LE MAGAZINE DE LA HIGH-TECH

01net

HORS-SÉRIE

N° 97 · 5,50€

MARS - AVRIL 2017

M 05458 - 97H - F: 5,50 € - RD

VIRUS RANÇONGICIELS VOL DE DONNÉES PROTÉGEZ-VOUS !

100 PAGES DE TUTORIELS ILLUSTRÉS

01net HORS-SÉRIE N°97

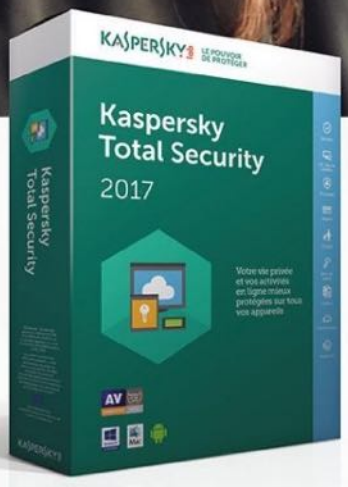
VIRUS, RANÇONGICIELS, VOL DE DONNÉES : PROTÉGEZ-VOUS !

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

Je veux une solution de sécurité qui m'aide à préserver ma vie privée en ligne et qui protège tous mes appareils contre les virus.

Kaspersky Total Security
Protection disponible en magasin et sur Kaspersky.fr

KASPERSKY lab LE POUVOIR DE PROTÉGER



Aux armes, cybercitoyens !

Avez-vous une idée du nombre de victimes de rançongiciels (ransomwares) dénombrées en France par l'éditeur d'antivirus Avast rien que pour l'année 2016 ? Pas moins de 250 000 ! Ainsi, Locky, Petya et autres Jigsaw ont connu un impressionnant et terrifiant succès pour, au final, extorquer la coquette somme de près de 12 millions d'euros, toujours selon les estimations d'Avast.

Pas mal pour quelques lignes de code bien ficelées et beaucoup de malice ! Et ce n'est pas près de s'arrêter, tant l'arme est redoutable et rapporte gros. D'autant que les contre-attaques tardent souvent à venir. Dernier exemple en date : Dharma, un ransomware qui sévissait depuis mi-novembre 2016, a reçu son antidote… fin janvier 2017. Même si les éditeurs de logiciels de sécurité travaillent d'arrache-pied pour mener la vie dure aux pirates, ils ont toujours un train de retard. Aucun antivirus ne peut empêcher qui que ce soit d'ouvrir un fichier s'il le désire. Tout au plus, si la menace est déjà connue, il avertira que le document est infecté et qu'il vaudrait mieux s'abstenir. Bref, le point faible, c'est l'utilisateur derrière son écran.

Mais ne baissez pas les bras. Avec ce hors- série, *01net Magazine* vous aide à dresser toutes les barrières de protection possibles autour de vos ordis et appareils mobiles. Mais aussi à acquérir les bons réflexes afin de ne pas vous laisser embobiner et tomber dans les pièges tendus par les malveillants. Parce que, si le ransomware est la tendance de 2016-2017, d'autres modes d'infection dangereux (malwares, chevaux de Troie…) ou inoffensifs mais gênants (adwares) demeurent toujours d'actualité. Vous allez le voir, surfer sur le Web sereinement, surveiller votre réseau privé et garder le contrôle de vos données personnelles ne s'avère, finalement, pas si compliqué que ça. ■

01net

29, rue de Châteaudun
75308 Paris Cedex 09
Directeur de la publication
François Dieulesaint

ABONNEMENTS
Tél. : 0170 37 3174 (du lundi au vendredi de 8 h 30 à 18 h 30)
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.ediqroup.ch
Belgique : www.ediqroup.be
Autres pays : www.kiosque01.fr

Pour joindre votre correspondant, faites précéder les quatre chiffres entre parenthèses de 01 75 55

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

DIRECTEUR ARTISTIQUE
Jean-Paul Chantrieux (43 05)
jpchantrieux@groupelexpress.fr

COORDINATEUR DE CE NUMÉRO
Fabrice Brochain, chef de service (42 26)
fbrochain@groupelexpress.fr

RÉDACTION ET RÉALISATION
Alchimie Médias
www.alchimiemedias.com

ONT COLLABORÉ À CE NUMÉRO
Hervé Bourdieu
Hélène Brusetti (43 29)
hbrusetti@groupelexpress.fr
Christelle Denis (43 16)
cdenis@groupelexpress.fr
Thierry Lavanant (43 11)
tlavanant@groupelexpress.fr

PUBLICITÉ
Altice Media Publicité
Directrice déléguée
Sophie Vatelot Niclas
Directeur commercial Pôle News Culture
Pierre-Étienne Musson (10 62)
Directrice de publicité
Aline Ferrant (44 16)
Directrice de clientèle
Joanna Galou (44 27)
Directrice du développement international
Alice Macpabro (16 49)

DIFFUSION - FABRICATION
Directeur diffusion
Alexis Bernard
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 45

01NET
est édité par la société
Newsco Mag
Président
SFR Presse, représenté par François Dieulesaint
SASU au capital de 10 000 euros
Siège social : 29, rue de Châteaudun 75308 Paris Cedex 09
RCS : 799 351 341
Code APE : 5813Z
Siret : 799 351 341 00018
Principal actionnaire : SFR Presse

Commission paritaire
0321 K 78311 – ISSN 2266-7989
Dépôt légal : à parution
Distribution : Transports Presse

SOMMAIRE
HORS-SÉRIE N° 97

Un hors-série garanti sans virus, pour protéger vos appareils et vos données personnelles.

SUPPRIMER VIRUS ET MALWARES

PROTÉGER SON WIFI ET SON RÉSEAU

SÉCURISER SES DONNÉES

PRÉSERVER SA VIE PRIVÉE

ENJOY SAFER TECHNOLOGY™

30 JOURS D'ESSAI GRATUITS

Surfer, acheter, jouer, consulter ses comptes en ligne...

en toute sécurité, c'est possible !

Avec ESET Internet Security, naviguez sereinement sur Internet.
Vos données et votre vie numérique sont protégées !

Solution reconnue

Légère

100 VB100 AWARDS

AV comparatives

95% de clients satisfaits**

Testez et achetez en ligne sur
www.eset.com/fr/protection-donnees

*Profitez de la vie numérique en toute sécurité **Enquête réalisée en ligne en 2016 sur 1 159 répondants

NETTOYER

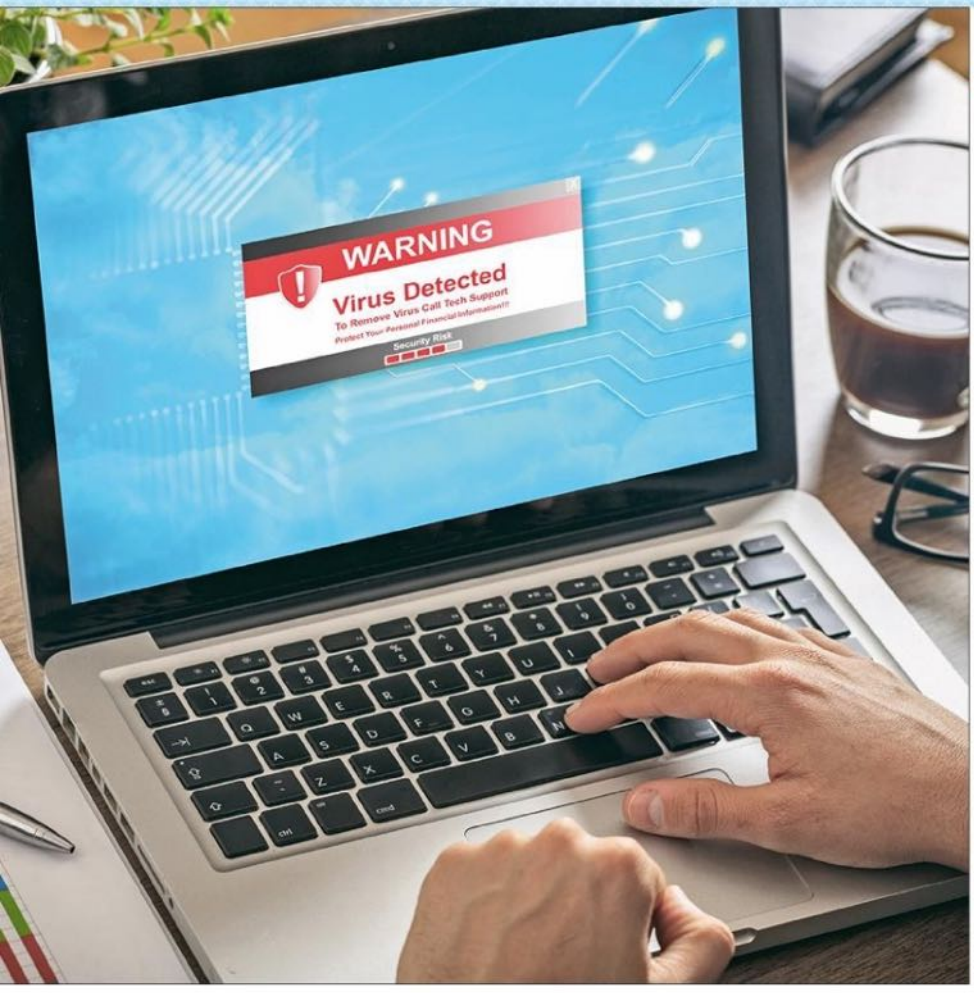
Comment les experts sécurité veillent sur nos PC


©Rawf8

SOMMAIRE

Avira, AVG, Avast, Norton, Sophos, Symantec, G-Data, F-Secure, ESET... Ces chasseurs de virus informatiques sont engagés depuis plus de vingt ans dans une guerre sans merci contre les pirates et les créateurs de malwares. Une bataille planétaire qui semble s'accélérer à mesure que le nombre d'objets connectés augmente. Selon les chiffres publiés par Symantec en avril 2016, 400 millions de personnes seraient victimes de cyberattaques chaque année dans le monde ! Un péril qui cible également les entreprises puisque, selon la même étude, 93 % d'entre elles ont déjà subi une tentative d'intrusion. Et si, pour un particulier, les conséquences se bornent souvent à quelques heures passées à remettre son ordinateur en état, elles s'avèrent plus sérieuses et dommageables pour les sociétés, allant jusqu'à interrompre temporairement leurs activités. Les logiciels de sécurité restent, quoi qu'on en dise, les meilleures armes contre les assauts des hackers.

Les éditeurs de solutions antivirus doivent s'adapter en permanence à l'imagination sans limite des cybercriminels. **Victimes de la mode.** La tendance du moment, ce sont les ransomwares (rançongiciels en français). En 2015, on a ainsi recensé plus de 391 000 agressions de ce type dans l'Hexagone, soit 2,6 fois plus qu'en 2014. Et si vous vous sentez à l'abri, retenez ce chiffre : le nombre de nouveaux programmes malveillants a atteint 430 millions rien qu'en 2015 ! Lutter contre les virus est non seulement une nécessité, mais un sacerdoce. Pour Jérôme Granger, responsable de la communication chez G-Data Software, *"le terme antivirus est aujourd'hui galvaudé. Certains avancent qu'une protection informatique ne sert à rien puisqu'il n'y aurait plus de risque. C'est pourquoi nous préférons utiliser le terme d'an-*



Virus, malwares, ransomwares... Sur Internet, jamais les risques n'ont été aussi variés et nombreux.

timalware. Un bon logiciel de sécurité doit protéger contre les virus, mais aussi contre les exploits (l'utilisation des failles logicielles), les chevaux de Troie, l'hameçonnage et tous les aléas qui pèsent sur l'intégrité des PC et des appareils mobiles." La difficulté consiste à rendre les programmes efficaces contre les périls connus, mais aussi capables de bloquer les nouveaux. Ceci, sans impacter les ressources de l'ordinateur ni gêner les usages quotidiens.

Jamais de risque zéro. D'un point de vue technique, rien n'empêcherait de développer une solution apte à repousser 100 % des attaques. Ce serait, hélas, au détriment de l'expérience des internautes, puisqu'il leur serait dès lors impossible d'installer la moindre appli, de télécharger des fichiers ou d'exécuter des scripts sur les pages Web. La mise en place de telles contraintes apparaît inacceptable. Elles constituent pourtant l'unique moyen d'assurer une étanchéité absolue car, comme le rappelle Jérôme Granger, *"le maillon faible, c'est l'utilisateur. Les logiciels ne peuvent pas tout faire!"* À défaut de gommer les négligences humaines, les éditeurs de solutions de sécurité sont engagés dans une course contre la montre avec les concepteurs de malwares. Car les criminels ont toujours un coup d'avance. *"Dans la lutte contre les dangers informatiques, la phase de collecte est primordiale. Elle repose en partie sur les logiciels antivirus installés chez les clients,* explique Jérôme Granger. *Dès*

430 millions de menaces ont été identifiées en 2015

EN SAVOIR PLUS

Cinq virus qui ont marqué l'histoire

1 Brain : le premier d'une longue série
Il faut remonter à 1986 pour trouver trace du premier virus. Inventé pour protéger un programme médical contre la copie illicite, Brain se propage par le biais de disquettes 5 pouces ¼ et ne provoque pas de dégâts.

2 Boza s'attaque à Windows
Boza apparaît en 1996 et vise spécifiquement Windows 95. Assez bénin, il se contente de se répandre pour infecter les fichiers et afficher un message le dernier jour de chaque mois.

3 Melissa en veut à la Terre entière
En se diffusant, en 1999, par le biais des messageries électroniques, Melissa est considéré comme le premier virus de masse. En cliquant sur la pièce jointe, le destinataire amorce un macrovirus qui contamine Office 97.

4 I Love You ou l'amour vache
Apparu en 2000, I Love You pollue des millions d'ordinateurs dans le monde au moyen d'un fichier attaché : un banal message d'amour ! Le script modifie la base de registre de Windows et masque l'extension de certains fichiers.

5 MyDoom.A se propage de lui-même
Créé en 2004, il se répand par mail ou via le service peer to peer Kazaa. Il infecte les contacts du carnet d'adresses des PC et ouvre une porte dérobée permettant une prise de contrôle à distance.

DO IT YOURSELF

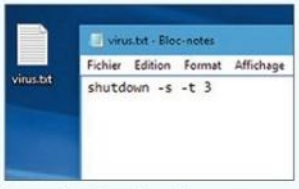
Fabriquez un virus en dix minutes chrono

Pour tester les réflexes de vos amis en matière de sécurité, tendez-leur un piège inoffensif. Ils vous diront merci !

ÉTAPE 1

Commencez par créer un document texte

Effectuez un clic droit sur une zone vierge du Bureau de Windows. Dans le menu contextuel, activez la commande ***Nouveau***, puis ***Document Texte***. Nommez ce fichier comme bon vous semble (***Virus***, dans notre cas, mais une appellation plus anodine facilitera sa diffusion !). Ouvrez le document dans l'appli ***Bloc-notes*** et saisissez-y ce texte : ***shutdown-s-t3***. Déroulez ensuite le menu ***Fichier***, ***Enregistrer***.

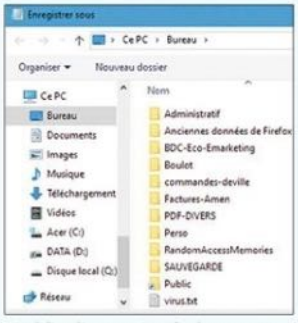


Une petite ligne de code compose votre virus. Simple et efficace.

ÉTAPE 2

Modifiez ensuite l'extension du fichier

Pour que cette ligne de code devienne un virus, une rapide manipulation s'impose. À ce stade, le fichier porte en effet l'extension ***.txt*** et se montre inapte à affecter un ordinateur. Déployez le menu ***Fichier*** et sélectionnez l'option ***Enregistrer sous***. Dans le champ ***Nom***, saisissez ***Virus.bat***. Une fois le document rebaptisé, son icône prend la forme d'engrenages, signifiant qu'il s'agit d'un script exécutable.



Modifiez l'extension du document pour en faire un fichier exécutable.

ÉTAPE 3

Testez le virus

Vous doutez de l'efficacité de votre création maison ? Alors faites un double clic sur le fichier. Votre ordinateur s'éteint sans délai, sans dommage bien sûr pour vos données, Windows se fermant tout en douceur. Si vous conservez le nom actuel (Virus.bat), personne ne cliquera dessus. Optez plutôt pour un intitulé plus engageant et expédiez-le par courriel à vos proches. Gageons que certains destinataires se laisseront prendre et exécuteront votre "virus" sans même réfléchir !

