accéder aux données, vous devrez saisir une clé de chiffrement. Ce mot de passe sert aussi à verrouiller le Firmware et empêche la réinitialisation de votre MacBook à partir d'un autre disque que le volume de démarrage. Si quelqu'un dérobe votre ordinateur, il ne pourra ni utiliser le mode de récupération ni démarrer macOS à partir d'un lecteur externe.

4 ACTIVEZ LA LOCALISATION

Même si la fonction **Localiser mon Mac** s'avère moins efficace que sur un iPhone, faute d'une connexion 4G permanente, elle constitue néanmoins une précaution utile pour retrouver votre bien en cas de vol ou de perte. Vous pourrez ainsi connaître la position du portable lors de sa dernière connexion à Internet. Même si elle est imparfaite, cette précaution augmente sensiblement les chances de remettre la main sur le MacBook égaré. Pour activer la fonctionnalité, ouvrez la fenêtre des Préférences Système, pointez sur l'intitulé **iCloud**, puis cochez l'option **Localiser mon Mac**.



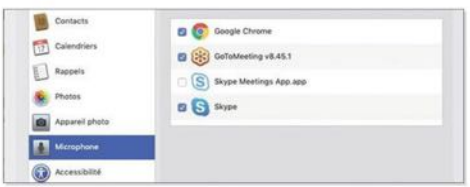
DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE SYSTÈME

GÉREZ L'ACCÈS AUX DONNÉES ET RESSOURCES DE VOTRE MAC

Identifiez et bloquez les applications qui accèdent à votre insu au contenu de votre disque dur, et pour certaines, trop curieuses, à vos données personnelles.

1 DRESSEZ UN ÉTAT DES LIEUX DES AUTORISATIONS

Dans les Préférences Système de macOS, cliquez sur l'icône **Sécurité et confidentialité**, puis sur l'onglet **Confidentialité**. Le volet gauche de la fenêtre répertorie les ressources auxquelles peuvent accéder les applications. Pointez sur l'un des intitulés, **Microphone** par exemple pour afficher liste des applications autorisées à lire les données captées par le micro de votre Mac. Passez-les en revue et assurez-vous que l'usage du micro est légitime et utile. Si la réponse à ces deux questions est non, révoquez le droit d'accès sans tarder.



2 CONFIRMEZ OU NON LES DROITS DES APPLIS

Dans l'angle inférieur droit de la fenêtre, double-cliquez sur le cadenas, saisissez votre mot de passe administrateur et pointez ensuite sur la commande **Déverrouiller** de façon à débloquer l'accès aux réglages système (Apple limite par défaut le potentiel de nuisance des utilisateurs). Vous pouvez maintenant gérer les autorisations accordées aux applications. Décochez la case devant le logiciel pour lui couper l'accès au micro. Si vous constatez à l'usage que cela empêche le bon fonctionnement du programme, revenez en arrière.

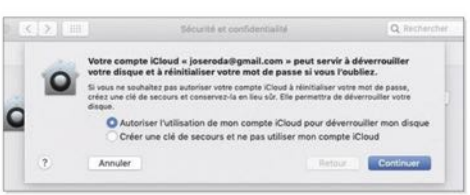
DIFFICULTÉ MODÉRÉE TEMPS 1 H DOMAINE CRYPTAGE

CHIFFREZ LES FICHIERS AVEC FILEVAULT

Vous manipulez des données confidentielles ? Alors n'hésitez pas à chiffrer le contenu de votre Mac.

1 RENDEZ VOS DONNÉES INVIOLABLES

FileVault est un système de sécurité intégré à macOS. Il permet non seulement de chiffrer le contenu de vos dossiers personnels, mais aussi l'ensemble du disque dur système. Vos données ne pourront ainsi être lues qu'après avoir saisi le mot de passe utilisateur au démarrage de l'ordinateur. Pour mettre en place cette protection, allez dans les Préférences Système, cliquez sur **Sécurité et confidentialité**, puis sur **Activer FileVault**. Indiquez si vous souhaitez conserver la clé de chiffrement sur iCloud et validez par **Continuer**.



2 ANNULEZ LA PROTECTION DU DISQUE DUR

Le chiffrement du volume système peut alors débuter. Soyez patient. Il faut plusieurs heures à macOS pour réaliser cette opération. Une jauge vous informe en temps réel de l'avancée de la procédure. Il est possible d'utiliser le Mac durant ce temps. Votre travail n'en sera pas perturbé ni ralenti. Si vous changez d'avis et souhaitez mettre fin au chiffrement des données, il suffit de désactiver FlleVault dans les Préférences Système. Vous devez simplement attendre pour cela que la phase de cryptage soit terminée.

DIFFICULTÉ MODÉRÉE TEMPS 40 MIN DOMAINE ARCHIVAGE

SAUVEGARDEZ TOUT LE CONTENU DE VOTRE MAC

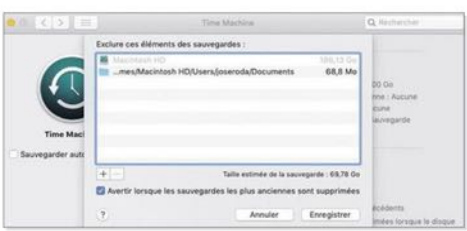
macOS dispose d'une arme pour prévenir la perte des données. Intégré au cœur du système, Time Machine réalise des sauvegardes régulières des fichiers et plus globalement, de votre configuration. Des copies qui seront utiles en cas de panne.

1 PRÉPAREZ TIME MACHINE

Pour ne plus être pris au dépourvu en cas de défaillance matérielle, prenez le temps de configurer l'outil de sauvegarde de macOS. Commencez par brancher un disque dur externe à votre Mac. Par mesure de précaution, assez compréhensible, le dispositif refuse de copier les fichiers de secours sur une partition du disque système. Une fois le volume connecté et formaté, ouvrez les Préférences Système et pointez sur la commande **Time Machine**. Cliquez sur le cadenas pour déverrouiller l'édition des paramètres et cochez la case **Sauvegarder automatiquement**. Pointez ensuite sur le lien **Choisir un disque de sauvegarde** et désignez le support de stockage externe.

2 PERSONNALISEZ LA SAUVEGARDE

Par défaut, Time Machine enregistre des images instantanées de votre système si le support de stockage dispose d'assez d'espace. Ces sauvegardes sont réalisées quotidiennement. Pour économiser de la place, vous pouvez exclure du périmètre de la sauvegarde les dossiers qui ne contiennent pas de données critiques. Pour cela, pointez sur le bouton **Options** dans les préférences de Time Machine. Dans la fenêtre **Exclure des éléments des sauvegardes**, activez le bouton + et parcourez l'arborescence du disque dur pour désigner un à un les emplacements à ignorer. En cas d'erreur, revenez sur vos choix en pointant cette fois sur le bouton -.

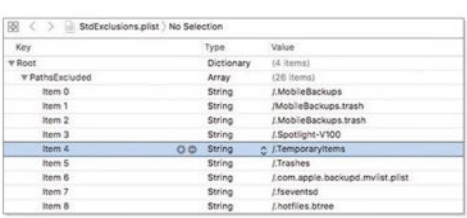


3 CHANGEZ DE VOLUME D'ENREGISTREMENT

Si le disque externe dédié à la sauvegarde arrive à saturation, branchez un support d'une capacité supérieure. Accédez à la section **Time Machine** des Préférences Système, puis cliquez sur **Options**. Sélectionnez le nouveau disque dur. Une sauvegarde est effectuée dans les 120 secondes qui suivent. L'historique des sauvegardes enregistrées sur le précédent volume Time Machine n'est pas transféré. Il reste néanmoins accessible. Ainsi, si vous avez besoin de restaurer une version antérieure d'un fichier, vous pouvez le faire depuis l'ancien disque (sous réserve qu'il n'ait pas été reformaté).

4 ACCÉDEZ AUX PROPRIÉTÉS AVANCÉES DE L'OUTIL

Depuis le Finder, cliquez sur **Macintosh HD** et suivez le chemin **Système/Bibliothèques/CoreServices**. Effectuez un clic droit sur le fichier **BackUpD.Bundle** et pointez sur **Afficher le contenu**. Accédez ensuite au dossier **Content/Ressources** et ouvrez le fichier **StdExclusions.plist** avec l'appli XCode. Développez la branche **PathExcluded** pour afficher la liste des dossiers exclus de la sauvegarde. Pour inclure de nouveau un emplacement, cliquez sur l'icône - à côté de son nom. Activez le bouton **Unlock** de façon à confirmer le déverrouillage du fichier et enregistrez les réglages par **Fichier**, **Save**.



DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE SYSTÈME

GARDEZ MACOS, LES APPLIS ET LES PILOTES À JOUR

Apple déploie très régulièrement des correctifs destinés à améliorer la sécurité et la stabilité de son système d'exploitation. Ces mises à jour sont essentielles pour assurer la bonne santé de votre Mac.

1 PROCÉDEZ MANUELLEMENT

Automatiser l'installation des mises à jour garantit de disposer d'un système sûr. Vous avez néanmoins toute latitude pour adopter ces correctifs quand bon vous semble ou forcer la recherche. Accédez aux Préférences Système de macOS depuis le menu **Pomme** du Bureau. Pointez ensuite sur la commande **Mise à jour de logiciels** de façon à lancer la recherche. Patientez quelques secondes. Si aucun fichier n'est disponible, le bouton **Mettre à jour** demeure grisé. Dans le cas contraire, pointez dessus afin d'afficher le détail du correctif et d'en estimer l'importance. Actionnez le bouton **Mettre à jour maintenant** pour télécharger et installer le correctif.

2 AFFICHEZ LES OPTIONS

Si vous préférez que macOS se charge de tout, veillez à cocher l'option **Mettre à jour automatiquement mon Mac** au bas de la fenêtre **Mise à jour de logiciels**. Une recherche de correctifs s'effectuera dès lors quotidiennement sans que vous ayez à vous en soucier. Pointez ensuite sur le bouton **Avancé** pour accéder à plus de paramètres et gérer la recherche, le téléchargement et l'installation des mises à jour disponibles. Si vous possédez un Mac ancien dont les performances pourraient être affectées par l'installation d'une nouvelle version de macOS, automatisez la recherche et le téléchargement des mises à jour, mais gardez l'initiative quant à leur installation.

3 N'OUBLIEZ PAS LES APPLIS

Pour ce qui concerne la mise à jour des applications, vous n'avez qu'à vous en remettre au Mac App Store. Cliquez sur l'icône de la boutique présente dans le Dock. Observez le volet gauche et pointez sur la commande **Mises à jour**. Quand une nouvelle version est disponible, il vous suffit d'activer le bouton **Obtenir** pour procéder au téléchargement puis à l'installation de l'appli. Attention toutefois, les problèmes de mise à jour n'interviennent pas toujours au moment de l'installation. Il arrive que des dysfonctionnements se manifestent dès le téléchargement.

4 ANNULEZ UN CORRECTIF VIA LE MAC APP STORE

Si vous ne parvenez pas à finaliser le transfert du programme d'installation d'une appli, connectez-vous sur le site **apple.co/2PtJB5t**. Si des pastilles rouges apparaissent devant les lignes **Mac App Store** et **Mise à jour de logiciels mac OS**, patientez jusqu'au rétablissement du service. Dans le cas où le téléchargement de la mise à jour via le Mac App Store est bloqué, vous pouvez annuler l'opération. Appuyez pour cela sur le bouton **alt** (**Options**) du clavier. La commande **Pause/Reprendre** affichée par le Mac App Store se transforme alors en un bouton **Annuler**.

DIFFICULTÉ MODÉRÉE TEMPS 10 MIN DOMAINE SYSTÈME

PROTÉGEZ VOTRE MOBILE DES VIRUS ET DES MALWARES

Les smartphones sont devenus de véritables ordinateurs de poche. Rien d'étonnant dès lors que les cybercriminels en fassent des cibles de choix. Avez-vous pris toutes les mesures pour sécuriser votre téléphone des attaques menées par les virus, les ransomwares et les malwares ?

Boîte à outils

Pour ce pas à pas, nous avons utilisé

Clean Master

Un smartphone sous Android

Malwarebytes Sécurité Antivirus & Anti-Malware

Avast 2019

Les cybercriminels visent en priorité les systèmes d'exploitation les plus répandus et les moins bien protégés. Avec près de 2 milliards d'appareils en circulation dans le monde, Android fait office de cible privilégiée, au même titre que Windows. Il est donc devenu indispensable de veiller à la sécurité de son téléphone. Une tâche désormais familière sur un ordinateur, mais que beaucoup d'utilisateurs négligent encore quand il s'agit de leurs appareils mobiles. Pourtant, 93 % de la population française possède un smartphone, beaucoup d'entre nous s'en servant pour gérer les mails et naviguer sur Internet (34 % du tra c Internet s'est effectué depuis un mobile en 2018, en hausse de 49 % sur un an selon l'observatoire BDM). Un accès à Internet rendu permanent grâce aux réseaux cellulaires 4G et qui renforce la vulnérabilité des téléphones.

Connectés 24 h/24, les mobiles sont les cibles permanentes des tentatives menées par les criminels. Hameçonnage, virus, malwares et ransomwares prolifèrent et empruntent tous les vecteurs d'infection imaginables : mails piégés, applis infectées, sites Internet détournés. Il suffit de cliquer sur un lien dans un message ou sur une page Web pour laisser entrer un ennemi invisible ! Les jeux et les applis que vous téléchargez sur le Play Store de Google peuvent aussi présenter des risques. La boutique officielle d'Android héberge des applications infectées et destinées à dérober vos données personnelles. Statista évalue à 40 000 le nombre d'applis n'ayant rien à faire sur le store, dont plus de 2000 renfermeraient un malware. Alors, toujours pas décidé à vous protéger ?●

1 EFFECTUEZ UN NETTOYAGE PRÉVENTIF

Avant d'installer une suite de sécurité sur votre téléphone, prenez le temps de procéder à un nettoyage en règle. Supprimez tout d'abord les applis que vous n'utilisez plus et faites le ménage dans le dossier des téléchargements. Poursuivez l'opération en vous aidant d'un utilitaire spécialisé dans la recherche des éléments inutiles. Ouvrez le Play Store et installez Clean Master (**bit.ly/321xS4G**). Touchez ensuite le bouton **Ouvrir**, accordez les autorisations demandées puis exécutez la commande **Nettoyer maintenant** pour identifier les fichiers indésirables, ceux conservés dans le cache ou encore les APK, éléments d'installation des applis. Validez leur suppression en effleurant le bouton **Nettoyer les éléments indésirables**.

2 ÉRADIQUEZ LES MALWARES

Maintenant que votre mobile est délesté des éléments inutiles, il est temps de supprimer les éventuels logiciels malveillants. Vous pouvez utiliser à cette fin l'outil antimalware Malwarebytes Sécurité Antivirus & Anti-Malware (**bit.ly/2FldrjG**). Une fois celui-ci installé, effleurez le bouton **Lancez-vous** et validez les autorisations requises. Vous bénéficiez gratuitement de la version Premium de l'appli durant un mois, sans avoir à enregistrer un moyen de paiement. Appuyez sur **Analyser maintenant** et patientez quelques minutes. Une fois l'examen terminé, effleurez le bouton **Corriger maintenant** pour confirmer la mise en quarantaine des fichiers infectés. Explorez ensuite les options avancées de l'appli pour une protection renforcée.

3 DOTEZ-VOUS D'UN ANTIVIRUS

Les principaux éditeurs déclinent dorénavant leurs suites de sécurité sous Android. Le Play Store propose ainsi Avast Mobile Security 2019 (**bit.ly/2FldrjG**). Très efficace, cet outil brille aussi par sa capacité à identifier les faux positifs, c'est-à-dire les services pris à tort pour des éléments malveillants. La version Ultimate de l'appli (24 €/an) ajoute un pare-feu, le verrouillage des applications, un VPN et vous débarrasse des publicités.

4 LANCEZ UNE PREMIÈRE ANALYSE

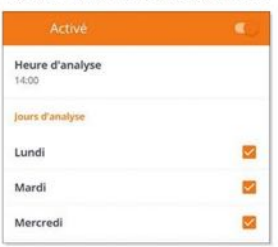
La version gratuite de l'antivirus s'avère suffisante dès lors que vous évitez de rooter votre téléphone, ou d'installer des applications en dehors du Play Store. Appuyez sur **Démarrer**, puis sur le bouton **Analyser**. Accordez les autorisations demandées par Avast et attendez le résultat de cette première vérification. L'appli vous signale les éventuels problèmes rencontrés ou indique que vous êtes protégé. Appuyez sur la flèche retour arrière en haut de l'écran pour revenir sur l'écran d'accueil de l'antivirus. Vérifiez que Clean Master n'a pas laissé d'éléments inutiles derrière lui en touchant le bouton **Nettoyer**. Si Avast Mobile Security détecte des fichiers ou des applis obsolètes, supprimez-les en allant sur le menu **Safe Clean**.

5 SÉCURISEZ LES CONNEXIONS SANS FIL

Appuyez sur **Analyser Wi-Fi** afin qu'Avast teste la robustesse du mot de passe de votre Box Internet. Activez l'analyse automatique du Wifi pour être protégé en permanence. Revenez sur l'accueil et ouvrez le menu de l'application. Lancez un test de vitesse de façon à vérifier que le débit de la ligne est en adéquation avec votre abonnement fibre ou ADSL. Notez qu'Avast Mobile Security ne protège pas les échanges en Bluetooth. Pensez à couper ce mode de connexion quand vous ne l'utilisez pas.

6 PLANIFIEZ LA VÉRIFICATION

Poursuivez la procédure de vérification en effleurant le bouton **Augmenter la Ram** pour fermer les applications qui s'exécutent en tâche de fond et qui sont susceptibles de vous espionner. Revenez ensuite sur l'écran d'accueil de l'appli. Déroulez la page vers le bas jusqu'au menu **Activer l'analyse quotidienne**. Indiquez le moment idéal pour lancer la recherche de virus en pointant sur l'intitulé **Heure d'analyse**. Avast effectue un diagnostic chaque jour. Si vous ne souhaitez pas être importuné le week-end, décochez les cases **samedi** et **dimanche**. Outre cette surveillance quotidienne, procédez chaque semaine à une recherche détaillée en actionnant la commande **Réaliser une analyse approfondie** depuis le tableau de bord de l'application.



7 ACTIVEZ L'ALERTE ANTIVOL

Ouvrez le menu d'Avast et pointez sur **Antivol**, **Configurer maintenant**, **Définir un code PIN**. Cochez votre compte Google, entrez votre mot de passe et validez par **Continuer**. Touchez **Connectez-vous à votre compte Avast**, **Configurez le contrôle web** et créez un compte **Avast**. Si vous perdez votre mobile, connectez-vous au site Avast et déclarez l'appareil comme perdu pour le verrouiller à distance.

DIFFICULTÉ MODÉRÉE TEMPS 30 MIN DOMAINE PUB

GARDEZ LES PUBLICITÉS À DISTANCE

Les bandeaux et les fenêtres à caractère commercial fleurissent sur les mobiles plus encore que sur les ordinateurs. Pour naviguer en paix, offrez un bloqueur de pubs à Firefox ou Google Chrome.

1 ACCÉDEZ AUX MODULES COMPLÉMENTAIRES DE FIREFOX

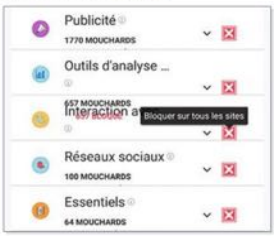
Firefox pour Android (**bit.ly/2vNF8SO**) peut accueillir diverses extensions. Parmi ces modules additionnels, certains, à l'image de uBlock Origin ou Ghostery, sont dédiés au blocage des publicités. Pour les découvrir, ouvrez le menu du navigateur, appuyez sur **Modules complémentaires**, **Parcourir les extensions recommandées de Firefox**.

2 PARAMÉTREZ UBLOCK ORIGIN

Effleurez l'icône **uBlock Origin**, puis le bouton **+ Ajouter à Firefox** pour l'installer. Dans le menu **Modules complémentaires**, pointez sur **uBlock Origin**, **Options** et effleurez le bouton **Mettre à jour maintenant**. L'onglet **Paramètres** comporte plusieurs options. Cochez les cases **Désactiver les infobulles**, **Empêcher la fuite des adresses IP locales via WebRTC** et **Bloquer les rapports CSP** pour protéger votre vie privée.

3 PROFITEZ DE GHOSTERY

Installez de la même façon l'extension Ghostery, complémentaire de la surveillance opérée par uBlock Origin. Déroulez la page d'accueil du module vers le bas et appuyez sur **Modifier la configuration**, **Oui**, **Choisissez parmi les options de la liste**. Cochez **Réseaux sociaux**, **Essentiels** et **Interaction avec les clients**.



4 OPTEZ POUR FIREFOX FOCUS

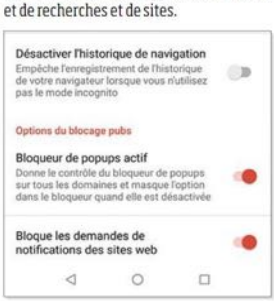
Si vous n'avez pas de navigateur attitré, intéressez-vous à Focus (**bit.ly/2WJvzEv**), une version de Firefox qui fait la part belle à la confidentialité de vos données. Ce navigateur travaille par défaut en mode furtif, bloquant les traqueurs et les publicités. Déroulez le menu de l'appli et dirigez-vous vers **Vie privée et sécurité**. Cochez **Bloquer les autres traqueurs de contenu**, puis pointez sur **Cookies et données de sites** et optez pour **Interdire les cookies tiers uniquement**.

5 PRÉFÉREZ LE BUTINEUR ADBLOCKER

Si vous êtes totalement allergique aux publicités, adoptez Adblocker, un navigateur gratuit basé sur le moteur de Google Chrome et qui a pour particularité de bloquer les annonces commerciales (**bit.ly/2Xn88wo**). Accédez à un site Web qui a pour habitude de vous abreuver de réclames. Déroulez le menu à droite et effleurez **Bloqueur de pubs**. Vous serez informé du nombre de pubs interceptées.

6 SUPPRIMEZ LES PUBS DE YOUTUBE

Adblocker peut également interdire les publicités dans YouTube. Cela implique bien sûr de visionner les vidéos à partir du navigateur et non de l'appli YouTube. Affichez le menu d'Adblocker et désactivez le curseur **Ouvrir YouTube dans l'appli YouTube**. Profitez de l'occasion pour mettre en action la fonction **Bloque les demandes de notifications des sites web**. Vous éviterez ainsi les alertes à caractère publicitaire. Pour optimiser la confidentialité, activez l'interdiction du suivi puis décochez les options associées aux suggestions d'erreur et de recherches et de sites.



DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE ANTIVOL

LOCALISEZ VOTRE MOBILE EN CAS DE VOL

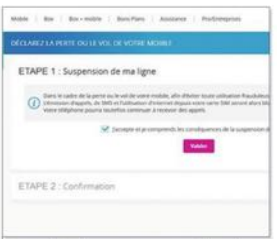
Égarer ou se faire dérober son portable n'arrive pas qu'aux autres. Google a prévu un dispositif pour vous aider à localiser votre appareil. Si le vol est avéré, vous avez la possibilité d'effacer les données à distance.

1 SUSPENDEZ LA LIGNE

La première chose à faire après le vol de son téléphone consiste à désactiver la carte SIM. L'opération s'effectue depuis l'espace client du site de l'opérateur auquel vous êtes abonné. Recherchez la section dédiée à la carte SIM, pointez sur l'intitulé **Mobile perdu ou volé** et suivez la procédure de déclaration qui va automatiquement suspendre votre ligne. Celui qui détient votre mobile ne pourra plus émettre d'appels ni accéder à Internet en 4G.

2 PRENEZ LES DEVANTS

L'opération suspend momentanément votre ligne, jusqu'à ce que vous receviez une nouvelle carte SIM par courrier et que vous l'activiez. En attendant, les outils de localisation déployés par Google peuvent vous aider à retrouver votre appareil. Pour en profiter, il faut que le téléphone soit associé à votre compte Google. Vous devez également avoir activé la localisation dans les paramètres d'Android et opté pour le mode **Haute précision** dans les paramètres de confidentialité.



En cas de vol, commencez par désactiver la carte SIM sur le site de l'opérateur.

3 LOCALISEZ L'APPAREIL

En cas de perte ou de vol, connectez-vous à votre compte Google, de préférence avec le navigateur Chrome. Placez-vous sur l'onglet **Sécurité** puis pointez sur le nom du téléphone dans la section **Vos appareils**. Cliquez ensuite sur **Retrouver un appareil perdu ou volé**. Sélectionnez le mobile et tapez votre mot de passe Google pour accéder au menu dédié. Faites-le sonner pour vous assurer qu'il ne se trouve pas dans l'une de vos poches. Si rien ne se passe, tentez de le localiser sur la carte.

4 EFFACEZ LES DONNÉES À DISTANCE

Si ces actions vous confortent dans l'idée que le mobile a été dérobé, vous devez prendre des mesures pour en protéger le contenu. Cliquez sur **Sécuriser l'appareil** afin de le verrouiller. Vous pouvez aussi faire apparaître un message à l'écran pour promettre une récompense à celui qui le trouverait. En dernier recours, allez sur **Effacer les données de l'appareil**. Cette option plus radicale préserve votre vie privée en supprimant de manière définitive les données et fichiers personnels qui se trouvent en mémoire.

DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE SANS FIL

SÉCURISEZ LE PARTAGE DE CONNEXION 4G

Cette option est très pratique pour accéder à Internet depuis un PC en l'absence de signal Wifi.

1 ACTIVEZ LE PARTAGE SUR ANDROID

En vacances ou dans le train, il n'est pas toujours possible de brancher son PC sur une box Internet ou une borne Wifi. Si votre téléphone bénéficie d'une couverture 4G, créez un réseau local auquel vos autres appareils se connecteront. Dans les paramètres d'Android, touchez **Réseau et Internet**, **Point d'accès et partage de connexion**. Activez le **Wi-Fi** et effleurez **Configurer le point d'accès Wi-Fi**. S'il s'agit seulement de naviguer avec votre portable, préférez l'option **Partage par USB**, bien plus sûr puisque la liaison s'opère au moyen d'un câble.

2 SÉCURISEZ LA CONNEXION

Changez le nom du point d'accès afin que vos proches l'identifient facilement. Déroulez le menu **Sécurité** et activez la protection **WPA2 PSK**. Si vous conservez le mode **Aucune**, n'importe qui peut se connecter sans votre consentement. Définissez ensuite un mot de passe que vous communiquerez à votre entourage. Appuyez sur **Enregistrer** pour activer le partage. Votre téléphone apparaît à présent dans la liste des réseaux Wifi disponibles.

Le partage de connexion est sécurisé par un mot de passe et un cryptage WPA2.

3 PARTAGEZ LE FLUX DE VOTRE IPHONE

Le téléphone d'Apple propose lui aussi le partage de connexion. Pour en faire profiter votre MacBook ou votre iPad, allez dans **Réglages**, **Données cellulaires**. Pointez sur le menu **Partage de connexion**, activez cette fonctionnalité puis choisissez un mot de passe. Comme Android, iOS offre la possibilité d'activer le partage 4G via une liaison Bluetooth ou en reliant l'iPhone à l'ordinateur au moyen d'un câble USB. Pensez à désactiver le partage de connexion quand vous n'en avez plus besoin.

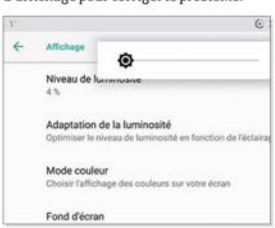
DIFFICULTÉ ÉLEVÉE TEMPS 30 MIN DOMAINE DÉPANNAGE

RÉACTIVEZ UN MOBILE PLANTÉ

Quand un téléphone Android ne répond plus, les causes peuvent être multiples, au même titre que les réponses à apporter pour le remettre en état. Panne mineure ou gros souci, voici comment réagir.

1 VÉRIFIEZ LA BATTERIE

Si le mobile refuse de s'allumer, branchez-le à une source de courant en utilisant le chargeur d'origine et patientez une dizaine de minutes. Si l'appareil dispose d'une batterie amovible, retirez-la puis remettez-la en place. Toujours pas d'image ? Vérifiez que vous n'avez pas réglé la luminosité au minimum. Allez dans une pièce très sombre et accédez aux paramètres d'affichage pour corriger le problème.



2 UTILISEZ L'OPTION SANS ÉCHEC

Une seconde solution consiste à démarrer en chargeant un minimum de services. Appuyez longuement sur le bouton **Marche / Arrêt** puis sur la commande **Éteindre** jusqu'à l'apparition de la fenêtre **Redémarrer en mode sans échec**. Validez par **OK**. Android devrait se relancer sans charger les applis. Si l'opération réussit, supprimez les dernières applications installées sur le téléphone. Quittez le mode sécurisé en redémarrant normalement l'appareil.

3 ACCÉDEZ AU MODE RECOVERY

En cas de panne persistante, éteignez le téléphone, puis appuyez longuement sur les boutons de volume haut et bas et sur **Marche / Arrêt**. Vous arrivez alors directement sur l'écran du mode **Recovery**. Si ce n'est pas le cas, utilisez les boutons **Vol.+** et **Vol.-** pour vous déplacer dans les menus et validez vos choix avec **Marche/Arrêt**.

4 REVENEZ AUX RÉGLAGES D'USINE

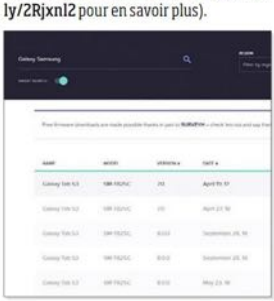
En fonction des modèles, les menus peuvent être francisés ou non. Ils présentent plusieurs options dont certaines ne doivent pas être activées au risque de bloquer définitivement le téléphone. Pour vérifier s'il ne s'agit pas d'un problème lié à l'écran, lancez un test graphique (**run graphics test**) si celui-ci est disponible. Le moyen le plus efficace pour reprendre le contrôle du mobile consiste à restaurer les valeurs d'usine (**Wipe data/factory reset**). Attention, l'opération effacera vos données.

5 FAITES APPEL AUX SERVICES D'UN PROGRAMME DE RÉCUPÉRATION

Le logiciel FoneLab Android Data Recovery (**bit.ly/2ADa4bx**) s'utilise à partir d'un PC et offre la possibilité de récupérer les données d'un téléphone ayant subi des dommages sérieux empêchant sa remise en état (écran en panne, perte de la zone tactile, etc.). L'application accède à la mémoire interne de l'appareil et en copie le contenu. Commencez par vérifier que FoneLab Android Data Recovery est compatible avec votre mobile en installant la version gratuite du programme.

6 PLONGEZ AU CŒUR DU SYSTÈME

Si vous êtes fin connaisseur d'Android et que vous savez comment rooter un mobile, vous pouvez tenter de restaurer un appareil inutilisable en effaçant ses données et en reflashant une ROM. Vous avez besoin pour cela d'un PC, des utilitaires Fastboot et ADB, inclus dans Android Studio (**bit.ly/2M3WrXd**) et qui assureront la communication avec le téléphone. Munissez-vous par ailleurs d'une custom recovery (TWRP par exemple, disponible sur le site **bit.ly/2FfiPfC**) et d'une ROM compatible avec votre appareil (consultez le site **bit.ly/2RjxnI2** pour en savoir plus).



DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE SYSTÈME

BLOQUEZ LES APPLICATIONS TROP CURIEUSES

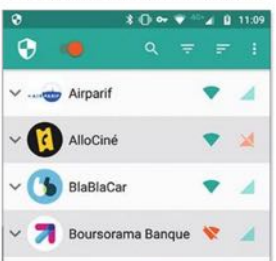
La plupart des applis présentes sur votre téléphone continuent à envoyer et recevoir des données même lorsque vous ne les utilisez pas. Coupez court à ces échanges pour réduire les risques et économiser votre connexion 4G.

1 INITIALISEZ NETGUARD

Accédez au Play Store et installez l'application NetGuard (**bit.ly/2smR6B6**). Lors de la première utilisation, vous êtes invité à activer ses différentes fonctionnalités à l'aide du curseur situé en haut à gauche de la page d'accueil. Autorisez la connexion VPN intégrée et excluez NetGuard du scénario d'optimisation de la batterie d'Android. Autorisez le fonctionnement en arrière-plan et l'accès sans limitation à la connexion cellulaire ; Le curseur d'activité doit alors s'afficher en rouge.

2 DÉFINISSEZ LES AUTORISATIONS

Après avoir redémarré, NetGuard affiche la liste des applis installées. Certaines sont masquées par des encadrés informatifs. Appuyez sur **OK** pour les faire disparaître. Accédez au menu détaillé de chacune d'elles en effleurant la flèche pointant vers le bas à gauche de leur nom. Vous pouvez décider de les bloquer quand l'écran est verrouillé ou lorsque vous voyagez à l'étranger (touchez la coche **itinérance**).



NetGuard administre les données émises et reçues par les applications.

3 ACTIVEZ LE BLOCAGE PERSONNALISÉ

Les icônes **Wifi** et **réseau mobile** (suivies de la mention **R** indiquant que le mode itinérance est suspendu) figurent à droite du nom de chaque appli. Il suffit d'appuyer sur ces liens pour couper l'accès au réseau sans fil ou au réseau cellulaire. Utilisez les commandes de la barre de titre pour rechercher une appli et changer les critères de tri. Pour bloquer tous les échanges, effleurez les points à droite et cochez l'option **Verrouiller le trafic**.

4 PERSONNALISEZ LE FILTRAGE À L'AIDE DE LISTES D'EXCEPTIONS

Déroulez le volet de menu, puis effleurez les intitulés **Paramètres**, **Valeurs par défaut**. Actionnez les différents curseurs pour personnaliser le fonctionnement de NetGuard. Les règles définies sur cette page concernent l'ensemble des applications. Pour gérer des exceptions, allez sur l'écran d'accueil, sélectionner une appli et décochez l'option **Appliquer les règles et conditions**. Utilisez les options avancées du menu **Paramètres** pour filtrer le trafic, surveiller l'activité du réseau ou générer le journal des accès à Internet.

DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE SYSTÈME

VERROUILLEZ L'ACCÈS AU CONTENU DU MOBILE

Interdisez les modifications des ressources système du smartphone et l'installation d'applis inconnues.

1 ACTIVEZ L'OPTION DÉVELOPPEURS

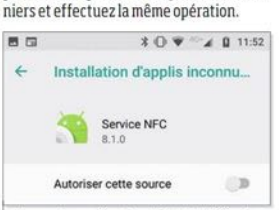
Quand vous reliez votre téléphone à un ordinateur, Android se contente de basculer en mode recharge. Les données du mobile n'apparaissent pas dans l'Explorateur de fichiers de Windows. Pour être certain que cette option soit activée par défaut, débloquez le mode Développeur en pointant sur **Paramètres**, **Système**, **A propos du téléphone** et en touchant à sept reprises l'intitulé **Numéro de build**.

2 INTERDISEZ LE MODE DÉBOGAGE

Retournez sur la page Système des paramètres et appuyez sur **Options développeurs**. Dirigez-vous vers la section **Mise en réseau** et pointez sur **Sélectionner une configuration USB**. Cochez le mode **Batterie en charge**. Allez ensuite dans **Débogage**. Vérifiez que le curseur **Débogage USB** est désactivé et appuyez sur **Annuler les autorisations relatives au débogage USB**. Cela évitera que l'on puisse rooter le téléphone ou envoyer des commandes système depuis le PC.

3 BLOQUEZ LES APPLIS INCONNUES

Les dernières versions Android limitent grandement les possibilités de nuisance d'applis en provenance de sources autres que le Play Store. Dorénavant, le système peut afficher la liste des applis à travers lesquelles ce type d'installation demeure possible. Ouvrez les paramètres du mobile, effleurez **Applis et notifications**, **Paramètres avancés**, **Applis : accès spécial**, **Installation d'applis inconnues**. Vérifiez que la liste ne comporte pas la mention **Autorisées**. Si c'est le cas, désactivez le curseur **Autoriser cette source**. Appuyez sur les points à droite, puis sur **Afficher les processus système**. Inspectez ces derniers et effectuez la même opération.



Les versions récentes d'Android offrent un contrôle accru sur l'installation des APK.

DIFFICULTÉ MODÉRÉE TEMPS 30 MIN DOMAINE SYSTÈME

PRÊTEZ VOTRE TÉLÉPHONE

N'ayez plus peur de confier votre mobile à un proche. Faites appel aux comptes utilisateurs et au mode invité d'Android pour masquer vos données personnelles et limiter l'usage de certaines applis.

1 ACTIVEZ LE MODE INVITÉ

Très pratique si vous devez confier votre mobile dans l'urgence à un ami, la session invité ne permet pas d'accéder à vos données ni à vos applis. Ouvrez les paramètres de l'appareil et touchez **Système**, **Options avancées**, **Utilisateurs** Multiples. Effleurez l'engrenage pour autoriser les appels téléphoniques, puis l'intitulé **Invité**. Pour fermer la session, déroulez le panneau des notifications, pointez sur l'avatar et sur **Supprimer l'invité**, **Supprimer**.

2 CRÉEZ PLUSIEURS PROFILS

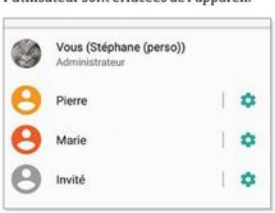
Vous avez l'habitude de prêter votre téléphone à vos enfants ? Dans ce cas, mieux vaut leur aménager des profils spécifiques. Dans **Paramètres**, **Système**, **Options avancées**, **Utilisateurs Multiples**, effleurez **Ajouter un utilisateur**, **OK**. Pointez sur l'engrenage pour activer l'usage de la ligne téléphonique et l'envoi de SMS. Appuyez sur **Nouvel utilisateur**, **Configurer**. Touchez le bouton **Continuer** pour personnaliser la session.

3 CONFIGUREZ LE COMPTE

Entrez l'adresse mail associée au compte Google du nouvel utilisateur, puis son mot de passe. Confirmez avec **J'accepte**. Autorisez ensuite la localisation de l'appareil par les services de Google et validez avec **Accepter**. Il reste au bénéficiaire du profil à définir le mode de verrouillage de sa session et à installer ses applis favorites.

4 GÉREZ LES PROFILS UTILISATEURS

En tant que propriétaire, vous avez toute latitude pour ajouter et supprimer des comptes. Vous pouvez aussi révoquer l'accès à la ligne cellulaire en cas d'abus. Pour revenir à votre session administrateur, déployez le panneau des notifications, effleurez la silhouette au bas du volet puis l'avatar de votre profil et l'engrenage à droite du profil dont vous souhaitez vous défaire. Pointez sur les boutons **Supprimer**, **Supprimer**. Toutes les données de l'utilisateur sont effacées de l'appareil.



5 PASSEZ FACILEMENT D'UN ESPACE UTILISATEUR À L'AUTRE

Le principe des comptes multiples peut être mis à profit pour assurer la cohabitation d'un profil personnel et d'un environnement dédié au travail sur un même téléphone. Pour basculer de l'un à l'autre, ouvrez le panneau des notifications, touchez la silhouette au bas du volet puis le nom de la session. Il vous reste alors à vous identifier (code PIN, empreintes, etc.).

6 AUTORISEZ UN PROCHE À CONSULTER SES MAILS OU LES RÉSEAUX SOCIAUX

Si un ami souhaite accéder à son compte de messagerie ou à un réseau social depuis votre téléphone, utilisez Parallel Space - Multicompte (**bit.ly/30bxleJ**) pour définir une seconde instance de l'application Facebook, Gmail, WhatsApp ou Twitter. Pointez sur le bouton **Ajouter une App**, sélectionnez l'un des services installés sur le téléphone et validez avec **Ajouter**. Pointez de nouveau sur l'icône de l'appli et renseignez les identifiants de connexion du nouveau compte. L'emprunteur n'aura qu'à le supprimer une fois qu'il en aura terminé.

DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE SYSTÈME

ÉVITEZ LES LOGICIELS ESPIONS

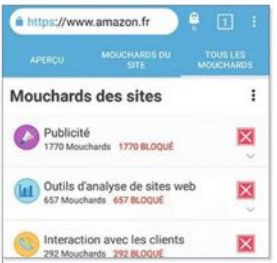
Vous n'avez pas idée du nombre de mouchards qui se cachent dans le code des pages Web et des applications que vous installez sur votre mobile ! Ghostery vous protège contre les services un peu trop curieux.

1 DÉNICHEZ LES FOUINEURS

L'appli Ghostery Privacy Browser (**bit.ly/2Yyf0Im**) fait à la fois office de navigateur Internet et d'appli anti-espion. Lors du premier démarrage, décochez la case de partage des données et appuyez sur le bouton **Naviguer**. Entrez l'URL d'un site dont la sécurité vous semble incertaine, puis effleurez l'icône en forme de fantôme dans le menu supérieur. Le nombre de logiciels espions détectés sur la page s'affiche.

2 DÉCOUVREZ QUI VOUS ESPIONNE

Si vous estimez que le site est sans danger, pointez sur le lien **Se fier à ce site** afin que Ghostery lève ses défenses lors de la prochaine connexion. Effleurez au contraire le bouton **Restreindre** pour activer le blocage. Vos choix sont mémorisés par le navigateur. Pour identifier les éléments interceptés par l'application, rendez-vous sur **Mouchards du site**, appuyez sur la flèche à droite, puis dans **Aperçu**, déployez le panneau **Options**. Assurez-vous alors que tous les modes de blocage sont actifs.



Ghostery fonde sa surveillance sur une base de données géante.

3 BLOQUEZ LES MOUCHARDS PAR CATÉGORIE

Les outils de protection de Ghostery s'appuient sur plusieurs listes de programmes espions régulièrement mises à jour. Vous pouvez consulter cet annuaire de menaces en pointant sur le fantôme dans le menu supérieur, puis sur **Tous les mouchards**. Les logiciels espions sont classés par catégories (publicité, outils d'analyse, etc.). Pour bloquer tous les éléments liés à une catégorie (les réseaux sociaux par exemple), cochez la case située à droite de son intitulé. Pour agir plus finement, déroulez le contenu d'une catégorie et indiquez les mouchards devant être bloqués.

4 PARAMÉTREZ GHOSTERY

Ouvrez le volet de menu de l'application. Pointez sur **Paramètres**, **Vie privée** et cochez **Bloquer les nouveaux mouchards**. Effleurez ensuite la liste **Cookies** et optez pour **Autorisés, sauf cookies tiers**. Activez l'option **Effacer mes traces à la fermeture** de façon à purger l'historique de navigation et à effacer les cookies et la mémoire cache. Définissez enfin un **mot de passe principal** pour barrer l'accès à Ghostery.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE SYSTÈME

DOTEZ VOTRE MOBILE D'UNE ALARME ANTIVOL

Voici comment faire retentir une sirène dès que l'on saisit le téléphone laissé sur le coin d'un bureau.

1 ACTIVEZ LES ALERTES

Installez Alarme antivol (**bit.ly/2NyGL2N**) et associez l'appli à votre compte Facebook ou Google. Cet outil permet de paramétrer le déclenchement d'une alerte sonore quand le chargeur est déconnecté ou lorsque le téléphone est déplacé. Activez ces différentes options de sécurité en explorant chacun des menus. Définissez un code PIN. Effleurez de nouveau le menu puis éteignez l'écran.

2 RÉGLEZ LES PARAMÈTRES DE DÉCLENCHEMENT DE L'ALARME

L'application dispose également d'un mode capable de vous alerter si l'appareil est retiré de votre poche. Dans tous les cas, et même après redémarrage, l'alarme continuera de sonner tant que le code de sécurité n'est pas renseigné. Effleurez l'engrenage dans le menu inférieur et allez sur **Tonalité d'alarme** et sélectionnez la sonnerie de votre choix. Pointez sur **Temps supplémentaire avant la détection** et optez pour la valeur **15 secondes**.

3 DÉFINISSEZ LE NIVEAU DE SENSIBILITÉ DU CAPTEUR

Si vous estimez que les alertes se déclenchent un peu trop facilement, dirigez-vous vers les paramètres de l'appli et pointez sur **Capteur**. Réglez la sensibilité sur **Milieu** ou **Faible**. Pour décourager un peu plus encore les voleurs, cochez les modes **Dispositif** et **Lumières** au bas du menu **Paramètres**. En plus de l'alarme sonore, les tentatives d'effraction donneront lieu à l'activation du vibreur et du flash du téléphone. Si les publicités affichées par l'appli vous dérangent, passez à la version Pro (moins de 1 €) qui offre en outre la possibilité de recevoir des notifications sur différentes adresses mail en cas d'urgence.

Activez Alarme Antivol dès que vous vous éloignez de votre mobile.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE CONFIDENTIALITÉ

N'EXPOSEZ PAS VOS INFOS PERSONNELLES

Android et iOS peuvent afficher des notifications sur l'écran de verrouillage de votre téléphone. Une attention louable, mais susceptible d'exposer certaines données confidentielles aux regards indiscrets.

1 FAITES LE TRI DANS LES NOTIFICATIONS D'IOS

Afin de modifier le contenu et l'apparence des notifications elles-mêmes, commencez par faire le tri dans les applications susceptibles d'émettre des alertes. C'est là le meilleur moyen d'éviter les déconvenues. Sur l'écran d'accueil de l'iPhone, effleurez **Réglages** puis **Notifications**. Passez en revue la liste des applis autorisées à prendre la parole et ne conservez que les communications essentielles (Mail, Messages, le cas échéant Facebook et Twitter).

2 RENONCEZ À L'APERÇU SUR L'ÉCRAN VERROUILLÉ

Un aperçu des notifications s'affiche sur l'écran de verrouillage. N'importe qui peut ainsi lire les premiers mots du message ou consulter la vignette d'une photo. Pour éviter cela, rendez-vous sur l'écran de configuration des notifications, touchez **Afficher les aperçus et** cochez l'option **Si déverrouillé**.

3 MODIFIEZ LE COMPORTEMENT DES NOTIFICATIONS SOUS ANDROID

Par défaut, toutes les notifications apparaissent sur l'écran de verrouillage d'Android, qu'il s'agisse de l'objet d'un mail ou de l'amorce d'un SMS. Un choix loin d'être idéal si vous privilégiez la sécurité et la confidentialité. Rendez-vous dans les paramètres du téléphone et pointez sur **Applis et notifications**, **Notifications**, **Sur l'écran de verrouillage**. Cochez le mode **Masquer les contenus sensibles** de façon à limiter les informations proposées au strict minimum. Si ces données vous semblent encore de trop, optez pour le mode le plus restrictif : **Ne pas afficher les notifications**.

Réservez l'affichage des notifications aux moments ou votre iPhone est déverrouillé.

4 RESTREIGNEZ LES NOTIFICATIONS

Pour aller plus loin dans la maîtrise des informations qui s'affichent dans le panneau des notifications et sur l'écran de verrouillage de votre smartphone, opérez un tri parmi les applications autorisées à émettre des alertes. Allez sur la page **Paramètres**, **Applis et notifications**, puis touchez les commandes **Notifications** et **Affichées Récemment** de manière à afficher la liste des applis qui ont généré des notifications au cours des derniers jours. Pointez sur le curseur à droite du nom d'un élément pour mettre fin aux alertes.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE MOBILE

MODÉREZ LA CURIOSITÉ DES APPLICATIONS

Certaines applis bénéficient d'un droit d'accès indu à vos données et aux ressources de votre téléphone.

1 ACCÉDEZ AUX RÉGLAGES D'IOS

Même sur l'App Store d'iOS, et malgré le cahier des charges rigoureux mis en place par Apple, un grand nombre d'applications (gratuites le plus souvent) exigent un droit accès à des informations inutiles à leur fonctionnement. Ces privilèges touchent à vos données (contacts, photos, etc.), mais aussi aux ressources de l'iPhone (caméra, micro, téléphone). Ces demandes sont accordées lorsque vous installez les applis.

2 PERSONNALISEZ LES AUTORISATIONS

Pour effectuer un tri, touchez l'icône des **Réglages** sur l'écran d'accueil, puis affichez la rubrique **Confidentialité**. Passez ensuite la liste en revue et révoquez les privilèges que vous jugez hors de propos (une appli lampe torche n'a pas besoin d'accéder au calendrier ou à l'appareil photo !) en effleurant le curseur situé en regard du nom de l'application.

3 GÉREZ LES AUTORISATIONS ANDROID

Ouvrez les paramètres du téléphone et rendez-vous à présent à la rubrique **Applis et notifications**. Faites défiler la page et touchez le lien **Autorisations des applis**. La liste des ressources du téléphone apparaît à l'écran. Pointez sur l'une des rubriques (**Localisation** par exemple) de façon à découvrir les éléments autorisés à accéder à ces informations.

4 RESTREIGNEZ LES AUTORISATIONS.

Touchez le curseur de l'appli dont les privilèges semblent sans fondements et validez avec **Refuser quand même**. Si l'appli refuse de fonctionner après cette opération, réactivez simplement l'autorisation. Pour afficher les accès accordés à une appli, sélectionnez-la sur la page **Paramètres**, **Applis et notifications**, **Afficher les XX applications** et pointez sur **Autorisations**.

Coupez l'accès aux images de la caméra ou aux fichiers enregistrés sur le mobile.

QUAND
VOUS REFERMEZ
UN 

UNE NOUVELLE VIE
S'OUVRE À LUI.

EN TRIANT VOS JOURNAUX,
MAGAZINES, CARNETS, ENVELOPPES,
PROSPECTUS ET TOUS VOS AUTRES
PAPIERS, VOUS AGISSEZ POUR UN MONDE
PLUS DURABLE. DONNONS ENSEMBLE
UNE NOUVELLE VIE À NOS PRODUITS.
CONSIGNESDETRI.FR

CITEO
Le nouveau nom d'Eco-Emballages et Ecofolio

DIFFICULTÉ MODÉRÉE TEMPS 25 MIN DOMAINE SYSTÈME

COMBLEZ LES FAILLES DE SÉCURITÉ

Les pirates ont souvent un temps d'avance sur les éditeurs de solutions de sécurité. Ne leur facilitez pas la tâche en laissant votre téléphone sans défense. Gardez Android, iOS et vos applis à jour.

1 AFFICHEZ LA VERSION D'ANDROID

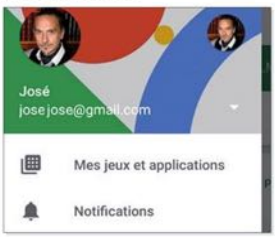
La fréquence des mises à jour d'Android dépend de votre modèle de téléphone. La disponibilité des correctifs vous est automatiquement notifiée. Il suffit alors d'accepter le téléchargement puis l'installation de la mise à jour. Si vous ne voyez rien venir, touchez l'icône des **Paramètres**, puis accédez à la rubrique **Système**. Déployez le volet **Options avancées** et pointez sur **Mise à jour du système**.

2 LANCEZ UNE RECHERCHE MANUELLE

Cette page permet d'identifier la version d'Android présente sur le téléphone et de connaître précisément la date du dernier correctif rapatrié. Pour être sûr qu'un fichier n'a pas échappé à la vigilance du service d'actualisation d'Android, effectuez une tape sur la commande **Rechercher les Mises à jour**. Le téléphone interroge alors les serveurs du fabricant. Si un nouveau correctif est identifié, lancez le téléchargement, puis procédez à son installation.

3 PERSONNALISEZ LES MISES À JOUR DES APPLIS

Les applications du Play Store constituent la principale source de propagation des virus sous Android. Il est donc capital d'adopter les correctifs proposés régulièrement par les éditeurs. Ouvrez le menu de la boutique d'Android et effleurez l'intitulé **Mes jeux et applications**.

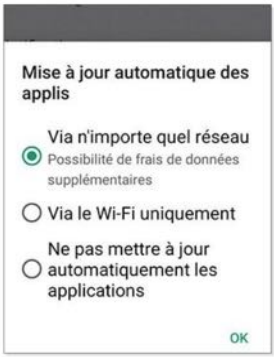


4 INSTALLEZ LES MISES À JOUR

Effleurez l'onglet **Mises à jour** pour afficher la liste des applications pour lesquelles des correctifs sont en attente. Si votre appareil est équipé d'une version récente d'Android, vous pouvez procéder à une installation massive en pointant sur la commande **Tout mettre à jour** au sommet de l'interface. Avec un téléphone ancien, mieux vaut préférer une intervention à la carte en choisissant les mises à jour dont vous êtes certain qu'elles sont compatibles avec votre version d'Android.

5 AUTOMATISEZ LES MISES À JOUR DES APPLIS ANDROID

Si vous ne souhaitez plus avoir à vous soucier de l'installation des correctifs ou des versions actualisées de vos applications, déployez le menu du Google Play Store et effleurez l'intitulé **Paramètres**. Activez la commande **Mise à jour automatique des applis** et optez pour le mode adapté à votre forfait 4G : **mises à jour en Wi-Fi uniquement, via n'importe quel réseau** ou **Ne pas mettre à jour automatiquement les applis**. Enregistrez les réglages d'une tape sur le bouton **OK**.



6 GARDEZ VOTRE IPHONE ET VOS APPLIS AU TOP DE LEUR FORME

Sous iOS, deux manipulations différentes doivent être effectuées pour automatiser la mise à jour des applications et du système. Touchez l'icône **Réglages** puis votre nom et enfin l'intitulé **iTunes Store et App Store**. Pour automatiser la mise à jour des applications, activez l'option **Mises à jour** dans la rubrique **Téléchargements automatiques**. Il faut ensuite faire en sorte de récupérer et d'installer automatiquement les dernières évolutions d'iOS, accédez à la rubrique **Général**, **Mise à jour logicielle** des **Réglages** et activez la commande **Mises à jour automatiques**.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE APPLIS

BLOQUEZ L'ACCÈS AUX APPLIS SENSIBLES

Si vous n'y prenez pas garde, quiconque ouvre Gmail sur votre téléphone peut lire vos mails, mais aussi consulter les informations de connexion de vos comptes de messagerie. La solution ? Imposer un verrou.

1 PARAMÉTREZ APPLOCK

Android n'offre pas la possibilité de conditionner le lancement des applis à la saisie d'un mot de passe. Pour bénéficier de cette fonctionnalité, il est indispensable de recourir à un utilitaire comme Serrure - AppLock (**bit.ly/2JRGB12**), disponible gratuitement sur le Google Play Store. Une fois l'appli opérationnelle, effleurez le bouton **Accepter**. La première étape consiste à dessiner un schéma de verrouillage sur l'écran du téléphone. Ce code secret sera exigé par la suite pour accéder à AppLock et aux applications protégées. Reliez les différents points et confirmez le schéma.

2 ASSOCIEZ VOTRE COMPTE GOOGLE

AppLock vous demande ensuite d'associer un compte Google à l'application. Si vous préférez utiliser une adresse autre que celles enregistrées sur le téléphone, cochez **Ajouter un compte** et indiquez vos identifiants. Validez avec **OK**.

3 SÉLECTIONNEZ LES APPLIS QUE VOUS SOUHAITEZ PROTÉGER

Activez à présent l'onglet **Vie Privée**. Faites défiler la page pour parcourir la liste des applications installées sur le téléphone. La rubrique **Avancé** regroupe les outils système : **Paramètres**, **Google Play store**, etc. La section **Bouton de verrouillage** permet de verrouiller l'activation et la mise en veille du Bluetooth et du Wifi. Les autres applis, installées par le fabricant de votre téléphone ou téléchargées sur le Play Store, figurent sous l'intitulé **Général**. Pointez sur le nom d'une application pour activer le verrouillage (un cadenas de couleur verte confirme la mise en place de la protection). Quittez AppLock et tentez de lancer l'appli en question. L'opération est bloquée et suspendue au tracé du schéma de verrouillage.

AppLock bloque l'accès aux applications que vous jugez sensibles.

4 PERSONNALISEZ LE MODE INVITÉ

Utilisez la barre d'outils au bas de l'écran pour activer les différents modes de verrouillage. Touchez la première icône (**Profils**) puis les points à droite de l'intitulé **Invité**. Pointez sur la commande **Modifier** et cochez les applications à protéger quand un proche emprunte votre téléphone. Validez par **Enregistrer**. Déroulez de nouveau le menu du mode **Invité** et choisissez **Raccourci**, Ajouter **automatiquement** pour créer un lien d'activation rapide sur l'écran d'accueil du téléphone.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE CONTRÔLE PARENTAL

SURVEILLEZ L'ACTIVITÉ DE VOTRE ENFANT

Tous les contenus sur Internet ne sont pas adaptés au jeune public. Gardez le contrôle avec Family Link.

1 COMMENCEZ PAR INSTALLER FAMILY LINK SUR VOTRE SMARTPHONE

Installez l'appli de contrôle parental et associez-la à votre compte Google. Répondez aux questions de l'assistant de configuration après avoir indiqué que vous étiez un parent. Si votre enfant dispose de son propre compte Google, touchez le bouton **Oui** et indiquez son adresse mail. Sinon, l'appli vous amène vers la page dédié à la création de compte.

2 ASSOCIEZ LES DEUX MOBILES

Vous devez ensuite associer votre mobile et l'appareil de votre enfant. Assurez-vous que les deux téléphones se trouvent à proximité l'un de l'autre puis installez l'application Google Family Link pour les enfants et les adolescents sur le smartphone à surveiller. Une fois l'opération achevée, désignez le compte Google de l'enfant et lancez l'appairage. Validez en saisissant le code de sécurité qui s'affiche à l'écran de votre mobile, puis en confirmant la supervision de l'appareil.

3 PILOTEZ LES ACTIVITÉS À DISTANCE

Grâce à Family Link, vous pouvez surveiller ce que votre progéniture fait sur son smartphone et le protéger des risques auxquels il s'expose, le plus souvent sans même le savoir. Pour cela, vous pouvez gérer les autorisations d'achat et de téléchargement sur le Play Store, par exemple. Il est également possible d'appliquer des restrictions d'accès à certains contenus depuis le navigateur Google Chrome, de filtrer les résultats des recherches de Google ou d'activer la localisation. Vous pouvez enfin définir les horaires d'utilisation. Pensez toutefois à adapter la configuration de Family Link et les filtres de contenus à mesure que l'enfant grandit.

À vous de choisir les horaires auxquels votre enfant peut utiliser son mobile.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE VERROUILLAGE

PROTÉGEZ L'ACCÈS À VOTRE IPHONE

Exploitez les différents modes de protection intégrés à iOS pour éviter que vos données soient exposées aux regards indiscrets quand vous abandonnez votre téléphone sur un coin de table.

1 DÉFINISSEZ UN CODE PIN RENFORCÉ

Si vous utilisez encore un code de verrouillage numérique à quatre chiffres (le format original des codes PIN), modifiez-le sans tarder et optez pour une combinaison plus complexe composée de six chiffres. Touchez l'icône **Réglages** sur l'écran d'accueil, puis **Touch ID et code** et **Changer le code**. Saisissez et confirmez le nouveau verrou.

2 ACTIVEZ LA RECONNAISSANCE D'EMPREINTES

L'activation d'un code numérique à quatre ou six chiffres constitue un préalable à l'utilisation des dispositifs biométriques proposés sur l'iPhone. Apparue avec l'iPhone 5S, la reconnaissance d'empreintes Touch ID permet ainsi de déverrouiller rapidement l'écran mais aussi de valider des paiements ou le téléchargement d'applications. Effleurez l'icône **Réglages** et activez **Touch ID et code**. Dans la section **Utiliser Touch ID pour**, activez les curseurs **Déverrouiller l'iPhone**, **Apple Pay** et **iTunes Store et App Store**.

Créez un code PIN avant de configurer la reconnaissance faciale ou d'empreintes.

3 ENREGISTREZ L'EMPREINTE D'UN OU PLUSIEURS DE VOS DOIGTS

Pour faire face à toutes les situations et vous identifier à coup sûr, mieux vaut enregistrer les caractéristiques de plusieurs doigts. Les deux pouces constituent un minimum. Pour ajouter une empreinte, suivez les indications de l'assistant. Posez le doigt sur le capteur et retirez-le quand vous ressentez une vibration. Répétez l'opération autant de fois que nécessaire. Un message apparaît à l'écran quand iOS a terminé de modéliser l'empreinte.

4 CONFIGUREZ FACE ID

Le dispositif de reconnaissance du visage Face ID a remplacé le capteur d'empreinte sur les modèles de la famille iPhone X. Pour profiter de cette fonctionnalité, accédez aux réglages de l'appareil, puis pointez sur **Face ID et code**. Saisissez le code d'accès à six chiffres, effleurez la commande **Configurer Face ID** puis le bouton **Démarrer**. Regardez droit vers la caméra frontale de l'iPhone et positionnez votre visage dans le cadre. Bougez doucement la tête pour compléter le cercle et suivez les consignes pour finaliser la reconnaissance.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE VERROUILLAGE

PRÉPAREZ L'IPHONE AVANT DE LE PRÊTER

Si vous confiez votre téléphone à un proche, assurez-vous qu'il ne peut pas accéder à certaines données.

1 ACTIVEZ LES RESTRICTIONS

Depuis le déploiement d'iOS 12, l'année passée, la mise en place de restriction sur un iPhone a sensiblement évolué. Touchez l'icône **Réglages** sur l'écran d'accueil du téléphone puis l'intitulé **Temps d'écran** dans la section **Général**. Rendez-vous ensuite au bas de la page. Pointez sur la commande **Restrictions relatives au contenu et à la confidentialité** et activez le curseur **Restr. Cont.& conf.**

2 APPLIQUEZ DES FILTRES POUR INTERDIRE L'ACCÈS À VOS CONTENUS

Pour éviter les déconvenues, accédez à la rubrique **Achats dans iTunes et l'App Store** et interdisez l'ajout et la suppression d'applications. Exigez par ailleurs la saisie systématique de votre mot de passe Apple ID avant tout téléchargements. Accédez ensuite à la rubrique **Restriction de contenus** et appliquez les filtres qui vous semblent appropriés en fonction de la personne à qui vous vous apprêtez à confier votre téléphone (votre conjoint, un enfant ou un ami). Vous pouvez ainsi préserver vos données les plus confidentielles.

3 VERROUILLEZ LES APPLICATIONS

Affichez maintenant le contenu de la rubrique **Apps autorisées**. Là, actionnez les curseurs des applications de façon à indiquer si elles pourront être utilisées sans restriction ou au contraire, si la saisie du code de verrouillage de l'iPhone est exigée. Lorsque le curseur est de couleur verte, l'accès à l'application est autorisé ; quand il est grisé, iOS en bloque l'exécution en attendant que vous vous authentifiiez. Ce dispositif est tout indiqué dans le cas où vous êtes amené à prêter régulièrement votre mobile, les applis sensibles - et leurs données - étant ainsi protégées.

Le menu Temps d'écran permet de restreindre l'accès aux applications.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE VIRUS

TRAITEZ UN IPHONE INFECTÉ

Les virus profitent des opérations les plus anodines pour s'installer : affichage d'une page Web, téléchargement d'un fichier d'une application. Voici comment procéder si votre téléphone est victime d'une attaque.

1 ENTAMEZ LA RÉINITIALISATION
Commencez par solliciter les services d'une application antivirus pour tenter de résoudre la situation. Si le problème persiste, la solution consiste à restaurer les réglages d'usine de l'iPhone. L'opération peut être réalisée par le biais du panneau **Réglages** à condition que vous ayez toujours le contrôle du mobile. Affichez le contenu de la section **Général** et touchez la commande **Réinitialiser** au bas de l'écran. Choisissez le mode **Effacement des données et des paramètres**.

2 SAUVEGARDEZ LES DONNÉES
Si vous avez activé la commande **Effacer**, une alerte s'affiche. Elle vous demande de confirmer votre choix (qui peut s'avérer sans retour) et vous suggère de sauvegarder les données via votre compte iCloud. Nous vous recommandons de suivre ce conseil pour éviter de perdre des fichiers précieux. Une fois la sauvegarde achevée, le processus de réinitialisation reprend son cours automatiquement, sans que vous ayez à intervenir. Après quelques minutes, vous retrouverez un iPhone pleinement fonctionnel et débarrassé du virus.

Sauvegardez vos fichiers pour les restaurer après la réinitialisation.

3 RÉINITIALISEZ UN IPHONE BLOQUÉ
Si vous avez été victime d'une attaque sérieuse, il se peut que l'iPhone refuse de redémarrer. Il existe toutefois une procédure de secours. Pour forcer la remise à zéro de votre smartphone, gardez les boutons **Veille** et **Accueil** enfoncés pendant une dizaine de secondes. Relâchez la pression quand le logo Apple (la fameuse pomme) apparaît à l'écran.

4 RESTAUREZ VOS DONNÉES ET APPLIS
La procédure de réinitialisation consiste à restaurer la configuration d'usine de l'iPhone. L'appareil se trouve alors tel que vous l'aviez trouvé à la sortie de sa boîte, à un détail près : il conserve le bénéfice de la dernière version d'iOS que vous y aviez installée. Pour revenir à un environnement familier, associez le téléphone à votre compte Apple ID et activez les options de synchronisation. Si vous possédez une sauvegarde, restaurez-la depuis iTunes après avoir branché l'iPhone à votre Mac.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE SÉCURITÉ

LOCALISEZ ET BLOQUEZ UN IPHONE ÉGARÉ

Impossible de mettre la main sur votre mobile ? Qu'il soit volé ou perdu, n'attendez pas pour agir.

1 AUTORISEZ LA LOCALISATION
Pensez à active la fonctionnalité **Localiser mon iPhone**. Touchez pour cela l'icône Réglages, puis en haut de la page, touchez votre nom pour afficher les propriétés d'iCloud. Faites défiler l'écran vers le bas et pointez sur **Localiser mon iPhone**. Actionnez ensuite les curseurs **Localiser mon iPhone** et **Envoyer la dernière position**. Saisissez vos identifiants Apple ID pour valider l'opération.

2 ACTIVEZ LE MODE PERDU
Le jour où vous ne parvenez pas à remettre la main sur votre iPhone, accédez au smartphone d'un ami ou à votre ordinateur. Lancez un navigateur Internet et connectez-vous sur votre compte iCloud (**https://www.icloud.com/#find**). Après vous être identifié, la page Web affiche la dernière position connue de votre smartphone. Si l'appareil n'est pas à proximité immédiate, ou que vous soupçonnez un vol, activez le mode **Perdu**.

3 INTERAGISSEZ À DISTANCE
Cette fonctionnalité permet de verrouiller l'appareil à distance à l'aide d'un code d'accès, d'afficher un message personnalisé sur l'écran de verrouillage afin de communiquer un numéro de téléphone où vous joindre à la personne qui trouverait le mobile. Vous avez également la possibilité de suivre à la trace les déplacements du voleur. Si le vol est avéré, ne prenez aucun risque. Pour éviter que les données personnelles enregistrées sur le téléphone tombent entre de mauvaises mains, pointez sur le bouton **Effacer iPhone** pour forcer la réinitialisation à distance. Signalez la perte ou le vol de votre smartphone à votre opérateur de façon à bloquer les appels et à recevoir une nouvelle carte SIM.

Utilisez le mode Perdu pour verrouiller ou effacer les données de l'iPhone.

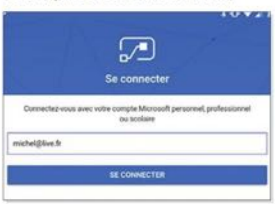
DIFFICULTÉ ÉLEVÉE TEMPS 30 MIN DOMAINE DONNÉES

SURVEILLEZ VOS DOSSIERS CLOUD

Photos, documents, formulaires, il n'a jamais été aussi facile de partager des fichiers. Sollicitez l'application Flow de Microsoft pour être notifié dès qu'un collaborateur apporte des modifications à l'un de ces dossiers.