Attribuez à votre programme un nom qui donne envie de cliquer !

que nos radars détectent un code suspect, ils le transmettent anonymement à nos serveurs, à des fins d'analyse." D'autres méthodes sont aussi employées pour identifier les menaces inédites. Par exemple, des machines appelées "pots de miel" attirent et piègent les agents malintentionnés. Des robots de navigation explorent par ailleurs la Toile, en quête de pages pernicieuses (hameçonnage) ou infectées. Toutes ces données sont étudiées de façon automatique, 24 h/24 et 7 j/7, afin de déceler les fichiers dangereux et d'ajouter, dans l'heure, leur signature à la base de référence des logiciels qui veillent sur nos ordis et nos smartphones. L'efficacité de la protection réside dans cette faculté à répondre le plus vite possible – sinon instantanément. Pour récolter les infos, les éditeurs déploient des infrastructures complexes, composées de serveurs, de bots, de machines learning, mais aussi de spécialistes... en chair et en os. "*Les humains demeurent indispensables pour décortiquer les codes les plus sophistiqués*", soutient le porte-parole de G-Data.

Au plus profond du Darknet. Les concepteurs d'antivirus opèrent en sous-marin, en devant admettre, humblement, que l'outil parfait n'existe pas. Les défenses qu'ils imaginent seront toujours battues en brèche par des cybercriminels très inventifs. "*Nous devons améliorer en permanence nos techniques de détection proactives.*" Pour cela, tous les moyens sont bons ! Au sein des laboratoires de G-Data, un groupe de collaborateurs concentre ses recherches sur le Darknet, le Web parallèle accessible via le navigateur Tor. Leur mission consiste à infiltrer les forums, à récupérer des "kits exploits" pour examen, à repérer les dernières tendances en matière de logiciels hostiles. Une activité délicate car les pirates restent méfiants. Il faut souvent apporter une preuve de sa "bonne foi" – sous forme d'un code malveillant ou de données volées – pour pénétrer ces sites d'échanges... lesquels ne sont parfois accessibles que par cooptation. Pour parvenir à leurs fins, les agents doubles doivent ainsi recourir à des stratagèmes dignes des films d'espionnage en endossant, par exemple, plusieurs identités pour corroborer des informations fictives.. Leur seule limite ? "*Ne jamais payer pour soutirer des renseignements.*" ■

F-SECURE TOTAL

Une solution antivirus tout-en-un qui protège aussi votre vie privée

F-SECURE TOTAL – SÉCURITÉ ET VIE PRIVÉE sécurise tous les appareils de la maison (ordis, tablettes et smartphones) et veille à la confidentialité des informations personnelles.

01

PROFITEZ DE VOTRE VERSION D'ÉVALUATION

Pour profiter des 30 jours d'essai gratuit de la solution F-SECURE TOTAL sur trois de vos appareils (PC, Mac, smartphone ou tablette), rendez-vous sur le site **www.f-secure.com/total**. Cliquez sur le bouton *Essayer gratuitement* pour accéder au formulaire de création du compte My F-Secure. Renseignez votre adresse mail afin de recevoir le lien d'activation qui permettra de finaliser l'inscription.

02

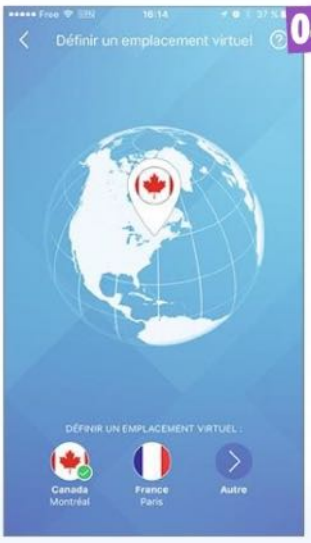
INSTALLEZ L'ANTIVIRUS SAFE SUR VOTRE ORDI

Une fois connecté à votre compte, cliquez sur *+Ajouter un appareil* puis sur *Ajouter votre premier appareil* pour télécharger et installer l'antivirus SAFE sur votre ordinateur (PC ou Mac). Afin de bénéficier de la *Protection de navigation*, vous êtes invité à ajouter une extension à votre navigateur Internet habituel (Firefox, Safari, Chrome, etc.) Voilà, tous les voyants sont au vert, votre ordinateur est protégé !

03

SÉCURISEZ AUSSI UN SMARTPHONE

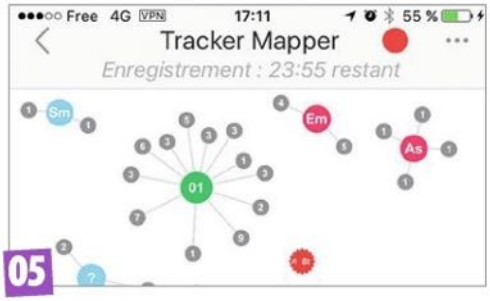
Depuis votre compte My F-Secure, ajoutez votre téléphone, ou celui d'un membre de la famille, à la liste des appareils protégés. Cliquez sur *+Ajouter un appareil, Ajouter une personne*. Renseignez le formulaire et activez *Envoyer une invitation*. Le destinataire reçoit ses identifiants de compte par mail et est invité à poursuivre l'installation sur son appareil mobile : Android, iPhone, Windows Phone…



04

PROTÉGEZ VOTRE VIE PRIVÉE

Tout ce que vous faites sur Internet peut être pisté, surveillé. Depuis votre compte, activez le logiciel F-SECURE FREEDOME afin de rester anonyme lorsque vous naviguez sur la toile depuis un ordi, un smartphone ou une tablette. FREEDOME protège votre connexion et votre vie privée. Vous pouvez modifier votre position géographique à volonté pour accéder à tous les contenus habituellement bloqués dans votre pays. Choisissez par exemple d'apparaître au Canada pour profiter de beaucoup plus de vidéos.



05

NE VOUS LAISSEZ PLUS PISTER !

Votre navigation laisse des traces. Certains sites n'hésitent d'ailleurs pas à vous pister pour utiliser ces infos – principalement à des fins publicitaires. FREEDOME identifie et bloque ce tracking intrusif. Mieux, grâce à la fonction *Traker Mapper*, vous accédez en temps réel à une carte qui répertorie les sites ayant tenté de vous pister. Impressionnant !

SYSTÈME macOS 10.12 et +, Windows 7 et +, Android 4.1 et +, iOS 8 et + **PRIX** à partir de 79,99 €/an **VERSION D'ÉVALUATION** à télécharger sur **www.f-secure.com/total**

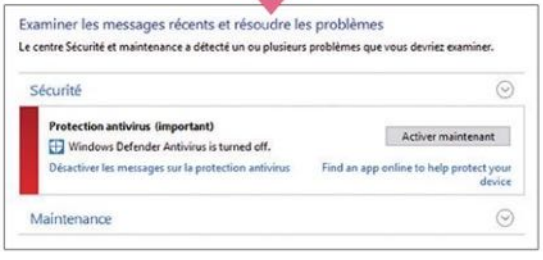
Dressez des barbelés

Pour se protéger des virus et autres malwares, inutile d'aller chercher très loin. Windows dispose d'un outil de sécurité efficace dès lors qu'il est correctement configuré.

Activez Windows Defender

L'antivirus de Microsoft est installé par défaut sur les PC équipés de Windows 10. Mais il se peut que le constructeur ait décidé d'y implanter une suite de sécurité proposée par un partenaire. Pour décliner ces offres commerciales, il suffit de mettre en service Windows Defender. Supprimez l'ancien antivirus (***Paramètres***, ***Système***, ***Applications et fonctionnalités***), puis redémarrez l'ordinateur. Windows indique que vous n'êtes plus protégé. Acceptez la notification, puis optez pour ***Activer maintenant***. Cliquez sur ***Activer***, au bas de la fenêtre de présentation des nouvelles fonctionnalités, et sur ***Fermer***. La protection en temps réel est restaurée.

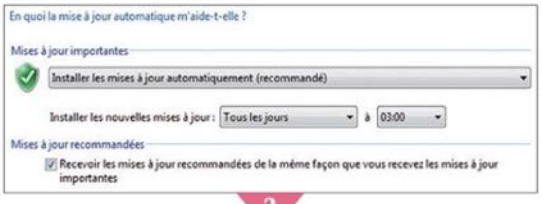
1



Actualisez la base des signatures

Coûte que coûte, Windows Defender doit être maintenu à jour, faute de quoi il deviendra inopérant face aux nouvelles menaces qui apparaissent quotidiennement et aux mutations de virus déjà connus. Après avoir activé le logiciel, rendez-vous sur l'onglet ***Mise à jour***. Vous êtes informé de la date et de l'heure de la dernière actualisation des définitions des virus et des logiciels espions. Cliquez sur le bouton ***Mettre à jour*** pour vérifier s'il n'existe pas des versions plus récentes de ces bases de données. Le téléchargement dure en principe moins d'une trentaine de secondes.

2



3

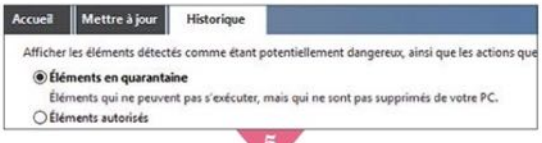
Assurez-vous de toujours disposer de la dernière version de l'antivirus

Windows Defender compte parmi les composants automatiquement mis à jour par Windows Update. Si vous utilisez la dernière mouture de Windows 10, vous n'avez donc à vous soucier de rien. Microsoft prend soin de systématiser le téléchargement et l'installation des correctifs de sécurité. Mais avec les versions 8.1 ou 7, il est possible que l'option de mises à jour automatiques soit suspendue. Procédez alors régulièrement à une recherche manuelle : ***Windows Update***, ***Rechercher des mises à jour***.

4

Lancez une première analyse du disque dur

Il existe un risque infime de voir votre PC infecté durant les minutes qui séparent la suppression de l'ancien antivirus et l'activation de Windows Defender. Depuis l'onglet ***Accueil***, cochez la case ***Complète*** dans la section ***Option d'analyse***, puis cliquez sur ***Analyser maintenant***. Windows Defender entreprend dès lors un examen approfondi du disque dur, passant en revue les composants système, données personnelles, fichiers temporaires...



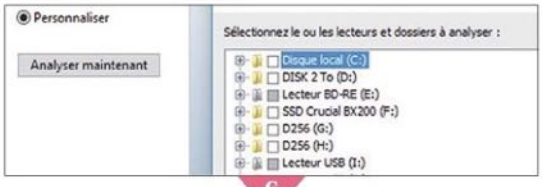
5

Éradiquez les menaces

Au terme de cette analyse minutieuse, Windows Defender affiche le nombre de fichiers traités. Pour en savoir plus sur les éventuels risques décelés, rendez-vous dans l'***Historique*** et activez ***Afficher les détails***. Les éléments jugés dangereux sont aussitôt écartés. Faites ***Supprimer tout*** pour les effacer définitivement.

DIFFICULTÉ
Modérée
TEMPS
30 min

autour de votre PC



6

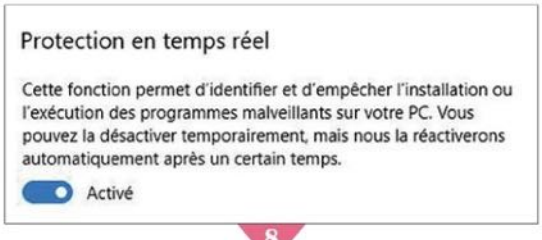
En cas de doute, procédez à un examen ciblé

Le principe d'un antivirus consiste à surveiller en permanence l'activité de votre PC. Une telle exploration n'est pas infaillible. Rien ne vous empêche donc de soumettre un fichier (ou un support de stockage externe) aux outils de détection de Windows Defender. Dans l'onglet ***Accueil***, optez pour ***Personnaliser***, puis pour ***Analyser maintenant***. Désignez un emplacement et approuvez (***OK***).

7

Profitez d'un niveau de sécurité optimal

Cliquez sur l'icône ***Paramètres*** en haut à droite de l'onglet ***Historique*** de Windows Defender. Vous voilà dirigé vers la page des ***Paramètres*** de Windows 10 dédiée à l'antivirus. Assurez-vous que l'option ***Protection dans le Cloud*** est activée. De cette façon, vous avez l'assurance d'être prémuni contre les dernières menaces identifiées sans devoir attendre la prochaine mise à jour des définitions des virus et des logiciels espions (étape 2).



8

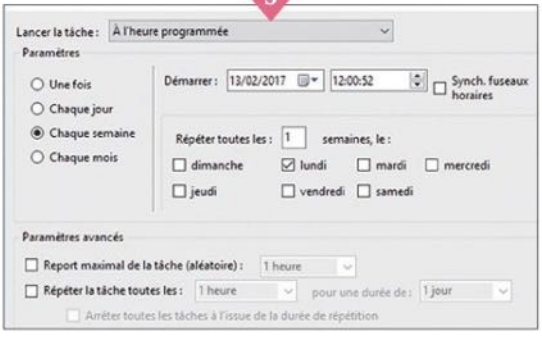
Suspendez la protection en temps réel pour installer un logiciel

Il arrive que Windows Defender considère l'appli que vous tentez d'importer comme un virus. Si vous êtes certain de l'innocuité de ce programme, ouvrez les ***Paramètres***, cliquez sur ***Mise à jour et sécurité***, ***Windows Defender*** et désactivez ***Protection en temps réel***. Rétablissez cette fonctionnalité une fois le logiciel en place.

Planifiez une analyse approfondie du PC

En matière de sécurité, on n'est jamais trop prudent... Si Windows Defender garantit une analyse constante, il est fortement conseillé de compléter cet audit par un examen périodique du contenu de l'ordinateur. Vous pouvez d'ailleurs confier au système le soin de planifier cette besogne. Saisissez ***Tâches planifiées*** dans la zone de recherche et activez ***Tâches planifiées-Panneau de configuration***. Dans le volet de navigation, déroulez le menu ***Bibliothèque du Planificateur de tâches***, ***Microsoft***, ***Windows***. Ouvrez le dossier ***Windows Defender***, puis double-cliquez sur ***Analyse planifiée de Windows Defender***. Optez pour l'onglet ***Déclencheurs***, puis pour le bouton ***Nouveau***. Là, définissez la fréquence de l'analyse (chaque mois, chaque semaine...) et décidez du jour de la semaine et de l'horaire auxquels aura lieu l'opération – préférez un moment où vous savez votre PC allumé. Enregistrez ces réglages (***OK***).

9



À votre convenance, faites cohabiter Windows Defender et un autre antivirus

Depuis Windows 10, rien n'empêche d'exploiter plusieurs outils de protection sur le même appareil. Vous pouvez ainsi déléguer la surveillance en temps réel à Avast ou à Eset, tout en continuant à mener des analyses périodiques avec Windows Defender. Ce dernier étant automatiquement désactivé lorsque vous installez un nouvel antivirus, accédez à ses ***Paramètres*** pour restaurer la fonction ***Analyse périodique limitée***. ■

10

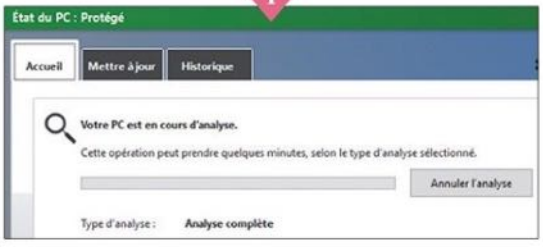
Reprenez le contrôle d'un ordinateur bloqué

Certains logiciels malveillants ont la peau dure. Voici comment réagir lorsque l'antivirus de votre PC échoue à déloger l'un d'entre eux ou si vous n'avez plus accès à Windows ni à Internet.

Effectuez une analyse approfondie

Commençons par le cas d'un ordinateur qui n'est pas encore bloqué, mais où vous percevez des réactions laissant penser à une infection : temps de chargement des pages Web trop long, logiciels qui ne démarrent pas ou qui plantent inopinément... Lancez alors votre antivirus, ici ***Windows Defender***, et procédez à une analyse approfondie du disque dur. Le logiciel de sécurité passe en revue tous les disques durs, partitions et dossiers du PC, y compris les fichiers temporaires. Si rien d'anormal n'est détecté, il faut envisager des mesures plus radicales.

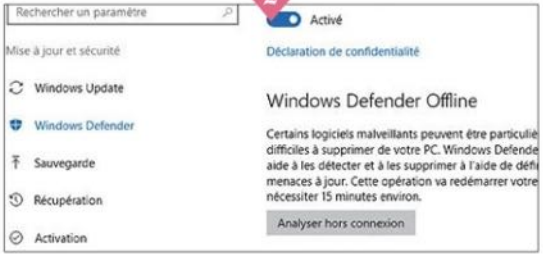
1



Lancez une recherche en mode hors ligne

Windows Defender offre un mode d'analyse off line qui traque les virus avant même le démarrage du PC. Il évite ainsi qu'un programme hostile prenne le contrôle de votre ordinateur, sans que vous puissiez plus tard l'y déloger. Enregistrez vos fichiers et coupez toutes les applis. Allez dans les ***Paramètres*** de Windows, cliquez sur ***Mise à jour et sécurité***, ***Windows Defender***, puis sur ***Analyser hors connexion***. L'appareil redémarre et affiche une fenêtre d'analyse. Voilà les menaces potentielles circonscrites. Windows se lance ensuite automatiquement.

2



3

Faites appel à un antivirus en ligne

Votre logiciel de sécurité se montre impuissant à repousser les ennemis ? Avant de songer à le remplacer, prenez le temps de solliciter un outil d'analyse en ligne. Ce dernier fonctionne à partir d'un navigateur Internet, après avoir installé une extension ou un programme très léger sur le PC. Attention toutefois, ces services en ligne ne procèdent à aucune analyse en temps réel. Réservez-les donc à un usage complémentaire et ponctuel. Rendez-vous sur le site de F-Secure Online Scanner : ***bit.do/detcw***.

4

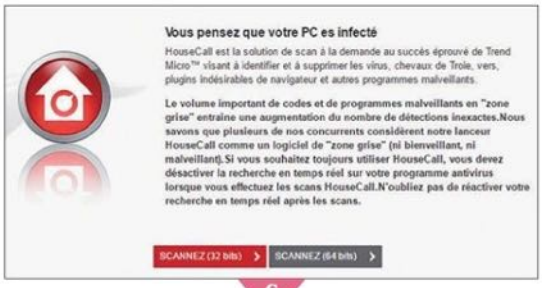
Installez le module sur votre ordinateur

Cliquez d'abord sur le bouton ***Lancer dès maintenant***. Vous déclenchez ainsi le téléchargement du fichier F-SecureOnlineScanner.exe. Faites un clic droit sur cet élément et activez la commande ***Ouvrir***. Pointez ensuite ***Accepter et Analyser***, puis confirmez l'exécution du programme. Celui-ci commence par rapatrier la base de données des signatures de virus et de malwares.

5

Vérifiez l'intégrité du PC

Une fois le téléchargement achevé, l'analyse démarre. Une jauge vous montre à tout instant son état d'avancement. F-Secure vérifie tour à tour les éléments de la mémoire vive et ceux du disque dur système. Tout fichier suspect est aussitôt mis en quarantaine.



6

Recueillez les avis de plusieurs experts

Les antivirus en ligne agissent sans jamais interférer avec votre logiciel interne de sécurité. Si F-Secure n'a identifié aucune menace, n'hésitez pas à solliciter d'autres services, dans le but d'affiner vos investigations: ***HouseCall de Trend Micro (bit.do/detyA), Panda Activescan (bit.do/detyJ), Bitdefender QuickScan (bit.do/detyv)...***

7

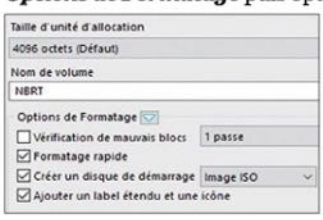
Prévoyez une clé USB de secours...

Votre navigateur Internet refuse de se connecter au moindre service en ligne et Windows ne répond plus, interdisant l'activation de l'analyse off line de Windows Defender? Vous devez transiter par un disque de secours pour chasser les logiciels venimeux. Puisque votre PC est bloqué, la création de ce support doit s'accomplir depuis un autre ordinateur. Lancez un browser et dirigez-vous vers la page ***bit.do/detzS***. Cliquez sur ***Télécharger***. Allez ensuite sur le site ***bit.do/detAd*** pour y récupérer l'utilitaire gratuit ***Rufus***.

8

... et rendez-la bootable

L'outil Rufus va rendre bootable la clé de secours. Faites défiler la page jusqu'à la section ***Téléchargement*** et activez le lien ***Rufus 2.12 portable***. Déplacez le fichier obtenu sur le Bureau. Opérez un clic droit pour autoriser la commande ***Exécuter en temps qu'administrateur***. Branchez une clé USB (de 2 Go minimum), déroulez le menu ***Options de Formatage*** puis optez pour ***Créer un disque de démarrage-Image Iso***. Sélectionnez l'icône située à côté, désignez le fichier ***nrbt.iso*** téléchargé à l'étape précédente. Pour finir, vous pouvez ***Démarrer***.



Changez la séquence de boot du PC

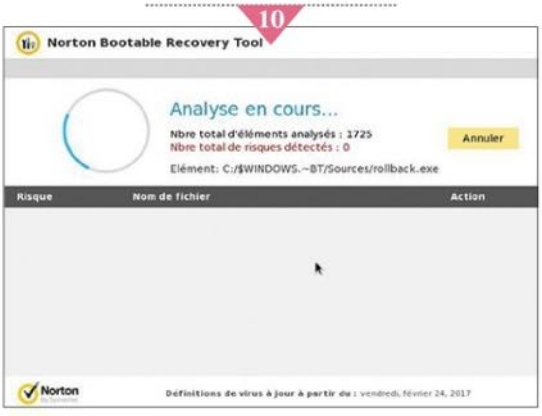
Votre clé est dorénavant prête. Débranchez-la et connectez-la au PC infecté. Son utilisation implique de la booter sur le support amovible. Déroulez le menu ***Démarrer***, cliquez sur ***Marche/Arrêt*** puis sur ***Redémarrer***. Si l'ordinateur boote sur Windows et non sur la clé USB comme voulu, vous devrez effectuer une modification dans le Bios. Relancez l'ordinateur et appuyez sur la touche d'accès au Bios: ***F2***, ***Suppr*** ou ***Esc***, selon la marque de votre carte mère. Repérer la section correspondant à la séquence de boot et placez l'option ***USB*** en tête de liste. Si vous utilisez un Bios UEFI – c'est le cas de la plupart des machines récentes –, inutile de changer la séquence de boot. Cliquez simplement sur ***Démarrage*** et désignez votre clé USB dans la liste des disques.

9

Chargez Norton Bootable Recovery Tool

Norton ***(bit.ly/2dC21Bh)*** présente tout d'abord un compte à rebours. Laissez les secondes s'égrainer et attendez qu'apparaisse la liste des langues. Choisissez ***Français***, puis cliquez sur ***OK*** et acceptez le contrat de licence. Vous pouvez alors lancer l'analyse du disque dur. L'opération peut durer plusieurs dizaines de minutes selon le nombre de fichiers à contrôler. Une fois la vérification terminée et la menace écartée, utilisez le menu ***Shut down the computer***, en bas à gauche de l'écran, pour redémarrer l'ordinateur et accéder à Windows. ■

10



Offrez à votre Mac une

Avec Apple, pas besoin d'antivirus. Si cette affirmation était peut-être vraie il y a quelques années, macOS subit désormais de nombreuses cyberattaques, au même titre que Windows.

Choisissez votre logiciel de protection

Il existe de nombreux antivirus gratuits, y compris pour macOS: Kaspersky Virus Scanner (***bit.do/daJ6G***), Avira Free (***bit.do/daJ6z***), AVG Antivirus (***bit.do/daJ6u***)... Vous avez l'embarras du choix. Ces solutions procurent un niveau de protection élevé, comparable aux versions payantes proposées par les éditeurs. Les différences résident principalement dans les options, plus nombreuses si vous acceptez de souscrire un abonnement à vos frais. La fréquence de mise à jour des bases de signatures constitue l'élément de choix essentiel. Kaspersky, Avira et AVG diffusent ainsi plusieurs actualisations par semaine. C'est aussi le cas d'Avast 8 que nous avons retenu ici. Ce dernier dispose d'un module de surveillance continue qui ne ralentira pas votre Mac.

1

Installez la solution antivirale Avast 8

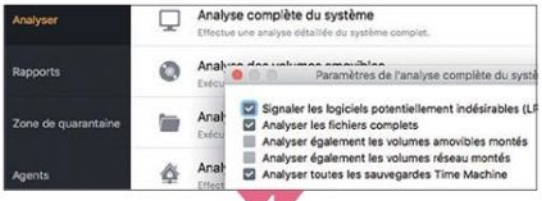
Afin de télécharger la version gratuite de l'antivirus, connectez-vous à l'adresse ***bit.do/daKaJ*** et glissez l'icône du logiciel dans le dossier ***Applications***. Mais avant toute chose, rappelez-vous qu'il ne faut jamais faire cohabiter deux antivirus sur un même Mac, au risque de provoquer des conflits. Pour supprimer les éventuelles solutions de sécurité déjà présentes, ouvrez le dossier ***Applications*** dans le ***Finder***, faites un clic droit sur l'icône de l'ancien antivirus et optez pour ***Placer dans la corbeille***. Sinon, libre à vous d'éliminer le doublon grâce à une appli spécialisée comme ***AppCleaner (bit.do/dfDhh)***.

2

3

Lancez une première analyse du Mac

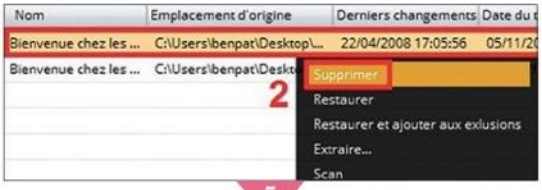
Au terme de l'installation, Avast actualise sa base de définition de virus et de logiciels malveillants. Une fois cette formalité accomplie, effectuez une première analyse de votre système. Pour ce faire, cliquez sur l'icône d'***Avast*** présente par défaut dans la barre des menus de macOS, puis sur la commande ***Ouvrir Avast***. Lorsque la console s'affiche, allez dans le volet de gauche, sur l'intitulé ***Analyser***. Activez ensuite le bouton ***Démarrer*** qui se trouve à droite de la commande ***Analyse complète du système***, dans le volet principal de la fenêtre.



4

Décidez ce qui sera ou non vérifié

Même si la protection en temps réel est censée vous avertir quand une menace apparaît, cela ne doit pas occulter la nécessité de procéder régulièrement à une analyse complète de votre ordinateur. Si cette opération dure trop longtemps à votre goût, vous pouvez restreindre le champ de la vérification. Sous ***Démarrer***, cliquez sur ***Paramètres***, puis sur le bouton ***+*** afin d'indiquer les dossiers que vous souhaitez ignorer.



5

Gérez la zone de mise en quarantaine

Dès qu'un intrus est détecté, une alerte s'affiche à l'écran. Il vous faut alors agir vite. Optez pour une suppression définitive de l'élément en question. En cas de doute, placez plutôt le fichier en zone de quarantaine. Ainsi, il ne pourra plus infecter votre ordinateur.

DIFFICULTÉ
Aucune
TEMPS
25 min

protection gratuite

6

Activez les différents modules de protection

Toujours depuis la console d'administration d'Avast 8, rendez-vous dans le volet gauche, sur la commande ***Agents***. L'antivirus gratuit s'articule autour de trois outils : l'agent des fichiers (qui porte sur le contenu des disques durs et des supports amovibles), l'agent de messagerie (pour vos boîtes de réception) et enfin l'agent Web (qui veille sur les contenus affichés et téléchargés depuis Internet). Pour arrêter ou personnaliser le fonctionnement de ces modules, validez successivement ***Préférences*** et ***Agents***.

7

Créez des listes d'exclusion de l'agent Web

Il est permis d'exclure certains sites Web, réputés sûrs, de la zone de vigilance de l'antivirus. Dans le panneau des ***Préférences*** d'Avast, activez la commande ***Paramètres***, près de l'intitulé ***Agent Web***. Optez ensuite pour ***Signaler les logiciels potentiellement indésirables***, puis ***Analyser les fichiers pendant le téléchargement***. Intéressez-vous ensuite à la section ***Serveurs exclus***. Actionnez le bouton + et saisissez une à une les adresses des sites et des domaines ne présentant a priori aucun risque.

8

Personnalisez les notifications

Pouvoir compter sur un antivirus qui veille sur son Mac, c'est toujours rassurant... Encore faut-il ne pas passer à côté des alarmes diffusées par Avast ! Dans les ***Préférences*** de l'appli, cliquez sur l'onglet ***Fenêtres indépendantes***, puis définissez la durée d'affichage et la position des boîtes d'alerte sur l'écran.

Configurez les mises à jour

Pour que votre antivirus demeure efficace, il doit être maintenu à jour. Cela concerne le programme lui-même, qui reçoit des améliorations régulières, mais aussi les bases de données qui lui servent à identifier les intrus. Pour ne plus vous tracasser à ce sujet, il suffit d'automatiser la mise à jour des signatures. Affichez pour cela la page des ***Paramètres*** d'Avast. Sélectionnez ensuite l'onglet ***Mises à jour***. Puis, dans la section ***Base de données virale***, cochez les options ***Mettre à jour la base de données virale automatiquement*** et ***Activer les mises à jour en continu***. Dans la rubrique ***Programme***, approuvez ***Mettre à jour le programme automatiquement*** et désactivez l'option ***Utiliser le canal bêta***.

9

Consultez les rapports d'activité

Avast 8 consigne son activité dans un journal : les analyses effectuées et leurs résultats, le nombre de pages Web et de fichiers contrôlés, etc. Pour en prendre connaissance, rendez-vous dans le volet gauche de la console, sur l'onglet ***Rapports***. Le tableau de bord qui apparaît dresse un bilan complet des actions menées au cours des trente derniers jours. En validant le bouton ***Ouvrir***, vous obtiendrez des statistiques plus détaillées. ■

10

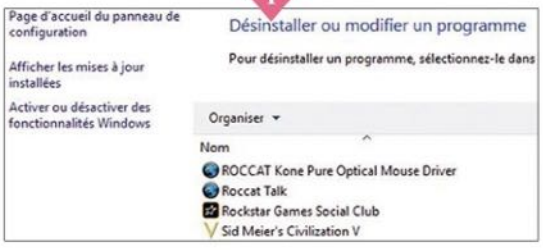
Débusquez et éradiquez les malwares pour de bon

Certains programmes très rusés ne perturbent pas de manière visible le fonctionnement de votre PC. Mais leur pouvoir de nuisance reste bien réel. Voici comment faire pour vous en débarrasser.

Éliminez les logiciels malveillants visibles

Un malware est un logiciel malveillant qui ne trouble pas forcément la stabilité de votre ordinateur. Il peut même tranquillement s'installer et s'inviter de temps à autre sur votre navigateur. Des annonces pop-up ou de fausses notifications de sécurité vous invitent alors à vous équiper... d'un antimalware aussi cher qu'inefficace ! Si l'indésirable est clairement identifié, faites un clic droit sur le menu ***Démarrer*** de Windows et accédez à la fenêtre ***Programmes et fonctionnalités***. Repérez-le dans la liste qui apparaît et procédez à sa désinstallation.

1



Installez l'utilitaire Malwarebytes

Quelques malwares se contentent d'afficher des publicités, tandis que d'autres s'avèrent dangereux. Ainsi, les ransomwares chiffrent vos fichiers et demandent une rançon en échange de la clé de déchiffrement. Les chevaux de Troie ou les enregistreurs de frappe (keylogger), capables d'intercepter les mots de passe que vous saisissez, constituent aussi des risques à prendre au sérieux. Pour les chasser, un utilitaire spécialisé s'impose, comme Malwarebytes (***bit.do/deue3***). Cliquez sur ***Téléchargez gratuitement***.

2

3

Recherchez les malwares déjà présents

Le programme se lance au terme de l'installation. Depuis le ***Tableau de bord***, assurez-vous en premier lieu que la base de données est à jour. Choisissez ensuite ***Analysez maintenant***. Rien de plus simple ! Une vérification régulière s'impose pour éloigner les menaces. Vous pouvez commander l'opération manuellement ou la planifier dans Windows (voir étape 9) – l'outil de planification de Malwarebytes étant réservé à la version payante.

4

Déclarez un faux positif

La version gratuite de Malwarebytes autorise peu d'options de personnalisation. On note toutefois la possibilité d'exclure les faux positifs, c'est-à-dire les éléments considérés à tort comme dangereux. Affichez l'onglet ***Paramètres***, cliquez sur ***Exclusions des programmes malveillants*** et désignez le fichier à ne plus analyser.

5

Consultez l'historique des menaces

Sélectionnez cette fois l'onglet ***Historique*** dans la section ***Quarantaine***. Les fichiers considérés comme nocifs s'affichent dans la fenêtre principale. S'il ne s'agit pas de faux positifs (auquel cas, pointez dessus et activez la commande ***Restaurer***), vous pouvez les supprimer.

6

Supprimez une publicité récalcitrante

À l'instar de certaines autres applications spécialisées, AdwCleaner se révèle très performant face aux logiciels publicitaires malintentionnés et autres barres envahissantes. Vous trouverez ce logiciel gratuit à l'adresse suivante : ***bit.do/deuSB***. Il fonctionne sans installation préalable et s'exécute depuis une clé USB.

7

Analysez, évaluez et effacez !

Une fois l'application en action, cliquez sur ***Analyser***. Si AdwCleaner détecte une ou plusieurs menaces, ne paniquez pas. Il ne s'agit pas d'un virus et votre ordi n'est pas forcément en danger. Lisez attentivement le résultat des analyses afin d'identifier le logiciel incriminé et d'évaluer le niveau de dangerosité : ce n'est parfois qu'une simple extension ajoutée à un navigateur, d'une clé de registre modifiée, d'un fichier corrompu... Désinstallez au besoin l'élément désigné, puis relancez une analyse. Si les symptômes persistent, cliquez sur ***Nettoyer***.