1 INSTALLEZ MICROSOFT FLOW SUR VOTRE TÉLÉPHONE

Cette application compte parmi les nombreux outils gratuits développés pour Android par Microsoft. Accédez au Play Store et recherchez Flow. Procédez à son installation et touchez le bouton **Ouvrir**. Connectez l'appli au compte Microsoft associé à votre abonnement Office 365 ou à votre espace OneDrive. Une fois cette formalité accomplie, pointez sur la commande **Flux** dans la barre d'outils située au bas de l'écran, puis sur **Créer entièrement**.

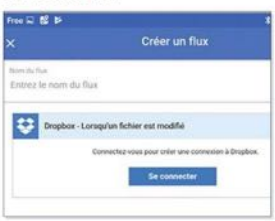


2 ÉLABOREZ UN NOUVEAU SCÉNARIO

Vous êtes ensuite invité à choisir le connecteur, c'est-à-dire le service concerné par le processus d'automatisation. Parcourez la liste et appuyez par exemple sur l'icône **Dropbox**. Indiquez ensuite l'action qui déclenchera l'émission du message d'alerte. Il s'agit ici d'être prévenu dès qu'un changement est apporté au contenu du dossier partagé. Activez le déclencheur **Dropbox**, **Lorsqu'un fichier est modifié**.

3 ASSOCIEZ VOTRE COMPTE DROPBOX ET L'APPLICATION FLOW

Avant de désigner l'emplacement à surveiller, connectez Flow à votre espace Dropbox personnel. Quand l'application vous y invite, touchez le bouton **Se connecter**. Saisissez vos identifiants Cloud (adresse mail et mot de passe) et autorisez Flow à accéder aux données de Dropbox. Si vous avez activé l'authentification à deux facteurs, entrez le code reçu par SMS avant de valider à l'aide de la commande **Autoriser**.



4 PRÉCISEZ LE DOSSIER À SURVEILLER

Touchez maintenant la section **Identificateur unique du dossier**. Parcourez l'arborescence de votre espace Dropbox et désignez le dossier partagé. Confirmez ce choix en effleurant le bouton **Terminé**. Le scénario ne peut englober qu'un seul dossier. Si vous souhaitez surveiller un autre emplacement, il vous faudra créer un nouveau flux en suivant cette même procédure.

5 ASSIGNEZ UNE ACTION À FLOW

Vous devez indiquer à présent à l'application l'action à déclencher quand une modification intervient dans le dossier partagé. Touchez pour cela la commande **Nouvelle étape** disposée au bas de l'écran, puis l'icône **Ajouter une action** de la barre d'outils qui apparaît en surimpression. Notez qu'il est également possible d'ajouter une seconde condition à l'exécution du script.

6 RECEVEZ UNE NOTIFICATION

Flow affiche ensuite une liste de connecteurs compatibles avec Dropbox et la surveillance des dossiers. Touchez le bouton **Notifications** et choisissez l'une des deux options disponibles : **Recevoir une alerte dans le volet de notification du téléphone** ou **Être informé par mail**. Saisissez le texte de la notification (« Attention un fichier a été modifié », par exemple) ou dans le cas d'un courriel, le texte du message et votre adresse mail. Nommez le flux et sauvegardez-le avec **Créer**.

DIFFICULTÉ AUCUNE TEMPS 15 MIN DOMAINE SYSTÈME

VERROUILLEZ L'ACCÈS À UN MOBILE ANDROID

Il est vivement déconseillé de laisser votre téléphone en libre accès. N'importe qui pourrait alors accéder à ses données. Android vous propose de très nombreux outils pour verrouiller votre mobile.

1 ACTIVEZ LE CODE PIN

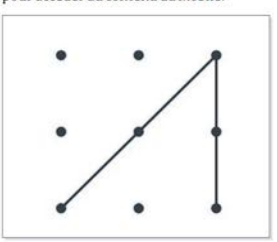
L'ajout d'un code numérique demeure la manière la plus simple et la plus rapide pour éviter qu'on vienne fouiller dans votre téléphone. Effleurez la roue crantée des paramètres et accédez à la section **Sécurité et localisation**, **Verrouillage de l'écran**, **Code PIN**. Définissez une combinaison constituée de six ou huit chiffres, puis pointez sur l'engrenage à droite de **Verrouillage écran** et activez le blocage instantané avec **Marche/Arrêt**.

2 AJOUTEZ UN MOT DE PASSE

Si vous avez peur que vos proches devinent trop aisément votre code PIN, préférez-lui un mot de passe associant lettres et chiffres ou une phrase du type **demainilferabeau**. Dirigez-vous vers **Verrouillage de l'écran**, tapez le code PIN puis pointez sur **Mot de passe**. Saisissez et confirmez la combinaison secrète (qui peut compter jusqu'à 17 caractères), en évitant d'utiliser les prénoms et les dates de naissance de vos enfants, par trop prévisibles.

3 ADOPTEZ UN SCHÉMA

Pour celles et ceux qui ne veulent pas s'ennuyer à taper un code ou un mot de passe sur le clavier virtuel de leur téléphone, Android propose de définir un schéma de déverrouillage à dessiner sur l'écran tactile. Pointez sur **Verrouillage de l'écran**, **Schéma** et définissez un tracé en reliant les points affichés à l'écran. Confirmez le dessin avec **Suivant**. Ce schéma sera exigé pour accéder au contenu du mobile.



4 PASSEZ À LA PROTECTION BIOMÉTRIQUE

La plupart des téléphones Android embarquent un capteur d'empreintes ou un dispositif de reconnaissance de visage (attention, ce dernier est souvent assez facile à tromper). Enregistrez les caractéristiques d'un premier doigt dans la section **Sécurité et localisation**, **Empreinte** en suivant les instructions de l'assistant. N'hésitez pas à mémoriser plusieurs doigts ou les empreintes de votre conjoint s'il a l'habitude d'emprunter le téléphone.

5 EXIGEZ UN CODE D'IDENTIFICATION À CHAQUE DÉMARRAGE

Cette option ajoute un niveau de sécurité. Après avoir défini un code d'accès (PIN, schéma, etc.), Android vous demande si vous souhaitez activer le démarrage sécurisé. Touchez **Oui**, **OK**. À la mise sous tension du téléphone, vous serez invité à renseigner le code PIN de la carte SIM, puis le code secret que vous avez défini.

6 DÉVERROUILLEZ L'APPAREIL AUTOMATIQUEMENT

Le menu **Smart Lock** de la section **Sécurité de l'appareil** renferme des options de verrouillage intelligent. Le blocage peut ainsi être suspendu automatiquement quand vous portez le mobile sur vous, quand vous vous trouvez dans un endroit particulier (**Lieux vérifiés**) ou encore à portée d'un périphérique Bluetooth appairé avec votre smartphone (**Appareils vérifiés**).

orange SFR bouygues free **DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE BOX**

PROTÉGEZ L'ACCÈS AU RÉSEAU WIFI DE VOTRE BOX INTERNET

Le boîtier mis à disposition par votre FAI cumule les talents. Décodeur TV et téléphone fixe, il fait aussi office de modem et de routeur, gérant les accès à Internet tout en assurant la communication entre les appareils connectés du foyer. Il constitue la première ligne de défense contre les cybermenaces.

Avec près de 12 millions de nouvelles variantes de malwares tous les mois, un nouveau malware est téléchargé toutes les quatre secondes selon le rapport Check Point Security. Les serveurs de la Nasa et des grandes multinationales ne sont pas moins exposés que vous ne l'êtes vous-même ! Vous pouvez installer sur votre ordinateur tous les antivirus, tous les antispywares disponibles sur le marché, ils peineront à vous protéger efficacement si, en amont, vous ne prenez pas soin de sécuriser votre box Internet.

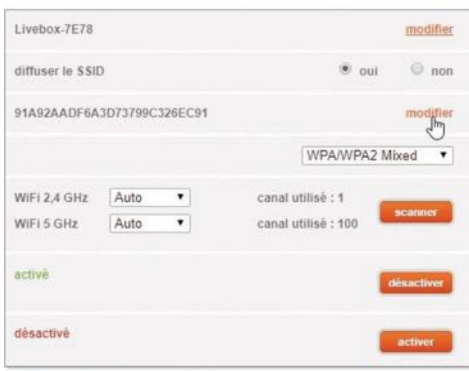
Cet accessoire devenu tellement familier forme une passerelle entre le Web et les appareils connectés. Les virus et les logiciels espions doivent franchir cette porte avant de contaminer ordinateurs, smartphones, mais aussi les disques durs réseau et les périphériques connectés (montres, balances, etc.). Les box Internet sont architecturées autour d'un modem-routeur auquel incombe la gestion du tra c Internet et des échanges entre vos appareils. Inspirées par les dispositifs réseau utilisés en entreprise, les box de Free, SFR, Orange et Bouygues Telecom intègrent des options de sécurité avancées qui s'administrent simplement à partir d'une interface Web, qui peine parfois à masquer le caractère pointu des outils disponibles !●

Boîte à outils

Pour ce pas à pas, nous avons utilisé

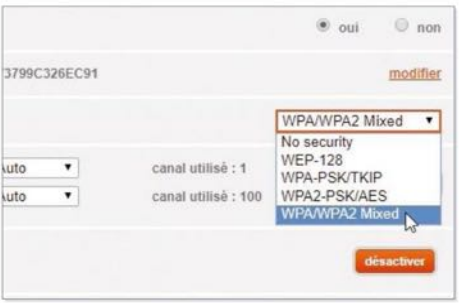
Un abonnement ADSL ou Fibre

Un PC ou un Mac



1 MODIFIEZ LA CLÉ WIFI DE LA BOX

Quel que soit l'opérateur à qui vous avez accordé votre confiance, vous avez reçu une box Internet préconfigurée et dotée d'un mot de passe prédéfini. Ce code secret est affiché au dos du boîtier. Il est très long, de façon à garantir la sécurité, ce qui le rend aussi difficile à mémoriser. Vous pouvez bien sûr le changer pour un mot de passe personnel que vous n'aurez aucun mal à retenir. Accédez à l'interface de configuration de la box (dans le cas d'une Livebox en saisissant **192.168.1.1** dans la barre d'adresse du navigateur). Pointez sur **Mon Wifi**, **Wifi Avancé** puis sur le bouton **Modifier** près de l'intitulé **Clé de sécurité**. Tapez le mot de passe dans le champ **Veuillez saisir la nouvelle clé de sécurité** et validez par **Enregistrer**.



2 PERSONNALISEZ LE MODE DE CHIFFREMENT

Le cryptage est un outil essentiel de la sécurisation des échanges sur les réseaux Wifi. Ce dispositif empêche les personnes indésirables d'espionner les informations qui transitent entre vos appareils et entre ceux-ci et Internet. Le choix du protocole de chiffrement influe sur le niveau de protection, mais aussi sur le débit, surtout si vous disposez d'une bande passante limitée. Si vous constatez une chute des débits après avoir changé de mode de chiffrement, revenez à la configuration initiale. Pour passer au cryptage WPA2, affichez les paramètres avancés de la connexion Wifi. Déroulez le menu **Chiffrement** dans la section **Mode de Sécurité** et optez pour le protocole le plus robuste : **WPA/WPA2 Mixed**.

3 ACTIVEZ LE PARE-FEU...

Ce n'est pas parce que Windows est pourvu d'un pare-feu, que le dispositif de filtrage de votre box Internet devient inutile. L'action de ces outils se combine pour une meilleure sécurité. Les filtres appliqués par les box Internet s'avèrent souvent plus sensibles et réactifs que le pare-feu logiciel de votre système d'exploitation. Accédez aux paramètres de configuration de votre box (ici la Livebox 4). Activez l'onglet **Configuration avancée**, puis dans le volet de navigation, pointez sur **Configuration pare-feu**. Vous pouvez alors ajuster le niveau de sécurisation (de faible à élevé). Il est bien sûr possible de revenir sur ce choix à tout moment si le filtrage entrave certains de vos logiciels ou de vos usages.

4 ... PUIS AJUSTEZ SES RÈGLES

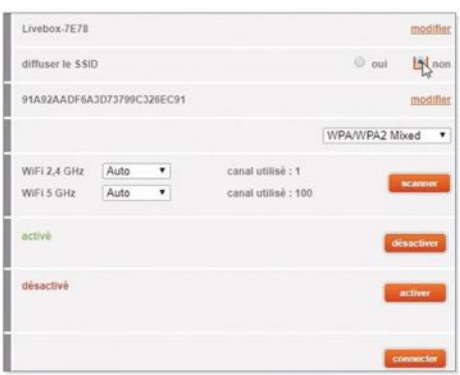
Les FAI ont tendance à masquer certains réglages avancés de façon à protéger leurs abonnés contre les manipulations hasardeuses. C'est le cas d'Orange. Si vous êtes à l'aise avec les problématiques réseau, cochez la case **Expert** pour débloquer l'accès aux modes et aux règles de filtrages des flux entrants et sortants de la Livebox. Cochez **Personnaliser** et pointez sur **Enregistrer**. Une nouvelle commande **Personnaliser** s'affiche. Cliquez sur le bouton orange pour basculer vers l'interface de configuration. Indiquez les ports que vous souhaitez ouvrir ou fermer et pour quels usages. Si vous souhaitez proscrire le téléchargement FTP, pointez sur cet intitulé et cliquez sur **Supprimer**. Les ports 20 et 21 sont alors fermés.

5 LIMITEZ LA FONCTION WPS

Le protocole WPS a été conçu pour faciliter l'association des périphériques au réseau Wifi de votre box. Une simplicité qui se paye sur le plan de la sécurité, votre réseau étant vulnérable durant les quelques secondes entre l'activation du WPS et l'appairage d'un nouvel appareil. Pour limiter l'usage du WPS, allez sur l'interface de configuration de la Livebox et cliquez sur l'onglet **Ma configuration Wifi et Livebox**. Dans la rubrique **Association WPS**, cochez l'option **Désactivée** dans le champ **Association WPS par écran**. Validez en pointant sur le bouton **Sauvegarder** au bas de la fenêtre. Si le réseau Wifi 5 GHz est différencié, vous devez également désactiver le bouton WPS pour ce réseau.

6 SURVEILLEZ ET PILOTEZ L'ACTIVITÉ SUR VOTRE RÉSEAU WIFI

La page d'accueil de l'interface de gestion de la Livebox offre d'une vue d'ensemble des équipements connectés à cet instant précis au réseau familial, qu'il s'agisse des appareils utilisant le Wifi ou de ceux branchés aux ports USB ou Ethernet de la box. Pour vous assurer que des équipements ne profitent pas de la connexion à votre insu, cliquez sur la rubrique **Équipements non connectés** dans le volet de navigation. Parcourez la liste des périphériques raccordés au réseau. Si vous détectez une anomalie, en d'autres termes une connexion qui n'a pas lieu d'être, changez immédiatement la clé de chiffrement ou activez le filtrage MAC (lire page suivante).



7 CACHEZ VOTRE RÉSEAU SANS FIL

Votre Box est reconnaissable par son nom. Cet intitulé peut être personnalisé ou même masqué afin de rendre le réseau familial invisible par les utilisateurs situés à proximité. Il sera ainsi moins exposé aux intrusions extérieures. Sur l'interface de gestion de la Livebox, pointez sur **Mon Wifi**, **Wifi avancé**. Dans **Connecter vos appareils en Wifi**, sous l'intitulé **Nom du réseau Wifi (SSID)**, décochez l'option **Diffuser le SSID**. Seuls les appareils déjà connectés continueront de le voir dans la liste des réseaux disponibles.

8 AFFICHEZ L'INTERFACE DE CONFIGURATION DE LA BBOX

Lancez votre navigateur Internet et saisissez **http://gestionbbox.lan** ou **192.168.1.254** dans la barre d'adresse pour accéder à la console d'administration de la box de Bouygues. Dans la section **Wifi**, cliquez sur **Réseau Wifi**, **Paramètres avancés** pour afficher la page des réglages du point d'accès sans fil et personnaliser le nom du réseau (SSID), le mot de passe et le mode de chiffrement.

9 PEAUFINEZ LA SÉCURITÉ DE LA FREEBOX

Les réglages de la Freebox Révolution s'effectuent depuis Freebox OS, une console d'administration Web accessible via votre navigateur Internet en saisissant l'URL **http://mafreebox.freebox.fr**. Identifiez-vous puis double-cliquez sur **Paramètres Freebox**. Allez dans **Mode avancé** pour trouver les options de sécurité. Pointez sur **Wifi** dans la section réseau local et placez-vous sur l'onglet **Configuration réseau**. Repérez la section correspondant aux protocoles de chiffrement et sélectionnez le mode WPA2-PSK/AES.

orange DIFFICULTÉ ÉLEVÉE TEMPS 20 MIN DOMAINE CONTRÔLE D'ACCÈS

ÉVITEZ LES CONNEXIONS PIRATES

Vous voulez avoir la garantie que personne ne se connectera à votre réseau Wifi sans votre autorisation ? Activez le filtrage par adresse MAC pour réserver l'accès à vos seuls appareils.

1 RÉCUPÉREZ LES ADRESSES MAC DE VOS PÉRIPHÉRIQUES

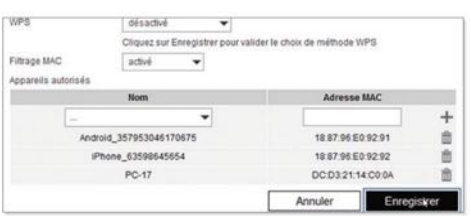
Chaque appareil susceptible de se connecter à Internet dispose d'un identifiant unique que l'on appelle adresse MAC. Cette référence est inscrite sur une étiquette au dos des imprimantes ou des disques durs réseau. Dans le cas d'un smartphone ou d'une tablette Android, l'information se trouve dans la section **À propos du téléphone**, **État**, **Adresse Mac Wi-Fi** des paramètres. Sur un PC équipé de Windows, saisissez **cmd.exe** dans le champ de recherche et validez par **Entrée**. Exécutez la commande **ipconfig /all** et notez l'adresse MAC de la carte réseau. Répétez cette opération pour chacun des ordinateurs.

2 CONFIGUREZ LE FILTRAGE DES APPAREILS

Il faut ensuite dresser la liste des matériels autorisés à se connecter. L'opération se déroule dans la console d'administration de la box, dans la section dédiée au filtrage MAC du volet **Sécurité**. Pour éviter tout problème, il est recommandé de réaliser ce réglage sur un ordinateur connecté à la box en Ethernet. Si vous appliquez le filtrage Mac avant d'avoir configuré le PC, vous ne pourrez plus accéder au réseau en Wifi. Lancez votre navigateur Internet, connectez-vous à l'interface de gestion de la Livebox et cliquez sur le menu **Wifi**. Dans la rubrique **Filtrage MAC**, sélectionnez **Activé**.

3 DONNEZ LES DROITS D'ACCÈS

Dans la colonne **Nom**, sélectionnez le type d'équipement que vous souhaitez ajouter à la liste des appareils que vous souhaitez appairer avec le réseau sans fil de la Livebox. Vérifiez que l'adresse MAC de l'équipement sélectionné apparaît et cliquez sur le bouton **+**. Répétez cette opération pour chacun des ordinateurs et des objets connectés utilisés au sein de votre foyer. Soyez vigilant, la moindre erreur de saisie dans les adresses MAC empêcherait la connexion. Sur une Livebox4, répétez l'opération pour les réseaux Wifi- 2,5 GHz et 5 GHz si vous avez activé les deux bandes de fréquence.



4 RÉVOQUEZ LES AUTORISATIONS ACCORDÉES PAR LE PASSÉ

Si vous changez de smartphone, de tablette ou d'ordinateur, ou que vous vendez un appareil, pensez à révoquer son autorisation d'accès au Wifi. Vous conserverez ainsi un contrôle total de la liste des périphériques autorisés et éviterez l'accumulation d'équipements connectés inutilement. Allez sur l'interface de gestion de la box Internet. Accédez à la liste des appareils autorisés dans la section **Filtrage MAC** et pointez sur le bouton **Supprimer** ou sur l'icône symbolisant une corbeille placée en face du nom de l'équipement concerné. Mémorisez la modification en cliquant sur le bouton **Enregistrer**.

orange

DIFFICULTÉ MODÉRÉE TEMPS 10 MIN DOMAINE CONTRÔLE D'ACCÈS

ENCADREZ LES USAGES DE VOS ENFANTS

Centre névralgique des activités numériques de la famille, les box Internet embarquent un outil de contrôle parental destiné à filtrer les contenus accessibles aux bambins et à éviter qu'ils ne passent trop de temps sur le Web. Pour mettre ce service en œuvre sur la Livebox 4 d'Orange, suivez le guide !

1 DÉSIGNEZ LES PÉRIPHÉRIQUES À SURVEILLER

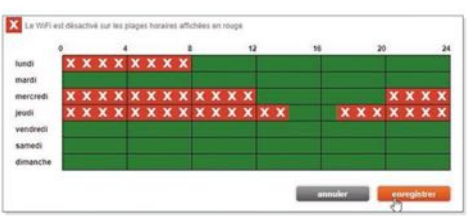
Pour profiter du contrôle parental de la box Internet d'Orange, il vous faut d'abord indiquer les équipements concernés par le filtrage. Cela évitera de couper l'accès au Web sur l'ordinateur ou la tablette de votre conjoint ! Connectez-vous à l'interface de gestion de la Livebox et authentifiez-vous à l'aide des identifiants administrateur (le mot de passe par défaut est constitué des huit premiers caractères de la clé Wifi). Accédez à la rubrique **Mes équipements connectés**. Parcourez la liste des appareils raccordés à la box en Wifi, en Ethernet ou en USB et cliquez sur l'intitulé de l'ordinateur ou du smartphone pour lequel vous souhaitez mettre en place le contrôle parental.

2 AFFICHEZ LE PLANIFICATEUR WIFI

Il faut ensuite définir les garde-fous qui éviteront à votre enfant d'accéder à des contenus inadaptés à son âge ou de développer une addiction au Web. Pour qu'il ne passe pas ses nuits et ses week-ends à naviguer et à visionner des films, faites appel au planificateur de la Livebox et imposez des plages d'utilisation. En dehors de ces horaires, la connexion Wifi de l'appareil sera automatiquement coupée. Dans la section **Paramétrer son accès à Internet**, cochez l'option **Planifier**. Plusieurs profils prédéfinis sont proposés : **Éco**, **Semaine**, **Vacances**, etc. Pour ajuster le contrôle parental à vos exigences, activez l'onglet **Personnalisé**.

3 DÉFINISSEZ LES PLAGES HORAIRES

Il vous reste à définir les plages horaires durant lesquelles la navigation sur Internet sera autorisée. Cochez la case **Non** à droite de l'intitulé **Activer le Wifi en permanence**. Reportez-vous à la grille hebdomadaire et cliquez sur les créneaux horaires que vous souhaitez proscrire. Une croix blanche sur fond rouge apparaît, confirmant le blocage du Wifi. Validez les réglages en pointant sur le bouton **Enregistrer**. Répétez l'opération pour chacun des appareils (ordinateurs, tablettes ou smartphones) utilisés par vos enfants pour accéder à Internet via la Livebox.



4 GÉREZ LE CONTRÔLE PARENTAL À DISTANCE

Il n'est pas nécessaire de se trouver devant un ordinateur, ni même chez soi, pour suivre les activités Internet de ses enfants. Il est en effet possible de gérer les équipements connectés à la box familiale à partir de l'application mobile Ma Livebox pour iOS et Android. Cet outil offre aussi l'opportunité de modifier les conditions du filtrage, et notamment de planifier les horaires d'utilisation, sans avoir à en passer par l'interface d'administration de la Livebox 4. Effleurez l'icône en forme d'horloge à droite du nom de l'appareil pour accéder aux options de contrôle parental.

DIFFICULTÉ MODÉRÉE TEMPS 10 MIN DOMAINE CONTRÔLE D'ACCÈS

COUPEZ LE WIFI QUAND VOUS N'ÊTES PAS À LA MAISON

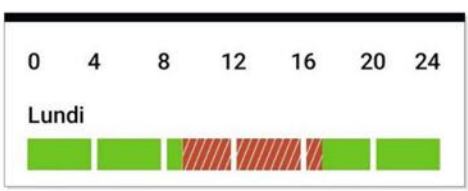
En dépit des protocoles de sécurité WEP et WPA, les réseaux Wifi restent vulnérables. Pensez à couper le signal Wifi pour éviter les intrusions lorsque vous vous absentez.

1 UTILISEZ L'OUTIL DE PLANIFICATION

Les cybercriminels disposent d'équipements sophistiqués capables de percer la sécurité des réseaux sans fil. S'il est peu probable que ces groupes mafieux s'en prennent à votre box, n'hésitez pas à suspendre la connexion Wifi en cas d'absence prolongée. Accédez à l'interface d'administration de la box (dans notre cas la Livebox d'Orange), affichez les paramètres **Mon Wifi** et dans la section **État de la connexion Wifi**, cliquez sur **Définir les plages d'activation du Wifi**. Définissez les plages d'inactivité et validez avec **Enregistrer**.

2 DÉSACTIVEZ LE WIFI VIA L'APPLI

Si vous possédez une Livebox 4, vous pouvez également utiliser l'application Ma Livebox pour gérer la connexion Wifi à distance. Lancez l'appli sur votre smartphone ou votre tablette, puis dans le menu **Paramètres Wifi**, touchez la commande **Planifier** et composez votre programme. Les horaires d'activation du Wifi apparaissent en vert dans le tableau, les plages où la connexion est suspendue en rouge. Enregistrez les paramètres (**Valider**). Il est aussi possible de couper le signal Wifi de la Livebox en pointant sur le bouton **Désactiver**.



DIFFICULTÉ MODÉRÉE TEMPS 10 MIN DOMAINE CONTRÔLE D'ACCÈS

PARTAGEZ LE MOT DE PASSE WIFI DE VOTRE BOX EN TOUTE SÉCURITÉ

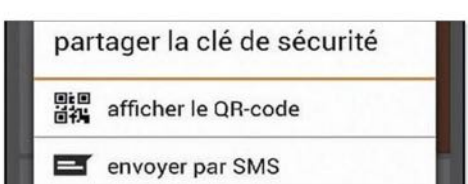
Facilitez l'accès au réseau sans fil à vos amis de passage en leur évitant la saisie d'une clé à rallonge.

1 PARTAGEZ UN MOT DE PASSE WIFI AVEC IOS

Accédez à l'iPhone qui souhaite se connecter à votre réseau, allez dans les réglages d'iOS et ouvrez la section **Paramètres Wi-Fi**. Appuyez sur le nom du réseau et patientez jusqu'à ce que l'écran **Saisir le mot de passe** s'affiche. Une fenêtre apparaît sur votre iPhone. Appuyez sur le bouton **Partager le mot de passe**. Le code d'accès Wifi de votre box Internet est alors envoyé sur l'appareil qui sollicite le partage. Une fois la connexion établie, ce dernier affiche la mention Terminé et peut profiter de la connexion Internet.

2 PARTAGEZ DEPUIS VOTRE LIVEBOX

Pour faciliter le paramétrage de la connexion sans fil de vos équipements, l'application Ma Livebox se propose de partager la clé de sécurité de votre box. Vous pouvez ainsi afficher le mot de passe, le copier dans le presse-papiers pour le transmettre par mail, l'envoyer par SMS ou encore générer un QR Code qui intègre les informations de connexion. Affichez la rubrique **Wifi** de l'application, touchez la clé Wifi puis effleurez le bouton **Partager**. Sélectionnez enfin le mode de partage souhaité.



DIFFICULTÉ MODÉRÉE TEMPS 10 MIN DOMAINE DÉPANNAGE

ACCÉDEZ À VOTRE PC À DISTANCE SANS CRAINTE

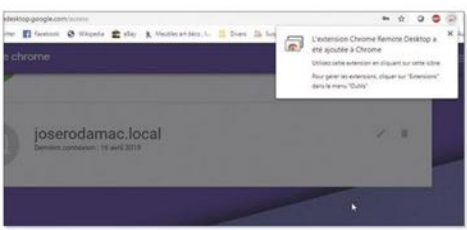
Les ordinateurs reliés à votre box sont en mesure d'envoyer et de recevoir des données vers Internet. Profitez de cette connexion pour accéder au contenu de votre PC où que vous soyez et en toute sécurité.

1 ACCÉDEZ AU BUREAU À DISTANCE DE GOOGLE

Inutile de chercher des solutions complexes. Si vous utilisez le navigateur Google Chrome, vous disposez en effet de tous les outils nécessaires pour prendre le contrôle d'un ordinateur à partir d'un poste d'emprunt ou de votre portable. L'application Google Chrome Bureau à distance présente l'intérêt de fonctionner sur différentes plateformes, ce qui signifie concrètement qu'il est possible d'intervenir sur un Mac à partir d'un PC sous Windows, et inversement. Pour commencer, préparez votre ordinateur fixe (dans cet exemple, un Mac). Connectez-vous au site **bit.ly/2XtcGFD**, cliquez sur le bouton **Commencer** et saisissez les identifiants de votre compte Google.

2 PARAMÉTREZ L'HÔTE CHROME DESKTOP

Activez ensuite l'onglet **Accès à distance** et pointez sur le bouton bleu au bas de la section **Configurer l'accès à distance**. Installez le module Google Chrome Bureau à distance en cliquant sur **Ajouter à Chrome**, **Ajouter l'extension**. Revenez sur la page de configuration et actionnez le bouton **Activer** pour autoriser l'accès à cet ordinateur. Vous êtes alors invité à personnaliser le nom de l'appareil. Cet intitulé servira à identifier le Mac ou le PC quand vous lancerez une session de prise de contrôle depuis un ordinateur distant. Validez par **Suivant**. Définissez ensuite un code de sécurité à six chiffres, confirmez la combinaison et pointez sur **Démarrer**.



3 PRÉPAREZ VOTRE MAC

La mention **En ligne** confirme la réussite de l'opération. Répétez la manipulation sur votre portable. Le nom du Mac apparaît désormais sous l'onglet Accès à distance. Il suffit de pointer sur cet intitulé, puis de saisir le code de sécurité défini un peu plus tôt pour accéder au Bureau du Mac. Si vous utilisez un ordinateur d'emprunt, demandez à votre conjoint ou votre enfant d'aller sur la page Web du Bureau à distance, d'activer l'onglet **Assistance à distance**, de cliquer sur le bouton **Générer un code** et de vous transmettre le mot de passe constitué de 12 caractères qui s'affiche à l'écran.

4 EFFECTUEZ LES OPÉRATIONS À DISTANCE

De votre côté, rendez-vous sur la page d'accueil du bureau à distance (**bit.ly/2XtcGFD**). Pointez sur l'onglet **Assistance à distance** et entrez le code d'association à 12 chiffres dans le champ **Code d'accès** de la section **Fournir de l'aide**. Validez avec **Se connecter**. Il reste à l'utilisateur distant à accepter la session en cliquant sur le bouton **Partager**. Dans les deux cas de figure, vous avez le contrôle complet du Mac ou du PC distant. Vous pouvez lancer un film, consulter votre messagerie, modifier les Préférences système ou exécuter un utilitaire pour résoudre la panne.

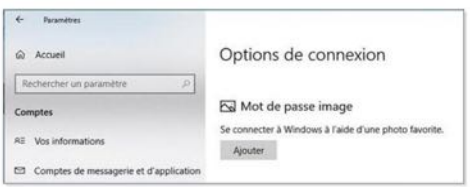
DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE SANS FIL

PROFITEZ DES AVANTAGES DU BLUETOOTH SANS LES RISQUES

Le protocole Bluetooth mise sur la simplicité pour faire communiquer vos appareils. Comme le Wifi, il nécessite quelques mesures de sécurité élémentaires.

1 ACTIVEZ LE VERROUILLAGE DYNAMIQUE SOUS WINDOWS 0

Le protocole Bluetooth est utilisé pour des connexions à courte distance. Ce n'est pas pour autant qu'il est à l'abri du piratage. Pour sécuriser les échanges, Windows propose une option peu connue : le verrouillage dynamique. Dans les Paramètres du PC, pointez sur **Comptes**, **Options de connexion**, **Verrouillage dynamique**. Cochez **Autoriser Windows à détecter quand vous êtes absent et à verrouiller automatiquement l'appareil**. Ainsi, le Bluetooth sera coupé quand vous vous éloignez de votre ordinateur.



2 LIMITEZ LA VISIBILITÉ BLUETOOTH

Il est pratique que vos périphériques Bluetooth soient visibles les uns des autres. Cela constitue néanmoins une brèche de sécurité, n'importe quel utilisateur situé à portée du signal pouvant aussi visualiser vos équipements. Pour y remédier, affichez les paramètres de Windows et accédez à la section **Périphériques**, Appareils **Bluetooth et autres**. Pointez sur le lien **Paramètres Bluetooth avancés** dans la section **Paramètres associés** et désactivez l'option **Détection - Autoriser les périph. à détecter ce PC**. Validez par **OK**.

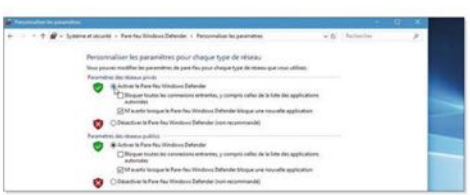
DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE FIREWALL

FILTREZ TOUT CE QUI TRANSITE PAR VOTRE ORDINATEUR

Une fois bien réglé, le pare-feu de Windows complète utilement celui de votre box Internet.

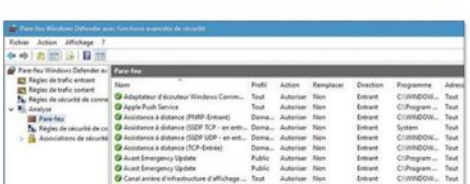
1 DÉMARREZ LE PARE-FEU SUR VOTRE PC...