8

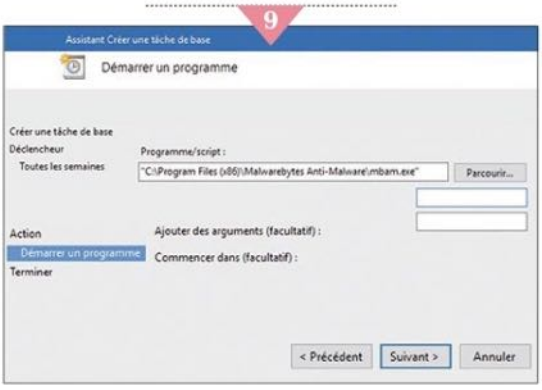
Préservez-vous des annonces avec Adblock Plus

Nous entrons là dans le domaine du préventif. Une bonne façon de se prémunir contre les malwares hérités de visites sur des sites Web infectés consiste à installer un bloqueur de pubs, tel Adblock Plus (***bit.do/dfDsd***). En interdisant les fenêtres pop-up et l'affichage forcé des onglets, cette extension vous garde des pages d'hameçonnage. Ne levez pas cette protection sans avoir la certitude que le site que vous parcourez ne présente aucun risque.

Programmez des vérifications

L'usage régulier d'un logiciel antimalware reste la meilleure arme contre les logiciels malveillants. Il s'agit d'un indispensable complément à votre antivirus. Si la version gratuite de Malwarebytes n'offre pas la faculté de planifier une analyse régulière, Windows permet de passer outre cette limitation. Recherchez et lancez le ***Planificateur de tâches***. Activez la commande ***Créez une tâche de base*** et nommez cet élément ***Scan de Malwarebytes***. Une fois sur la fenêtre ***Déclencheur***, définissez la périodicité souhaitée (***hebdomadaire***, par exemple) et indiquez le jour et l'heure auxquels aura lieu l'analyse. Dans les ***Types d'action***, cochez ***Démarrer un programme***. Cliquez sur ***Parcourir*** et repérez le fichier ***mbam.exe*** dans le dossier ***Malwarebytes***. Sélectionnez ***Suivant***, ***Terminer***. Malwarebytes s'exécutera désormais chaque semaine, à l'heure que vous avez décidée... pourvu que votre PC soit allumé.

9



Utilisez les patchs antimalware développés par les éditeurs de solutions de sécurité

Il existe des logiciels malveillants plus difficiles à éradiquer que d'autres. Si Malwarebytes ne réussit pas à éliminer l'un d'eux, jetez un œil à la liste des processus actifs affichés par le ***Gestionnaire des tâches***. Lancez ensuite une recherche sur le nom du malware dans ***Google*** ou dans la base de connaissance du site d'***Avast***, sinon dans celle de ***Microsoft***. Vous y trouverez peut-être un remède prêt à l'emploi, sous la forme d'un petit patch à exécuter plus tard sur votre PC. ■

10

Les applications qui vous protègent vraiment

À chaque menace sa réponse ! Ne croyez pas qu'un antivirus vous préserve de tous les traquenards. Pour naviguer et télécharger en gardant l'esprit tranquille, mieux vaut se constituer une trousse à outils des plus complètes.

Avira
Profitez d'un antivirus gratuit sans faiblesse

Microsoft recommande un certain nombre d'antivirus à ses clients réticents à confier la défense de leurs données à Windows Defender. Depuis le ***Panneau de configuration***, cliquez sur ***Système et sécurité***, ***Sécurité et maintenance*** et ***Rechercher une application en ligne pour renforcer***. Sélectionnez votre version de Windows. Optez pour le logiciel ***Avira***, puis pour ***Téléchargement gratuit***. Grand concurrent d'Avast, Avira se positionne dans le top 3 des meilleures solutions de sécurité dans les comparatifs 2016. L'édition gratuite protège des virus en temps réel et sécurise la navigation en bloquant les sites infectés. Il profite en plus d'une base de données dans le cloud. Les menaces, relayées par les millions d'utilisateurs du programme, sont ainsi collectées et analysées en direct afin de venir enrichir, instantanément, la base des signatures de virus. Pour bénéficier d'une protection des mails et d'un VPN, il faudra en revanche souscrire un abonnement payant.

Avira pour Windows et Mac – Gratuit
bit.do/c8KQg

AdwCleaner
Désinstallez les programmes publicitaires indésirables

Preuve de sa grande efficacité, le balai magique AdwCleaner a récemment été racheté par l'américain Malwarebytes, spécialiste de la lutte contre les logiciels malveillants. Il est important de l'activer au moins une fois par mois pour jouir d'une efficacité optimale. AdwCleaner recherche les programmes publicitaires, les softs indésirables, les barres d'outils additives dont on n'arrive jamais à se débarrasser, ainsi que les hijackers, ces logiciels qui remplacent la page de démarrage du navigateur par de la réclame. En quelques minutes, les menaces sont repérées, affichées et éradiquées. AdwCleaner est compatible avec toutes les versions de Windows, de XP à Windows 10, 32 bits et 64 bits.

AdwCleaner pour Windows – Gratuit
bit.do/c8KAJ

Bitdefender
La meilleure façon de protéger votre Mac

Bien qu'un Mac soit moins sujet aux virus qu'un PC, mieux vaut tout de même installer une solution de sécurité. Le risque zéro n'existe pas – pour preuve, la découverte l'an dernier du ransomware KeRanger dont le but consistait à soutirer de l'argent aux internautes pour leur restituer l'accès à leurs données rendues inaccessibles. Le coût

BITDEFENDER ANALYSE RAPIDE
Et si vous scanniez votre disque dur à la recherche d'éléments nocifs ?

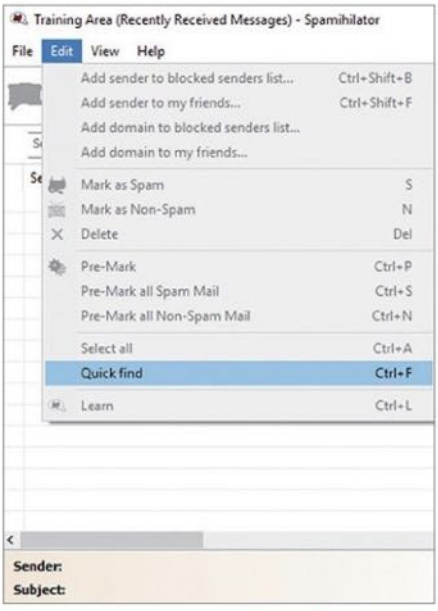
Pour savoir si un logiciel malveillant menace votre ordinateur, profitez d'une détection en ligne orchestrée par Bitdefender.

Même en disposant d'un antivirus actif et à jour sur votre PC, il n'est pas superflu, de temps à autre, de réaliser une analyse en ligne depuis les serveurs distants d'un éditeur de solutions de sécurité. Cette opération accroît les chances de déceler des menaces cachées que n'aurait pas forcément décelées votre programme habituel. Plusieurs spécialistes proposent ce type d'outils. Gratuites et sans obligation d'achat, ces applis se contentent en général de pointer les menaces, sans les éradiquer. Ce sera à vous d'activer plus tard un antivirus ou un antimalware, de façon à les placer en quarantaine.

En moins de soixante secondes, vous saurez si votre PC est infecté.

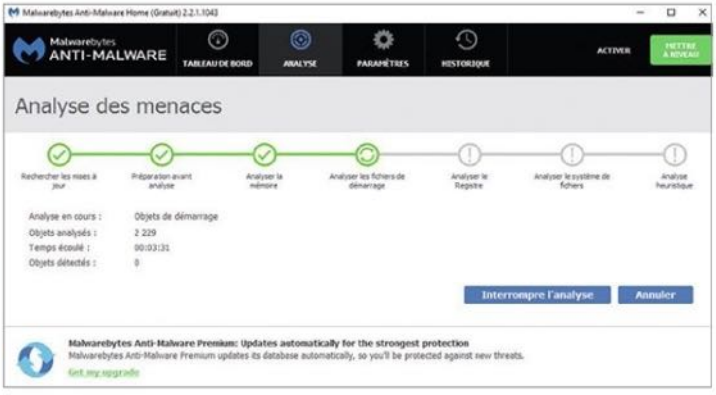
Nous vous conseillons d'effectuer ce type d'analyse environ une fois par mois. Le service antivirus de Bitdefender compte parmi les plus efficaces.

Bitdefender Analyse rapide pour Windows – Gratuit
bit.do/c8LFC



Spamihilator, s'intègre à votre logiciel de messagerie pour traquer les courriels publicitaires et les messages dangereux.

Malwarebytes analyse la mémoire, les fichiers au démarrage, la base de registre et le système de fichiers, à la recherche d'éléments suspects.



La solution de protection totale de F-Secure inclut un VPN qui masque votre adresse IP. L'anonymat de vos échanges sur Internet est ainsi préservé.

de la tranquillité ? La vingtaine d'euros nécessaire pour se payer les services de l'antivirus Bitdefender for Mac durant une année. Cet outil garantit un haut niveau de protection sans influer sur les performances de l'ordinateur. La version payante de Bitdefender lutte contre les virus et les malwares ; elle bloque en outre les logiciels publicitaires et s'avère plutôt douée pour déjouer les tentatives de chiffrement de vos données à des fins de rançon. Bitdefender sauvegarde pour cela les fichiers et les restaure en cas de problème.

Bitdefender pour Mac – 19,95 € pour un poste
bit.do/c8KHy

Malwarebytes
Luttez contre les menaces globales

Votre ordi ralentit de façon inexpliquée ? Votre navigateur Internet se réveille paré de barres d'outils et de pages d'accueil bizarres ? Les fenêtres pop-up pullulent ? Alors le recours à Malwarebytes s'impose sans tarder. Cet utilitaire détecte les programmes indésirables, du plus anodin au plus virulent. La version Premium, facturée quelque 40 € par an, veille en permanence sur l'état du PC et sert à planifier des analyses périodiques. Deux options dont est dénuée l'offre gratuite, limitée à un module de vérification qu'il faut activer manuellement.

Malwarebytes pour Windows – Gratuit
bit.do/c8KMX

F-Secure Total
Une solution universelle pour surveiller tous vos appareils

En 2016, F-Secure est sorti vainqueur du test Real World Protection du site spécialisé AV Comparative. Ce test confronte les antivirus à des attaques telles qu'elles apparaissent au quotidien. Faux sites Web, publicités non souhaitées, logiciels hostiles... F-Secure réagit à toutes les tentatives de contamination. Il préserve aussi la vie privée des utilisateurs grâce à un réseau fibré virtuel (VPN) intégré qui anonymise l'échange de données et qui neutralise les sites espionnant vos activités. F-Secure s'occupe encore des transactions bancaires en ligne, dispense un contrôle parental et se décline sur toutes sortes d'appareils : PC, Mac, Android, iOS...

F-Secure Total – 79,99 € pour trois appareils
bit.do/c8K6w

Spamihilator
Sus aux spams !

Les fonctionnalités intégrées aux clients de messagerie ne suffisent pas toujours à contrer les courriels indésirables. Spamihilator dissèque les mails qui vous parviennent, l'efficacité de son dispositif progressant au fil du temps et de l'analyse de votre correspondance. Le programme fonctionne avec de nombreux clients de messagerie, dont Outlook ou Thunderbird. Atout supplémentaire : sa gratuité.

Spamihilator pour Windows – Gratuit
bit.do/c8K8f

DIFFICULTÉ
Aucune
TEMPS
20 min

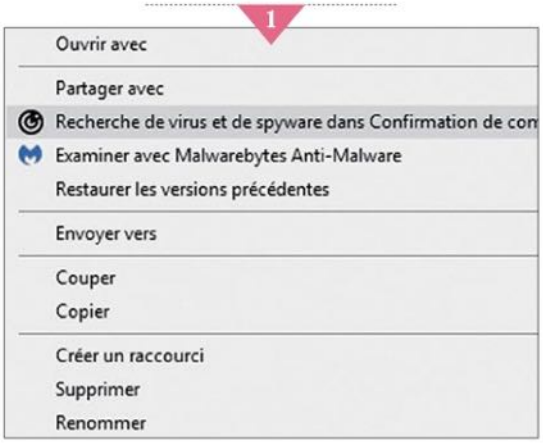
Vérifiez l'innocuité des fichiers que vous téléchargez

Mieux vaut prévenir que guérir... Vous aurez beau installer tous les logiciels de sécurité du monde, votre ordinateur demeurera vulnérable aux attaques si vous n'adoptez pas quelques précautions élémentaires. Voici lesquelles.

Avant d'ouvrir vos pièces jointes, passez-les toutes au crible

Si vous recourez à un client de messagerie, cliquez avec le bouton droit de la souris sur le fichier attaché au mail reçu. Dans le menu contextuel qui s'affiche, activez la commande ***Analyser*** ou ***Rechercher avec*** qui correspond à votre solution antivirus. Si vous ne trouvez pas ce raccourci, enregistrez le document sur le Bureau de Windows et effectuez l'opération précédente pour vérifier que le fichier ne comporte pas de menace.

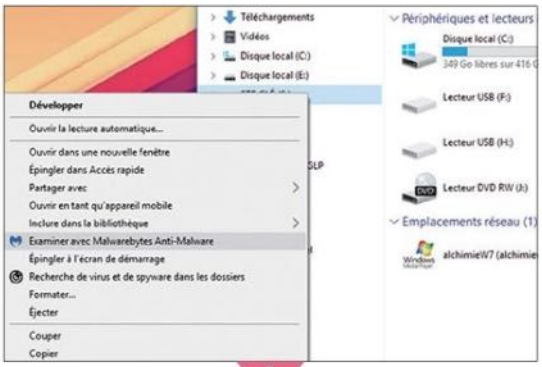
1



Pour plus de sécurité, préférez un webmail

Si vous avez opté pour un webmail (Outlook.com, Gmail...), sachez que les pièces jointes sont systématiquement analysées en amont. Ainsi, le service de messagerie de Google bloque les fichiers exécutables et les macros détectées dans les courriels. Dans tous les cas, n'ouvrez aucun document suspect sans l'avoir soumis, au préalable, à votre antivirus.

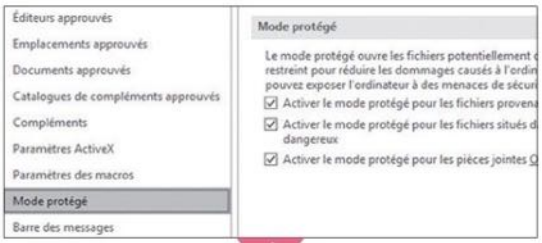
2



3

Inspectez les pièces rapportées

Pour être certain que la clé USB ou le disque dur externe que vous venez de brancher au PC ne contient pas de virus, ouvrez l'***Explorateur de fichiers*** de Windows à l'aide du raccourci clavier ***Windows*** + ***E***. Repérez l'icône du nouveau matériel dans le volet de navigation et opérez un clic droit. Activez ensuite la commande ***Recherche de virus***. Faites enfin un second contrôle avec un programme antimalwares si vous en avez installé un sur votre poste.



4

Désactivez les macros dans Microsoft Office

Les macros sont des commandes autorisant l'exécution automatique de tâches au sein d'un programme. Certaines peuvent avoir été écrites par un pirate pour introduire un virus. Mieux vaut donc les désactiver. Dans ***Microsoft Office***, accédez au ***Centre de gestion de la confidentialité*** en cliquant sur ***Fichier***, ***Options***, ***Centre de gestion de la confidentialité***, ***Paramètres du centre de gestion***, ***Paramètres des macros***. Cochez l'option ***Désactivez toutes les macros sans notification***, puis toutes les cases dans la section ***Mode protégé***. ■

DIFFICULTÉ
Modérée
TEMPS
15 min

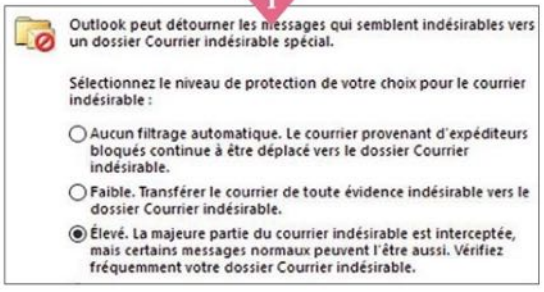
Bloquez les contenus potentiellement dangereux

Virus et malwares peuvent se propager à partir d'un logiciel installé à votre insu, mais aussi depuis un site Internet ou même un gif animé. Une vigilance de tous les instants s'impose.

Luttez contre les mails indésirables

Les courriels sont l'un des principaux vecteurs des cybermenaces, qu'il s'agisse de pièces jointes infectées ou de liens piégés. Dans ***Outlook***, le gestionnaire de courrier de la suite Office, dirigez-vous vers le ruban ***Accueil***. Déroulez le menu ***Courrier indésirable***, puis activez la commande ***Options***. Réglez le niveau de vigilance du filtre antispam sur ***Élevé***. Pensez à consulter de temps en temps le contenu du dossier ***Courrier indésirable***, histoire de vous assurer que des messages licites n'y ont pas été jetés par excès de zèle !

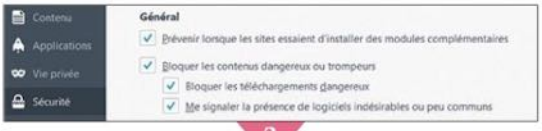
1



Évitez d'activer les éléments suspects contenus dans les courriels

Les messages au format HTML peuvent abriter des bouts de code informatique susceptibles de contaminer votre PC. Un client de messagerie comme Outlook est capable d'inhiber ces menaces. Déployez le menu ***Fichier, Options***. Cliquez sur ***Centre de gestion de la confidentialité, Paramètres du Centre de gestion de la confidentialité***, puis sur l'onglet ***Sécurité de messagerie électronique***. Cochez ***Lire tous les messages standard au format texte brut***. Dans l'onglet ***Paramètres des macros***, choisissez le filtre ***Désactiver toutes les macros***.

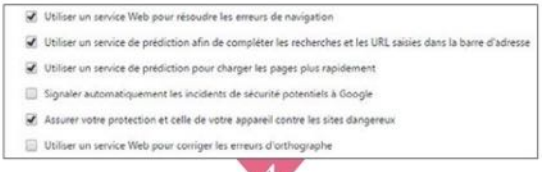
2



3

Naviguez en paix grâce à Firefox

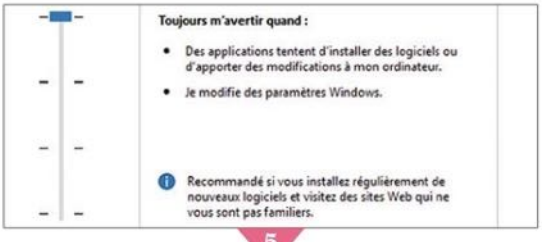
Le Web recèle 1001 pièges. Pour accéder aux outils de protection de Firefox, déroulez le menu du navigateur, cliquez sur ***Options, Sécurité***. Activez les options ***Prévenir lorsque les sites essaient d'installer des modules complémentaires, Bloquer les contenus dangereux ou trompeurs, Bloquer les téléchargements dangereux*** et ***Me signaler la présence de logiciels indésirables ou peu communs***. Voilà qui limitera les dégâts.



4

Demandez à Chrome de surveiller vos arrières

Pour examiner les réglages relatifs à la sécurité du navigateur de Google, cliquez sur les ***trois points*** dans le coin supérieur droit de la fenêtre. Choisissez ensuite ***Paramètres***, puis le lien ***Paramètres avancés*** situé au bas de la page. Dans la section ***Confidentialité***, sélectionnez l'option ***Assurer votre protection et celle de votre appareil contre les sites dangereux***.



5

Renforcez la vigilance de Windows contre les logiciels à risque

Quand vous tentez d'installer certains logiciels, une mise en garde s'affiche à l'écran et vous invite à confirmer l'importation. Pour systématiser cette alerte, tapez ***Contrôle de compte*** dans la zone de recherche de Windows. Cliquez sur ***Modifier les paramètres de contrôle de compte utilisateur*** et placez le curseur sur ***Toujours m'avertir***. Validez à l'aide du bouton ***OK***. ■

Débarrassez-vous enfin des barres d'outils !

Babylon, Ask, Incredibar... Elles se révèlent souvent aussi inutiles que difficiles à déloger ! Si toutes ne sont pas dangereuses, il vaut mieux supprimer les malwares qui en sont à l'origine.

De préférence, anticipez le problème

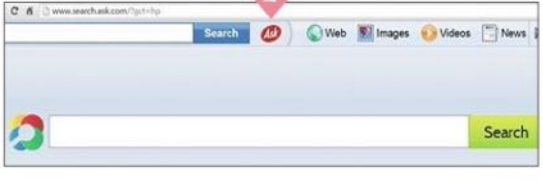
Les barres d'outils apparaissent en général après que vous avez téléchargé sans précaution un logiciel sur Internet. Avant de cliquer sur le bouton ***Suivant***, prenez plutôt l'habitude de lire attentivement chaque page de l'assistant d'installation. Arrêtez-vous dès que vous tombez sur une annonce sans rapport avec le programme initial. Regardez au bas de la fenêtre. Vous devriez y trouver une option pour refuser l'intégration de l'appli partenaire sur votre navigateur. Selon les cas, vous devez cocher ou décocher la case correspondante.

1

Supprimez le logiciel à l'origine de l'infection

Plus souvent gênantes que réellement dangereuses, les barres d'outils modifient le moteur de recherche et la page de démarrage du navigateur, multipliant par exemple les publicités sur les pages Web que vous visitez. Certaines s'avèrent très intrusives et s'intéressent même à vos données personnelles... Inoffensives ou non, mieux vaut les retirer. Le premier réflexe consiste donc à rechercher des éléments douteux dans la liste des applis présentes sur votre ordinateur. Faites un clic droit sur le menu ***Démarrer*** de Windows. Activez ***Programmes et fonctionnalités***, sélectionnez le logiciel suspect, puis le bouton ***Supprimer*** pour éliminer le malware.

2



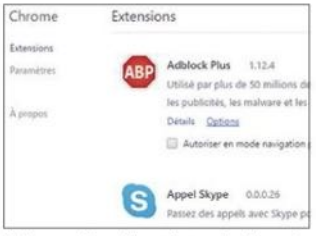
3

Analysez votre PC avec un antimalware

Certaines barres d'outils cachent des logiciels malveillants. Ils ne laissent pas de traces et n'apparaissent pas dans la liste des programmes pouvant être désinstallés. Pour les éradiquer, il faut employer un logiciel antimalware tel que AdwCleaner. Lancez une analyse approfondie de votre disque dur et supprimez les fichiers infectés. N'hésitez pas à solliciter plusieurs solutions antivirales.

4

Retirez l'extension de votre navigateur



D'autres barres prennent encore la forme d'extensions qui se greffent à votre browser. Déroulez le menu de ***Google Chrome***, cliquez sur ***Paramètres***, ***Plus d'outils***, et sur ***Extensions***. Repérez la barre d'outils et jetez-la dans la poubelle. Si vous utilisez Firefox, déployez le volet de menu et sélectionnez ***Modules***, ***Extensions***. Activez le bouton ***Supprimer***.

5

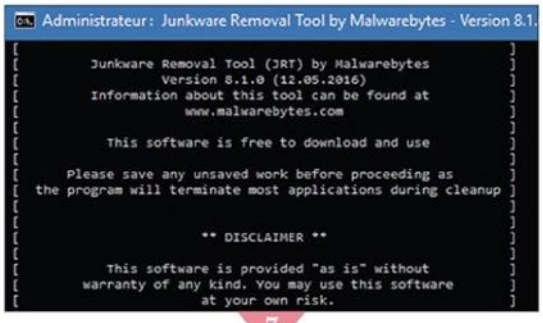
Récupérez votre page de démarrage

Il ne suffit pas toujours de supprimer la barre d'outils pour rétablir un fonctionnement normal du navigateur... Ces malwares imposent souvent leur propre page de démarrage. Rétablissez les paramètres initiaux dans la section ***Au démarrage*** des paramètres de ***Google Chrome***.

6

Rétablissez le moteur de recherche

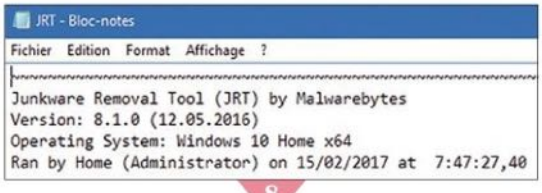
La barre d'outils a probablement aussi remplacé vos réglages de recherche par défaut. Allez dans les ***Paramètres*** de Chrome. Cliquez sur ***Gérer les moteurs de recherche***, puis sur la ***croix*** pour supprimer un élément. Passez le pointeur de la souris sur le nom du service de votre choix et exécutez l'option ***Utiliser par défaut***. Dans ***Firefox***, accédez aux ***Options***, sélectionnez l'onglet ***Recherche*** et optez pour un service dans le menu déroulant.



7

Utilisez Junkware Removal Tool

Votre ordi n'est pas encore doté d'un antimalware ? Rendez-vous sur le site ***bit.do/dfwCs*** et cliquez sur ***Télécharger*** pour récupérer l'appli Junkware Removal Tool (développée par Malwarebytes). Attendez la fin du transfert et double-cliquez sur le fichier exécutable. S'agissant d'un logiciel portable qui ne nécessite pas d'installation, Junkware s'exécute dans une fenêtre de commandes. Appuyez sur une touche du clavier et patientez jusqu'à l'issue de l'analyse. Un utilitaire spartiate mais efficace.



8

Vérifiez le résultat

Une fois l'examen terminé, un fichier de diagnostic nommé ***JRT.TXT*** s'enregistre sur le Bureau de Windows. Vous y découvrez la liste des éléments qui ont été supprimés du PC. Effectuez un second passage pour vous assurer qu'il ne reste aucun logiciel indésirable – adwares, junkwares... Copiez cet utilitaire avec AdwCleaner, sur une clé USB de sauvetage à dégainer en cas d'urgence !

Pour surfer serein, nettoyez les browsers

Toutes les solutions de sécurité proposent chacune leurs propres outils contre les programmes indésirables. Elles s'avèrent souvent complémentaires, les unes venant à bout des éléments qui ont trompé la vigilance des autres. Si vous aimez tester des logiciels récupérés sur Internet, nous vous conseillons de garder plusieurs chasseurs de malwares à portée de souris. Rendez-vous, par exemple, sur le site ***bit.do/de8Tc*** et activez ***Téléchargement gratuit*** pour obtenir le Nettoyeur de navigateur d'Avast. Cette appli fonctionne indépendamment de l'antivirus de l'éditeur. Procédez à son installation, puis lancez-le. Il analyse les browsers présents sur le PC et indique si un nettoyage s'impose. Sélectionnez ensuite un navigateur dans la colonne de gauche, cliquez sur ***Réinitialisez les paramètres*** et sur ***Effectuer le nettoyage gratuit***.

9

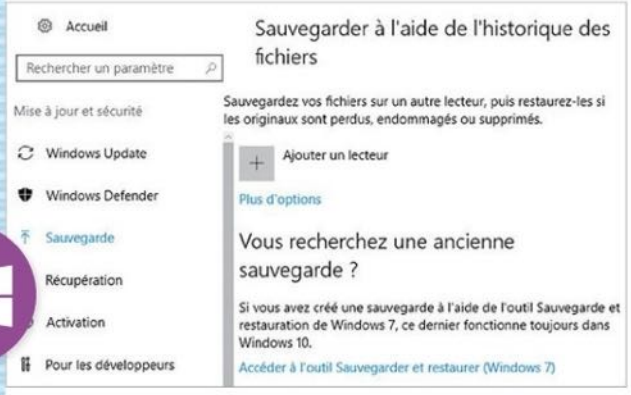
Examinez enfin les modules complémentaires

Le Nettoyeur d'Avast débarrasse les navigateurs des problèmes qui entravent leur bon fonctionnement : barres d'outils, extensions corrompues, résultats de recherche détournés... Relancez une analyse et vérifiez que l'utilitaire affiche cette fois le message ***Vos navigateurs ne semblent pas comporter de modules complémentaires disposant d'une mauvaise réputation***. Dans la colonne de gauche, décochez l'option ***Exclure les modules complémentaires disposant d'une bonne évaluation*** pour obtenir une vue d'ensemble des extensions installées. ■

10

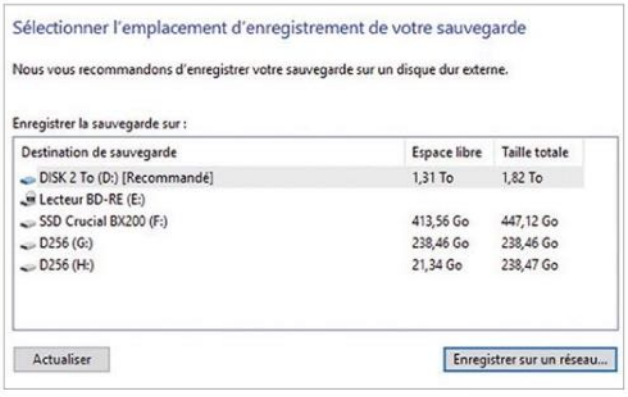
Créez une sauvegarde pour réagir en cas de "super virus"

Antivirus verrouillé, accès à Internet bloqué : certains logiciels malveillants n'offrent d'autre alternative que de réinstaller Windows pour reprendre le contrôle de son PC. Une mésaventure qui peut s'avérer sans grandes conséquences si vous avez pris soin d'enregistrer auparavant une image système de votre configuration. Mode d'emploi.



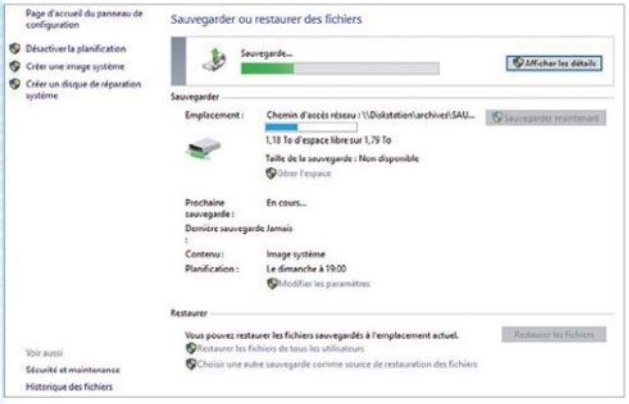
1. Accédez à l'utilitaire de sauvegarde

Pour enregistrer une image saine de votre PC, déroulez le menu ***Démarrer*** et cliquez sur ***Paramètres***, ***Mise à jour et sécurité***, ***Sauvegarde***. Sélectionnez le lien ***Accéder à l'outil Sauvegarder et restaurer (Windows 7)***.



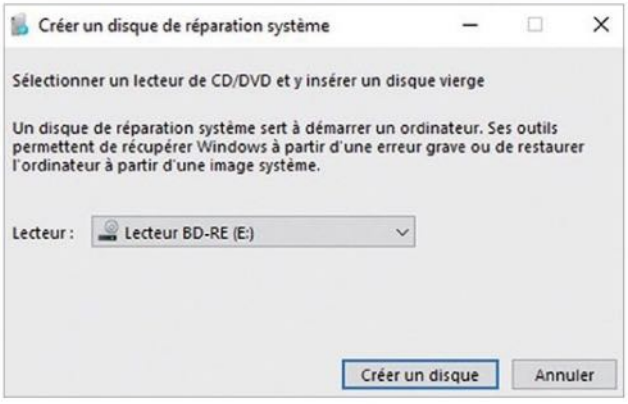
2. Indiquez le dossier de destination

Activez la commande ***Configurer la sauvegarde*** et désignez l'endroit où sera enregistré le fichier image. Il peut s'agir d'un disque dur local (autre que le volume système) ou d'un support externe (disque dur ou clé USB).



5. Lancez la sauvegarde

Activez l'option ***Inclure une image système de lecteurs*** avant de cliquer sur ***Suivant***. Vérifiez que les informations sont correctes. Vous pouvez maintenant ***Enregistrer les paramètres et exécuter la sauvegarde***.



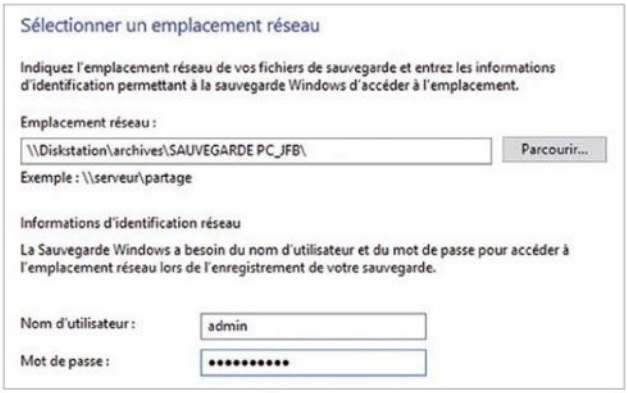
6. Gravez un disque de réparation système

Si un virus bloque Windows, la restauration de l'image système nécessitera un disque de réparation. Pour le graver, allez dans l'outil ***Sauvegarder et restaurer***, puis optez pour ***Créer un disque de réparation système***.

DIFFICULTÉ
Élevée
TEMPS
45 min

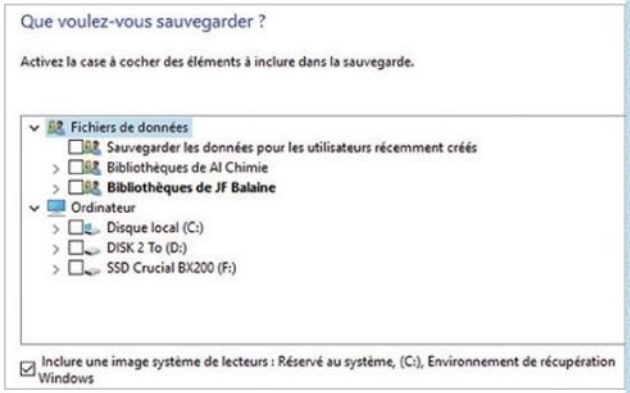
©Fotolia/ Tomasz Zajda

Grâce à l'image système sous Windows 10, vous êtes assuré de retrouver un PC opérationnel en quelques minutes. Avec tous vos réglages et logiciels... mais sans virus !