Saisissez *Pare-feu* dans le champ de recherche de Windows, puis cliquez sur le premier résultat (Pare-feu Windows Defender). Pointez ensuite sur **Activer ou désactiver le Pare-feu Windows Defender**. Personnalisez ensuite les options liées à votre box Internet. Définissez la façon dont les alertes vous parviendront dans **Modifier les paramètres de notification**, puis dans **Paramètres de réseaux privés**, cochez **Bloquer toutes les connexions entrantes, y compris celles de la liste des applications**.



2 ... ET PERSONNALISEZ SES FILTRES

Accédez ensuite à la section **Pare-feu Windows avec Fonctions avancées de sécurité**. Cliquez sur la commande **Analyse** pour obtenir un aperçu détaillé de la façon dont le pare-feu gère les données entrantes et sortantes sur votre ordinateur. Pointez sur **Règles de trafic entrant** et passez en revue la liste des applications et des processus autorisés à recevoir des données. Si vous souhaitez révoquer les privilèges accordés à un composant, faites un clic droit sur la règle et optez pour **Désactiver la règle** dans le menu contextuel.



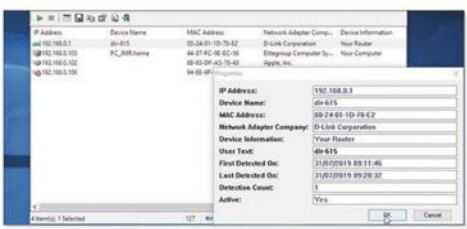
DIFFICULTÉ MODÉRÉE TEMPS 10 MIN DOMAINE SURVEILLANCE

IDENTIFIEZ LES ACTIVITÉS SUSPECTES SUR LE RÉSEAU

À force d'entendre parler de virus et de cyber-attaques, on pense immanquablement à une intrusion quand on perçoit un ralentissement sur le réseau familial. De la paranoïa ? Dans le doute, vérifiez qu'un intrus n'utilise pas votre connexion.

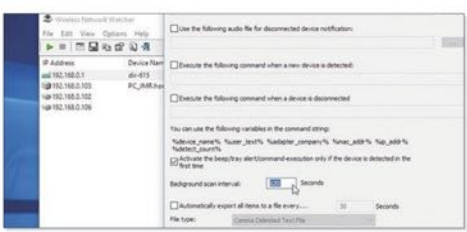
1 ANALYSEZ L'ACTIVITÉ DU RÉSEAU

Pour faire le point sur les activités en cours sur votre réseau, nous vous recommandons de télécharger l'application gratuite Wireless Network Watcher pour Windows (**bit.ly/33c7Qwq**). Lors de l'installation, votre antivirus risque fort d'émettre une alerte. Si le programme ne présente pas de danger, son fonctionnement peut apparaître suspect aux yeux des outils de sécurité, car il analyse en profondeur l'activité réseau. Ignorez ces notifications et laissez l'appli dresser la liste des périphériques reliés à l'ordinateur. Double-cliquez sur l'intitulé d'un appareil pour obtenir davantage de détails (adresses IP et MAC, nom, etc.).



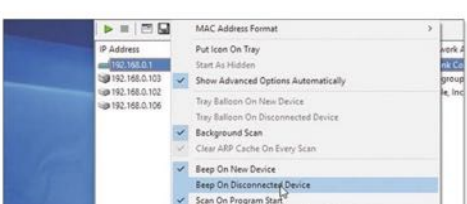
2 AJUSTEZ LES INTERVALLES DE SURVEILLANCE

Vous pouvez rafraîchir à tout moment la liste en appuyant sur la touche **F5** de votre clavier. Par défaut, Network Watcher lance une nouvelle analyse toutes les soixante secondes. Il est possible de modifier ce délai comme bon vous semble, de façon à appliquer une surveillance plus resserrée ou, au contraire, d'espacer un peu les recherches. Déroulez le menu **Options**, puis pointez sur l'intitulé **Advanced Options**. Une nouvelle fenêtre s'affiche alors. Portez votre attention sur la commande **Background Scan Interval**. La durée à entrer dans le champ de saisie s'exprime en secondes. Saisissez la valeur **120** pour effectuer une analyse toutes les deux minutes.



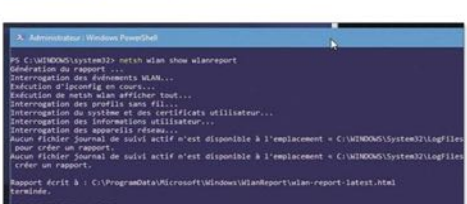
3 PILOTEZ L'ACTIVITÉ DU RÉSEAU SANS FIL

Il est inutile de garder les yeux rivés sur le tableau de bord. Network Watcher se propose en effet de vous alerter à chaque fois qu'un appareil se connecte ou quitte votre réseau sans fil. Pour mettre en place les notifications sonores, reportez-vous au menu déroulant **Options** et cochez les intitulés **Beep On New Device** et **Beep On Disconnected Device**. Si vous notez la présence d'un périphérique inconnu, agissez sans attendre et modifiez le mot de passe du point d'accès Wifi de la box Internet. L'opération s'effectue depuis la console d'administration Web.



4 UTILISEZ POWERSHELL POUR Y VOIR CLAIR

Poussez l'analyse des connexions réseau en utilisant les ressources de Windows. Faites un clic droit sur le bouton **Démarrer** et pointez sur **Windows Powershell (Admin)**. Saisissez la commande **netsh wlan show wlanreport** et validez par **Entrée**. Un rapport est généré et enregistré dans le document **wlan-report-latest.html**, accessible dans le dossier **C:\ProgramData\Microsoft\Windows\WlanReport**. Passez le pointeur sur une session pour afficher davantage de données. La rubrique **Wireless Sessions** informe sur les événements Wifi survenus au cours des dernières 72 heures.



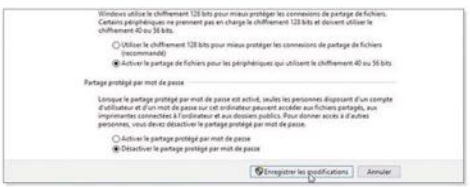
DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE ADMINISTRATION

PARAMÉTREZ VOTRE RÉSEAU ET VENEZ À BOUT DES PANNES

Windows est parfois capricieux. Il lui arrive de subir des coupures répétées de la connexion Wifi ou de ne plus afficher certaines ressources partagées.

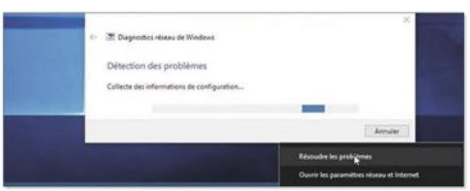
1 OPTIMISEZ L'ACCÈS AUX RESSOURCES PARTAGÉES

Si votre réseau local accueille des ordinateurs animés par différentes versions de Windows (et d'autres systèmes d'exploitation), vous risquez de vous heurter aux règles de sécurité de Windows 10. Accédez aux **Paramètres Réseau et Internet**. Pointez sur **Centre Réseau et partage**, **Modifier les options de partage pour d'autres profils réseau** et **Tous les réseaux**. Cochez **Activer le partage** pour que les autres utilisateurs puissent accéder à vos dossiers publics, puis **Désactiver le partage protégé par mot de passe**.



2 DÉPANNEZ LE RÉSEAU

Ralentissements inexplicables, ordinateur inaccessible ou débit très faible, avant de tenter des manipulations hasardeuses, pensez à lancer l'utilitaire de résolution des problèmes de Windows. Opérez un clic droit sur l'icône **Réseau** dans la barre des tâches et pointez sur la commande **Résoudre les problèmes**. Un assistant analyse alors l'ensemble des paramètres réseau pour effectuer un diagnostic complet. Au terme de l'analyse, appliquez les modifications suggérées. Vous devriez ainsi résoudre vos soucis.



DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE WIFI

GÉREZ L'ACCÈS WIFI SUR VOTRE TÉLÉPHONE

La connexion Wifi n'est pas sans conséquence sur l'autonomie de la batterie. Une saine gestion s'impose.

1 COUPEZ LA CONNEXION SANS FIL

Quand vous voyagez ou que vous marchez dans la rue, l'accès au Wifi est souvent inutile. N'hésitez pas à suspendre la recherche de réseaux sans fil afin d'éviter les risques de piratage et de réduire la consommation de votre téléphone. Pour désactiver temporairement le Wifi, déployez le volet des notifications en balayant l'écran de haut en bas. Observez la première icône de la section des actions rapides. Si ce raccourci est bleuté, le Wifi est actif. Un simple appui suffit à interrompre la connexion (l'icône apparaît alors en grisé).

2 ACTIVEZ AUTOMATIQUEMENT LE WIFI

Vous pouvez faire en sorte que le Wifi soit réactivé automatiquement quand des points d'accès que vous avez l'habitude d'utiliser se trouvent à portée de votre mobile. Ouvrez pour cela les Paramètres de l'appareil et saisissez **Préférences Wifi** dans le champ de recherche. Actionnez le curseur **Activation automatique du Wifi**.

3 SUSPENDEZ ET RÉACTIVEZ LE WIFI EN FONCTION DE LA SITUATION

Avec le service IFTTT (If Then Then That), vous avez la possibilité de définir des scénarios pour adapter l'activation de la connexion sans fil à vos habitudes. Une fois les scripts enregistrés, vous n'avez plus à vous préoccuper de quoi que ce soit. IFTTT est ainsi capable de couper le Wifi dès qu'il détecte que vous quittez votre domicile ou votre bureau. Un bon moyen de préserver l'autonomie de la batterie. Téléchargez l'application IFTTT sur le Play Store. Une fois l'appli installée, autorisez l'accès à vos données de localisation puis saisissez **Turn off Wifi** dans le champ de recherche. Pointez sur le bouton **Connected**, définissez la position géographique qui correspond à votre domicile, puis effleurez la coche en haut à droite de l'écran. La recette IFTTT est opérationnelle. Dès que vous vous éloignerez de chez vous de quelques dizaines de mètres, le Wifi sera désactivé sans intervention de votre part.

Coupez la connexion d'un appui sur l'icône Wifi du volet des Actions rapides.

DIFFICULTÉ MODÉRÉE TEMPS 1 H DOMAINE VIE PRIVÉE

LIMITEZ AU MAXIMUM VOTRE EMPREINTE NUMÉRIQUE

Il faut se faire à l'idée que la vie privée n'existe pas - ou peu - en ligne, car les services se rétribuent souvent en commercialisant les données de leurs utilisateurs. Il est cependant possible de préserver quelques îlots de confidentialité en agissant sur les paramètres des navigateurs et des sites.

Boîte à outils

Pour ce pas à pas, nous avons utilisé

- Un PC ou un Mac
- Un smartphone
- Internet
- Comptes Google, Microsoft, Facebook

Le RGPD, le règlement général sur la protection des données entré en vigueur en mai dernier dans les pays de l'Union européenne (UE), vise à assurer une protection étendue aux citoyens. Les règles édictées concernent aussi bien les acteurs européens de l'Internet que les Gafam, tenus de respecter la loi dès lors qu'ils manipulent les données personnelles de clients installés dans l'UE.

La Cnil (Commission nationale de l'informatique et des libertés) a enregistré une hausse signi cative des plaintes émanant de particuliers ou d'associations (environ 11 000 en 2018 contre 3 000 auparavant) pour manquement au règlement. Les sanctions tardent néanmoins à être appliquées. Les consommateurs continuent à naviguer sur des sites et à fréquenter des services en ligne qui ne se privent pas de les pister. Du côté des cookies, les plateformes ont dorénavant l'obligation de signaler leur présence dès la page d'accueil et de solliciter l'acceptation des internautes (le fameux bouton J'ai compris). Un lien permet d'accéder aux paramètres des cookies et de limiter l'action de ces traqueurs. Les utilisateurs soucieux de préserver leur vie privée ont fort à faire face aux géants du numérique dont le but est de dresser la cartographie de nos habitudes et nous présenter des publicités ciblées.●

1 PRENEZ LE TEMPS DE RÉGLER LES COOKIES

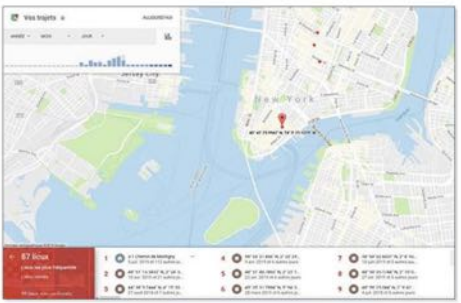
La grande majorité des sites finissant par .com ou .fr opère un pistage général des internautes qui croisent sur leurs pages. Pour freiner quelque peu leur curiosité, et éviter de se voir offrir des offres et services personnalisés par la suite, il est impératif de prendre le temps de cliquer sur le bouton de paramétrage des traqueurs. Ce lien revêt des formes différentes selon les sites visités : **J'ai compris**, **En savoir plus et paramétrer les cookies**. Sans intervention de votre part, vos moindres gestes seront scrutés, analysés et utilisés pour afficher des publicités en accord avec vos centres d'intérêt. Ne conservez que les cookies indispensables au fonctionnement du site. Désactivez en revanche les outils des sociétés partenaires.

2 RÉDUISEZ LE PISTAGE DES SITES DE STREAMING

Netflix, OCS, Spotify ou Deezer, les services de streaming audio et vidéo conservent en mémoire ce que vous écoutez ou visionnez de façon à proposer des programmes adaptés à vos goûts. Si vous trouvez ces algorithmes un peu trop conservateurs et souhaitez élargir votre horizon en accédant à des contenus en décalage avec vos habitudes de consommation, accédez aux paramètres de votre compte et trouvez les options d'historique ou de communication. Netflix autorise par exemple la suppression des anciens visionnages, ce qui réinitialise la base de données sur laquelle reposent les suggestions du service de SVOD. Effectuez ces réglages pour tous les services de streaming dont vous êtes membre.

3 VISUALISEZ VOTRE ACTIVITÉ GOOGLE

Pas d'Internet sans Google. Mais pas de Google non plus sans internautes ! Les bénéfices du géant de Mountain View sont basés sur la vente de publicités ciblées aux utilisateurs de ses services en lignes. Pour gérer les informations mémorisées par Google, connectez-vous à votre compte et cliquez en colonne gauche sur **Données de personnalisation**. Mettez à profit les commandes relatives à l'activité de confidentialité pour définir ce que vous souhaitez cacher (localisation, historique des recherches, etc.). Attention toutefois, le fait de désactiver certaines options peut supprimer l'accès à certains outils que vous utilisez peut-être, comme l'assistant Google. À vous de faire les bons choix !



4 MINOREZ L'HISTORIQUE DES PARCOURS

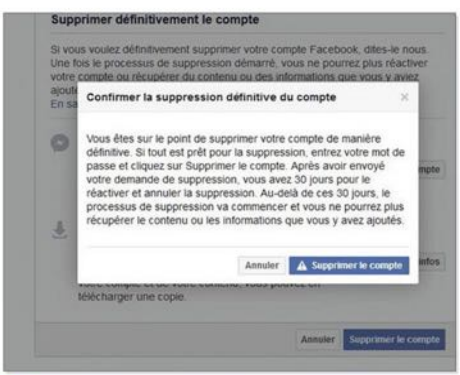
Google contrôle les applis Maps et Waze qui pilotent elles-mêmes vos déplacements. Ajoutez à cela que votre mobile vous localise en permanence et vous comprenez que Google vous suit à la trace et sait toujours où vous vous trouvez bien plus sûrement que votre famille ! Dans la partie **Données personnalisation du compte**, pointez sur **Activités et trajets**, **Vos trajets**. Les points rouges correspondent à l'historique de vos positions. Déroulez le menu rouge à gauche pour afficher des détails. Si vous trouvez que Google en sait un peu trop, accédez à **Gérer l'historique des positions**, **Appareils associés à ce compte** et décochez votre téléphone. Désactivez enfin le curseur **Historique des positions**.

5 FERMEZ LE COMPTE GOOGLE

Avant de prendre une mesure aussi radicale, gardez en tête que vos appareils sous Android utilisent largement les outils de Google. Si vous souhaitez malgré tout clôturer votre compte, commencez par télécharger vos données. Allez sur la page de rapatriement (**bit.ly/2JfGayF**) et cliquez sur **Étape suivante**. Validez avec **Créer une archive** et attendez de recevoir fichier de sauvegarde. Revenez alors sur l'accueil du compte et dirigez-vous vers **Données et personnalisation**. Dans la partie **Télécharger, supprimer ou planifier l'avenir de vos données**, accédez à **Supprimer un service ou un compte**, **Supprimer votre compte**. Cochez les deux cases d'acceptation et cliquez sur **Supprimer le compte**.

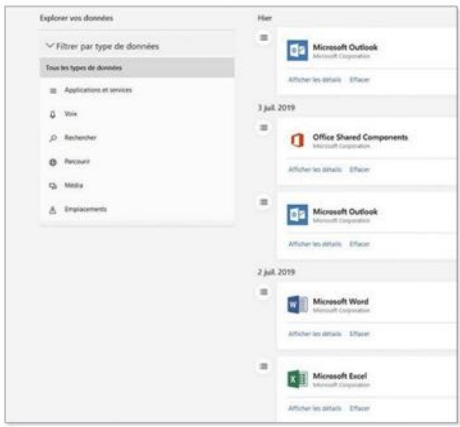
6 RÉCUPÉREZ VOS DONNÉES SUR FACEBOOK

À l'image de Google, Facebook note scrupuleusement vos publications, vos commentaires, vos likes, etc. Pour savoir ce que le réseau social sait de votre vie privée, accédez à votre compte et pointez sur la flèche noire en haut à droite de la page d'accueil. Cliquez sur **Paramètres**, **Vos informations Facebook** en colonne gauche, puis accédez à **Télécharger vos informations**. Facebook compile par défaut l'intégralité de vos données personnelles. Validez avec **Créer un fichier**. Vous serez notifié dès que la copie est prête. Vous pouvez aussi activer le lien **Accéder à vos informations** pour les visualiser sans les télécharger.



7 FINISSEZ-EN UNE BONNE FOIS POUR TOUTES

Vous en avez assez de Facebook ? Deux solutions s'offrent à vous. Désactiver le compte pour prendre le large quelques semaines ou le supprimer. Dans le premier cas, accédez à la section **Gestion du compte** des paramètres généraux et cliquez sur **Désactiver**. Indiquez la raison de votre escapade et validez avec **Désactiver**. Si vous préférez partir pour de bon, allez sur la page **bit.ly/2BT1qqr**. Dirigez-vous vers **Supprimer le compte**. Entrez vos identifiants de connexion et confirmez votre décision par **Supprimer le compte**.



8 JETEZ UN ŒIL À VOTRE ACTIVITÉ MICROSOFT

La gestion des données collectées par Microsoft s'effectue pour partie en ligne, pour l'autre dans Windows 10 (voir page suivante). Pour consulter votre historique, accédez à votre compte (**bit.ly/2XsGQEy**). Cliquez sur **Confidentialité**, **Historique d'activités**. Déroulez la page vers le bas pour obtenir des infos sur les applis ouvertes tel jour. Utilisez le menu à gauche pour filtrer les données.

9 SUPPRIMEZ VOTRE COMPTE

La fermeture du compte va bloquer l'usage de certaines applications. Si vous détenez un abonnement Office 365, la suite bureautique ne sera plus accessible. Pensez-y avant de procéder ! Allez sur la page **bit.ly/2XmzKBC**. Suivez les instructions affichées à l'écran puis cliquez sur **Suivant**. Cochez toutes les cases, justifiez votre départ et validez avec **Marquer le compte pour fermeture**. Passé le délai de 60 jours, vos données seront définitivement détruites (durant ce laps de temps, vous pouvez revenir en arrière).

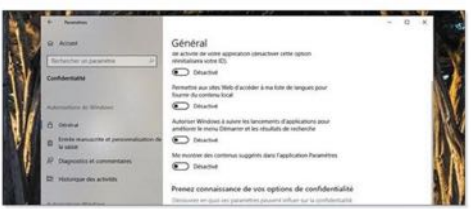
DIFFICULTÉ MODÉRÉE **TEMPS** 30 MIN **DOMAINE** VIE PRIVÉE

DITES-EN MOINS À WINDOWS

Les options de vie privée ne sont pas réglées par défaut de façon à préserver la confidentialité des données des utilisateurs. Microsoft a toutefois aménagé de nombreux réglages à cette fin.

1 DÉSACTIVEZ LA PUBLICITÉ CIBLÉE

Microsoft dresse votre profil publicitaire précis dans le but d'analyser vos centres d'intérêt et de vous abreuver d'informations en lien avec vos attentes. Pour ne plus bénéficier de ces notifications ciblées, accédez aux paramètres du PC (**Windows + I**) et pointez sur **Confidentialité**. Dans la partie **Général**, **Modifier les options de confidentialité**, désactivez les curseurs associés. Vous ne verrez plus ainsi de contenus suggérés et éviterez que les sites Web que vous visitez affichent des contenus localisés. Cliquez sur **En savoir plus** pour connaître le fonctionnement de l'identifiant de publicité.

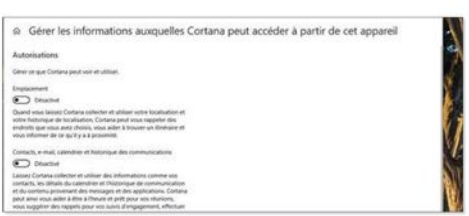


2 SUPPRIMEZ LA LOCALISATION ET L'HISTORIQUE

À moins que vous ne lui interdisiez, Windows mémorise en permanence vos données de localisation en s'appuyant sur la position des points d'accès Wifi auxquels vous vous connectez (ou aux données GPS si votre portable est équipé d'une telle puce) ; Sur l'onglet **Confidentialité** des paramètres, pointez sur **Emplacement**, puis **Modifier**. Désactivez la fonction et effacez l'historique de localisation. Cliquez sur **Historique des activités** en colonne gauche. Décochez les deux cases d'enregistrement et d'envoi de données, désactivez l'affichage de l'activité du compte et purgez l'historique.

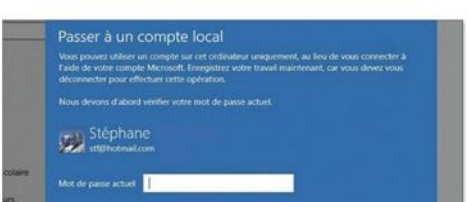
3 FAITES TAIRE CORTANA

L'assistant de Windows 10 est utile mais surtout très intrusif. Pour éviter d'être épié, mieux vaut le désactiver totalement. Cliquez sur l'icône en forme de cercle à droite du bouton **Démarrer** de la barre des tâches puis sur l'icône en forme d'engrenage pour accéder aux paramètres de l'assistant. Désactivez le curseur **Hey Cortana** ainsi que ceux du raccourci clavier et de l'écran de verrouillage. Pointez ensuite sur **Autorisations et historique**, sur le lien **Gérer les informations auxquelles Cortana peut accéder à partir de cet appareil**. Désactivez tous les curseurs de ce menu.



4 OPTEZ POUR UN COMPTE LOCAL

Dans les paramètres de confidentialité, dirigez-vous vers le menu **Diagnostics et commentaires**. Optez pour le mode **De base**. Désactivez les curseurs d'expériences personnalisées et supprimez les données de diagnostic. Pointez sur **Informations sur le compte**. Suspendez l'accès aux infos du compte (bouton **Modifier**) et empêchez les applis à accéder à ces données. Pour éviter que Microsoft n'en sache trop sur vous, nous vous invitons à supprimer le compte Microsoft de l'ordinateur et à passer à un compte local. Allez dans **Paramètres**, **Comptes**, **Se connecter plutôt avec un compte local**.



DIFFICULTÉ AUCUNE TEMPS 20 MIN DOMAINE PISTAGE

MODÉREZ LA CURIOSITÉ DE VOTRE NAVIGATEUR

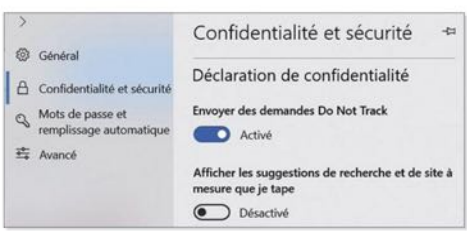
Chrome, Firefox et Edge enregistrent une foule de données, parfois à votre insu, qu'il s'agisse des sites que vous visitez, de votre position géographique ou encore de vos mots de passe. Pour couper court à cet espionnage en règle, faites un détour par les réglages de votre navigateur.

1 SURFEZ EN TOUTE DISCRÉTION AVEC CHROME

Pour purger la mémoire de Chrome, cliquez sur l'icône **Personnaliser et contrôler** (les points en haut à droite de la fenêtre de Chrome), puis sur **Historique** et sélectionnez **Effacer les données de navigation**. Activez le lien **Paramètres avancés**. Pour faire un grand ménage, pointez sur **Effacer les données**. Pour éviter que Chrome ne collecte des infos sur votre PC ou votre Mac, dissociez le navigateur de votre compte Google en cliquant sur votre avatar à droite de la barre d'adresse, puis sur **Synchronisation**, **Désactiver**. Dans la section **Saisie automatique** des Paramètres, désactivez les options, **Mots de passe**, **Mode de Paiement** et **Adresses**.

2 PROTÉGEZ VOTRE VIE PRIVÉE DANS MICROSOFT EDGE

Ouvrez les paramètres du navigateur de Windows 10 (**Alt** + **X**), pointez sur **Afficher dans la barre d'outils** et **Historique**. Cliquez ensuite sur l'icône **Historique** à droite de la barre d'adresse puis sur le lien **Effacer l'historique**. Décochez les éléments que vous souhaitez conserver et validez avec **Effacer**. Basculez le curseur **Toujours effacer lorsque je ferme le navigateur** en position active afin qu'Edge fasse automatiquement le ménage à la fin de chaque session de navigation. Retournez sur l'onglet **Confidentialité et sécurité** des paramètres et activez l'option **Do Not Track** de façon à ce qu'Edge bloque les sites qui tentent de recueillir vos données personnelles.

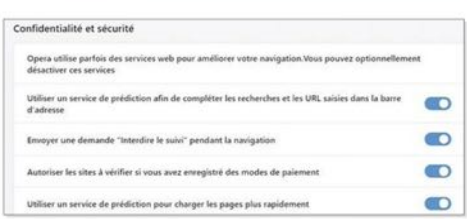


3 GARDEZ VOTRE ANONYMAT AVEC FIREFOX

Cliquez sur l'icône **Ouvrir le menu** à droite de la barre d'adresse du navigateur, puis sur **Options**, **Vie privée et sécurité**. Dans **Blocage de contenu**, imposez le mode **Strict**. Si des sites venaient à refuser de se lancer après ce réglage, repassez ponctuellement au mode **Standard**. Cochez **Toujours** sous **Envoyer aux sites web un signal « Ne pas me pister »**. Optez pour **Supprimer les cookies à la fermeture de Firefox** dans **Cookies et données du site** et imposez la règle **Ne jamais conserver l'historique** dans la section **Historique**. Cliquez sur **Effacer l'historique**, **Effacer maintenant**.

4 SÉCURISEZ LA NAVIGATION AVEC OPÉRA

Cliquez sur **Configuration facile**, **Aller aux réglages du navigateur**, **Avancé**. Dans **Confidentialité et sécurité**, activez les commandes **Envoyer une demande « Interdire le suivi » pendant la navigation** et **Me protéger des sites malveillants**. Pointez sur **Effacer les données de navigation**, **Avancé** et cochez les éléments à supprimer avant de valider avec **Effacer les données**. Retournez sur la page d'accueil des paramètres et cliquez sur **Paramètres du site**, **Cookies** pour cocher **Bloquer les cookies tiers** et **Ne conserver les données locales que jusqu'à ce que je quitte ma session**.



DIFFICULTÉ ÉLEVÉE TEMPS 10 MIN DOMAINE PRÉVENTION

SURFEZ SANS PRENDRE AUCUN RISQUE

Pour ne pas risquer de contaminer votre ordinateur en visitant des sites potentiellement dangereux, exécutez votre navigateur Internet dans un bac à sable.

1 EXPLOITEZ LA SANDBOX DE WINDOWS 10 PRO

L'option **Sandbox** est réservée aux utilisateurs des versions Professionnel et Entreprise de Windows 10. Pour l'activer, tapez **Fonctionnalité** dans le champ de recherche, puis sélectionnez **Activer ou désactiver des fonctionnalités Windows**. Cochez la case **Bac à sable Windows**. Si votre ordinateur n'est pas compatible, l'option apparaît en grisé. Dans ce cas, en attendant que Microsoft étende son service à la version Famille de Windows 10, rendez-vous sur le site **bit.ly/2ik4EbE** pour télécharger et installer l'application Sandboxie.

2 NAVIGUEZ EN TOUTE SÉCURITÉ AVEC SANDBOXIE

Glissez simplement le raccourci de votre navigateur Internet du Bureau sur la fenêtre **Sandboxie** ou déroulez le menu **Démarrer** de Windows, faites un clic droit sur l'icône de Firefox, par exemple, et choisissez **Plus**, **Ouvrir l'emplacement du fichier**. Dans le menu contextuel du fichier exécutable (**firefox.exe**), optez pour **Propriété** et copiez le contenu du champ **Cible**. Opérez un clic droit sur l'icône **Sandboxie** dans la zone de notification de Windows, pointez sur **DéfaultBox**, **Exécuter un programme** et collez le chemin de Firefox.

DIFFICULTÉ AUCUNE TEMPS 10 MIN DOMAINE ERGONOMIE

DÉBARRASSEZ-VOUS D'UNE BARRE D'OUTILS INDÉSIRABLE

Il n'est pas toujours simple de donner congé à ces raccourcis. Certains se montrent aussi collants qu'intrusifs.

1 CHASSEZ LES ÉLÉMENTS NÉFASTES AVEC ADWCLEANER

Ces barres d'outils apparaissent souvent après l'installation d'un logiciel infecté par un malware. Dans le meilleur des cas, elles ont vocation à afficher de la publicité. Allez sur la page **Applications** des paramètres du PC pour supprimer le programme responsable. Si le nom de la barre n'apparaît pas dans la liste des logiciels, il s'agit d'un sans doute malware. Téléchargez et lancez ADWcleaner (**bit.ly/2GVAkD3**) en double-cliquant sur le fichier **adwcleaner_7.4.exe**. Pointez sur **Analyser maintenant** puis sur **Nettoyer et réparer**.

2 RÉINITIALISEZ VOTRE NAVIGATEUR INTERNET

Si la barre d'outils n'a pas disparu, essayez de réinitialiser votre navigateur. Avec Chrome, ouvrez le menu **Personnaliser et contrôler**, pointez sur **Paramètres** puis sur le lien **Paramètres avancés**. Dans la section **Réinitialiser et nettoyer**, activez la commande **Restaurer les paramètres par défaut**, **Réinitialisez les paramètres**. Redémarrez le navigateur. Si vous utilisez Firefox, ouvrez le volet de menu et choisissez **Aide**, **Informations de dépannage**, **Réparer Firefox** pour éliminer les éléments et extensions indésirables.

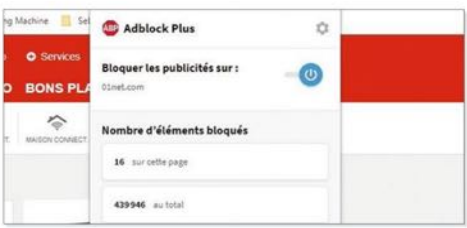
DIFFICULTÉ AUCUNE TEMPS 10 MIN DOMAINE CONTENUS

INSTALLEZ ET CONFIGUREZ UN BLOQUEUR DE PUBS

La publicité finance bon nombre de sites Internet et représente le prix à payer pour disposer de services gratuits. Certains acteurs en abusent toutefois. La tentation devient grande alors de s'en affranchir. Surtout quand les pubs vous espionnent.

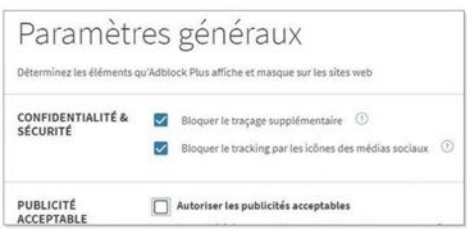
1 DÉBARRASSEZ-VOUS DES RÉCLAMES DANS CHROME

Rendez-vous sur le Chrome Web Store et installez l'extension Adblock Plus. Cet outil intercepte la plupart des publicités, qu'il s'agisse de pop-up ou de bandeaux. Si un site détecte la présence du bloqueur et vous empêche d'accéder à son contenu, cliquez sur l'icône **Adblock Plus** à droite de la barre d'adresse de Chrome, puis glissez le curseur **Bloquer les publicités sur** pour suspendre l'extension. Pointez sur **Actualiser** pour forcer le rafraîchissement de la page. Certains sites refusent de s'afficher quand Adblock veille au grain, mais sans vous en tenir informé. En cas de problème sur une page de confiance, ayez le réflexe de désactiver l'extension.



2 LEVEZ LES RESTRICTIONS DANS ADBLOCK PLUS

Les réglages initiaux d'Adblock Plus n'assurent pas un filtrage optimal. Pour aller plus loin, pointez sur l'icône de l'extension, puis sur l'icône en forme d'engrenage. Sur l'onglet des **Paramètres généraux**, cochez les options **Bloquer le traçage supplémentaire** et **Bloquer le tracking par les icônes des médias sociaux**. Dans **Publicité acceptable**, décochez **Autorisez les publicités acceptables**. Pour être un peu moins strict, choisissez le mode **Autoriser seulement les annonces sans traçages tiers**. Cliquez sur **Sites Web sur liste blanche** et collez les adresses des pages et domaines pour lesquels vous acceptez l'affichage des publicités.