3. Utilisez un dossier partagé

Vous pouvez aussi garder l'image dans un emplacement réseau. Cliquez sur ***Enregistrer sur un réseau*** au bas de la fenêtre, puis sur ***Parcourir***. Renseignez le nom d'utilisateur et le mot de passe si l'accès au lecteur est protégé.

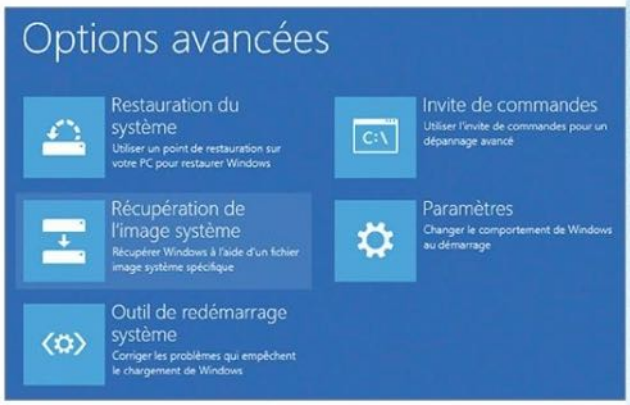


4. N'enregistrez que l'image système

Cochez l'option ***Me laisser choisir*** et faites ***Suivant***. Afin d'éviter que la sauvegarde ne prenne trop de place, excluez les dossiers abritant vos fichiers personnels. Il vous suffira de synchroniser ces derniers dans le cloud.

7. Préparez une clé USB de démarrage

Si vous ne possédez pas de graveur, rendez-vous sur le site ***bit.do/ddoez*** et téléchargez-y l'appli ***Media Creation Tool***. Celle-ci sert à de transférer votre version de Windows sur une clé USB bootable.



8. Restaurez l'image système

En cas de problème, démarrez le PC sur la clé de secours. Accédez aux options de démarrage avancées, choisissez ***Dépannage***, ***Options avancées***, ***Récupération de l'image système*** et indiquez l'emplacement du fichier.

Quelques astuces pour

LA PRUDENCE N'ÉLOIGNE PAS TOUT À FAIT LE DANGER. IL SUFFIT DE LAISSER L'ACCÈS DE SON PC QUELQUES MINUTES À UN PROCHE MOINS SENSIBLE AUX PROBLÉMATIQUES DE SÉCURITÉ POUR "ATTRAPER" UN VIRUS OU UN MALWARE. VOICI QUELQUES CONSEILS QUI VOUS AIDERONT À PRÉVENIR LES DANGERS OU À REMETTRE L'ORDI EN ÉTAT DE MARCHE SI LE PIRE SURVENAIT.

Créez une clé USB de récupération antivirus

Un virus bloque votre logiciel antivirus et l'accès à Internet, interdisant ainsi d'exécuter une analyse en ligne du disque dur. Un redémarrage de l'ordinateur n'y change rien, le logiciel malveillant prenant le contrôle du PC avant que Windows Defender n'ait le temps d'intervenir.

LA SOLUTION Il est très difficile de se débarrasser des virus de ce type, qui inhibent les logiciels de sécurité et les navigateurs Internet. Faute de pouvoir lancer une analyse à l'aide des outils en ligne de Bitdefender, F-Secure ou Secuser.com, vous devez préparer un disque de démarrage de secours et y implanter un antivirus. Accédez au site ***avast.com//fr-fr*** à partir d'un autre poste que celui infecté. Puis téléchargez et installez ***Avast Essentiel***. Sur la page d'accueil de l'antivirus, cliquez sur ***Outils***, ***Disque de secours***. Branchez une clé USB et ouvrez l'***Explorateur de fichiers*** de Windows pour vérifier qu'elle ne contient pas de données importantes – son contenu sera en effet effacé au cours de l'opération. Retournez dans ***Avast*** et optez pour ***Créer le disque de secours***. Sélectionnez votre clé dans la liste des supports détectés, choisissez ***Installer sur USB*** et confirmez (***Oui***). Avast télécharge les fichiers et les définitions de virus nécessaires au disque de secours. Il vous reste ensuite à booter le PC contaminé sur cette clé de démarrage et à effectuer l'analyse du disque dur pour supprimer le virus et reprendre le contrôle de la machine.

Le disque de secours créé par Avast contient une version bootable de l'antivirus.

Détectez toute activité anormale sur votre PC

Bien sûr, vous savez quels logiciels vous utilisez ! Mais que se passe-t-il donc en votre absence ? Quelles applis se lancent en arrière-plan sans que vous le soupçonniez ?

LA SOLUTION Les malwares ont la fâcheuse habitude de s'exécuter de façon discrète, souvent au démarrage de Windows. Le programme gratuit Apps Tracker (***bit.do/dfwE4***) vous aide à suivre les activités de votre PC. Une fois en place, il enregistre en temps réel la liste des logiciels sollicités, ainsi que le nom des fichiers et des pages Web regardées sur l'ordinateur. Tous ces accès sont consignés dans un journal d'activité, consultable à tout moment.

Suspendez temporairement la reconnaissance des clés de stockage

Vous devez vous absenter quelques jours et vous voulez être sûr que vos enfants n'en profitent pas pour copier toutes sortes de fichiers sur votre PC.

LA SOLUTION Films, jeux, applis, films ou musique... Il est probable que vos bambins se servent d'une clé USB ou d'un disque dur externe pour tenter d'y introduire leurs fichiers sur votre PC. Avant de partir, vous pouvez désactiver la reconnaissance automatique des périphériques USB

Avec cette manip, Windows ne détectera plus les disques durs externes connectés au PC.

afin qu'ils ne s'affichent pas dans l'Explorateur de fichiers. Ouvrez l'***Éditeur du registre*** en tapant ***Regedit*** dans le champ de recherche, puis en appuyant sur la touche ***Entrée*** du clavier. Déroulez la branche ***HKEY_LOCAL_MACHINE, SYSTEM, CurrentControlSet, Services, USBSTOR***. Double-cliquez sur ***Start*** dans le volet de droite et remplacez le contenu du champ ***Données de valeur*** par ***4***. Pour revenir à un fonctionnement normal, restaurez la valeur initiale (***3***).

Interdisez la copie de vos données

Vous partagez votre ordinateur en famille ou avec des collègues, mais vous ne souhaitez pas que l'on puisse emprunter vos documents personnels.

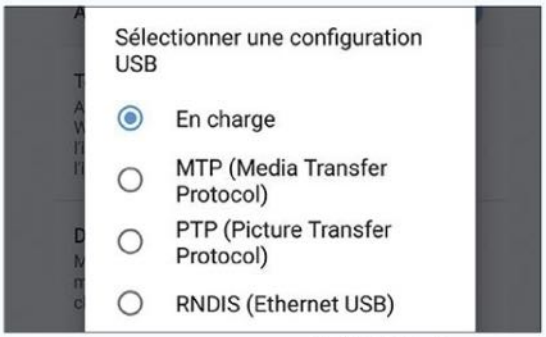
LA SOLUTION Il vous suffit pour cela d'interdire la copie des données sur les périphériques de stockage USB. lancez d'abord ***Regedit***, puis déroulez la branche ***HKEY_LOCAL_MACHINE, SYSTEM, CurrentControlSet, Control***. Créez une clé intitulée ***StorageDevicePolicies***, puis une valeur DWord 32 bits nommée ***WriteProtect*** à laquelle vous attribuerez la valeur ***1***. Redémarrez maintenant votre PC. Pour rendre la copie possible, remplacez la valeur ***1*** par ***0***.

sécuriser PC et tablettes

Empêchez l'installation d'applis sur votre tablette

Vous prêtez souvent votre tablette Android et il est déjà arrivé que les emprunteurs, armés des meilleures intentions du monde, y installent par mégarde des applis infectées.

LA SOLUTION Si même le Play Store d'Android n'est pas exempt d'applis infectées par des malwares, le risque principal provient des éléments installés à partir de fichiers APK en provenance du Web ou des stores alternatifs. Vous pouvez éviter que les personnes à qui vous confiez votre précieux appareil n'y implantent des applis. Ouvrez pour ce faire les paramètres de la tablette. Accédez à la rubrique ***Sécurité***, puis désactivez l'option ***Source inconnue***. Vous pouvez pareillement compliquer la tâche de ceux qui souhaiteraient y copier des fichiers – potentiellement dangereux – en activant par défaut le mode ***Recharge USB*** plutôt que ***MTP (Media Transfer Protocol)*** lorsque la tablette est connectée à un ordinateur. Pour cela, depuis les ***Paramètres***, appuyez sur ***Options pour les développeurs***, puis sur ***Sélectionner une configuration USB***. Dorénavant, le contenu de l'appareil n'apparaîtra plus dans l'Explorateur de fichiers.



Tant que le mode En charge est activé, Windows ne peut pas accéder à la mémoire de votre tablette.

Partez à la chasse aux malwares

Votre navigateur Internet souffre d'un fonctionnement anormal, peut-être à cause d'un logiciel malveillant. Votre antivirus n'a pourtant rien repéré.

LA SOLUTION En matière de sécurité, deux avis valent mieux qu'un. Avant d'importer un utilitaire spécialisé, commencez par solliciter l'antimalware intégré à Windows depuis Windows XP. Tapez la commande ***mrt.exe*** dans le champ de recherche et pressez sur ***Entrée***. Cliquez sur ***Suivant*** et effectuez une analyse complète de l'ordinateur. Si des menaces sont détectées, l'outil de suppression des logiciels malveillants de Windows supprimera automatiquement les fichiers corrompus.

Protégez le fichier autorun de vos périphériques USB

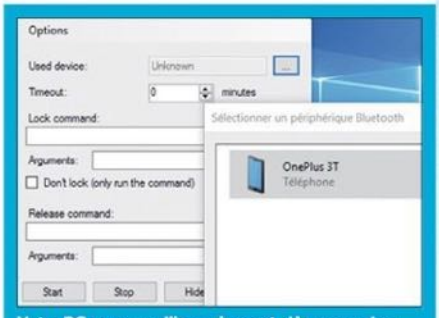
Vous recourez à différentes clés USB pour échanger des données avec vos proches. Comment vous assurer que les supports de stockage amovibles ne se transforment pas en vecteur d'infection ?

LA SOLUTION Certains virus ont la faculté de modifier le fichier autorun.info qui est exécuté par Windows quand vous branchez une clé USB à un ordinateur. L'utilitaire gratuit USB-set vaccine les supports amovibles et interdit aux virus de changer leur fichier d'amorce. Téléchargez (***bit.do/defGi***) et installez cette appli sur votre PC. Connectez les lecteurs que vous souhaitez protéger, puis lancez ***USB-set***. Activez l'onglet ***Vaccination***, puis le bouton ***Vacciner tous les lecteurs***.

Gérez le mode Veille grâce au Bluetooth

Afin de sécuriser vos données, vous avez activé la mise en veille automatique de Windows 7. Problème : il suffit que vous soyez occupé au téléphone ou à discuter avec quelqu'un, juste à côté, pour que l'écran de veille s'allume après cinq minutes d'inactivité. Conséquence : vous passez votre temps à saisir votre mot de passe pour déverrouiller le PC.

LA SOLUTION Activez la mise en veille seulement quand vous vous éloignez trop loin de votre ordinateur. Téléchargez et installez l'utilitaire gratuit ***BtProx (bit.do/defDT)***. Associez votre PC et votre mobile par Bluetooth, puis ouvrez ***BtProx***. Sélectionnez le téléphone dans la liste des appareils détectés et réglez le paramètre ***Time Out*** sur ***0***. Validez (***Start***). ■



Votre PC se verrouille seulement si la connexion Bluetooth avec votre mobile est interrompue.

DIFFICULTÉ
Élevée
TEMPS
20 min

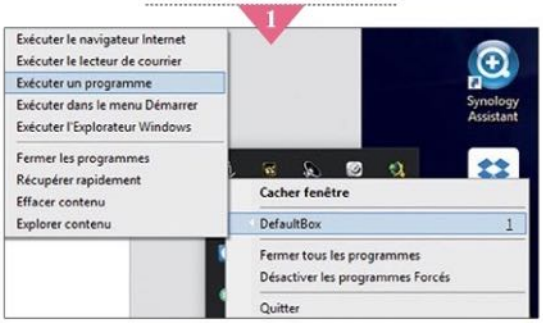
Essayez de nouveaux logiciels sans prendre de risques

Vous pensiez installer une appli inoffensive... Vous voici maintenant aux prises avec d'improbables barres d'outils et divers logiciels non sollicités. Pour éviter cette mésaventure, lancez vos nouveaux programmes dans un espace sécurisé.

Équipez votre ordinateur d'un bac à sable

Sauf à n'employer que des programmes archiconnus, tester une nouvelle appli réserve parfois de drôles de surprises. La bonne parade consiste à exécuter les logiciels dont l'origine n'est pas sûre dans un environnement appelé bac à sable. Cela limite les interactions avec le reste de la configuration. Saisissez l'URL ***bit.do/daKXL***. Téléchargez la version gratuite de ***Sandboxie***. Faites un clic droit sur l'icône de l'appli et activez la commande ***DefaultBox, Exécuter un programme***.

1



Testez une application en toute quiétude

Vous pouvez recourir à Sandboxie pour essayer des logiciels déjà en place ou des applis portables ne nécessitant pas d'installation. Cliquez sur le bouton ***Naviguer*** et désignez l'exécutable du programme (vlc.exe, par exemple). Validez. Un filet jaune, autour de la fenêtre du logiciel, indique qu'il fonctionne en mode sécurisé.

2

3

Exécutez des extensions ou chargez des pages Web en évitant le danger

Grâce à Sandboxie, surfer sans mettre son PC en péril, c'est possible ! Effectuez un clic droit sur l'icône de l'appli et validez la commande ***Exécuter le navigateur Web***. Une session sécurisée du navigateur Internet par défaut s'ouvre alors sur l'écran. Ni les sites que vous consultez ni les extensions que vous récupérez ici et là ne sont plus susceptibles d'endommager ou de corrompre Windows et vos fichiers.

4

Installez une machine virtuelle

Si vous aimez expérimenter les applis les plus improbables, le mieux est de dédier un ordi à cette tâche ou, à défaut, d'implanter une émulation au cœur de Windows. Ce "PC dans le PC" vous servira à faire tourner des programmes sans exposer le reste de la configuration. Allez sur le site ***bit.do/c8rdM***. Rapatriez l'appli gratuite ***VirtualBox***, créez une machine virtuelle et installez-y une version de Windows dont vous possédez la licence. ■

DIFFICULTÉ
Élevée
TEMPS
20 min

Refusez le chantage et ne payez pas la rançon !

En plein essor, les ransomwares chiffrent le contenu du disque dur. Il devient dès lors impossible d'y accéder sans s'acquitter du tribut exigé par les cybercriminels.

Préparez-vous à affronter la menace

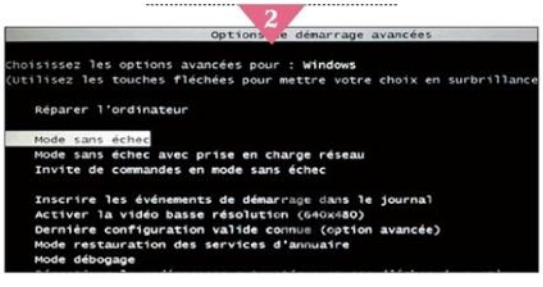
Pour vous épargner toute déconvenue, anticipez l'infection par un ransomware en vous dotant des armes spécifiquement conçues pour les mettre à mal. Connectez-vous au site ***bit.do/daMNu***. La bibliothèque de secours de Bitdefender regroupe des dizaines de patchs de sécurité prêts à riposter. Cliquez sur les liens associés aux principales menaces (***BDRemoval_Trojan_Ransom_IcePol.exe***, par exemple, pour éradiquer Icepol, l'un des rançongiciels les plus actifs). Le téléchargement de l'exécutable ne prend que quelques minutes. Composez votre propre catalogue de patchs en compilant un maximum d'outils. Conservez ces programmes bien au chaud sur un disque réseau ou sur une clé USB.

1

Redémarrez en mode sans échec

Le jour où un ransomware se manifeste, il faut agir vite et appliquer le correctif adapté. Pour cela, redémarrez votre PC en mode sans échec avec prise en charge réseau. De cette façon, vous serez en mesure de télécharger l'utilitaire si vous ne l'avez pas fait en amont. Forcez l'arrêt de l'ordinateur en maintenant le doigt appuyé pendant plusieurs secondes sur le ***bouton de mise sous tension***. Rallumez-le et enfoncez la touche ***F8*** (ou ***F2***, selon le Bios) du clavier. Sélectionnez l'option ***Mode sans échec avec prise en charge réseau***.

2



3

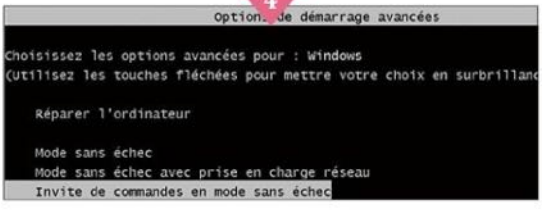
Nettoyez sans tarder votre ordinateur

Accédez maintenant à l'utilitaire de désinfection. Effectuez un clic droit sur le fichier et activez la commande ***Exécuter en tant qu'administrateur***. Si vous utilisez ***Removal Tool***, faites ***Lancer l'analyse***. Plusieurs minutes sont nécessaires à l'assainissement de votre ordinateur. Au terme du processus, un bilan affiche le nombre de fichiers traités. Redémarrez votre PC.