3 FAITES PLACE NETTE DANS FIREFOX

Le navigateur de Mozilla embarque par défaut un bloqueur de contenus. Une partie des publicités est ainsi écartée, ainsi que les traqueurs, cookies et les tentatives d'exploiter les ressources de votre PC pour miner des cryptomonnaies. Vous pouvez renforcer ce filtrage en installant une extension spécialisée. Ouvrez menu du navigateur et cliquez sur **Modules complémentaires**. Recherchez l'extension **Ghostery** et pointez sur **Ajouter à Firefox**. Autoriser le module à s'exécuter dans une fenêtre de navigation privée puis cliquez sur **J'ai compris** pour finaliser l'installation.

4 PARAMÉTREZ GHOSTERY

Vous pouvez ajuster le comportement de Ghostery à chaque site. Quand vous arrivez sur une page qui refuse la lecture à cause de votre bloqueur, cliquez sur l'icône **Ghostery** puis sur **Se fier à ce site**. Vous pouvez aussi choisir **Pause** et indiquer la durée de la suspension du filtrage. Pointez sur **Restreindre le site** pour l'ajouter à la liste noire. Les mouchards et les traqueurs seront ainsi bloqués à chaque connexion sur cette page. Activez l'icône du module **Ghostery** puis les trois points et choisissez **Paramètres** et **Se fier** ou **Limiter** pour afficher les sites placés en liste noire ou liste blanche.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE VIE PRIVÉE

EMPÊCHEZ LES SITES ET LES APPLIS DE VOUS GÉOLOCALISER

Votre position géographique constitue une information précieuse pour les plateformes de publicité. L'application Location Guard empêche que l'on vous suive à la trace.

1 ÉVITEZ UNE LOCALISATION TROP PRÉCISE

Location Guard est une extension disponible pour les navigateurs Chrome (**bit.ly/2S8ZLU3**) et Firefox (**mzl.la/2Ld5dVi**). Une fois installée, autorisez-la à accéder aux informations de localisation. Votre position s'affiche sur la carte et peut être masquée de deux façons. La première méthode consiste à brouiller les pistes en empêchant une localisation trop précise. Cliquez sur **Privacy Levels** et définissez le périmètre de protection (en bleu) ainsi que la durée du brouillage au moyen des curseurs placés au-dessus de la carte.

2 OPTEZ POUR UNE POSITION FICTIVE

Si les sites ne sont plus en mesure de vous repérer avec précision, ce brouillage ne masque pas complètement votre position. Si vous le souhaitez, Location Guard peut vous téléporter virtuellement dans le pays ou la ville de votre choix ! Cliquez en colonne gauche sur **Fixed location**. Déplacez le curseur à l'endroit voulu sur la carte. Effectuez un zoom avant pour préciser la localisation. Quand un site Web demandera l'autorisation de vous localiser, pointez sur l'icône **épingle** pour lui indiquer cette fausse adresse.

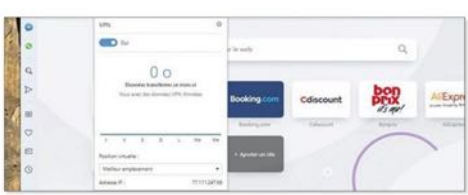
DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE ANONYMAT

NAVIGUEZ INCOGNITO EN UTILISANT LE VPN D'OPERA

Ce navigateur est le seul à proposer un VPN gratuit. Une bonne raison de le préférer à Chrome et Firefox.

1 INSTALLEZ LE NAVIGATEUR OPERA

Un VPN (Virtual Private Network pour Réseau Privé Virtuel) introduit un tunnel chiffré entre votre adresse IP et un serveur localisé en France ou à l'étranger qui vous attribue une adresse IP temporaire. Avec Opera, vous disposez de ce service gratuitement tant que vous utilisez le navigateur pour explorer le Web sur votre ordinateur (**bit.ly/2x2Xf8t**) ou votre smartphone (**bit.ly/2KugSyq**). Une fois Opera installé, pointez sur l'engrenage en haut de la barre de menu verticale puis sur **VPN**. Une infobulle indique que celui-ci est actif.



2 PERSONNALISEZ VOTRE EMPLACEMENT GÉOGRAPHIQUE

Accédez aux paramètres du VPN en cliquant sur l'icône **Configuration facile** en haut à droite. Déroulez le panneau vers le bas et choisissez **Aller aux réglages du navigateur**, **VPN**, **Avancé**. Le premier curseur sert à activer ou désactiver le filtrage, le second à continuer d'utiliser votre véritable emplacement pour effectuer des recherches. Pour personnaliser la géolocalisation, pointez sur l'icône bleue **VPN** à gauche de la barre d'adresse, ouvrez le menu **Position virtuelle** et optez pour **Europe**, **Amérique** ou **Asie**.

DIFFICULTÉ AUCUNE TEMPS 15 MIN DOMAINE ANONYMAT

RESTEZ DISCRET GRÂCE AU MODE PRIVÉ

Certaines sessions Internet gagnent à être classées secret-défense. Faites en sorte que votre navigateur ne retienne rien de votre passage. Activez pour cela le mode navigation privée qui ignore l'historique des sites visités et des recherches. Chut, je surfe !

1 NAVIGUEZ ANONYMEMENT AVEC CHROME

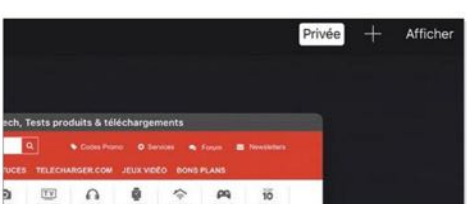
Pour ouvrir une session anonymisée sur votre PC ou votre Mac, ouvrez le menu **Personnaliser et contrôler** et pointez sur la commande **Nouvelle fenêtre de navigation privée** (ou utilisez le raccourci **Crtl + Maj + N**). Attention, si la navigation privée ne laisse pas de traces, elle ne vous protège pas des sites malveillants. Si vous utilisez Chrome sur un smartphone, accédez au menu et touchez **Nouvel onglet de navigation privée**. Autre méthode : fermez tous les onglets actifs et effleurez l'icône qui représente un chapeau et une paire de lunettes. Pour revenir à une session de navigation classique, il suffit de quitter les onglets ouverts en mode privé.

2 PASSEZ INAPERÇU AVEC FIREFOX

Sur un ordinateur, déployez le menu de Firefox et pointez sur **Nouvelle fenêtre de navigation privée**. Il est possible de garder actif ou au contraire de mettre en veille les modules complémentaires durant cette session anonyme. Toujours dans le menu, cliquez sur **Modules complémentaires**, **Extensions**. Sélectionnez le module dont vous souhaitez gérer les autorisations, descendez à la ligne **Exécution dans les fenêtres privées** et cochez **Autoriser**. Sur un mobile, effleurez le masque en haut à droite de la fenêtre pour passer en mode privé. Vous pouvez facilement alterner entre navigation anonyme et classique en activant cette icône.

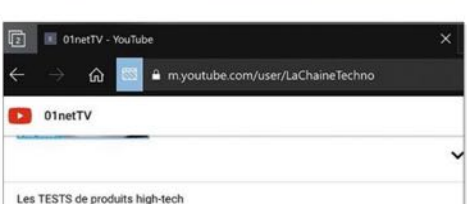
3 NE VOUS FAITES PAS PISTER PAR SAFARI

Dans le navigateur de macOS, déroulez le menu **Fichier**, **Nouvelle fenêtre privée**. Il est possible de forcer le mode privé au lancement du navigateur. Cliquez sur **Préférences**, **Général**. À côté de l'intitulé **Au démarrage Safari ouvre**, choisissez **Une nouvelle fenêtre privée**. Allez sur **Fichier**, **Nouvelle fenêtre** pour repasser en mode normal. Sur un iPhone ou un iPad, tapotez l'icône formée de deux carrés en haut à droite de la fenêtre puis l'option **Privée**. Toutes les fenêtres s'ouvriront alors en mode anonyme. Effleurez de nouveau l'icône et **Privée** pour basculer vers une session classique.



4 NE LAISSEZ PAS DE TRACE SUR EDGE

Dans le navigateur de Windows 10, cliquez sur l'icône **Paramètres et plus** (**Alt + X**) puis **Nouvelle fenêtre InPrivate**. Tous les nouveaux onglets que vous ouvrez dans cette session resteront anonymes. Pour revenir à la fenêtre de navigation classique, appuyez sur les touches **Alt + Tab**. Sur un téléphone, la manipulation est la même : touchez l'icône **Paramètres** puis **Nouvel onglet InPrivate**. Tapotez l'icône avec deux carrés en haut à gauche de la fenêtre puis **Onglet** pour repasser en mode normal. Les sites ouverts en mode privé ne sont pas fermés. Pointez sur **InPrivate** pour les restaurer.



DIFFICULTÉ AUCUNE TEMPS 30 MIN DOMAINE RECHERCHE

ÉVITEZ QUE GOOGLE ESPIONNE VOS REQUÊTES

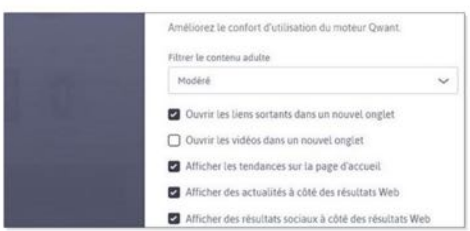
Fort de ses algorithmes et de sa base de référencement sans pareille, le moteur de recherche de Google règne en maître. Un challenger européen, Qwant, tente de rivaliser en misant sur le respect de la vie privée.

1 LANCEZ UNE RECHERCHE SUR QWANT

Rappelons d'abord que les moteurs de recherche sont gratuits et qu'ils se financent en vendant de l'espace commercial et en plaçant des résultats sponsorisés en bonne place dans la liste des résultats des requêtes que les internautes leur soumettent. Le projet européen Qwant se montre plus respectueux de vos données que Google. Allez sur le site **Qwant.com** et utilisez les outils du volet latéral pour lancer une recherche par images, sur les actualités ou les réseaux sociaux. Qwant présente de nombreuses fonctionnalités. Vous pouvez ainsi lire une vidéo sans ouvrir le site d'origine dans la section **Vidéo** ou profiter d'un moteur conçu pour les plus jeunes (**Junior**).

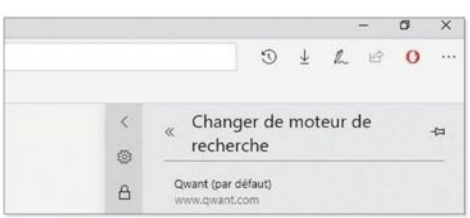
2 MODIFIEZ ET SAUVEGARDEZ LES PARAMÈTRES

Cliquez sur **Menu d'application** puis sur **Thèmes** pour passer en mode sombre. Pointez ensuite sur **Paramètres** et cochez les raccourcis que vous souhaitez garder actifs. Si les **Qoz** ajoutent des publicités à votre navigateur, les revenus générés sont distribués à des associations. Passez les filtres adultes sur **Strict** si un jeune enfant accède à votre PC. Cochez ensuite les différents critères (**Ouvrir les liens sortant dans un nouvel onglet**, **Affichez les tendances sur la page d'accueil**, etc.) selon vos goûts. Il est possible de créer un compte Qwant pour sauvegarder les réglages. Sinon, enregistrez le lien en bas du volet et glissez-le dans les favoris.



3 FAITES DE QWANT VOTRE MOTEUR PAR DÉFAUT

Sur Edge, activez le raccourci **Alt + X** puis cliquez sur **Paramètres**, **Avancé**. Dans **Changer de fournisseur de recherche**, sélectionnez **Qwant** puis **Définir par défaut**. Pour afficher le moteur de recherche sur la page d'accueil du navigateur, appuyez sur **Alt+X**, **Paramètres**, **Ouvrir Microsoft Edge avec** et choisissez **Une ou des pages spécifiques**. Collez l'adresse **qwant.com** dans **Indiquer un URL**. Enregistrez les réglages. Avec Chrome, cliquez sur **Personnaliser et contrôler**, **Paramètres**, **Gérer les moteurs de recherche**, puis sur **Autres actions** en bout de ligne. Activez la commande **Utiliser par défaut**.



4 AJOUTEZ DES FAVORIS ET CRÉEZ VOS CARNETS

Cliquez sur **Connexion** et créez un compte Qwant. Quand vous effectuez une requête, pointez sur l'icône des options (trois points) pour ajouter un lien aux favoris ou au carnet. Dans le premier cas, vous retrouverez le lien vers la page suggérée par Qwant dans le volet des favoris, accessible d'un clic sur l'icône en forme d'étoile dans la barre de menu située en haut de la page de recherche. Les carnets sont des dossiers thématiques où vous pouvez ranger les résultats de recherche (pratique pour préparer un exposé par exemple). Cliquez sur l'icône **Menu d'application** puis **Boards** pour les retrouver.

DIFFICULTÉ AUCUNE TEMPS 20 MIN DOMAINE MAINTENANCE

GÉREZ LES EXTENSIONS DÉFAILLANTES

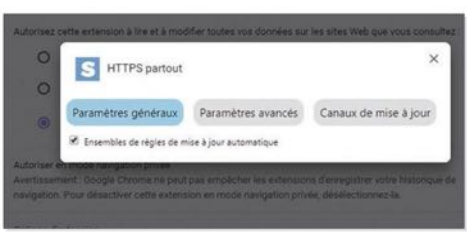
Si les modules additionnels offrent d'enrichir Chrome et Firefox, et d'améliorer l'ergonomie de ces navigateurs, ce sont aussi des sources potentielles de plantages. Pensez à mettre à jour les extensions et à supprimer celles qui ne sont plus d'actualité.

1 DÉSACTIVEZ LES MODULES DANS CHROME

Ouvrez le menu **Personnaliser et contrôler** (l'icône formée de trois points dans le coin droit de la fenêtre du navigateur). Pointez sur **Paramètres**, **Extensions** pour afficher la liste des modules complémentaires intégrés au navigateur. Si vous soupçonnez l'une d'elles d'être à l'origine de ralentissements ou de bugs, commencez par glisser le curseur bleu vers la gauche pour désactiver l'extension. Si les soucis ont disparu, supprimez-la, sinon procédez à sa réactivation. Cliquez sur **Détails** et dans la section **Accès au site** cochez **En cas de clic**. De cette manière, l'extension ne démarrera qu'après que vous ayez pointé sur son icône à droite de la barre d'adresse.

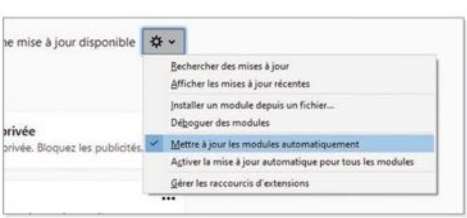
2 MODIFIEZ LES PARAMÈTRES D'UNE EXTENSION

Naviguer en mode anonyme ne vous immunise pas contre les logiciels malveillants ni les publicités. Si vous utilisez une extension liée à votre vie privée ou à la sécurité, calez le curseur **Autoriser en mode navigation privée** sur **Activé**. Certaines extensions sont susceptibles d'enregistrer votre historique de navigation pour leur fonctionnement. Il faut dans ce cas les désactiver durant les sessions de navigation privée. Toujours dans la fenêtre des **Paramètres**, cliquez sur **Options d'extensions** pour découvrir les réglages prévus par le développeur (ne soyez pas surpris si vous ne trouvez rien, tous les modules ne proposent pas d'options spécifiques).



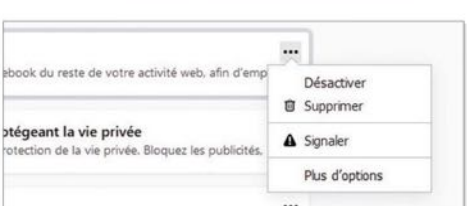
3 VÉRIFIEZ LES PLUG IN INSTALLÉS DANS FIREFOX

Accédez au volet de menu du navigateur de Mozilla et cliquez sur **Modules complémentaires** (ou activez le raccourci **Ctrl** + **Maj** + **A**), puis **Outils pour tous les modules**. Cochez la ligne **Mettre à jour automatiquement les modules**. Si vous avez un doute sur l'efficacité d'une extension, sélectionnez cet élément et prenez connaissance des jugements déposés par les utilisateurs (note, nombre de votants). Il existe un indice encore plus probant : la coupe orange à côté du nom signifie que la fondation Mozilla recommande cette extension. Autorisez-la ensuite, ou non, en mode navigation privée.



4 DÉSACTIVEZ OU SUPPRIMEZ UN ÉLÉMENT

Les modules complémentaires peuvent dissimuler des logiciels malveillants ou, faute de mises à jour, perturber le fonctionnement du navigateur après l'installation d'une nouvelle version de Firefox. Si vous avez un doute sur l'intégrité d'un module, ouvrez le menu d'options en cliquant sur les trois points à droite de son intitulé et choisissez la commande **Désactiver**. Vous craignez d'avoir installé une extension renfermant un malware ? Pointez sur **Signaler**, indiquez le motif de votre démarche et validez par **Suivant**. Pour vous débarrasser d'un module douteux, optez pour la commande **Supprimer**.



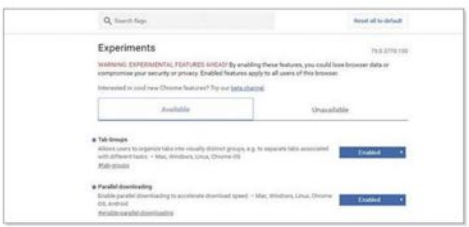
DIFFICULTÉ ÉLEVÉE TEMPS 30 MIN DOMAINE RÉGLAGES

ACCÉDEZ AUX OPTIONS CACHÉES DES NAVIGATEURS

Firefox, Chrome et Edge ne se dévoilent qu'à moitié. En fouillant un peu, vous découvrirez des réglages réservés aux développeurs ou aux experts, dédiés notamment à la sécurité.

1 DÉBLOQUEZ UNE FONCTIONNALITÉ EXPÉRIMENTALE

Avant de mettre les mains dans le cambouis, sachez que ces options sont généralement réservées aux versions bêta des navigateurs et qu'elles se destinent à un public averti. Mal utilisés, certains de ces outils sont susceptibles de provoquer des plantages ou de compromettre la sécurité. Avec Chrome, entrez l'URL **chrome://flags** dans la barre d'adresse et validez avec la touche **Entrée**. Utilisez le champ de saisie **Search flags** pour accéder à des commandes particulières à partir d'un mot-clé. Sélectionnez une fonctionnalité et pointez sur **Disabled**, **Enabled** pour l'activer. En cas de souci, utilisez le bouton **Reset all to defaut** en haut de la page **Experiments**.

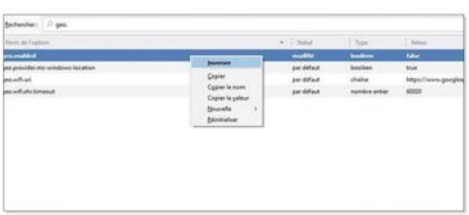


2 OPTIMISEZ LA SÉCURITÉ DE CHROME

Parmi les dizaines de fonctionnalités masquées de Chrome, certaines ont trait à la sécurité du navigateur. Dans la zone de recherche, tapez le terme **Security** et validez par **Entrée**. Repérez la ligne **Allow Signed HTTP Exchange certificates without extension**. Cliquez à droite sur **Default** et optez pour **Disabled**. Validez avec **Relaunch Now**. Cela vous protégera contre les échanges HTTP (connexions non chiffrées) signés avec des certificats sans extension. Activez d'autre part l'option **Enable AppContainer Lockdown** pour accroître la sécurité des processus du bac à sable (virtualisation) dans Windows 10.

3 MAXIMISEZ LA SÛRETÉ DE FIREFOX

Pour accéder aux options et outils cachés de Firefox, saisissez **about:config** dans le champ de recherche et validez avec **Entrée**. Cliquez sur **Je prends le risque**. La valeur **True** signifie que la fonctionnalité est activée, **False** qu'elle ne l'est pas. Pour éviter qu'un logiciel malveillant n'arrive sur votre PC par le biais de code JavaScript, recherchez la ligne **javascript.enabled**. Opérez un clic droit sur la barre bleue et pointez sur **Inverser**. Attention, cette option risque de bloquer l'affichage de certains sites Web un peu anciens. Pour stopper la géolocalisation, passez la commande **geo.enabled** sur **False**.



4 MASQUEZ VOTRE ADRESSE IP DANS EDGE

Le navigateur de Windows 10 dispose lui aussi d'un menu caché dont l'accès s'effectue en renseignant **about:flags** dans la barre d'adresses. Afin d'optimiser la confidentialité de vos échanges en ligne, cochez l'option **Masquer mon adresse IP locale sur les connexions WebRTC (communications en temps réel)**. Veillez par ailleurs à ce que la commande **Activer les fonctionnalités JavaScript expérimentales** soit bien désactivée. Si votre PC ne possède pas d'écran tactile, décochez la ligne **Activer la navigation à l'aide du stylet tactile et la Sélection du bouton du stylet**.

DIFFICULTÉ MODÉRÉE TEMPS 30 MIN DOMAINE AUTHENTIFICATION

PASSEZ À LA DOUBLE AUTHENTIFICATION

L'usurpation d'identité sur les réseaux sociaux et le piratage des comptes mails s'étendent comme une traînée de poudre. Pour lutter contre ce fléau, les services proposent un dispositif de sécurité renforcé, dit à double facteur, destiné à vérifier votre identité lors des tentatives de connexion depuis un nouvel appareil.

1 PROTÉGEZ VOTRE COMPTE MICROSOFT

Connectez à votre compte habituel (**bit.ly/2LD8nT4**). Dans la section **Sécurité**, cliquez sur **Mise à jour, Mettre à jour mes informations, Ajouter des informations de sécurité**. Indiquez votre numéro de mobile si ce n'est pas déjà fait et confirmez-le à l'aide du code reçu par SMS. Retournez sur la page **Options de sécurité supplémentaire** et cliquez sur **Configurer la vérification en deux étapes, Suivant, Terminer**. Déconnectez-vous et tentez de vous reconnecter sur un autre appareil. Votre numéro de téléphone sera désormais exigé pour vous identifier. Pour supprimer la double activation, retournez dans les paramètres de sécurité.

2 SÉCURISEZ VOS INFORMATIONS GOOGLE

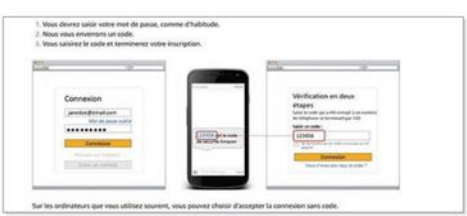
Google propose lui aussi un dispositif de ce type. Connectez-vous à votre compte (**bit.ly/2JBanai**) et pointez sur l'onglet **Sécurité** dans le volet gauche de la page d'accueil. Dans la section **Méthodes pour nous permettre de vérifier votre identité**, ajoutez un numéro de téléphone de récupération, puis revenez en arrière. La validation en deux étapes s'active automatiquement. Si vous avez renseigné plusieurs appareils, vous pouvez choisir celui à utiliser lors de la demande de connexion. Votre mobile est requis pour authentifier les connexions. Google va plus loin avec la possibilité d'utiliser des codes de secours à usage unique ou une clé de sécurité physique.

3 SURPROTÉGEZ VOS IDENTIFIANTS FACEBOOK

Depuis votre compte Facebook, cliquez sur la petite flèche en haut à droite et choisissez **Paramètres, Général**. Pointez sur **Contact, Ajouter une autre adresse e-mail ou un autre numéro de téléphone, Ajouter votre numéro de téléphone**. Confirmez le numéro en choisissant l'option d'envoi d'un SMS ou en vous faisant rappeler par une boîte vocale. Une fois l'opération effectuée, allez sur **Sécurité et connexion, Utiliser l'authentification à deux facteurs** et suivez la procédure d'activation. Dans **Connexions autorisées**, vous pouvez supprimer les appareils que vous n'utilisez plus.

4 CONNECTEZ-VOUS SEREINEMENT À AMAZON

Le géant du commerce en ligne ne transige pas avec la sécurité de ses clients. Il a adopté des mesures strictes, mais qui demeurent optionnelles. Pour les activer, pointez sur **Votre compte** dans **Compte et listes**, puis sur **Connexion et paramètres de sécurité**. Indiquez votre numéro de téléphone portable et validez par **Terminer**. Pointez sur **Modifier** dans la section **Paramètres de sécurité avancés**. Déroulez l'assistant de vérification en deux étapes après avoir cliqué sur **Pour commencer**. Vous serez notamment invité à renseigner un code de validation envoyé sur votre mobile.



DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE TÉLÉCHARGEMENT

ANALYSEZ LES FICHIERS AVANT DE LES OUVRIR SUR VOTRE PC

Attention, danger. N'installez pas un logiciel téléchargé sur Internet sans l'avoir analysé avec un antivirus. Une précaution indispensable pour éviter les soucis.

1 VÉRIFIEZ L'INTÉGRITÉ DES TÉLÉCHARGEMENTS

Un logiciel malveillant peut se cacher dans n'importe quel fichier rapatrié sur votre PC et s'activer discrètement lorsque vous lancerez l'application ou ouvrirez un document Word. Pour être certain qu'il ne contient pas de menace, lancez l'Explorateur de fichiers et ouvrez le dossier des téléchargements. Faites un clic droit sur l'élément à inspecter et pointez sur **Analyser avec Windows Defender** ou si vous n'utilisez pas la solution de sécurité de Microsoft, le lien vers votre logiciel antivirus (Avast, BitDefender, etc.).

2 OPTIMISEZ LES PARAMÈTRES DE VOTRE NAVIGATEUR

Dans la section **Téléchargements** des paramètres avancés de Chrome, activez le curseur **Toujours demander où enregistrer les fichiers** de façon à copier les éléments douteux dans un dossier de quarantaine que vous analyserez avec votre antivirus. Dans **Réinitialiser et nettoyer**, **Nettoyer l'ordinateur**, vérifiez l'intégrité du navigateur. Avec Firefox, activez les options du menu **Vie privée et sécurité**, **Sécurité**. Dans **Permissions**, cochez **Prévenir lorsque les sites essaient d'installer des modules complémentaires**.

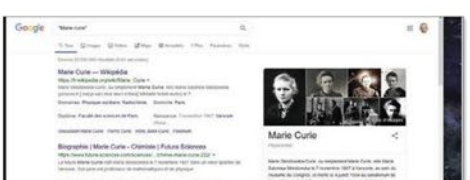
DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE VIE PRIVÉE

FAITES LE BILAN DE VOTRE RÉPUTATION EN LIGNE

Que révèle Internet de votre personne ? Pour le savoir, appliquez les méthodes de recherche ad hoc.

1 GOOGLELISEZ-VOUS

La première chose à effectuer consiste simplement à saisir nom et prénom encadré par des guillemets dans le champ de recherche de Google. Déroulez les résultats et pointez sur les sites qui parlent de vous. Utilisez les filtres **Actualités**, **Images**, **Vidéos** pour restreindre la liste à des contenus spécifiques. Le contenu des deux dernières rubriques risque de vous surprendre ! Si d'anciennes photos ou vidéos vous paraissent inappropriées, n'hésitez pas à demander leur retrait en vous rendant sur le site **bit.ly/2NMISkE**.



2 FAITES APPEL À UN SERVICE SPÉCIALISÉ

Sollicitez WebMii (**bit.ly/2JHDkBB**) pour tester en profondeur votre réputation en ligne. Outre un score de visibilité, vous accéderez à une foule d'informations. Déclinez simplement votre identité et découvrez votre profil public (photos, réseaux sociaux, etc.).Pour être informé dès qu'une publication vous mentionne, créez une alerte Google (**bit.ly/2LiAG8o**), saisissez vos nom et prénom, ouvrez le menu **Afficher les options** et choisissez **Quand le cas se présente** et **Tous les résultats**. Validez avec **Créer l'alerte**.

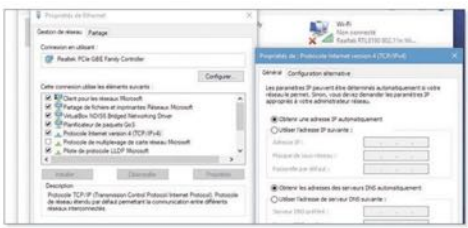
DIFFICULTÉ MODÉRÉE TEMPS 10 MIN DOMAINE VIE PRIVÉE

ADOPTEZ UN DNS RAPIDE ET TRÈS DISCRET

Le choix du DNS peut accélérer le temps de chargement des pages et la confidentialité. Ces annuaires font le lien entre les adresses Web que vous soumettez à votre navigateur et les serveurs où sont hébergés les sites.

1 ACCÉDEZ AUX PROPRIÉTÉS DNS DE VOTRE PC

Lorsque vous naviguez sur Internet, votre fournisseur d'accès vous connecte à des serveurs DNS. Et pour être sincère, il met tout en œuvre pour que vous n'ayez pas accès à ces données pour vous imposer son choix. Pour connaître les coordonnées du DNS défini par Windows 10, faites un clic droit sur l'icône **Réseau** dans la barre des tâches et pointez sur **Ouvrir les paramètres réseau et internet**. Sous **Modifier vos paramètres réseau**, optez pour **Modifier les options de l'adaptateur**. Opérez un clic droit sur la connexion (Ethernet par exemple), puis sur **Propriétés**. Sélectionnez **Internet Protocol Version 4 (TCP/IPv4)** et pointez sur **Propriétés**.



2 AFFICHEZ LES PRÉFÉRENCES RÉSEAU SOUS MACOS

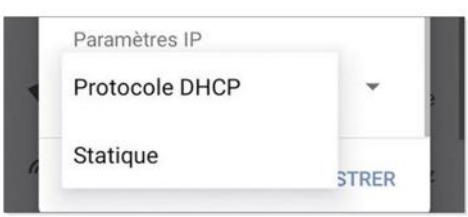
Pour connaître l'état de votre configuration réseau, accédez aux Préférences Système de macOS, soit en cliquant sur l'icône présente dans le Dock, soit en déroulant le menu **Pomme**, **Préférences Système**. Ouvrez la section **Réseau**. L'écran qui s'affiche fait apparaître les différentes connexions disponibles sur l'ordinateur. Sélectionnez celle que vous utilisez prioritairement (Wifi ou Ethernet), pointez sur le bouton **Avancé** au bas de l'écran. Activez l'onglet **DNS**. Si vous avez activé le mode **DHCP**, une seule adresse est mentionnée. Si rien ne s'affiche, c'est la configuration par défaut de votre fournisseur d'accès Internet qui prévaut.

3 IMPOSEZ LES ADRESSES DES SERVEURS D'OPENDNS

Pour modifier les serveurs DNS par défaut, il faut déjà identifier des solutions alternatives. Pour cela, lancez votre navigateur Internet et connectez-vous au service OpenDNS (**bit.ly/315kQBU**). Ce service propose des offres cloud et DNS qui peuvent être utilisées gratuitement. Faites défiler les informations de la page d'accueil pour trouver les deux adresses des serveurs DNS. Notez ces informations, puis répétez les manipulations décrites dans les deux étapes précédentes. Remplacez alors les coordonnées des serveurs DNS par les adresses IP fournies par OpenDNS.

4 MODIFIEZ AUSSI LES RÉGLAGES SOUS ANDROID

Les mobiles et les tablettes font également appel à des DNS pour accéder à Internet. Comme sur un ordinateur, ces paramètres peuvent être modifiés. Déployez le volet des notifications de votre smartphone Android et effleurez l'icône **Paramètres**. Touchez ensuite les intitulés **Réseau & Internet**, Wi-Fi. Appuyez longuement sur le nom du réseau Wifi et activez la commande **Options Avancées**. Sous **Paramètres IP**, effleurez **Protocole DHCP**, puis dans le volet qui se déploie, **Statique**. Saisissez les adresses des serveurs DNS d'OpenDNS dans les champs **DNS1** et **DNS2** et enregistrez les réglages.



DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE NAVIGATION

SURFEZ VRAIMENT INCOGNITO AVEC TOR BROWSER

Tor est un réseau décentralisé qui offre la possibilité de naviguer de façon anonyme. Le projet a donné naissance à Tor Browser, un navigateur basé sur le moteur de Firefox qui fait la place belle aux impératifs de confidentialité.

1 ÉQUIPEZ-VOUS DU NAVIGATEUR ADÉQUAT

Pour installer Tor Browser sur votre PC Ubuntu, vous pouvez recourir au Terminal et saisir la commande **sudo apt-get install torbrowser-launcher**. Si vous n'êtes pas à l'aise avec les lignes de commande, cliquez sur l'icône **Logiciels Ubuntu** dans le lanceur, tapez **Tor Browser** dans le champ de recherche. Pointez sur le nom de l'appli dans les résultats, puis sur **Installer**. Au besoin, entrez le mot de passe du compte administrateur. Au terme de l'installation, cliquez sur le bouton **Lancer**. Tor Browser est prêt.

2 NAVIGUEZ EN TOUTE DISCRÉTION

Le premier lancement de Tor Browser donne lieu au téléchargement d'un certain nombre de composants (environ 100 Mo de données). Patientez le temps nécessaire au transfert. Finalisez l'opération d'un clic sur **Install Tor Browser**. Une clé de chiffrement est générée. Par la suite, au lancement du navigateur, les outils Tor et Vidalia sont lancés automatiquement, assurant l'anonymisation des données et leur chiffrement à l'intérieur du réseau Tor. Avec Tor Browser, vous naviguez classiquement, mais sans laisser de trace.

DIFFICULTÉ AUCUNE TEMPS 10 MIN DOMAINE VIE PRIVÉE

EXERCEZ VOTRE DROIT À L'OUBLI NUMÉRIQUE

Les réseaux sociaux disposent tous d'une page dédiée pour les demandes de retrait de certains contenus privés.