Si le vers est coriace, appliquez le correctif en mode Invite de commandes

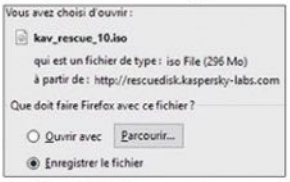
Au cas où le mode sans échec avec prise en charge réseau n'a pas pu résoudre le problème, redémarrez Windows en mode Invite de commandes. Attendez que la console apparaisse. Saisissez la commande ***explorer.exe*** à la suite de la ligne ***C:\Windowssystem32***, puis pressez la touche ***Entrée*** du clavier. Insérez la clé USB contenant l'utilitaire de désinfection. Accédez à son contenu en tapant le chemin ***Ordinateur/Poste de travail*** et lancez l'outil d'analyse comme évoqué précédemment.

4



5

Préparez un disque de secours



L'éditeur Kaspersky fournit lui aussi une batterie d'utilitaires redoutables. Vous pouvez en acquérir une version bootable sur ***bit.do/daMP4***. Importez le fichier ISO. Gravez-le sur un CD vierge ou copiez-le sur une clé à l'aide d'un programme capable de rendre le support démarrable, comme Rufus (***bit.do/dfaRR***). En cas d'infection, servez-vous de ce disque de secours pour neutraliser la menace. ■

Désinfectez aussi vos mobiles et tablettes

Avec plus de deux milliards de smartphones et de tablettes dans le monde, les terminaux mobiles sont devenus une cible de choix pour les concepteurs de virus. Il existe heureusement des logiciels pour protéger et nettoyer vos précieux appareils.

ANDROID

1

Désinstallez les applis

Les malwares qui ralentissent votre mobile ou qui vous submergent de publicités sont parfois de banales applis. Commencez par explorer le tiroir d'applications du téléphone et retirez tous les programmes suspects. Appuyez de façon prolongée sur l'icône de l'appli et glissez-la sur le lien ***Désinstaller*** qui s'affiche tout en haut de l'écran.

Faites le grand ménage

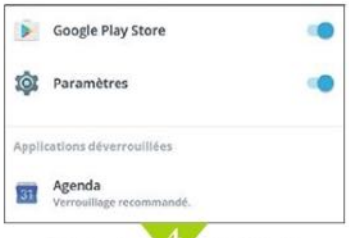
Les logiciels malveillants ne se laissent pas tous attraper aussi facilement... Les virus non plus ! Accédez au ***Play Store***. Recherchez et installez la suite de sécurité ***Avast Gratuit pour Android***. Lancez l'utilitaire et pressez sur ***Analyser cet appareil***. Autorisez l'appli à accéder aux dossiers système et laissez l'antivirus remplir son office.

2

3

Blindez votre smartphone

Les programmes dédiés à la sécurité sur Google Play sont pour quelques-uns curatifs, mais la plupart privilégient la protection de vos informations personnelles. La plus grande menace reste l'interception de données lorsque vous vous connectez à un point d'accès Wifi peu sécurisé ou à la suite de la perte ou du vol de l'appareil. Pour commencer, activez ***Verrouillage des applications***.



4

Interdisez l'accès aux applications sensibles

Avast vous demande d'enregistrer un code PIN. Vous pouvez ensuite verrouiller l'accès aux paramètres de l'appareil, au Play Store (pour éviter que vos enfants ne mettent n'importe quoi sur la tablette familiale...) et à une appli de votre choix. Pour protéger davantage d'applis, vous devrez passer à la version payante pour mobile, soit 7,99 € pour un an.

5

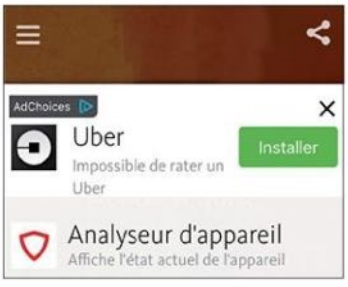
Détruisez les malwares

Pour empêcher les ennemis de coloniser votre smartphone pour de bon, installez la version mobile de ***Malwarebytes***. Effectuez une première analyse. Si vous avez suivi l'étape précédente, il vous sera demandé d'entrer votre code PIN. Rien à voir avec Malwarebytes : Avast s'assure simplement que vous autorisez cette nouvelle appli à accéder à votre système. L'antimalware nettoie ensuite automatiquement votre mobile.

6

Quand tout va de travers, réinitialisez l'appareil

Si un virus rend votre portable instable et que vous n'en venez pas à bout, vous devrez vous résoudre à revenir à la configuration d'usine. Pensez surtout à sauvegarder les fichiers importants. Puis, dans les ***Paramètres*** de l'appareil, touchez ***Sauvegarde et réinitialisation***, ***Rétablir la configuration d'usine***.



IOS

1

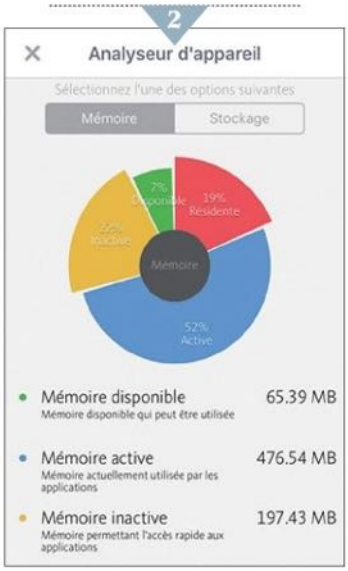
Sécurisez vos données

Les virus restant assez rares sur iOS, les solutions de sécurité proposent avant tout des services pour défendre l'accès aux données sensibles. Lookout, par exemple, localise le mobile, sauvegarde les contacts et les images, personnalise l'écran de verrouillage (avec vos coordonnées en cas de perte)... Le tout dans une interface très ergonomique.

Protégez votre navigation

L'application Avira n'est que l'élément d'une suite tournée vers la conservation des photos et des mots de passe (Avira Vault) et la navigation sécurisée par VPN (Avira Phantom VPN). Parmi les services embarqués, l'analyseur affiche l'utilisation de la mémoire. L'outil de protection d'identité surveille l'accès à vos contacts et à la boîte de réception.

2



3

Placez les fichiers au coffre

L'application McAfee transforme votre iPad en chambre forte numérique. L'accès aux fichiers est ainsi protégé par code PIN. C'est le cas aussi de l'appareil photo, ce qui évite de se faire aspirer ses images. En cas de perte de l'iPhone ou de l'iPad, l'appli localise l'engin. Elle prend même un cliché de l'utilisateur après plusieurs tentatives infructueuses de saisie du code secret – cliché que vous recevez par mail.

4

Évitez les applis douteuses

Quel que soit le logiciel de sécurité choisi, celui-ci s'invite dans vos photos, vos carnets d'adresses et vos applications. Aussi, mieux vaut accorder votre confiance aux éditeurs réputés (Avira, McAfee...) et fuir les prestataires plus exotiques. Pour minimiser les conflits et les plantages, n'empilez pas non plus les outils de même nature. Contentez-vous d'un seul antivirus. En cas de doublon, mieux vaut donc en désactiver un.

Surfez en toute sécurité

Sessions anonymes, VPN, bloqueurs de publicités... Vous avez pris l'habitude de vous blinder quand vous naviguez sur un ordinateur. Mais qu'en est-il sur votre iPhone ? Les menaces existent pourtant bel et bien. La suite F-Secure Safe (80 € par an pour trois appareils) contient un navigateur qui s'occupe de fiabiliser vos passages sur le Web. Il bascule en mode sécurisé quand vous accédez à votre banque et s'interpose dès qu'un logiciel malveillant pointe le bout de son nez.

5

Réinitialisez votre iPhone

Quand rien ne va plus, il reste une méthode radicale : réinitialiser l'iPhone... même à contrecœur ! Appuyez sur l'icône ***Réglages*** de l'appareil. Effleurez ensuite l'onglet ***Général*** puis la commande ***Réinitialiser***. Choisissez alors l'option ***Réinitialisez tous les réglages***, puis ***Effacer contenu et réglages***. Après le redémarrage, connectez l'appareil à votre compte Apple ID pour retrouver contacts, achats et données enregistrés dans iCloud. ■

6

SURVEILLER

Comment les hackers piratent votre réseau


© Minerva Studio

SOMMAIRE

Forcer l'accès à un réseau n'a jamais été aussi facile. Si l'exercice était naguère réservé aux hackers chevronnés, la généralisation des box Internet et des connexions Wifi a mis nos données (presque) en libre-service pour les pirates du monde entier ! Les réseaux sans fil se montrent tout particulièrement vulnérables. Au-delà des voisins, qui profiteraient bien d'une connexion Internet gratuite, le risque le plus important provient des adeptes du Wardriving. War pour Wireless Access Research (recherche des accès sans fil). Leur méthode consiste à parcourir les rues équipés d'un matériel léger afin de détecter les réseaux Wifi et de s'y immiscer pour aspirer les données.

Mais War aussi comme guerre. Car c'est bien une bataille sans merci que nous, internautes, devons livrer afin de protéger nos fichiers et nos informations personnelles. Un hacker confirmé et motivé parviendra toujours à battre en brèche les défenses que nous imaginons. Après tout, nous ne sommes pas des experts en réseau. Mais ce type de cybercriminel reste rare et, finalement, peu intéressé par les données des particuliers. La grande majorité des attaques provient d'amateurs. Cherchez un peu sur le Web et explorez les forums spécialisés : vous tomberez sur des applications de ce genre, telles qu'Aircrack-ng ou Backtrack. Pas besoin d'être un génie du code pour piloter ces programmes. Ils sont accessibles à n'importe quel passionné maîtrisant les commandes DOS, la création de clé bootable et l'utilisation de Linux. Avec un peu d'expérience et de patience, accéder aux réseaux les moins sécurisés devient un jeu d'enfant.

Remise de clés. S'il n'y a pas de hackers dans la rédaction – seulement des journalistes avec de solides notions d'informatique –, nous y sommes parvenus en peu de temps. Simplement avec un outil, Wifiphisher. Celui-ci ne cherche pas à craquer les mots de passe. Il se contente de déconnecter les utilisateurs du point

À la moindre résistance du réseau qui les retarderait, les pirates changent de proie.

d'accès de façon à les contraindre à s'identifier de nouveau. On retrouve une technique de phishing très connue : les usagers sont détournés vers une page Web qui les invite à confirmer la clé de sécurité du réseau suite à une mise à jour du routeur. Un procédé simple et terriblement efficace pour récupérer la clé WPA (Wi-Fi-Protected Access) sans coup férir !

Certes, rechercher à pénétrer des réseaux Wifi avec un portable sur les genoux n'est pas des plus discrets. Afin de rester invisibles, les hackers ont donc développé des solutions fonctionnant depuis un simple smartphone. Là encore, pas besoin d'un doctorat en informatique appliquée pour opérer. Il nous a suffi d'un téléphone rooté tournant sous Android sur lequel nous avons implanté une application. Et voilà ! Le réseau Wifi de la rédaction était "craqué". Les résultats obtenus par notre équipe ne sont guère rassurants. Ce qui nous mène à vous alerter et à vous recommander d'optimiser la sûreté de votre réseau.

Précautions élémentaires. Les cibles les moins bien protégées constituent des proies de choix. Opposer un peu de résistance incitera la plupart des pirates à passer leur chemin. Vous trouverez dans les pages suivantes tous les conseils pratiques afin de renforcer la sécurité de votre réseau sans fil. Ce qui implique de prendre quelques précautions élémentaires comme changer régulièrement la clé WPA ou WPS (Wifi-Protected Setup) et d'opérer de petits réglages dans les paramètres avancés de la box Internet. Passons aux travaux pratiques. ■

Une simple appli sur Android suffit à détourner un réseau Wifi

CONSEILS PRATIQUES

Renforcez la sécurité de votre réseau en six étapes

1 **Durcissez le chiffrement** Les données échangées entre les appareils et la box sont chiffrées. Si votre routeur utilise le protocole WEP par défaut, passez sans tarder au WPA2, bien plus sûr.

2 **Masquez votre réseau** Le nom du point d'accès Wifi, public, s'affiche lorsque quelqu'un situé à portée de votre box lance une recherche de réseau. Cachez le SSID (votre identifiant) afin de ne pas tenter les hackers.

3 **Renouvelez la clé d'accès** De la même façon que vous avez pris l'habitude de changer périodiquement le mot de passe de votre compte Facebook ou Dropbox, veillez à renouveler la clé WPA de votre réseau Wifi.

4 **Ne divulguez pas votre mot de passe** Gardez cette info aussi secrète que possible. Si vous avez communiqué la clé WPA à vos invités d'un soir, pensez à modifier le code associé après leur départ.

5 **Coupez l'accès distant.** Si vous ne vous servez pas de la fonction NAS (stockage en réseau) de votre box, désactivez-la, car c'est une des portes d'entrée des intrusions.

6 **Surveillez le trafic** Utilisez l'outil de gestion de trafic de votre box ou une appli pour contrôler quels appareils se connectent à votre Wifi. En cas d'ingérence, changez immédiatement le nom du réseau et modifiez sa clé.

Contrôlez et identifiez

Les pages Web prennent un temps fou à s'afficher alors que vous ne téléchargez pas de gros fichiers ? Un processus utilise sans doute la bande passante à votre insu.

Vérifiez que personne n'a installé d'applis en votre absence

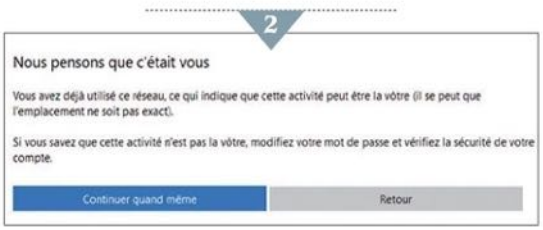
Le logiciel qui détourne la bande passante a pu être mis en place, de façon involontaire, par un utilisateur du PC familial. Ouvrez ***Programmes et fonctionnalités*** des ***Paramètres*** et supprimez les éléments suspects. Certains ne laissent pas de traces. Pour savoir ce qui s'est passé sur l'ordi connecté à votre compte Microsoft en votre absence, rendez-vous sur ***bit.do/c8LJV***. Cliquez sur ***Découvrez votre activité récente***, ***Afficher quand et où vous avez utilisé votre compte***, puis choisissez un horaire afin d'accéder aux détails et observer l'activité de session.

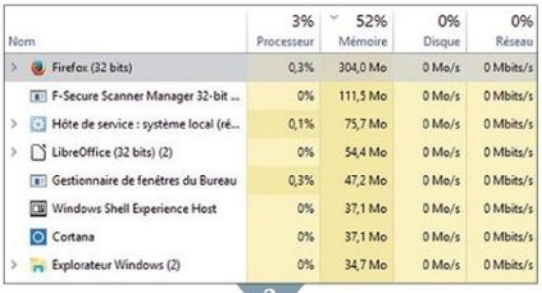
1

Protégez votre compte Microsoft et le PC

En cas de doute, activez l'intitulé ***Protéger votre compte***. Appliquez la procédure de modification du mot de passe et de sécurisation à votre compte Microsoft. Cela empêchera quiconque d'y pénétrer. Mais votre ordinateur reste accessible même si vous y avez défini un code PIN ou un mot de passe image. Dans ce cas, vous devez également penser à renouveler ces derniers. Déroulez pour ce faire le menu ***Démarrer***, optez pour ***Paramètres***, ***Comptes***, ***Options de connexion***, puis sélectionnez le mode de protection activé sur le PC.

2

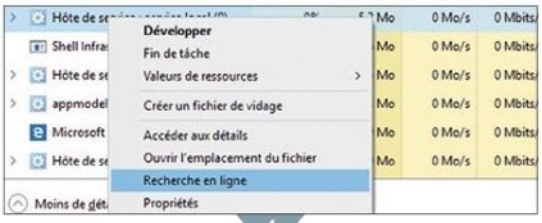




3

Affichez les fonctions les plus gourmandes

Si la machine reste lente, il y a de fortes chances que cela soit dû à l'exécution d'une activité inhabituelle en tâche de fond. Appuyez simultanément sur les touches ***Ctrl*** + ***Alt*** + ***Suppr*** du clavier et allez sur ***Gestionnaire des tâches***. Ce module dresse la liste les programmes actifs. Ouvrez ***Plus de détails*** : les colonnes Processeurs et Mémoire désignent les processus les plus gourmands susceptibles de perturber votre travail.