1 DEMANDEZ L'EFFACEMENT À FACEBOOK ET TWITTER

Google n'est pas le seul à proposer la suppression d'infos personnelles dans le cadre du RGPD *(lire p. 69)*. Les autres ténors d'Internet lui ont emboîté le pas. C'est le cas de Facebook. Accédez à la page **bit.ly/2XMNZjg**. Sélectionnez l'objet de votre requête dans la liste et suivez les indications de signalement portées à l'écran. Le réseau social se chargera de faire disparaître le contenu abusif ou indésirable. Si vous êtes utilisateur de Twitter, utilisez le lien suivant pour demander la suppression d'une publication (**bit.ly/2KY7TDn**).

2 FAITES DE MÊME AVEC INSTAGRAM, SNAPCHAT ET LINKEDIN

Respecter le RGPD est un impératif pour les réseaux sociaux sous peine de poursuites. Pour supprimer une image affichée sur Instagram, suivez le lien **bit.ly/2G5qjkj**. Indiquez que vous possédez un compte et répondez aux questions posées. Avec Snapchat, contactez le support (**bit.ly/32IC6o0**) et indiquez le type de problème rencontré. Sur YouTube, la procédure de réclamation de la vie privée s'effectue sur la page **bit.ly/2JCpfFv**. Quant à LinkedIn, la réclamation devra être effectuée en anglais sur le site **bit.ly/2GclKoh**.

DIFFICULTÉ MODÉRÉE TEMPS 30 MIN DOMAINE VIE PRIVÉE

ÉVITEZ DE VOUS EXPOSER SUR LES RÉSEAUX SOCIAUX

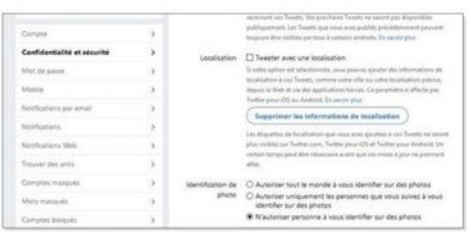
Quand on sévit sur Facebook, YouTube ou Twitter, mieux vaut prendre quelques précautions pour préserver un peu sa vie privée. Plongez dans les paramètres de confidentialité des réseaux sociaux pour choisir quoi publier et qui le verra.

1 RÉGLEZ LA CONFIDENTIALITÉ SUR FACEBOOK

Pour ne pas qu'une image un peu trop personnelle ne tombe entre les mains d'un recruteur, optez pour une diffusion ciblée. Cliquez sur la flèche noire en haut à gauche puis sur **Paramètres**, **Confidentialité**, **Qui peut voir vos futures publications**. Déroulez le menu à droite de **Publier** et optez pour **Amis**. Si vous ne souhaitez pas que tous voient vos contributions, accédez à **Amis sauf** et retirez certains contacts de la liste. Pour agir sur une publication existante, allez sur votre page et sélectionnez le message ou la photo concerné. Pointez sur la liste à droite de la date de publication et remplacez le paramètre **Public** par **Amis**.

2 TWEETEZ EN TOUTE DISCRÉTION

Twitter ne cesse d'étoffer ses paramètres de confidentialité. Cliquez sur votre avatar et sur **Paramètres et confidentialité**, **Confidentialité et sécurité**. Une bonne façon de protéger votre vie privée consiste à protéger les tweets afin que seules les personnes habilitées puissent les lire. Désactivez la localisation, puis dans **Identification de photo**, optez pour **N'autoriser personne à vous identifier sur des photos**. Dans **Messages privés**, décochez **Recevoir** pour interdire aux inconnus de vous envoyer des messages. Dans **Détectabilité**, empêchez que l'on vous trouve grâce à votre mail ou numéro de téléphone. Validez avec **Enregistrer les modifications**.



3 PRENEZ EN MAIN VOTRE VIE NUMÉRIQUE SUR INSTAGRAM

Il est facile de suivre et d'être suivi par n'importe qui. Ouvrez l'appli sur votre téléphone et effleurez les traits horizontaux à droite. Pointez sur **Paramètres**, **Confidentialité**. Dans **Confidentialité du compte**, optez pour **Privé**. Seules les personnes approuvées pourront ainsi voir vos photos. Allez sur **Identifications** et décochez l'option **Ajouter automatiquement** pour maîtriser la publication sur votre profil. Accédez au menu **Story**, désactivez le choix des lieux et autorisez les messages venant de vos seuls abonnés. Évitez le repartage dans les stories ainsi que le partage de vos photos et vidéos.

4 GÉREZ LA CONFIDENTIALITÉ DES VIDÉOS YOUTUBE

À partir du moment où vous créez une chaîne YouTube, vous vous exposez en ligne. Pour limiter la visibilité de vos vidéos, pointez sur votre avatar à droite puis sur **Paramètres**. Accédez à **Confidentialité**, activez les options **Garder privées** pour ne pas afficher vos abonnements et mentions **J'aime**. Pour vous réserver l'accès à une vidéo, cliquez sur **Version bêta de YouTube Studio** depuis votre avatar. Allez sur **Vidéos**, **Visibilité**, déroulez la liste **Publique** et optez pour **Privée**. Validez avec **Enregistrer**. Pour effacer une vidéo, pointez sur les points à droite de son nom et choisissez **Supprimer**.

ABONNEZ-VOUS !

01NET

Bulletin d'abonnement à retourner sous enveloppe non affranchie à :

01net - Service abonnements - Libre réponse 43420 - 60439 Noailles Cedex
Par e-mail: abonnement.01net@groupe-gli.com ou par tél.: 01 70 37 31 74 (N° non surtaxé)

Je choisis la formule de mon choix :

- ❑ **1 an à 01net + sa version digitale** pour **59** au lieu de ~~85,80 €*~~ (soit près de 31% de réduction)
- ❑ **1 an à 01net + ses 6 Hors-séries + sa version digitale** pour **79** au lieu de ~~118,80 €*~~ (soit près de 33% de réduction)

A19H112

Plus simple, plus rapide, je m'abonne en un clic avec mon code partenaire A19H112 www.kiosque01.fr

Je règle par :

- ❑ Chèque bancaire à l'ordre de **01net**
- ❑ Carte bancaire (CB, Visa, Mastercard)

N° | | | | | | | | | | | | | | | | |

Expire n | | | | Date et signature obligatoires

Mes coordonnées: ❑ Mme ❑ M.

Nom: .....

Prénom: .....

Adresse: .....

Code postal | | | | | |

Localité: .....

Tél.: | | | | | | | | | | |

Date de naissance | | | | | | | | |

E-MAIL OBLIGATOIRE POUR RECEVOIR LA VERSION DIGITALE

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

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

* Prix de vente au numéro. Offre valable jusqu'au 31/12/2019 pour les nouveaux abonnés en France métropolitaine uniquement. L'Editeur s'engage à livrer votre magazine sous un délai maximum de 5 semaines. Conformément à l'article L221-18 du code de la consommation, vous bénéficiez d'un délai de rétractation de 14 jours à compter de la réception du premier numéro de l'abonnement. Pour faire jouer ce droit, vous pouvez télécharger le formulaire sur notre site www.kiosque01.fr/retractation et nous l'envoyer à : 01net Mag - Service Abonnements - 4, rue de Mouchy 60438 Noailles Cedex.

Les informations 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.

Siège social : 01net Mag - 2 rue du Général Alain de Boissieu 75015 Paris - SARL au capital de 10 000 - RCS Paris 799 351 341

DIFFICULTÉ MODÉRÉE TEMPS 30 MIN DOMAINE NETTOYAGE

FAITES LE MÉNAGE AVANT DE CÉDER VOTRE ORDINATEUR

Quand vous donnez ou vendez votre PC, prenez soin de supprimer toutes les données personnelles qu'il renferme : fichiers, comptes de messagerie, historique de navigation et applications.

1 SAUVEGARDEZ VOS FICHIERS

À condition de disposer de la fibre et de suffisamment d'espace de stockage, la solution idéale consiste à copier les fichiers sur le Cloud. Les titulaires d'un abonnement à Office 365 profitent ainsi d'une dotation de 1 To, de quoi accueillir musique, photos, documents de travail et même des vidéos. L'espace offert avec les offres gratuites de Drive, Dropbox, iCloud ou OneDrive s'avère en revanche trop juste. Il faut alors se tourner vers un disque dur externe. Vous trouverez des modèles USB d'une capacité de 3 To à 5 To pour moins de 100 €. Une fois la sauvegarde effectuée, supprimez les données du PC et videz la corbeille pour empêcher leur restauration.

2 EFFACEZ VOS TRACES ET DÉSINSTALLEZ LES APPLICATIONS

Si vous cédez l'ordinateur à un membre de la famille, il peut être utile de conserver certains programmes. Installez l'utilitaire Privazer (**bit.ly/2Gb890D**) et lancez une analyse en profondeur du contenu du disque dur. Attendez que le rapport s'affiche à l'écran et désignez les éléments dont vous souhaitez vous débarrasser (historique de navigation, cookies, registre, cache, etc.). Déconnectez-vous des applications liées à un compte personnel (Outlook, Netflix, Deezer, Dropbox, etc.) et utilisez ensuite IObit Uninstaller (**bit.ly/2OWI3oE**) pour désinstaller les logiciels qui nécessitent une clé d'activation et que vous envisagez de réimplanter sur votre nouvel ordinateur.

3 RÉINITIALISEZ WINDOWS 10

Un simple nettoyage se révèle insuffisant si vous choisissez de revendre votre PC à un inconnu. Pour vous assurer qu'aucun fragment de votre vie privée ne subsiste, nous vous conseillons de réinitialiser l'ordinateur. Microsoft a d'ailleurs intégré cette option dans Windows 10. Accédez aux paramètres à l'aide du raccourci clavier **Windows + I** et dirigez-vous vers **Mise à jour et sécurité**, **Récupération**. Dans **Réinitialiser ce PC**, cliquez sur **Commencer**, **Supprimer tout**. Désignez les disques durs dont vous souhaitez effacer le contenu et continuez avec **Supprimer les fichiers et nettoyer le lecteur**.

4 PRÉPAREZ VOTRE MAC POUR LA REVENTE

Les ordinateurs d'Apple conservent une cote élevée sur le marché de l'occasion. Vous n'aurez aucun mal à trouver preneur. Avant de le céder, transférez son contenu sur votre nouveau Mac avec l'assistant de migration de macOS. Procédez ensuite à un nettoyage minutieux au moyen du logiciel CleanMyMac X (**bit.ly/2JkwzbK**). Pour aller plus loin et effacer toutes vos traces, démarrez votre Mac en gardant les touches **cmd + R** enfoncées. Choisissez **Utilitaire de disque**, **Effacer**, **Effacer** pour formater le disque système. Fermez la fenêtre de l'utilitaire de disque (**cmd+Q**) et pointez sur **Réinstaller macOS**.

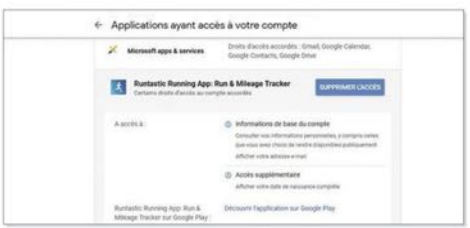
DIFFICULTÉ MODÉRÉE TEMPS 30 MIN DOMAINE APPLIS

GÉREZ LES AUTORISATIONS ACCORDÉES AUX SERVICES

Quand vous vous connectez à une application ou à un service en utilisant votre compte Google, Facebook ou Microsoft, vous donnez accès à certaines données personnelles. Il serait peut-être temps de faire le point sur ces autorisations.

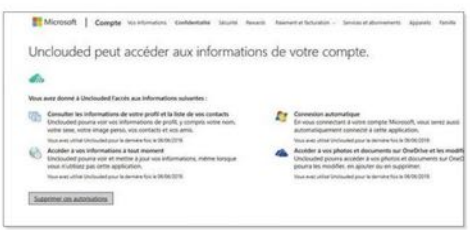
1 VÉRIFIEZ LES ACCÈS À VOTRE COMPTE GOOGLE

Plutôt que de créer un compte spécifique, de nombreux services en ligne proposent d'utiliser vos identifiants Google ou Facebook. Une procédure rapide qui expose toutefois vos données. Pour faire le point sur les autorisations, connectez-vous à l'espace de gestion de votre compte Google (**bit.ly/2Y0chq8**). Ouvrez l'onglet **Sécurité** à gauche, puis pointez sur la commande **Gérer les accès tiers** dans la section **Applications tierces ayant accès à votre compte**. Parcourez la liste des services qui bénéficient d'une autorisation. Si vous repérez un élément dont vous n'avez plus l'usage, dissociez-le de votre compte Google avec **Supprimer l'accès**.



2 METTEZ DE L'ORDRE DANS LES AUTORISATIONS MICROSOFT

Connectez-vous à votre compte (**bit.ly/2Gl1QaR**). Vous trouverez les informations liées aux autorisations accordées aux services tiers et aux applications dans la section **Confidentialité**, **Vue d'ensemble**. Déroulez ce menu vers le bas jusqu'à la rubrique **Autres paramètres de confidentialité**. Cliquez sur **Applications et services autorisés à accéder à vos données** à droite. Un tableau dresse alors la liste complète des acteurs qui ont accès à votre compte. Il est probable que certains de ces liens ne soient plus d'actualité (Microsoft indique la nature et la date du dernier accès). N'hésitez pas à révoquer les privilèges devenus obsolètes (**Supprimer ces autorisations**).

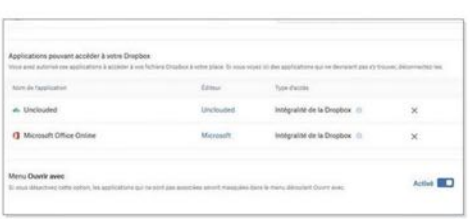


3 LISTEZ LES SERVICES ASSOCIÉS À FACEBOOK

Quand vous utilisez Facebook pour accéder à un service tiers, celui-ci peut visualiser certaines données privées mémorisées sur le réseau social. Pour faire le point sur ces autorisations, cliquez sur la flèche noire située à droite de la barre de menus de la page d'accueil de Facebook, puis sur **Paramètres**, **Apps et sites web** en colonne gauche. La liste des services et sites actifs apparaît. Si vous souhaitez mettre fin à certains de ces liens, cochez la case devant leurs intitulés et validez avec **Supprimer**. Vous retrouvez la trace des autorisations récemment révoquées dans le menu **Supprimé**.

4 EXAMINEZ LES ACCÈS À DROPBOX ET TWITTER

Vous pouvez être amené à ouvrir un accès aux données de votre Cloud. C'est le cas, par exemple, quand vous créez un script avec les services d'automatisation IFTTT ou Flow de Microsoft. Accédez à votre compte Dropbox, pointez sur votre avatar à droite et dirigez-vous vers **Applications connectées**. Dans la partie **Applications pouvant accéder à votre Dropbox**, cliquez sur le bouton **X** pour suspendre l'autorisation. Validez avec **Déconnecter**. Dans le cas de Twitter, allez sur **Plus** en colonne gauche, **Paramètres et confidentialité**, **Données et autorisations**, **Applications et sessions**.



DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE PARTAGE

ÉCHANGEZ DES FICHIERS SANS RISQUE SUR LE CLOUD

Les services de stockage en ligne ont changé la vie des utilisateurs. Il n'est plus nécessaire de penser à sauvegarder ses fichiers ou de s'encombrer d'une clé USB quand on voyage ou que l'on jongle entre plusieurs ordinateurs. Le partage de documents s'en trouve également facilité.

Boîte à outils

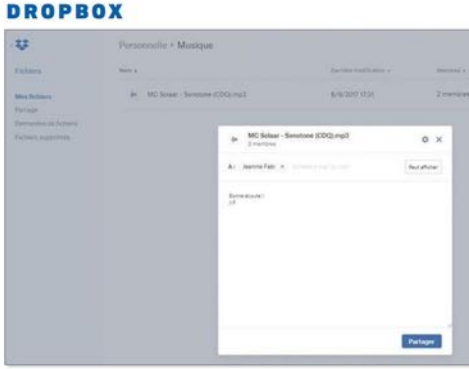
Pour ce pas à pas, nous avons utilisé les éléments suivants :

- Un ordinateur PC ou un mac
- Un smartphone
- Un compte Dropbox, Google Drive ou OneDrive
- Internet

Le cloud transforme en profondeur la façon dont nous appréhendons l'accès aux données. Qu'il s'agisse de conserver des éléments professionnels ou personnels, le stockage physique s'efface peu à peu au pro t de disques durs virtuels. Documents, photos, musique et vidéos sont dorénavant hébergés sur des serveurs distants gérés par les services cloud.

Dès lors que nos chiers se trouvent dans un dossier synchronisé, plus besoin de se préoccuper de la santé de nos disques durs. Les data centers de Dropbox, OneDrive ou Google Drive sont protégés des intrusions, comme des pannes matérielles et des défaillances logicielles. Duplication des données, redondance des composants (processeurs, disques durs, alimentation), tout est fait pour assurer une disponibilité 24h/24, 7j/7. Les acteurs du cloud assurent aussi la con dentialité des chiers que vous leur con ez. Ceux-ci sont chiffrés et lisibles par vous seul. Vous pouvez par ailleurs verrouiller l'accès à votre compte en activant un dispositif d'authenti cation en deux temps. Un code à usage unique sera alors envoyé sur votre mobile a n de con rmer les tentatives d'identi cation effectuées depuis un nouvel appareil *(lire p. 79)*. Le cloud simpli e en n le partage des chiers. Là encore, en toute sécurité.●

DROPBOX

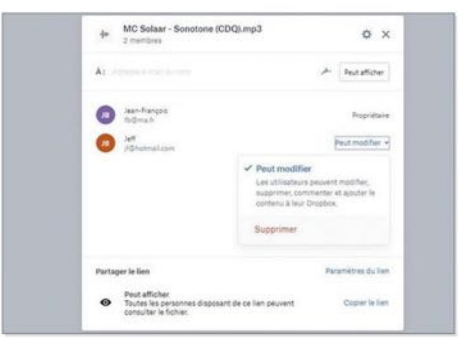


1 ACTIVEZ LE PARTAGE DEPUIS L'INTERFACE WEB

Allez sur **dropbox.com** et identifiez-vous. Affichez l'onglet **Fichiers**, survolez avec le curseur de la souris le nom de l'élément que vous souhaitez rendre accessible à vos proches et cliquez sur le bouton **Partager**. Indiquez l'adresse mail des personnes qui recevront une invitation accompagnée d'un lien vers la ressource mise en commun. Ajoutez un message et validez l'envoi avec **Partager**. Si vous préférez utiliser un autre biais que le mail pour lancer l'invitation (Skype par exemple), activez la commande **Créer un lien** au bas de la fenêtre puis **Copier le lien** pour l'ajouter dans le presse-papiers. Il ne vous reste plus qu'à le coller à l'aide du raccourci **Ctrl + V** dans le corps du message ou à le transmettre via Skype, par exemple.

2 PARAMÉTREZ LES PROPRIÉTÉS DU LIEN DE PARTAGE

Si vous disposez d'un compte Dropbox Premium ou Entreprise, vous pouvez définir les règles de partage des fichiers. Pointez pour cela sur **Paramètres du lien**. Déroulez le menu **Toute personne disposant**... dans la section **Accès** et optez pour **Toute personne disposant du mot de passe** pour verrouiller l'accès au fichier. Il est également possible de limiter la validité du lien dans le temps ou d'interdire le téléchargement du document par les invités. La procédure est identique pour partager un dossier. Par défaut, les personnes qui ont accès à cet emplacement sont habilitées à supprimer ou ajouter des éléments (**Peut modifier**). Pour révoquer ce privilège, activez le mode **Peut afficher**.



3 GÉREZ LES RESSOURCES MISES EN COMMUN

La colonne **Membres** mentionne le nombre de personnes autorisées à accéder à vos contenus. Si vous changez d'avis, déroulez le menu d'option du dossier ou du fichier et cliquez sur **Partager**. Ouvrez le menu **Peut modifier** ou **Peut afficher** à droite du nom du contact dont vous souhaitez révoquer les droits, pointez sur **Supprimer** et validez. Allez sur l'onglet **Partage** du volet de navigation de Dropbox pour visualiser les ressources mises à disposition par vos contacts. Le partage peut aussi s'opérer directement depuis l'Explorateur de fichiers de Windows. Installez l'appli Dropbox Desktop (**bit.ly/2ypbo0d**) et associez-la à votre compte. Paramétrez ensuite la synchronisation des dossiers.

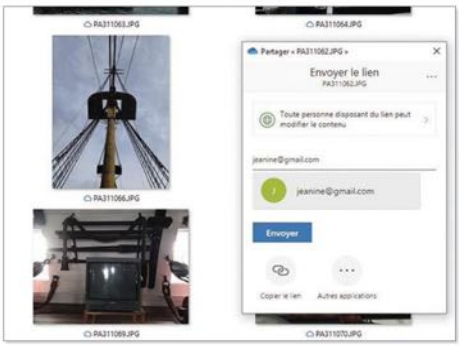
4 ÉCHANGEZ DEPUIS WINDOWS OU UN MOBILE

Ouvrez l'Explorateur de fichiers de Windows. Déroulez la section **Dropbox** du volet de navigation pour afficher la liste des éléments synchronisés. Faites un clic droit sur un dossier ou un document et activez la commande **Partager** dans la rubrique **Dropbox** du menu contextuel. Sur votre téléphone, assurez-vous d'avoir installé l'appli Dropbox pour Android ou iOS. Identifiez-vous, touchez les trois points à droite du nom de la ressource et **Partager** (vous pouvez aussi utiliser le lien **Partager avec Dropbox** qui apparaît dans le menu de partage des applications). Revenez au menu contextuel, pointez sur **Gérer l'accès** pour annuler le partage d'un dossier ou mettre fin aux privilèges accordés à l'un ou l'autre de vos contacts.

ONEDRIVE

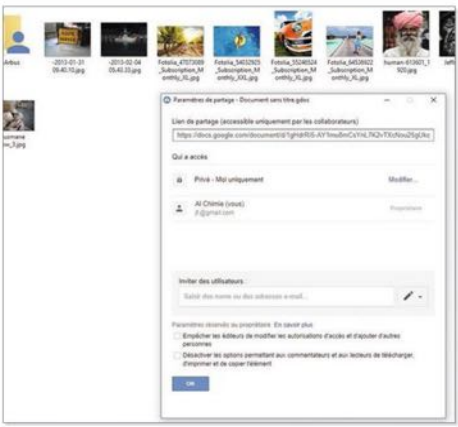
1 RECOUREZ À LA WEB APP

Le cloud rend vos données accessibles depuis n'importe quel ordinateur, y compris quand il s'agit d'un matériel d'emprunt. OneDrive propose une interface Web très complète. Allez sur **onedrive.live.com** et saisissez vos identifiants Microsoft. Activez l'onglet **Fichiers**, sélectionnez un dossier et pointez sur **Partager**. Déroulez la liste **Toute personne disposant du lien peut**... et définissez une date d'expiration pour le partage ou un mot de passe pour contrôler les accès. Indiquez ensuite les adresses mails des contacts qui seront autorisés à afficher vos contenus et validez par **Envoyer** ou cliquez sur **Copier le lien** pour émettre des invitations via Skype ou une messagerie instantanée.



2 UTILISEZ L'EXPLORATEUR DE FICHIERS DE WINDOWS

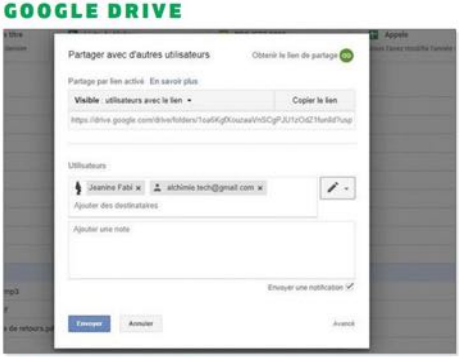
Sans surprise, OneDrive s'intègre parfaitement dans Windows 10. Votre disque dur virtuel est accessible dans l'Explorateur de fichiers sans que vous ayez à faire quoi que ce soit. Pointez sur l'intitulé **OneDrive** du volet de navigation pour afficher la liste des éléments conservés dans le cloud. Faites un clic droit sur l'un d'eux et choisissez **Partager**. Déclinez l'identité de vos invités ou copiez le lien de partage dans le presse-papiers. La marche à suivre est identique avec l'application mobile OneDrive, qui se décline sous Android et iOS. Il suffit d'effleurer la commande **Partager** du menu des options d'un document ou d'un dossier.



2 INTÉGREZ GOOGLE DRIVE À WINDOWS

Sur la page **bit.ly/2XkbWPj**, cliquez sur **Télécharger Sauvegarde et synchronisation**. Une fois l'appli installée, une section Google Drive est ajoutée à l'Explorateur de fichiers de Windows. Ce raccourci donne accès au contenu du disque dur virtuel. Faites un clic droit sur un dossier ou un fichier, déroulez le menu **Google Drive**, **Partager** et pointez sur **Obtenir le lien de partage**.

GOOGLE DRIVE



1 OPÉREZ DEPUIS LE WEB

Ouvrez votre navigateur Internet et allez sur la page **www.google.com/drive**. Identifiez-vous. Cliquez sur **Mon Drive** pour retrouver le contenu de votre cloud et sélectionnez un fichier ou un dossier. Pointez sur l'icône **Obtenir le lien partageable** ou **Partager** (une silhouette surmontée du symbole +) sous le champ de recherche. Dans le premier cas, vous êtes invité à saisir l'adresse mail des bénéficiaires. Cliquez sur l'icône en forme de stylo et indiquez si vos invités pourront modifier ou seulement consulter les données.

3 PROCÉDEZ DEPUIS VOTRE SMARTPHONE

L'application Google Drive est installée par défaut sur les téléphones Android. Touchez son icône sur l'écran d'accueil, puis déroulez le volet d'options d'un dossier ou d'un fichier. Effleurez la commande **Partager** pour envoyer un lien par mail. Indiquez les contacts, ajoutez un message et validez en pointant sur la flèche en haut à droite. Si vous préférez obtenir une URL vers le fichier et la diffuser par d'autres moyens, appuyez sur l'intitulé **Partager par lien** puis sur l'intitulé **Copier le lien**.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE PARTAGE

RENFORCEZ LA SÉCURITÉ DU CLOUD

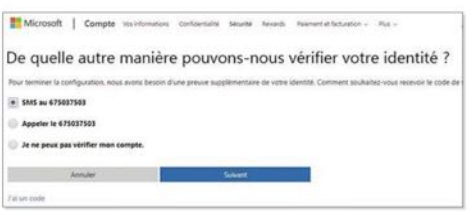
Vous n'envisagez pas de laisser votre PC sans défense ? Accessibles depuis Internet, les données confiées au cloud sont bien plus exposées que votre disque dur. Redoublez de prudence !

1 DRESSEZ DES BARBELÉS AUTOUR DE DROPBOX

Accédez à votre espace personnel sur **Dropbox.com**. Cliquez sur votre avatar en haut de la fenêtre, puis sur **Paramètres**. Placez-vous sur l'onglet **Sécurité** et pointez sur **Modifier le mot de passe** pour définir un code secret fort. Activez le dispositif de validation en deux étapes et choisissez le dispositif qui sera utilisé pour vérifier les accès opérés depuis un nouvel appareil (un code envoyé par SMS sur votre mobile par exemple). Pour dissocier un ordinateur ou un mobile de votre compte Dropbox, revenez sur l'onglet **Sécurité** et cochez l'option **Supprimer les fichiers** dans la section **Appareils**.

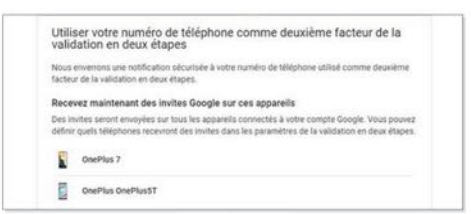
2 PROTÉGEZ VOTRE COMPTE ONEDRIVE

Vous ne trouverez pas de réglages liés à la sécurité dans les paramètres du cloud de Microsoft. L'éditeur a en effet choisi de regrouper tout ce qui touche à la protection de ses services en ligne dans l'espace d'administration des comptes Microsoft (**bit.ly/2GFXaN1**). Vous pouvez y changer le mot de passe commun à tous les services Microsoft (OneDrive, Outlook, Office 365), accéder à l'historique d'activité du compte ou encore activer le dispositif d'authentification à deux facteurs en cliquant sur **Autres options de sécurité**, puis sur le lien **Configurer la vérification en deux étapes**.



3 SÉCURISEZ GOOGLE DRIVE

À l'instar de OneDrive, vous devez accéder aux paramètres de votre compte Google pour personnaliser la sécurité de Drive. Pointez sur votre avatar en haut de la page, puis sur **Compte Google**, **Sécurité**. Utilisez les options de la section **Se connecter à Google** pour créer un mot de passe fort ou activer la validation en deux étapes quand un nouvel appareil tente de se connecter. Retournez dans Drive, cliquez sur l'icône en forme d'engrenage, puis sur **Paramètres**, **Gérer les applications**. Pour empêcher un service d'accéder à votre cloud, déroulez le menu **Options**, **Déconnecter de Drive**.



4 RENFORCEZ L'ACCÈS À VOTRE CLOUD SUR UN TÉLÉPHONE

Quand votre mobile n'est pas verrouillé, il est très facile de consulter les fichiers conservés sur Dropbox, Drive ou OneDrive. Seul le service cloud de Google ne permet pas de remédier à ce défaut de sécurité. Avec Dropbox, déroulez le menu de l'appli, touchez **Paramètres**, **Configurer le code secret**, **Activer le code secret**. Définissez le mot de passe qui sera exigé au lancement de l'application. Si vous utilisez OneDrive, effleurez votre avatar, puis **Paramètres**, **Code secret**, **Demander un code**. Cochez **Utiliser une empreinte digitale** si votre téléphone dispose de ce dispositif biométrique.

DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE PRÉVENTION

ENTRETENEZ VOTRE DISQUE DUR

Plus que les virus et les ransomwares, la sécurité de vos données personnelles est sous la menace d'une panne des supports de stockage qui accueillent vos fichiers. Prenez-en le plus grand soin.

1 PRENEZ LE POULS DE VOTRE SUPPORT

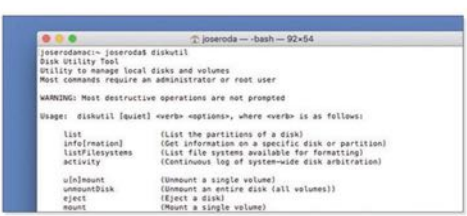
Le système de surveillance SMART (Self-Monitoring, Analysis, and Reporting Technology) veille en permanence sur l'état général des disques durs. Implantés sur le contrôleur du disque, les capteurs SMART transmettent une série d'informations détaillées qui sont ensuite interprétées par le système d'exploitation de votre PC ou de votre Mac. Cette technologie est d'un grand secours pour prédire les défaillances des disques durs. Si SMART n'est pas activé, redémarrez votre PC et accédez au BIOS. Dans la section HDD, sélectionnez le disque système et appuyez sur **Entrée**. Pointez sur **Surveillance SMART**, choisissez l'option **Activé** et validez par **Entrée**.

2 UTILISEZ SMART AVEC MACOS

La technologie SMART est également disponible dans l'univers Apple. Pour accéder aux prévisions, téléchargez un utilitaire comme Disk Drill (**bit.ly/2YGQQix**). Une fois l'application installée, cliquez sur son icône dans la barre de menus et pointez sur **Configurer Surveillance SMART**. Vous serez dorénavant tenu informé en temps réel de l'état de santé global des supports de stockage installés sur l'ordinateur. Cette surveillance ne constitue pas la panacée. Elle se limite en effet à un diagnostic et n'intègre pas de volet réparation. En cas de doute sur l'état d'un support, commencez par sauvegarder son contenu sans tarder sur le cloud ou sur un disque dur externe.

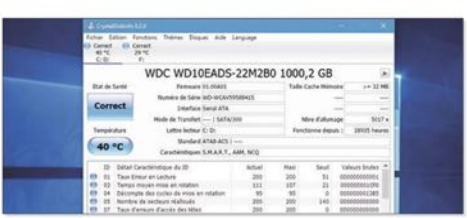
3 PRENEZ SOIN D'UN DISQUE MAC AVEC DISKUTIL

Effectuez ensuite les opérations de maintenance. Sur un Mac, ouvrez le Finder et lancez le Terminal à partir du dossier **Applications**, **Utilitaires**. Exécutez la commande **diskutil** pour afficher la liste des options disponibles, puis **Diskutil list** pour inventorier les disques et les partitions. Repérez le nom du disque à analyser et lancez la commande **diskutil info support** en remplaçant **support** par l'identifiant du disque (**disk0s2** par exemple). Saisissez **diskutil disk verifyVolume support** (le nom du disque). Validez par **Entrée**. Les éventuelles anomalies sont automatiquement corrigées.



4 DÉCRYPTEZ LES DONNÉES SMART AVEC CRYSTALDISK INFO

Les éléments d'analyse venant des disques durs doivent être décryptés. Vous pouvez faire appel pour cela au logiciel gratuit Crystal Disk info (**bit.ly/315vLLU**), disponible pour macOS et Windows. L'analyse se déroule en quelques secondes. Si le support est en bonne santé, la mention **Correct** apparaît dans la section **État de santé**. Crystal Disk Info indique également la durée d'utilisation du disque dur depuis sa mise en service ou le nombre de mises sous tension (**Nbre d'allumage**). Pour en savoir plus, reportez-vous aux données affichées dans la colonne **Actuel** des différents critères.



DIFFICULTÉ MODÉRÉE **TEMPS** 15 MIN **DOMAINE** CRYPTAGE

CHIFFREZ VOS DOCUMENTS AVANT DE LES EMPORTER

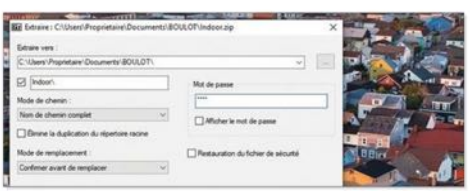
S'il existe des clés USB dotées d'un dispositif de chiffrement intégré, ces supports restent rares et chers. Pour limiter vos dépenses, regroupez simplement vos documents dans un dossier protégé.

1 PRÉPAREZ LA COMPRESSION

Installez l'utilitaire 7-Zip (**bit.ly/2A6ickZ**), en choisissant la mouture adaptée à votre version de Windows (32 bits ou 64 bits). En cas de doute, appuyez sur **Windows + I**, pointez sur **Système**, **Informations système** et reportez-vous à la ligne **Type du système** dans **Spécifications de l'appareil**. Gratuit, 7-Zip gère différents formats d'archives et propose une option de protection. Faites glisser vos fichiers sur l'interface de l'appli. La fenêtre **Ajouter à l'archive** apparaît. Indiquez le dossier de destination et renommez-le au besoin.

2 ACTIVEZ LE CHIFFREMENT

Conservez les options de compression par défaut. Déroulez le menu **Méthode de chiffrement** et sélectionnez le mode **AES-256**. Définissez un code secret (cochez la case **Afficher le mot de passe** pour vous assurer de ne pas commettre d'erreur), puis validez avec **OK**. Les éléments sont intégrés dans une archive chiffrée. Glissez le fichier ZIP sur une clé USB. Pour restaurer les documents, faites un clic droit sur l'icône du dossier et optez pour **7-ZIP**, **Extraire les fichiers**. Renseignez le mot de passe et pointez sur **OK**.



DIFFICULTÉ AUCUNE **TEMPS** 10 MIN **DOMAINE** SURVEILLANCE

AFFICHEZ L'HISTORIQUE DES CONNEXIONS USB À VOTRE PC

USB History Viewer mémorise la liste des périphériques amovible branchés en votre absence.

1 SÉLECTIONNEZ L'ORDINATEUR À INSPECTER

Dans un environnement de travail ou simplement sur le PC familial, il peut s'avérer intéressant d'identifier les appareils connectés et utilisés quand vous vous absentez. Vous saurez ainsi si quelqu'un a branché une clé USB pour copier des fichiers. Lancez l'utilitaire gratuit USB History Viewer (**bit.ly/2xX80y6**). Il s'agit d'un logiciel portable, inutile de l'installer. Entrez le nom de votre PC dans le champ **Computer Name** ou cliquez sur les points à droite et déroulez la section **Réseau** pour désigner un autre ordinateur.

2 VÉRIFIEZ LES CONNEXIONS RÉCENTES

Lancez l'analyse de l'activité des ports USB en cliquant sur le bouton **Start**. Ignorez l'étape 2 consacrée à l'authentification, USB History Viewer utilisant le compte Windows par défaut. Le nom des derniers matériels connectés s'affiche dans la fenêtre **Step 3**. Pour en savoir plus, pointez sur les flèches placées devant les différents appareils. Vous découvrez l'identifiant complet du périphérique (**ID**) ainsi que l'heure de la connexion (**Last Used**). La mention **TRUE** à droite de **Mounted** désigne les appareils actuellement branchés.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE CRYPTAGE

COMMENT RETROUVER UN MOT DE PASSE OUBLIÉ

Les règles élémentaires de sécurité nous invitent à choisir un identifiant différent pour chaque service en ligne. Au point que parfois, la mémoire nous joue des tours.

1 PROCÉDEZ À L'INSTALLATION DE RECALL

Impossible de vous souvenir du mot de passe mis en place pour protéger un document Word ou verrouiller un programme installé sur votre ordinateur ? Ne cédez pas à la panique. Lancez votre navigateur Internet et allez sur la page du programme recAll (**bit.ly/2SVDQ34**). Celui-ci est capable de récupérer les mots de passe de plus de 300 programmes (courrier électronique, navigateurs Web, messageries instantanées, clients FTP, Wifi, etc.) ainsi que les clés de licence de près de 3 000 applications.

2 LANCEZ LA DÉTECTION DES MOTS DE PASSE

L'application propose plusieurs modes de récupération. Le plus simple consiste à cocher l'option **Récupération automatique** et à pointer sur **Suivant** pour démarrer la recherche. L'analyse peut durer plusieurs minutes. La liste des sésames identifiés sur l'ordinateur s'affiche progressivement. Pour exporter cet annuaire, cliquez à nouveau sur le bouton **Suivant** et désignez le format d'exportation. Vous pouvez ainsi garder à portée de main l'ensemble des mots de passe utilisés sur le PC.

DIFFICULTÉ MODÉRÉE TEMPS 10 MIN DOMAINE FICHIERS

CACHEZ LES APPLIS ET LES DOCUMENTS IMPORTANTS

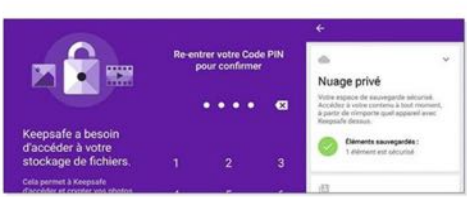
Ne vous contentez pas de verrouiller votre téléphone. Masquez également les contenus les plus sensibles.

1 DISSIMULEZ DES DONNÉES SUR UN MOBILE ANDROID

Pour mettre à l'abri certains fichiers, installez **Masquer les Fichiers** disponible sur le Play Store (**bit.ly/2WK76ir**). Lancez l'appli et autorisez-la à accéder aux ressources du smartphone. Désignez ensuite les dossiers et les fichiers que vous souhaitez dissimuler. Touchez l'icône symbolisant un classeur dans la barre d'outils, parcourez l'arborescence de l'appareil et cocher les cases situées devant le nom des éléments concernés (il peut s'agir de fichiers ou de dossiers). Effleurez le bouton **OK** pour confirmer l'ajout.

2 PROTÉGEZ LES PHOTOS DE L'IPHONE AVEC KEEPSAFE

Téléchargez l'application sur l'App Store ou directement depuis iTunes (**apple.co/2K4ppa1**). Keepsafe préserve vos photos des regards indiscrets. L'application utilise pour cela un astucieux dispositif de camouflage, se faisant passer pour un antivirus afin de tromper les curieux. Keepsafe active un écran de saisie de code PIN factice. Il s'agit d'un leurre. La saisie d'un faux mot de passe a pour effet de déverrouiller faussement l'application et d'ouvrir une galerie photos factice, sans rapport avec vos clichés !



DIFFICULTÉ AUCUNE TEMPS 15 MIN DOMAINE PRÉVENTION

ÉVITEZ L'EXÉCUTION DE FICHIERS STOCKÉS SUR UNE CLÉ USB

Les supports de stockage amovibles sont un vecteur de contamination majeur. Pour prévenir les risques, analysez soigneusement les clés USB avant d'ouvrir un fichier.

1 ANALYSEZ LES SUPPORTS EXTERNES

Pour éviter de petits ou grands problèmes, mieux vaut prendre les devants et vérifier l'intégrité des clés USB et des disques durs externes avec l'utilitaire USB Fix Free (**bit.ly/206ILk9**). Cet outil détecte et bloque les logiciels malveillants. Il peut aussi sécuriser vos supports de stockage amovibles contre de futures attaques. La version gratuite de l'application offre les fonctionnalités essentielles. Lancez USB Fix. Le nombre de disques détectés s'affiche à droite. Pointez sur **Analyser les disques USB**, **Rapport**.

2 VACCINEZ LES PÉRIPHÉRIQUES

Le rapport d'activité indique si l'un des disques est contaminé. Si c'est le cas, il vous suffit de le confier à votre antivirus habituel. Pour que la mésaventure ne se reproduise pas, vaccinez le périphérique. Cliquez sur l'icône **Maison** à gauche puis sur **Vaccination**, **Vacciner les disques**. Validez avec **OK**. USB Fix ajoute un dossier caché **autorun.inf** à la racine du support, bloquant ainsi l'exécution des programmes malveillants à l'insertion de la clé ou du disque dur. Si vous souhaitez renommer le support, activez **Supprimer les vaccins**.

DIFFICULTÉ AUCUNE TEMPS 20 MIN DOMAINE PROTECTION

CONFIEZ VOS CODES D'ACCÈS À UN NAVIGATEUR WEB

Si vous avez un peu de mal à mémoriser vos sésames, optez pour la gestion automatisée de Chrome et Firefox.

1 DEMANDEZ À CHROME DE GÉRER LES MOTS DE PASSE

Déroulez le menu **Personnaliser et contrôler...** (les 3 points en haut à droite de la fenêtre) et cliquez sur **Paramètres**, **Paramètres avancés**. Dans **Saisie automatique**, choisissez **Mots de passe** et activez les curseurs **Enregistrement** et **Connexion**. Les données que vous saisissez dans les formulaires d'authentification seront dorénavant mémorisées. Retournez sur la page **Mots de passe** des paramètres. Pointez sur l'icône **Œil** pour afficher le code d'accès d'un site, sur les 3 points et sur **Supprimer** pour effacer les infos d'un compte.

2 LAISSEZ FIREFOX S'OCCUPER DE TOUT

Ouvrez le menu du navigateur et choisissez **Options**, **Vie privée et sécurité**. Dans la section **Identifiants et mots de passe**, cochez la case **Proposer d'enregistrer**. Déployez le menu et cliquez sur **Identifiants et mots de passe**. La fenêtre **Enregistrement des identifiants** affiche l'URL des sites et le nom d'utilisateur. Cliquez le bouton **Afficher les mots de passe** pour faire apparaître les codes d'accès. Opérez un clic droit sur une ligne et optez pour **Modifier le mot de passe** si vous souhaitez actualiser cette information.

DIFFICULTÉ MODÉRÉE TEMPS 30 MIN DOMAINE CRYPTAGE

GARDEZ VOS MOTS DE PASSE À L'ABRI

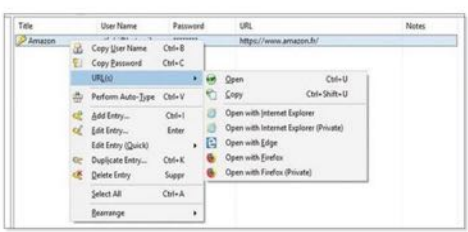
L'emploi d'un gestionnaire de mots de passe comme KeePass présente deux avantages. Il mémorise et restitue codes d'accès et identifiants quand vous en avez besoin, et les conserve dans un espace sécurisé.

1 CONSTITUEZ LA BASE DE DONNÉES

Installez la version 2.42.1 de KeePass (**bit.ly/2CooOoY**) pour Windows. Pointez sur le bouton **Démarrer** en bas à gauche du Bureau et lancez le programme depuis la section **Récemment ajoutées**. Autorisez la vérification de mises à jour (**Enable**), puis déroulez le menu **File**, **New**, **OK**. Donnez un nom à la base de données et décidez de son emplacement. Validez avec **Enregistrer**. Vous devez ensuite concevoir un mot de passe maître qui protégera l'accès à vos données. Conservez ce code en lieu sûr et ne le perdez pas (il ne peut être réinitialisé). Cliquez ensuite sur **Group**, **Add Group** en colonne gauche pour créer un nouveau dossier thématique.

2 MÉMORISEZ LES CODES D'ACCÈS...

Entrez le nom du groupe (**Shopping** dans notre cas, cet emplacement étant destiné à accueillir les identifiants de nos comptes Amazon, Cdiscount, etc.). Le dossier est ajouté en colonne gauche. Sélectionnez-le, déroulez le menu **Entry**, **Add Entry**. Indiquez le nom d'un site web, puis vos identifiants de connexion (**User name** et **Password**). Copiez-collez son URL dans la zone dédiée à l'adresse et validez avec **OK**. Pour utiliser ces données, opérez un clic droit sur le nom du site et optez pour **Copy User Name**. Ouvrez de nouveau le menu contextuel et pointez sur **URL(s)**, **Open**. Collez le mail de connexion et répétez l'opération avec le mot de passe (**Copy Password**).



3 ... PUIS VÉRIFIEZ LEUR SOLIDITÉ

Pour gagner du temps, vous pouvez faire glisser les informations depuis la fenêtre principale de KeePass plutôt que de passer par le presse-papiers. Une fois les identifiants mémorisés, validez avec le bouton de connexion pour accéder au site et remplir automatiquement le formulaire d'identification. Répétez l'opération avec la colonne **Password**. Pour découvrir si vos mots de passe sont suffisamment sécurisés, dirigez-vous vers **Find**, **Password Quality**. La colonne **Quality** évalue le niveau de protection à l'aide d'un code couleur. Renforzer les mots de passe qui n'apparaissent pas en vert.

4 ADOPTEZ DES SÉSAMES FORTS

Plus un sésame est long et comporte des caractères spéciaux, plus il est difficile à percer. Ouvrez le menu **Tools**, **Generate Password**. Cochez la case **Generate using character set**, fixez la longueur souhaitée dans le champ **Length** puis cochez toutes les options proposées. Validez d'un clic sur l'icône en forme de disquette. Nommez et enregistrez le profil (**OK**). Faites un clic droit sur l'un des mots de passe et pointez sur **Edit Entry**, **Generate a password**, **Repeat**. Sélectionnez le profil que vous venez de définir. Un nouveau mot de passe est créé. Copiez-le et remplacez l'ancien code d'accès du site.

DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE PARTAGE

ÉCHANGEZ DES FICHIERS SANS LES EXPOSER DANS LE CLOUD

Au contraire des services cloud, l'application Sync Home conserve les contenus partagés sur votre ordinateur. Ils ne risquent donc pas d'être interceptés et ouverts en chemin.

1 CRÉEZ LE DOSSIER PARTAGÉ

Allez sur le site **bit.ly/2Gn3Lf8** et pointez sur **Free download** pour récupérer le programme. Installez puis lancez Resilio Sync Home. Choisissez le nom qui sera affiché lors de l'envoi et de la réception des fichiers, puis cochez les options au bas de la fenêtre. Cliquez sur **Démarrer**. Ouvrez l'Explorateur de fichiers de Windows et créez un nouveau dossier **Resilio** dédié au partage dans la bibliothèque **Documents**. Dans la fenêtre de l'appli, pointez sur l'icône **+**, sur **Dossier standard** et indiquez l'emplacement que vous venez de créer.

2 METTEZ LE LIEN EN COMMUN

La fenêtre des autorisations et des partages s'affiche alors. La section **Sécurité** sert à approuver les pairs, à gérer les droits d'accès aux contenus partagés et à décider de la durée de validité du lien de partage. Indiquez dans la rubrique **Autorisation** si vous souhaitez autoriser vos correspondants à modifier les fichiers. Glissez un fichier dans le dossier partagé depuis l'Explorateur. Dans Sync Home, cliquez sur **Dossiers**, survolez le répertoire mis en commun et optez pour **Partager**, **Copier**. Envoyez ensuite le lien de partage.

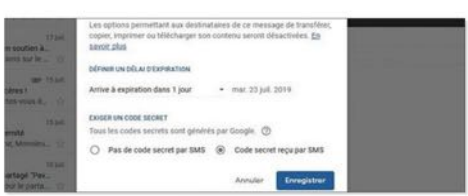
DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE CONFIDENTIALITÉ

LIMITEZ L'EXPOSITION DES FICHIERS PARTAGÉS

Assurez-vous que les documents que vous envoyez ne seront accessibles que pendant une durée bien définie.

1 UTILISEZ LE MODE CONFIDENTIEL DE GMAIL

La messagerie de Google propose depuis peu un mode confidentiel qui permet de contrôler l'accès aux pièces jointes. Composez un nouveau message, puis insérez le fichier à transmettre. Allez sur l'icône **Activer/Désactiver le mode confidentiel** en bas à droite. Fixez le délai d'expiration (de un jour à cinq ans) et activez l'option **Code secret reçu par SMS**. Validez avec **Enregistrer**. Renseignez le numéro de portable du destinataire afin que le code secret lui soit envoyé et qu'il confirme son identité, puis cliquez sur **Envoyer**.



2 PASSEZ PAR LE SERVICE SEND DE FIREFOX

La fondation Mozilla, qui développe le navigateur Firefox, a mis au point un service d'envoi de fichiers. Send est accessible à l'adresse **bit.ly/2CZaIXG**. Si vous possédez un compte Firefox, identifiez-vous afin de pouvoir transmettre des fichiers d'une taille maximale de 2,5 Go (1 Go autrement). Glissez vos contenus dans la zone de réception depuis le Bureau de votre ordinateur. Utilisez le menu **Expire après** pour limiter la validité du lien dans le temps (de 5 min à 7 jours) ou fixer un nombre de téléchargements. Validez par **Envoyer**.

DIFFICULTÉ ÉLEVÉE TEMPS 30 MIN DOMAINE STOCKAGE

SÉCURISEZ LES ACCÈS À UN NAS

Une fois hébergées sur un disque dur réseau, vos données peuvent être partagées facilement entre les ordinateurs de la maison ou à distance via Internet. Pensez à protéger l'accès à double tour !

1 CHANGEZ LE MOT DE PASSE ADMINISTRATEUR

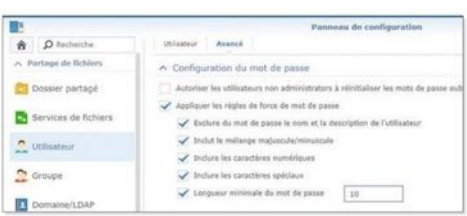
L'administration des NAS s'opère depuis une interface Web. Pour y accéder, lancez votre navigateur Internet et saisissez l'adresse IP fournie dans la documentation de votre appareil. Entrez les identifiants du compte administrateur par défaut (admin et password par exemple) et validez. Le statut d'administrateur donne la haute main sur les réglages du NAS, y compris la réinitialisation du disque dur. Pour éviter les soucis, modifiez le mot de passe du compte principal et réservez celui-ci aux opérations d'administration. Créez un autre compte à votre nom pour accéder aux contenus, protégé par un code secret différent et attribuez-lui les privilèges d'administrateur.

2 CRÉEZ UN PROFIL POUR CHAQUE UTILISATEUR

Vous avez l'opportunité de définir très précisément les droits accordés aux personnes qui se connectent au réseau. Dans l'interface d'administration, ouvrez la rubrique **Utilisateurs** et pointez sur **Créer un utilisateur**. Remplissez le formulaire d'inscription en indiquant le nom du titulaire du profil, son adresse mail et un mot de passe. Dans le cas d'un enfant, réservez-vous le droit de modifier le mot de passe. Attachez ensuite le compte à un groupe d'utilisateurs si vous prévoyez d'attribuer des privilèges similaires à plusieurs membres de la famille. Précisez les droits d'accès aux dossiers : lecture seule, lecture/écriture, pas d'accès.

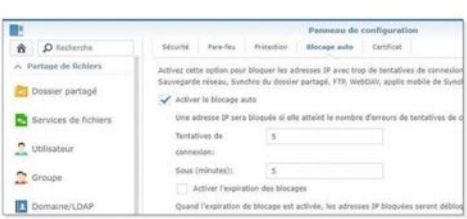
3 PRÉCISEZ LES PRIVILÈGES D'ACCÈS AUX DONNÉES

Il n'est pas nécessaire d'intervenir sur chaque profil utilisateur pour modifier les droits d'accès d'un dossier. Allez dans la section **Dossiers partagés** de la console d'administration, pointez sur l'emplacement à paramétrer puis sur **Modifier**. Ajustez le niveau de privilèges accordés et enregistrez les réglages. Selon la marque de votre NAS, vous bénéficiez de plus ou moins d'options. Avec DSM, le système d'exploitation de Synology, pouvez définir des règles de force pour les mots de passe (majuscules, de minuscules, de chiffres, de caractères spéciaux, nombre de caractères type de caractères).



4 ACTIVEZ LES OPTIONS AVANCÉES DE SÉCURITÉ

Les fonctionnalités liées à la sécurité des données et des accès varient d'un modèle à l'autre. Les NAS disposant d'un système d'exploitation évolué, comme ceux de Synology ou Qnap, sont bien sûr les mieux dotés. Synology propose de limiter le nombre de tentatives de connexion autorisées pour une même adresse IP. Une fois atteinte, il faut attendre un délai prédéfini pour effectuer un nouvel essai. Il est aussi possible de créer une liste d'adresses IP pour réserver l'accès au NAS aux appareils que vous jugez fiables ou encore de contrôler les ports d'entrée/sortie à l'aide d'un pare-feu.



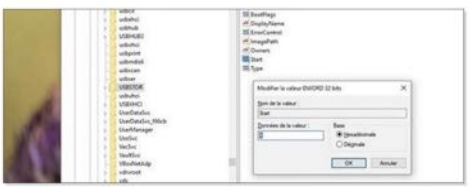
DIFFICULTÉ ÉLEVÉE TEMPS 20 MIN DOMAINE SYSTÈME

BLOQUEZ L'ACCÈS AUX SUPPORTS DE STOCKAGE USB

Pour éviter les vols de données, rien de plus efficace que de verrouiller les ports USB de votre PC. Une opération qui s'effectue en partie en modifiant le registre de Windows.

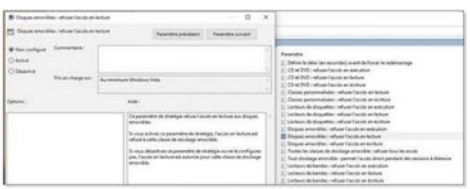
1 MODIFIEZ LA BASE DE REGISTRE

Accédez au registre en appuyant sur **Windows + R**, tapez **regedit** et validez par **Entrée**. Déployez la branche **HKEY_LOCAL_MACHINE**, **SYSTEM**, **CurrentControlSet**, **Services**, **USBSTOR**. Faites un clic droit sur **Start** à droite et choisissez **Modifier**. Remplacez la valeur par défaut (3) par 4. Fermez le registre et redémarrez le PC. Les supports USB ne s'affichent plus dans l'Explorateur de fichiers. Pour retrouver l'usage des prises USB, retournez dans Regedit, restaurez la valeur initiale de la clé **Start** et relancez votre ordinateur.



2 DÉSACTIVEZ LES PRISES USB AVEC L'ÉDITEUR DE STRATÉGIE DE GROUPE DE WINDOWS 0 PROFESSIONNEL

Si vous possédez la version Professionnelle de Windows 10, il est possible d'activer le blocage par un autre biais. Appuyez sur les touches **Windows + R**, tapez **gpedit.msc** et validez par **Entrée** pour ouvrir l'Éditeur de stratégie de groupe locale. Allez sur **Configuration ordinateur**, **Modèles d'administration**, **Système**, **Accès au stockage amovible**. Double-cliquez sur les lignes **Disques amovibles** et cochez la case **Activé**, **Appliquer**, **OK**. Redémarrez le PC.



DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE CRYPTAGE

RENDEZ VOS FICHIERS INACCESSIBLES AVANT DE PRÊTER VOTRE PC

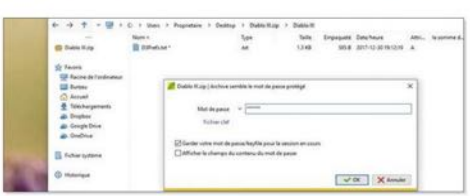
Soustrayez de la vue vos contenus confidentiels pour être certain que nul ne les consulte à votre insu.

1 UTILISEZ LA FONCTION CACHER DES DOSSIERS

Ouvrez l'Explorateur de fichiers (**Windows + E**) et allez sur l'onglet **Affichage**. Décochez la case **Éléments masqués** et opérez un clic droit sur le dossier que vous souhaitez masquer. Dans la section **Attributs** de l'onglet **Général**, cochez l'option **Caché** et validez avec **Appliquer**. Il faut ensuite indiquer si l'opération de camouflage s'étendra ou non aux sous-dossiers. Validez avec **OK**. L'emplacement disparaît de la vue. Faites-le réapparaître en cochant **Éléments masqués** et en décochant **Caché** dans les attributs du dossier.

2 CHIFFREZ LES DOSSIERS PERSONNELS

Téléchargez la version 6.8.1 de PeaZip (**bit.ly/207SuFv**). Ce logiciel autorise la compression des fichiers et des dossiers, mais aussi leur chiffrement de manière à les rendre inutilisables. Durant l'installation, prenez soin de franciser l'interface (**FR**). Ouvrez l'Explorateur de fichiers et effectuez un clic droit sur l'élément à protéger. Allez sur **PeaZip**, **Add to archive**. Cliquez sur **Entrer le mot de passe/un fichier clef**. Définissez un code d'accès, pointez vers le dossier d'enregistrement et validez avec **OK**.



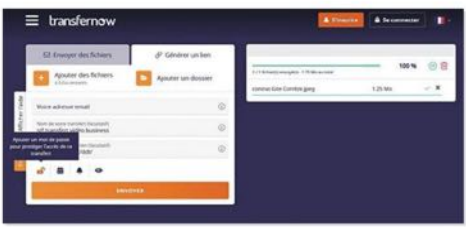
DIFFICULTÉ ÉLEVÉE TEMPS 30 MIN DOMAINE TRANSFERT

ENVOYEZ DES FICHIERS EN MODE HYPERSÉCURISÉ

Factures, RIB, papiers d'identité, certains documents ne doivent pas tomber entre de mauvaises mains. Il existe des services en ligne, souvent méconnus, capables d'assurer des transferts parfaitement sûrs.

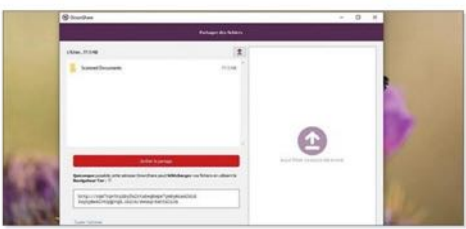
1 TRANSFÉREZ JUSQU'À GO AVEC TRANSFERNOW

Ce service offre la possibilité d'envoyer des fichiers de très grande taille (jusqu'à 4 Go) gratuitement. Il propose des options très pratiques, qu'il s'agisse du verrouillage par mot de passe, de l'envoi différé, de la protection HTTPS ou encore du suivi des transmissions. Allez sur le site **bit.ly/2JI8PwC** et cliquez sur le bouton **Démarrer**. Sélectionnez l'élément à transférer. Indiquez l'adresse mail du destinataire ou générez un lien de partage. Pointez sur le cadenas pour ajouter un code d'accès, sur le calendrier pour fixer une date d'expiration et enfin sur la cloche afin de recevoir une notification quand le fichier aura été récupéré par votre correspondant.



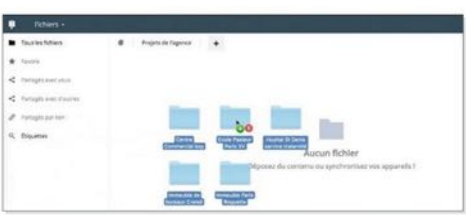
2 PARTAGEZ DES CONTENUS AVEC ONIONSHARE

Connectez-vous sur la page d'accueil du service (**bit.ly/2LzMf1q**) et installez l'application. OnionShare utilise le réseau Tor pour acheminer les données en toute confidentialité. Seule contrainte : l'expéditeur et le destinataire doivent tous deux utiliser OnionShare ou Tor. Déposez votre document dans la fenêtre du logiciel, puis cliquez sur **Commencer le partage**. Copiez le lien généré et envoyez-le via une messagerie sécurisée. Votre correspondant accédera à l'élément depuis OnionShare ou avec le navigateur Tor (**bit.ly/32JKWMs**). L'appli propose des réglages, comme la minuterie de démarrage et d'arrêt qui sert à définir le jour et l'heure de début et de fin du partage.



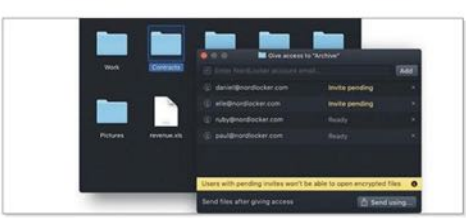
3 OPTEZ POUR LE CLOUD SOUVERAIN FRANÇAIS AVEC J.DOC

Ce service professionnel dont les serveurs sont situés dans l'hexagone (spécifications du cloud Souverain Français) répond à la norme de sécurité ISO 27001, ainsi qu'aux recommandations de l'Anssi. Il vous en coûtera 490 € par an. Vous pouvez tester J.Doc gratuitement pendant un mois (**bit.ly/2JItOPK**). Le partage s'effectue au moyen d'un lien de téléchargement associé à un mot de passe et à une date de péremption. Pour une sécurité accrue, chaque envoi s'opère dans un serveur virtuel individuel. L'accès aux données stockées sur le cloud est assuré via une connexion chiffrée de type SSL.



4 CHIFFREZ ET ÉCHANGEZ AVEC LE VPN NORDLOCKER

Nord VPN est un service de cryptage de données et de masquage des adresses IP très performant. Il propose depuis cet été, un nouvel outil de chiffrement de fichiers stockés sur le micro ou dans le cloud. NordLocker exploite deux algorithmes (AES-256 et 4096-bit RSA) pour préserver l'inviolabilité des données. Au-delà de la protection renforcée, le service offre la possibilité à l'expéditeur de gérer les autorisations d'accès aux fichiers transmis. Le chiffrement s'effectue d'un simple glisser-déposer dans le dossier **Locker**. Pour vous familiariser avec Nord Locker, rendez-vous sur le site **bit.ly/2Z8AVq0**.



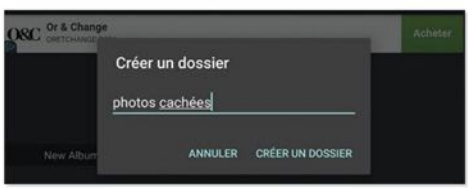
DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE CONFIDENTIALITÉ

EMPÊCHEZ QUE L'ON EXPLOITE LE CONTENU DE VOTRE IPHONE

En refusant de prêter votre téléphone, vous risquez d'apparaître peu sociable. Montrez-vous partageur sans pour autant exposer votre vie privée.

1 MASQUEZ DES FICHIERS

Disponible sur l'app Store, l'appli Cacher des photos - Hide it Pro (**bit.ly/2Yi1YIA**) a pour objet de masquer les photos, vidéos, musique et applications présentes sur l'iPhone. Pour rester discrète, elle apparaît sous l'intitulé **Audio Manager** une fois installée. Faites un appui prolongé sur cette icône et définissez un code PIN ou un mot de passe. Indiquez ensuite une adresse mail de récupération. Pour rendre des photos invisibles, appuyez longuement sur **Audio Manager** puis sur **Images** et **+**. Créez un nouveau dossier.



2 FAITES RÉAPPARAÎTRE TOUS VOS ÉLÉMENTS

Effleurez le dossier, pointez sur **+**, **Galerie** et sélectionnez les images. Validez par **Masquer**, **OK**. Pour vous assurer du succès de l'opération, utilisez le gestionnaire de fichiers de l'iPhone. Le dossier n'y apparaît plus. Pour afficher les photos, effectuez un appui prolongé sur l'icône **Audio Manager**, entrez le code PIN puis accédez à la bibliothèque **Images** et au dossier qui renferme les clichés masqués. Touchez l'icône **Crayon**, **Tout sélectionner**, **Afficher**. Choisissez un dossier de destination et validez avec **Afficher**.

DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE RÉCUPÉRATION

RESTAUREZ DES FICHIERS EFFACÉS PAR ERREUR

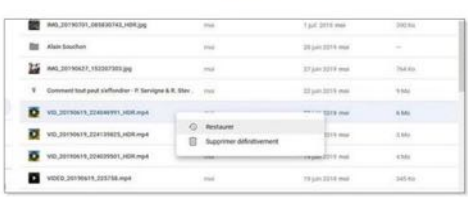
Nous sommes nombreux à vider la corbeille sans avoir vérifié son contenu. Profitez de votre droit à l'erreur !

1 TENTEZ UNE RÉCUPÉRATION AVEC RECUVA

Plus vous tardez et plus les chances de récupérer les fichiers effacés s'amenuisent. Installez et lancez la version gratuite de l'application Recuva (**bit.ly/2JVxWLd**). Cochez le type d'éléments à retrouver, cliquez sur **Next** et indiquez le dossier où ils se trouvaient avant leur suppression (dans le doute choisissez le mode **I'm not sure**). Validez avec **Next** et **Start**. L'option **Deep Scan** effectue une recherche approfondie, mais très longue. Sélectionnez votre document dans la liste des fichiers retrouvés et pointez sur **Recover** en bas à droite.

2 REPÊCHEZ DES FICHIERS DANS LE CLOUD

Avec Google Drive et Dropbox, vous bénéficiez d'un garde-fou efficace. Ces services conservent en effet les éléments effacés durant 30 jours avant de procéder à leur destruction. Avec Google Drive, pointez sur la corbeille à gauche, faites un clic droit sur le fichier concerné et activez la commande **Restaurer**. Dans le cas de Dropbox, pointez sur l'onglet **Fichiers** en colonne gauche, puis sur **Fichiers supprimés**. Cochez les éléments à récupérer (en utilisant au besoin le champ de recherche pour les trouver) et validez avec **Restaurer**.



DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE MESSAGERIE

IDENTIFIEZ ET DÉJOUEZ LES TENTATIVES D'HAMEÇONNAGE

Si les cybercriminels ne cessent d'affiner leurs techniques d'attaque, ils tirent toujours d'immenses profits du phishing. Ce dispositif fondé sur l'envoi de courriels piégés mise sur la crédulité des utilisateurs pour obtenir leurs codes d'accès ou des données bancaires. Rudimentaire mais efficace !

Une étude récente menée par Kaspersky Lab indique que le nombre de tentatives de phishing a plus que doublé entre 2018 et 2019. Loin des technologies de pointe employées par les hackers pour percer les défenses des systèmes d'information des grandes entreprises ou des administrations, l'hameçonnage repose quant à lui sur le maillon faible de la chaîne de sécurité : l'utilisateur !

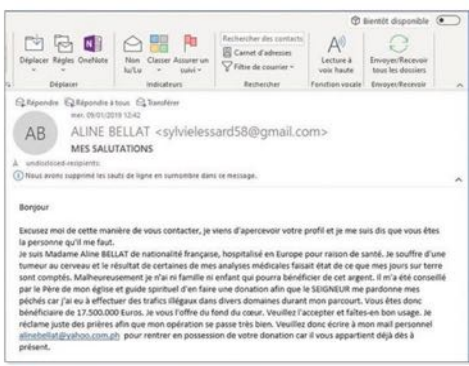
Pour mener ces attaques, pas besoin de programme complexe ni de code caché. Un simple mail suffit pour attirer les internautes sur un site factice et leur soutirer des données personnelles. Certains cybercriminels se contentent d'exploiter la cupidité des utilisateurs au travers de mails annonçant un gain à la loterie ou un héritage venu d'Afrique. Ces tentatives cousues de l blanc peuvent être déjouées avec un peu de bon sens. Le phishing s'appuie le plus souvent sur des mails imitant l'aspect de correspondances venant d'un FAI, d'un opérateur téléphonique, d'une banque ou encore de l'administration scale. Des expéditeurs habitués à communiquer par messages électroniques et auxquels nous accordons notre con ance. Les faussaires n'ont de cesse de parfaire leurs pièges, au point qu'il est parfois très difficile de démêler le vrai du faux.●

Boîte à outils

Pour ce pas à pas, nous avons utilisé

Un PC ou un Mac

Un smartphone



1 NE TOMBEZ PAS DANS LES PIÈGES GROSSIERS

Tous les criminels ne s'embarrassent pas de sophistication. Des millions de mails circulent chaque jour pour promettre monts et merveille aux internautes. Gros lots à la loterie, cadeau en attente, camping-car à céder gratuitement ou héritage de plusieurs millions de dollars à saisir, rien n'est trop beau pour appâter les plus crédules. Des promesses trop belles pour être vraies. Si vous trouvez un tel message dans votre boîte de réception, lisez-le sans ouvrir les fichiers attachés en pièce jointe ni cliquer sur le moindre lien. Supprimez simplement le mail ou déclarez-le comme indésirable : dans Outlook pour Windows, faites un clic droit sur l'intitulé du message et choisissez **Courrier indésirable**, **Bloquer l'expéditeur**.

2 FILTREZ LES MESSAGES INATTENDUS

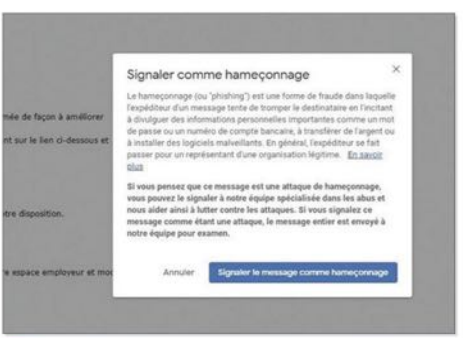
Canal+, Free ou Netflix n'ont aucune raison d'exiger de vous des informations si vous n'êtes pas leur client. Si les messages de ce type se multiplient, définissez des règles de filtrage pour les diriger automatiquement dans le dossier des indésirables. Dans Outlook, pointez sur **Accueil**, **Règles**, **Gérer les règles et les alertes**, **Nouvelle règle**. Sélectionnez **Déplacer les messages qui contiennent des mots spécifiques dans l'objet vers un dossier** et cliquez sur **Suivant**. Cochez **Contenant des mots spécifiques dans l'objet et avec des mots spécifiques dans l'en-tête**. Indiquez le nom des services détournés par les auteurs des attaques, désignez le dossier des spams et sauvegardez la règle.

3 VÉRIFIEZ LES ADRESSES DES EXPÉDITEURS

Un bon moyen pour identifier les faux mails consiste à passer l'identité de l'expéditeur aux rayons X. Une entreprise ou une administration utilise son propre nom de domaine et non des comptes Gmail ou Outlook. Le leurre est parfois moins grossier. Il faut alors s'attacher à l'adresse associée au nom de l'émetteur du message. L'un des courriels suspects reçus par la rédaction portait l'intitulé *Les Services clients Netflix* et pointait vers le compte **corporate@goes.com.ve**, à l'évidence sans rapport avec la plateforme de SVOD. Le texte de ces mails contient aussi des indices révélateurs : fautes de syntaxe et d'orthographe grossières, caractères parasites, logos pixélisés, absence des mentions légales.

4 N'ACTIVEZ PAS LES LIENS DANS LES MAILS SUSPECTS

Les mails piégés utilisent des adresses factices reprenant le nom de domaine d'une banque ou d'un service. Pour repérer le détournement, survolez le lien qui vous incite à accéder à votre compte avec le pointeur. L'URL associée au raccourci s'affiche dans un cartouche. S'il est sans rapport avec l'expéditeur présumé, vous pouvez conclure à la dangerosité du message. Les courriels d'hameçonnage sont sans effet tant que vous n'activez pas les liens ni les fichiers attachés. De façon générale, ne répondez pas aux mails qui sollicitent des informations personnelles via un formulaire de saisie. Effectuez ces opérations depuis votre espace client, accessible sur la page officielle et sécurisée du service concerné.



5 SIGNALEZ LES TENTATIVES D'HAMEÇONNAGE

Les adeptes du phishing ciblent large. Leurs messages sont envoyés à des centaines de milliers de contacts dans l'espoir de toucher quelques utilisateurs plus crédules que la moyenne. Les webmails de Microsoft et Google invitent leurs usagers à faire remonter les informations relatives à ces attaques. Accédez à votre boîte aux lettres Outlook.com, sélectionnez le mail concerné. Pointez sur l'onglet **Courrier indésirable** de la barre de menu, puis sur **Hameçonnage**, **Signaler**. Avec Gmail, affichez le courrier présentant un danger, déroulez le menu **Autres** (les trois points à droite du raccourci **Répondre**), activez la commande **Signaler comme hameçonnage** et validez (**Signaler comme hameçonnage**).

DIFFICULTÉ MODÉRÉE TEMPS 20 MIN DOMAINE FICHIERS

CHIFFREZ VOS DOCUMENTS AVANT DE LES ENVOYER

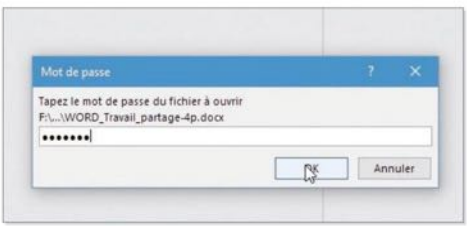
Les fichiers que vous adressez, tant dans le cadre personnel que professionnel, n'ont pas vocation à être lus au-delà de leurs destinataires. Protégez vos documents en les verrouillant au moyen d'un mot de passe.

1 CRYPTEZ UN DOCUMENT OFFICE

La suite bureautique de Microsoft permet de conditionner l'affichage des documents Word, Excel ou PowerPoint à la saisie d'un mot de passe. Ce dispositif s'appuie sur une clé de chiffrement, aussi prenez soin de noter le code secret. En effet, sans lui, il vous sera impossible d'accéder à vos fichiers ! Ouvrez le document dont vous souhaitez préserver la confidentialité. Activez ensuite l'onglet **Fichier** et pointez sur **Protéger le document**, **Chiffrer avec mot de passe**. Dans la fenêtre qui apparaît, tapez le mot de passe de votre choix (optez pour une combinaison complexe en évitant votre prénom ou 1234). Confirmez le code en le saisissant à nouveau.

2 ÔTEZ LA PROTECTION D'UN DOCUMENT PROTÉGÉ

La manipulation pour appliquer le chiffrement par mot de passe est identique pour toutes les applications de la suite Office 365, que vous travailliez sous Windows ou macOS (dans ce cas, déroulez le menu **Outils**, **Protection du document**). Une fois l'opération effectuée, enregistrez et fermez le document. Rouvrez le fichier. Une fenêtre s'affiche, vous invitant à entrer le code secret. Pour lever la protection, placez-vous sur l'onglet **Fichier** du ruban d'outils et cliquez sur **Protéger le document**, **Chiffrer avec mot de passe**. Appuyez sur **Ctrl** + **A** pour sélectionner le contenu du champ de saisie, puis sur **Suppr.** Validez par **OK**, puis enregistrez le fichier (**Ctrl** + **S**).

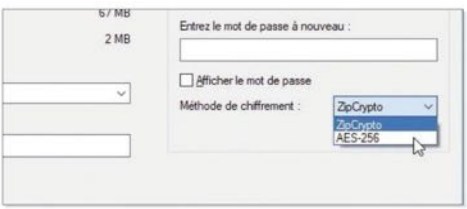


3 VERROUILLEZ UNE FEUILLE DE CALCUL GOOGLE SHEETS

Si vous possédez un compte Google, vous utilisez peut-être les outils bureautiques en ligne associés à Drive. Le tableur Sheets se pose ainsi en alternative à Excel. L'appli de Google offre la possibilité de verrouiller un classeur, non pas à l'aide d'un mot de passe, mais en intervenant sur les options de partage. Ouvrez le document et pointez sur **Outils**, **Protéger la feuille**. Dans le volet **Feuilles et plages protégées**, activez l'onglet **Feuille**, cliquez sur **Définir les autorisations**. Déroulez la liste **Vous uniquement**, choisissez **Personnalisée** et entrez les adresses mail des personnes habilitées à éditer le tableau.

4 PROTÉGEZ UNE ARCHIVE ZIP

Si vous utilisez la fonction **Envoyer vers dossier compressé** de Windows 10, vous n'avez pas la possibilité de protéger les archives obtenues par un mot de passe. Pour bénéficier de cette fonctionnalité, vous devez recourir à un utilitaire comme 7-Zip (**bit.ly/2A6ickZ**). Une fois celui-ci installé, faites un clic droit sur dossier à compresser. Dans la section **Chiffrement** de la fenêtre de configuration de l'archive, saisissez un mot de passe, confirmez-le puis optez pour l'une des méthodes de chiffrement disponibles : **ZipCrypto** ou **AES-256** (préférez cette dernière, plus sécurisée).



DIFFICULTÉ MODÉRÉE TEMPS 5 MIN DOMAINE MESSAGERIE

ÉCHANGEZ DES MAILS CHIFFRÉS GRÂCE AU SERVICE TUTANOTA

Mais que se passe-t-il vraiment entre le moment où vous envoyez un mail et celui où votre contact le reçoit ? Pour rester zen, optez pour le chiffrement de vos missives.

1 CRÉEZ UN COMPTE GRATUIT

Tutanota est un service qui peut être utilisé gratuitement. Il s'occupe de chiffrer vos messages et de les acheminer jusqu'à l'ordinateur de vos correspondants où ils seront affichés en clair. Connectez-vous sur le site **bit.ly/2Ki80cY**. Cliquez sur **Tarifs** puis sur le lien **Sélectionner** qui se trouve sous l'option **Free**. IL faut ensuite créer votre compte Tutanota en saisissant l'adresse mail souhaitée, puis en définissant un mot de passe sécurisé. Acceptez les conditions d'utilisation et validez par **Suivant**.

2 LANCEZ LA DÉTECTION DES MOTS DE PASSE

Un code de récupération alphanumérique de 64 caractères est alors généré. Copiez-le et collez-le dans un document texte. Il constitue le seul moyen pour réinitialiser votre compte. Votre adresse de courriel Tutanota sera active après validation, dans un délai de 48 heures. Tutanota s'utilise ensuite comme n'importe quel webmail. Cliquez sur le bouton **Nouveau message** symbolisé par un crayon dans l'angle inférieur droit de l'interface. Indiquez l'adresse du destinataire, l'objet et le contenu du message et pointez sur **Envoyer**.

DIFFICULTÉ MODÉRÉE TEMPS 5 MIN DOMAINE MESSAGERIE

UTILISEZ UNE ADRESSE DE COURRIER ÉLECTRONIQUE ÉPHÉMÈRE

Plutôt que d'exposer votre adresse mail, servez-vous d'un compte jetable pour vous inscrire aux services en ligne.

1 GÉNÉREZ UNE ADRESSE JETABLE

Yopmail est un service gratuit et astucieux qui tient à votre disposition un générateur d'adresses électroniques temporaires pouvant être utilisées le temps de s'inscrire à un service. Une arme antispam imparable ! Lancez votre navigateur Internet et rendez-vous sur le site **bit.ly/2GFsRWt**. Notez l'adresse qui s'affiche ou copiez-la dans le presse-papiers. Ne fermez pas l'onglet Yopmail. Ouvrez un nouvel onglet, allez sur la page d'inscription du site qui exige une adresse mail et communiquez l'adresse fournie par Yopmail.

2 VALIDEZ VOTRE INSCRIPTION

Les demandes d'inscription de ce type donnent généralement lieu à l'envoi d'un lien d'activation. Yopmail met à votre disposition une boîte de réception temporaire associée à l'adresse éphémère que vous venez de créer. Revenez sur l'onglet Yopmail et pointez sur le bouton **Vérifier les emails**. Si aucun message n'est présent dans la boîte de réception, attendez quelques minutes et cliquez sur **Rafraîchir**. Activez le lien de confirmation pour valider l'inscription. Votre compte Yopmail cessera de fonctionner après quelques jours.

DIFFICULTÉ AUCUNE TEMPS 5 MIN DOMAINE PHISHING

DÉJOUEZ LES TENTATIVES DE PIRATAGE DU COMPTE GMAIL

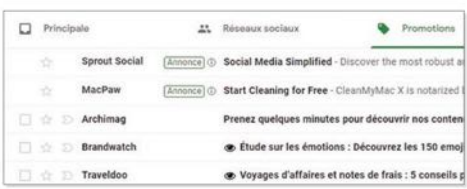
Le courriel est largement utilisé par les pirates pour dérober des données personnelles ou infecter des ordinateurs. Musclez vos défenses contre ces menaces.

1 INSTALLEZ L'EXTENSION UGLYMAIL

Développée pour les navigateurs Google Chrome et Firefox Uglymail est une extension dont l'objectif consiste à intercepter les messages dangereux, pour votre ordinateur ou vos données personnelles, qui arrivent dans votre boîte Gmail (les autres webmails ne sont pas gérés). Accédez d'abord à la page de téléchargement du module (**bit.ly/2GHeVLA**). Désignez votre navigateur et autorisez l'installation (pour vous assurer du succès de l'opération, pointez sur **Personnaliser et contrôler Google Chrome**, **Plus d'outils**, **Extensions**).

2 DÉCRYPTEZ LES SIGNAUX ENVOYÉS PAR UGLYMAIL

Le fonctionnement de l'extension UglyMail est très simple. Chaque nouveau message reçu est analysé. Si le mail comporte un traqueur ou un module susceptible de vous suivre à la trace ou d'analyser votre comportement (c'est le cas de 90 % des newsletters), un œil s'affiche devant l'objet du message. Une fois informé de la présence du mouchard, à vous de décider en connaissance de cause de lire ou non le mail. Si vous le jugez dangereux, supprimez-le sans l'ouvrir ou déplacez-le dans le dossier des indésirables.



DIFFICULTÉ AUCUNE TEMPS 5 MIN DOMAINE MESSAGERIE

TESTEZ LA SÉCURITÉ DE VOTRE BOÎTE DE RÉCEPTION

À quelles données les destinataires de vos messages peuvent-ils avoir accès ? Email Privacy Tester vous dit tout !

1 ANALYSEZ VOTRE MESSAGERIE

Le risque auquel vous vous exposez à dévoiler trop d'informations concerne moins vos proches que tous les services en ligne que vous contactez via votre adresse électronique. Votre messagerie, mais aussi le service qui vous a fourni ladite adresse, peuvent être d'incorrigibles bavards ! Pour dresser un état des lieux complets des éventuelles fuites qui ont eu lieu, connectez-vous sur le site Email Privacy Tester (**bit.ly/2Mt00GR**). Indiquez votre adresse de courriel et pointez sur le bouton **Submit**.

2 DÉCOUVREZ LES INFOS ÉCHANGÉES À VOTRE INSU

Connectez-vous ensuite à votre boîte de réception Gmail ou Outlook. Vous devriez avoir reçu un message émanant de Email Privacy Checker. S'il n'apparaît pas, vérifiez dans le dossier des indésirables. Ce mail intègre un lien hypertexte servant à lancer l'analyse. Un nouvel onglet s'affiche dans le navigateur et dresse la liste des tests qui peuvent être réalisés. Pointez sur le bouton **Send Test mail**. Vous recevrez un nouveau mail contenant en pièces jointes les rapports dressant l'état des lieux des informations échangées à votre insu.

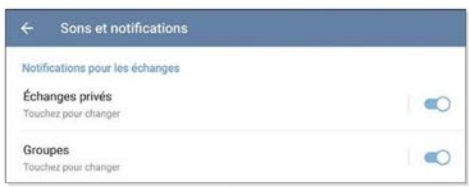
DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE TCHAT

ÉCHAPPEZ AUX OREILLES DES ESPIONS GRÂCE À TELEGRAM

Avec cette application, les messages que vous échangez avec vos proches sont chiffrés et rendus inaccessibles à quiconque ne possède pas la clé de sécurité.

1 COMMENCEZ UNE CONVERSATION

Installez Telegram Messenger à partir de l'App Store d'Apple ou du Play Store d'Android. Lancez l'appli, sélectionnez votre pays dans la liste et confirmez votre numéro de mobile. Touchez ensuite le bouton **Next**. Un SMS d'activation vous est aussitôt envoyé. Saisissez le code contenu dans le message et validez. Pensez à autoriser les notifications de façon à être alerté de l'arrivée des nouveaux messages. Pour lancer une conversation, touchez le bouton **Contacts** et choisissez un correspondant utilisant lui aussi Telegram.



2 SÉCURISEZ LES ÉCHANGES EN LIMITANT VOTRE VISIBILITÉ

Mis à part un chiffrement renforcé de bout en bout, les échanges avec Telegram Messenger ressemblent à vos applis de tchat habituelles. Pour effacer un message ou une conversation, effectuez un appui long sur le texte puis effleurez la commande **Supprimer**. N'importe quel utilisateur du service peut vous inviter à participer à une conversation. Pour éviter les mauvaises rencontres, touchez l'icône **Paramètres**, puis dans **Confidentialité et sécurité**, **Groupes et canaux**. Décochez **Tout le monde** en pointant sur **Mes Contacts**.

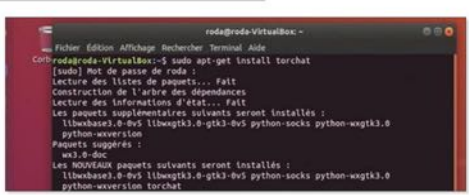
DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE TCHAT

CONVERSEZ EN TOUTE DISCRÉTION AVEC TORCHAT

Linux est le système d'exploitation idéal pour qui souhaite rester à bonne distance de la curiosité des Gafam. Le logiciel de messagerie instantané Torchat mise ainsi sur la confidentialité des échanges.

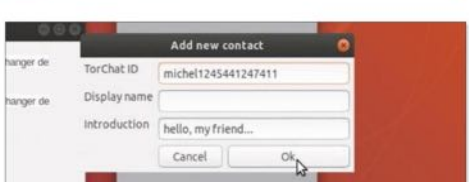
1 INSTALLEZ TORCHAT SUR VOTRE PC UBUNTU

Torchat est un client de messagerie instantané qui chiffre les conversations de bout en bout. Les échanges transitent par le réseau Tor et utilisent une connexion point à point (P2P). Pour installer l'application, lancez une instance du Terminal Ubuntu (**Ctrl** + **Alt** + **T**) et saisissez la commande **sudo apt-get install torchat**. Validez d'une pression sur la touche **Entrée** du clavier. Si Ubuntu vous y invite, tapez le mot de passe de votre compte administrateur. Au terme de l'installation du paquet, exécutez la commande **torchat**.



2 LANCEZ UNE CONVERSATION

L'application se résume à une simple fenêtre de conversation. Double-cliquez sur le contact avec lequel vous souhaitez communiquer. Si votre carnet d'adresses est vide, effectuez un clic droit et pointez sur **Add contact** dans le menu contextuel pour renseigner l'identifiant Torchat ID de votre correspondant. Une nouvelle fenêtre s'affiche alors. Activez le champ de saisie, libellez votre message et validez l'envoi avec la touche **Entrée**. La conversation est lancée et se poursuit comme avec n'importe quelle messagerie instantanée.



DIFFICULTÉ MODÉRÉE TEMPS 10 MIN DOMAINE MESSAGERIE

GARDEZ LES COURRIELS INDÉSIRABLES À DISTANCE

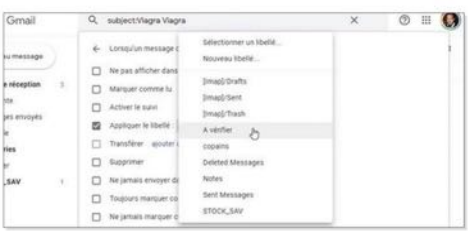
Offres de Viagra, héritages inespérés et sollicitations en tout genre constituent plus de 90 % des mails échangés sur Internet ! Sans un dispositif de filtrage efficace, ces messages finissent immanquablement par polluer votre boîte de réception.

1 APPLIQUEZ DES FILTRES DE GMAIL

Sous macOS ou Windows, accédez à la version webmail de Gmail. Vous y trouverez les fonctionnalités dédiées à la lutte contre les messages indésirables. Cliquez sur l'engrenage dans l'angle supérieur droit de l'écran, puis dans le volet qui s'affiche, pointez sur **Paramètres**. Activez l'onglet **Filtres et adresses bloquées** et la commande **Créer un filtre**. Vous pouvez alors définir un certain nombre de critères de tri des messages entrants. Le nom de l'expéditeur n'étant pas déterminant (il change en permanence), placez-vous dans le champ **Objet** et saisissez le mot **VIAGRA**. Faites de même dans le champ **Contient les mots**. Validez par **Créer un filtre**.

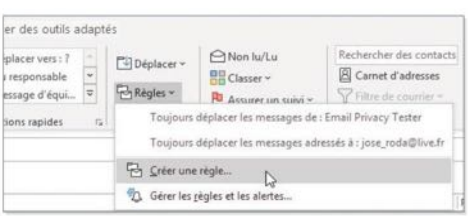
2 DÉFINISSEZ L'ACTION ASSOCIÉE AU FILTRE

Il faut maintenant décider du sort des messages qui répondent à vos critères de filtrage. Gmail propose différentes actions qui ne s'opposent pas forcément les unes aux autres et peuvent être combinées. Nous vous recommandons de ne pas opter d'emblée pour la case **Supprimer**. Mieux vaut contrôler que le filtre fonctionne bien et décider vous-même de la suppression des messages. Cochez **Appliquer le libellé**. Dans le volet qui se déploie, pointez sur **Nouveau Libellé** et nommez ce dossier *A vérifier*. Les mails interceptés par Gmail y seront automatiquement conservés en attendant que vous preniez la décision de les effacer. Activez le filtre avec **Créer un filtre**.



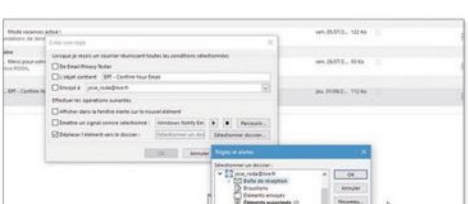
3 CRÉEZ UNE RÈGLE DE TRI AVEC OUTLOOK

Le client de messagerie Outlook disponible pour Windows et macOS propose également des options de filtrage des courriers indésirables. Vous pouvez vous décharger d'un certain nombre d'opérations en créant des règles de messages. Outlook se chargera ainsi d'automatiser le classement des mails à mesure qu'ils arrivent dans votre boîte de réception. En fonction de vos choix, l'application retournera une réponse automatique, déplacera un message vers la corbeille ou l'aiguillera dans un dossier spécifique. Activez l'onglet **Accueil** du ruban d'outils, Cliquez sur **Règles**, **Créer une règle**.



4 DÉFINISSEZ LES VARIABLES ET LES ACTIONS

Un assistant vous guide dans la définition du filtre. Cliquez dans le champ **Nom de la règle** et saisissez par exemple **Classement**. Pointez sur **Déplacer les messages qui contiennent des mots spécifiques dans l'objet vers un dossier**. Déroulez la liste **À l'arrivée d'un nouveau Message** et sélectionnez **Si une des conditions est remplie**. Choisissez le déclencheur (**De** pour définir l'expéditeur par exemple), puis les critères du filtre. Dans la section **Effectuer les opérations suivantes**, activez **Déplace le message** et désignez le dossier qui accueillera les mails interceptés par Outlook.



DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE TÉLÉPHONE

FILTREZ LES APPELS ET LES MESSAGES DES IMPORTUNS

Le mail n'est pas le seul moyen utilisé par les VRP et les démarcheurs de tout poil pour tenter de vendre leurs services. Votre téléphone aussi retentit d'appels commerciaux non souhaités. Mettez-y bon ordre.

1 REDIRIGEZ UN CONTACT VERS LA MESSAGERIE

Si les appels commerciaux peuvent tourner au harcèlement, ils ne sont pas les seuls que vous souhaiteriez éviter. Vous aimeriez peut-être filtrer votre patron et vos collègues durant vos vacances. Plutôt que de leur raccrocher au nez et de laisser sonner votre téléphone dans le vide, redirigez ces appels vers la messagerie. Ouvrez l'application **Contacts**. Saisissez le nom de la personne dans le champ de recherche et accédez à sa fiche. Touchez **Options** dans l'angle supérieur droit de l'écran et activez **Rediriger vers la messagerie**.

2 BLOQUEZ UN INTERLOCUTEUR DEVENU INDÉSIRABLE

Si vous subissez les assauts d'un contact un peu trop collant, bloquez-le ! Vous ne serez plus dérangé par ses appels ou ses SMS, ni même notifié de ces tentatives. Si cet individu figure déjà dans votre répertoire, ouvrez l'appli Contacts, touchez le bouton **Options** et activez la commande **Bloquer le numéro**. Dans la fenêtre qui s'affiche cochez **Signaler comme Spam** puis effleurez **Bloquer**. Si l'importun n'appartient pas à vos contacts, sélectionnez le numéro dans l'historique des appels de l'appli **Téléphone** et répétez la manipulation.

DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE MESSAGERIE

ENVOYEZ DES MAILS CONFIDENTIELS AVEC GMAIL

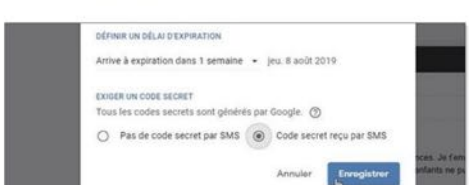
Le service de messagerie de Google s'est enrichi d'options dédiées à la confidentialité des envois.

1 RÉDIGEZ VOTRE MESSAGE COMME D'HABITUDE

Accédez à la version Web de Gmail ou lancez l'application mobile sur votre smartphone. Le mode confidentiel est dorénavant disponible sur toutes les versions de la messagerie. Entrez l'adresse du destinataire, puis tapez l'objet et le texte du message. Ajoutez des pièces jointes, votre signature ou encore des liens hypertexte. Jusqu'ici, rien ne change par rapport à un courriel ordinaire. Ce travail effectué, pointez sur la dernière icône de la barre d'outils au bas de la fenêtre de composition pour activer le mode **Confidentiel**.

2 FIXEZ LA DURÉE DE VIE DU MAIL OU UN MOT DE PASSE

Ce mode propose deux options clés. La première consiste à limiter la durée de vie du message. Passé un certain délai, compris entre 1 semaine et 5 ans, le mail s'autodétruira et ne pourra plus être lu ni imprimé par ses destinataires. Vous pouvez par ailleurs verrouiller le message et lier son affichage à la saisie d'un mot de passe. Dans la section **Exiger un code secret**, pointez sur l'intitulé **Standard**. Activez la commande **Code secret reçu par SMS** si vous souhaitez que votre correspondant reçoive le code sur son téléphone.



DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE MESSAGERIE

CONFIEZ VOS MAILS À UN POSTIER ÉPRIS DE SÉCURITÉ

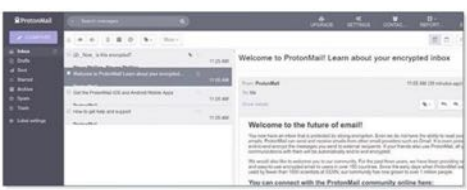
ProtonMail est une solution de messagerie gratuite qui présente l'originalité de protéger les échanges à l'aide d'un chiffrement renforcé. Autre atout, les mails sont conservés sur des serveurs hébergés en Suisse.

1 ACTIVEZ VOTRE BOÎTE DE RÉCEPTION

ProtonMail est accessible sur ordinateur, à travers une interface Web, aussi bien que sur les mobiles. Lancez le Play Store et installez l'application. Effleurez le bouton **Ouvrir**, puis **Créer un compte**. Sélectionnez l'offre gratuite (**Free**) qui offre 500 Mo d'espace de stockage pour vos mails et accepte jusqu'à 150 messages par jour. Définissez un nom d'utilisateur, touchez **Créer un compte** et choisissez le mot de passe qui sera utilisé pour chiffrer les messages. Réglez le niveau de sécurité sur **Élevée (2048bits)** et pointez sur **Continuer**.

2 RÉDIGEZ VOS PREMIERS MESSAGES

ProtonMail revêt l'apparence d'une boîte de réception ordinaire, ce qu'il n'est pas tout à fait. De fait, il propose des fonctionnalités liées à la confidentialité et à la sécurité que l'on ne retrouve pas dans les autres messageries. Effleurez l'icône en forme de crayon pour ouvrir la fenêtre de composition. Saisissez les adresses des destinataires du nouveau mail (abonnés ou non à ProtonMail), l'objet et le texte du courriel. Pointez sur le verrou et définissez le mot de passe que vous transmettrez à vos correspondants. Validez par **Envoyer**.



DIFFICULTÉ MODÉRÉE TEMPS 15 MIN DOMAINE MESSAGERIE

COMMUNIQUEZ EN TOUTE SÉCURITÉ AVEC MAIL

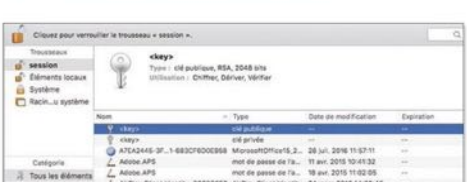
Vous utilisez le client de messagerie de macOS ? Alors profitez de l'option de chiffrement de vos messages.

1 GÉNÉREZ LE CERTIFICAT DE SÉCURITÉ

Pour assurer le chiffrement de votre boîte de réception et de vos prochains messages, il faut au préalable obtenir un certificat de sécurité auprès du service Comodo (**bit.ly/20y42lW**). Remplissez le formulaire qui s'affiche (Nom, prénom, adresse mail, pays d'origine, mot de passe). Allez ensuite dans Mail et attendez de recevoir le message émanant de Comodo qui contient un lien de téléchargement de votre certificat personnel. Pour l'utiliser, pointez sur le bouton **Click & install Comodo mail certificate**.

2 AJOUTEZ LE CERTIFICAT À MAIL

Ouvrez ensuite votre dossier de téléchargement et procédez à l'installation du certificat en double-cliquant sur le fichier portant l'extension **CRT.** Les informations sont automatiquement importées dans l'application Trousseau d'accès de macOS. Fermez puis relancez l'appli Mail. Cliquez sur le bouton **Nouveau message**. La fenêtre de composition arbore dorénavant une icône de couleur bleue qui indique que le message est signé numériquement par défaut. Activez ce raccourci pour envoyer le mail en mode normal.



SUZUKI

Way of Life!*

*Un style de vie !

Suzuki
IGNIS

CHANGEZ DE POINT DE VUE

Gamme à partir de
10 290 € (1)

PRIME À LA CONVERSION DÉDUITE

SUZUKI IGNIS, le SUV ultra compact.

HYBRID

Si vous avez envie de voir les choses autrement, venez essayer le premier SUV ultra compact de Suzuki. Système Hybrid SHVS (2), technologie exclusive 4 roues motrices AllGrip, position de conduite surélevée, freinage actif d'urgence avec double caméra, dans seulement 3m70... jamais une citadine ne s'est sentie aussi à l'aise partout.

Et vous, êtes-vous prêt à changer de point de vue ?
Retrouvez d'autres expériences Ignis et réservez votre essai sur www.suzuki.fr

Consommations mixtes CEE gamme Suzuki Ignis (l/100 km) : 4,3 à 4,8. Émissions CO (NEDC-WLTP) : 98 - 117 à 109 - 127 g/km.

Équipements selon version. (1) Prix TTC de la Suzuki Ignis 1.2 Dualjet Hybrid Avantage, hors peinture métallisée, après déduction d'une remise de 2 100 € o erte par votre concessionnaire et d'une prime à la conversion de 1 500 €**. O re réservée aux particuliers valable pour tout achat d'une Suzuki Ignis neuve du 05/08/2019 au 30/09/2019, en France métropolitaine dans la limite des stocks disponibles, chez les concessionnaires participants. **Modèle présenté : Suzuki Ignis 1.2 Dualjet Hybrid Pack : 13 340 €, remise de 1 800 € déduite et d'une prime à la conversion de 1 500 €** + peinture métallisée : 500 €.** Tarifs TTC clés en main au 05/08/2019. (2) Smart Hybrid Vehicle by Suzuki. **1 500 € de prime à la conversion conformément aux dispositions du décret n° 2019-737 du 16 juillet 2019 relatif aux aides à l'acquisition ou à la location des véhicules peu polluants. Voir conditions sur service-public.fr.

Garantie 3 ans ou 100 000 km au 1er terme échu.