4

Repérez les éléments dangereux

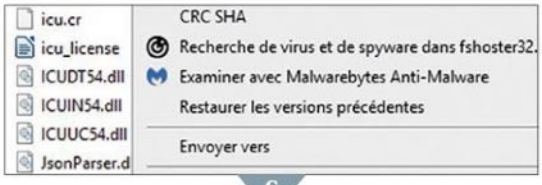
Le nom du programme qui mobilise une part importante des ressources de l'ordinateur vous est inconnu ? Cliquez avec le bouton droit de la souris sur son intitulé, puis lancez une recherche en ligne. Il vous suffit d'ouvrir les différents liens pour obtenir des informations et savoir s'il convient de s'attaquer à ce logiciel.

5

Mettez fin à une activité non souhaitée

Lors d'une activité malveillante (certains composants de Windows s'emballent parfois sans raison apparente), effectuez un clic droit sur son nom et exécutez la commande ***Fin de tâche***. Si le processus réapparaît, utilisez ***Ouvrir l'emplacement du fichier*** afin d'identifier le logiciel responsable et supprimez-le.

les activités suspectes



6

Supprimez les causes des perturbations

Le programme incriminé n'apparaît pas dans le module de désinstallation de Windows. Vous pouvez identifier le fichier désigné par le Gestionnaire de tâche manuellement. En cas de doute, laissez faire un logiciel spécialisé (reportez-vous aux pages 18 et 19 de ce guide pour découvrir la marche à suivre avec Malwarebytes).

7

Installez un agent de surveillance

L'utilitaire gratuit GlassWire (***bit.do/c8Mmz***) analyse en continu le flux de données entrant et sortant du PC dans le but de détecter les activités suspectes. L'onglet ***Graph*** affiche les programmes en cours d'exécution ainsi que les flux. Pour ne cibler que ces derniers, sélectionnez ***Traffic***. La colonne ***Type*** décortique les données entrantes et sortantes et les associe à une application (cette info figure dans la colonne ***App***). Vous devez vous alarmer en cas de pic soudain lié à un trafic inhabituel alors que vous ne sollicitez pas le PC.

8

Géolocalisez l'adresse IP distante

Si c'est le cas, référez-vous à l'onglet ***Alert*** de GlassWire. Activez le ***drapeau*** ou le nom du processus et copiez l'adresse ***IP distante***. Connectez-vous au site ***bit.do/c8MoH***. Collez l'adresse dans la zone de saisie ***Entrez une adresse IP à tracer ici*** et cliquez sur ***Localiser l'IP***. Vous saurez ainsi de quel pays émane la connexion.

Gardez un œil sur le trafic du réseau sans fil

Le point d'accès Wifi établi par votre box Internet constitue l'un des maillons faibles de la sécurité de votre réseau. En cas de ralentissement prolongé, intéressez-vous de près à ce qui s'y passe. Pour vous aider dans cette tâche, installez l'appli ***Wireless Network Watcher*** (***bit.do/c8Mqf***). Ce programme gratuit affiche en temps réel les appareils connectés au routeur de la box, en Ethernet et en Wifi. Faites un clic droit sur l'adresse IP d'un périphérique, puis lancez la commande ***Properties***. Vous découvrez ainsi de quel type de matériel il s'agit (***Device Name***), ainsi que son adresse MAC. De précieuses informations pour déterminer s'il s'agit bien de l'un de vos appareils (smartphone, tablette, ordi, TV, etc.) ou d'un intrus. ■

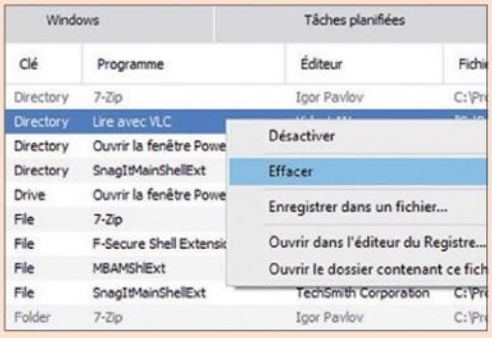
9

IP Address	Device Name	MAC Address
192.168.0.	DISKSTATION	00-11-32-06-78
192.168.0	PC_2015	88-88-88-88-87
192.168.0.	DESKTOP-RLJHGLP	20-CF-30-A8-F5-
192.168.0.		D8-50-E6-35-4F
192.168.0...		7C-C4-EF-50-83
192.168.0.	IMAC-DE-NICO	D4-9A-20-D0-A4-
192.168.0		88-CB-87-B8-08-

CCLEANER FREE

ALLÉGEZ LA SÉQUENCE DE DÉMARRAGE

Les programmes malveillants ont le chic pour se lancer dès le démarrage du PC, échappant ainsi aux radars des applis de sécurité. Faites un peu de ménage en installant puis en exécutant ***CCleaner Free*** (***bit.do/c8MsB***). Dans la colonne gauche, choisissez ***Outils***, ***Démarrage***. L'onglet ***Windows*** liste les programmes qui s'ouvrent automatiquement. Ceux dont l'intitulé est grisé n'agissent pas. Si vous avez un doute, effectuez une recherche Google sur le nom du logiciel ou de l'éditeur. Désactivez les items dont vous n'êtes pas sûr. Faites de même avec les menus ***Tâches planifiées*** et ***Menu contextuel***.



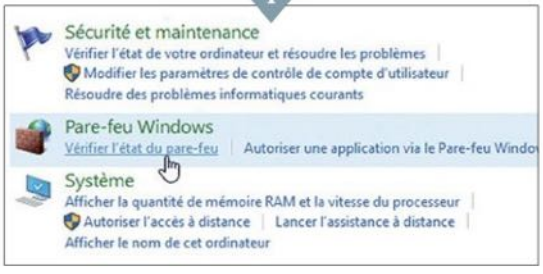
Activez le pare-feu du PC sans oublier la box !

Cet utilitaire agit comme un filtre entre les données émises et reçues par Windows. Avec les bons réglages, vous éviterez les mauvaises surprises et vous surferez sans risque.

Assurez-vous que la protection est assurée

Le pare-feu (ou firewall), vieux compagnon de Windows, reste souvent mal employé ou sous-employé. Avant tout, vérifiez que vous avez correctement activé cet outil. Pour cela, saisissez l'intitulé ***pare-feu*** dans le champ de recherche de Windows (si vous n'utilisez pas la version 10 de cet OS, accédez au ***Panneau de configuration***, puis sélectionnez ***Système et sécurité*** et la commande ***Pare-feu Windows***). Terminez en optant pour ***Vérifier l'état du pare-feu Windows***.

1



Examinez le niveau de sécurité

Lorsque la page Protéger votre ordinateur avec le pare-feu Windows s'ouvre, vous obtenez un aperçu général de la situation. Si des croix blanches sur fond rouge s'affichent face aux intitulés ***Réseaux Privés*** et ***Réseaux publics ou invités***, cela signifie que le niveau de sécurité actuel est insuffisant. Pour commencer, portez votre attention sur le volet gauche de la fenêtre et sélectionnez ***Activer ou désactiver le pare-feu***. Dans la fenêtre qui apparaît, cochez les cases ***Activer le Pare-feu Windows*** pour tous les types de réseaux.

2

3

Paramétrez le comportement du pare-feu pour les réseaux extérieurs

Le pare-feu distingue les connexions privées (sur votre box Internet) et publiques (dans une gare ou un hôtel, par exemple). Dans le volet gauche, activez ***Modifier les paramètres de notification***. Repérez la section ***Paramètres de réseaux publics*** et cochez l'option ***Bloquer toutes les connexions entrantes, y compris celles de la liste des applications***. Vous serez ainsi alerté à chaque demande de connexion, et vous devrez l'autoriser.

4

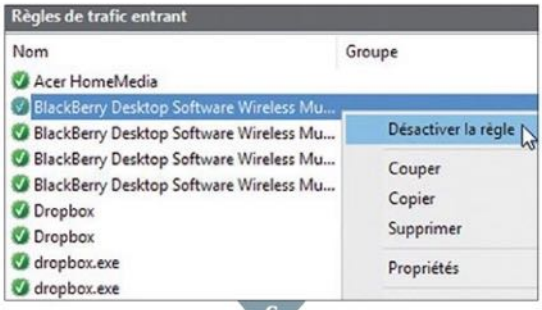
Affinez les réglages avancés

Avec les configurations de base que nous venons d'évoquer, la protection est suffisante pour des usages courants. Vous pouvez toutefois aller plus loin et choisir le lien ***Paramètres avancés*** du ***Panneau de configuration***. Vous accédez à une fenêtre appelée ***Pare-feu Windows avec fonctions avancées de sécurité***.

5

Faites le point sur la configuration

Dans le volet gauche, rendez-vous sur ***Analyse***. Vous obtiendrez ici un aperçu détaillé de la façon dont le firewall gère les données entrantes et sortantes sur votre ordinateur. L'intitulé ***Pare-feu*** dresse la liste de toutes les activités autorisées. Un bon moyen de vérifier si vous reconnaissez bien tous les processus...



6

Autorisez ou non les applications

Dans le volet gauche de Pare-feu avec fonctions avancées de sécurité, choisissez ***Règles de trafic entrant***. Passez en revue les applications et les activités autorisées à accéder à votre PC. Lorsque vous détectez des éléments qui n'ont pas, ou plus, lieu d'être (parce que vous avez cessé d'utiliser ce logiciel, par exemple), effectuez un clic droit sur son nom et optez pour la commande ***Désactiver la règle*** dans le menu contextuel.

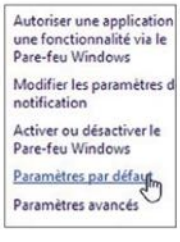
7

Modifiez les privilèges d'une fonctionnalité

À la base, les autorisations sont décidées au moment de l'installation des programmes. Mais il est possible de gérer et de modifier ces droits n'importe quand. Pour ce, revenez sur l'intitulé ***Pare-feu Windows*** du ***Panneau de configuration***. Dans le volet gauche, sélectionnez ***Autoriser une application ou une fonctionnalité via le pare-feu Windows***. Activez ensuite le bouton ***Autoriser une autre application***. Indiquez le chemin d'enregistrement vers le fichier exécutable de l'appli concernée, puis précisez pour quels réseaux vaut cette permission.

8

Rétablissez les paramètres par défaut

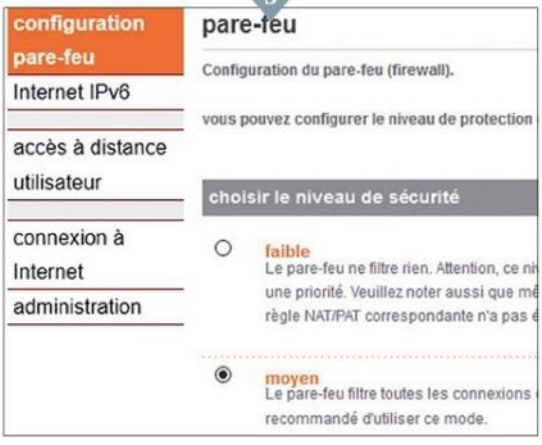


Si vous rencontrez des difficultés suite aux différentes modifications apportées au pare-feu, pas de panique ! Tout est réversible. Il vous suffit de revenir à l'écran d'accueil de cet utilitaire. Dans le volet gauche, placez-vous sur la commande ***Paramètres par défaut***. Vous récupérerez alors la configuration de sécurité minimale.

Associez Windows et votre box Internet

Quel que soit le fournisseur d'accès, votre box embarque son propre pare-feu. Contrairement aux programmes antivirus qui cohabitent très mal sur un même ordinateur, les actions des firewalls de la box et de Windows savent se combiner sans provoquer de conflit ni de ralentissement de la connexion Internet. Accédez à l'interface d'administration de votre box depuis un navigateur (en renseignant l'adresse IP indiquée dans la documentation). Identifiez-vous, puis cherchez la rubrique ***Sécurité*** ou ***Pare-feu***.

9



Définissez le niveau de sécurité de la box

Par défaut, les box Internet proposent un niveau de sécurité moyen. Vous le renforcerez en appliquant un filtrage plus drastique des données. Pour aller plus loin, n'hésitez pas à personnaliser le fonctionnement du pare-feu. Intervenez pour cela sur les réglages avancés (***Configuration avancée*** pour la Livebox d'Orange, par exemple), puis fermez et ouvrez les ports à votre convenance. ■

10

règles personnalisées

adresse IP statique

application / service	protocole	adresse IP source	port destination	action
	TCP			accepté
HTTP	TCP		80	accepter
HTTPS	TCP		443	accepter
POP3	TCP		110	accepter
POP3S	TCP		995	accepter

Suivez ces dix conseils pour sécuriser votre réseau

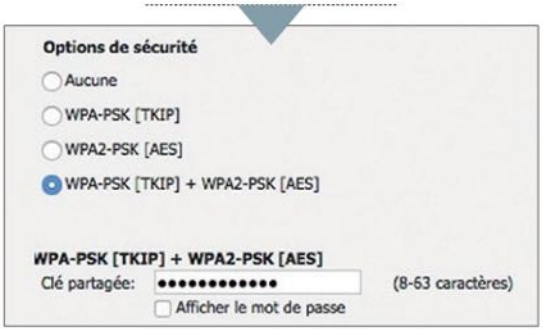
Votre box gère le trafic Internet des appareils connectés de la maison. Attention, cette porte ouverte sur le Web peut aussi conduire les curieux malintentionnés jusqu'à vos données !

1. Dissimulez-vous aux yeux indiscrets

Par défaut, le nom de votre réseau s'affiche dans la liste des points d'accès disponibles. Une première façon d'éloigner les pirates consiste à le rendre invisible. Allez dans la section des paramètres Wifi de la console d'administration de la box. Décochez l'option ***Activer la diffusion du SSID*** (SFR) ou ***Diffuser le SSID*** (Orange). Si votre box utilise plusieurs bandes de fréquence, comme c'est le cas pour la box Fibre SFR et la Livebox 4 d'Orange, masquez l'intitulé de chacun des réseaux. Vous avez aussi la possibilité d'en modifier le nom.

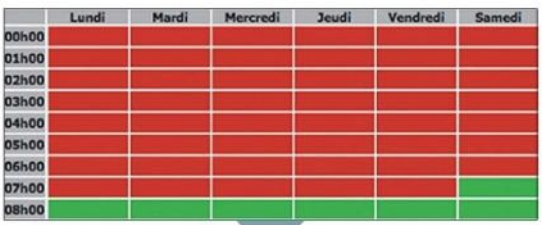
2. Choisissez un mode de chiffrement musclé

Les box Internet proposent différents niveaux de chiffrement, plus ou moins infaillibles. Le bon sens commande d'opter pour la sécurité maximale. Sur la box Fibre SFR, par exemple, cela passe par l'activation du mode ***WPA-PSK [TKIP] + WPA2-PSK [AES]***. Pensez à sélectionner ce même algorithme dans les options de sécurité quand vous vous connecterez en Wifi depuis un ordinateur, un smartphone ou une tablette.



3. Renouvelez régulièrement la clé de sécurité

Vous aurez beau redoubler d'effort et de discrétion, il se révèle très difficile d'assurer la confidentialité d'un mot de passe au-delà de quelques mois. Nous vous conseillons donc de renouveler la clé de sécurité très régulièrement (tous les deux mois, ou au moins deux fois par an). Cochez la case ***Afficher le mot de passe*** pour ne pas commettre d'impair et définissez une clé d'une dizaine de caractères, associant lettres minuscules, majuscules, chiffres et symboles.



4. Désactivez le Wifi quand vous n'en avez pas l'usage

Il vous est impossible de détecter une activité anormale sur le réseau familial lorsque vous dormez ou quand vous vous trouvez au travail. Votre réseau en devient d'autant plus vulnérable. La Livebox 4, comme la box Fibre SFR, autorise la définition de plages d'activation du Wifi. Les horaires peuvent varier selon les jours de la semaine afin de prendre en compte le week-end et la présence de vos enfants à la maison le mercredi après-midi, par exemple.

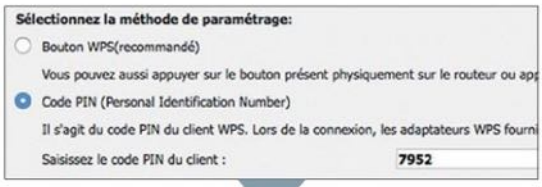
5. Coupez le réseau lorsque vous partez en vacances

Le mieux consiste à éteindre le réseau Wifi tout en gardant la box allumée, afin de pouvoir programmer des enregistrements TV ou d'accéder aux contenus multimédias à distance. L'extinction du Wifi s'effectue depuis la console d'administration Web ou, dans le cas de la Livebox 4, en appuyant sur le bouton Wifi en façade du modem.

DIFFICULTÉ
Modérée
TEMPS
30 min

6. Fermez l'accès à distance

Il n'est pas nécessaire de se trouver chez soi pour accéder à certaines ressources des box. Les fournisseurs d'accès ont prévu la possibilité de communiquer à distance à partir d'un smartphone, d'une tablette ou d'un ordinateur connecté à Internet. Ce qui constitue une faille dont pourraient tirer avantage les pirates. N'hésitez pas à fermer cet accès si vous n'utilisez pas la programmation TV à distance ni les fonctionnalités NAS de votre box.



7. N'utilisez pas le bouton d'appairage WPS

Le bouton WPS que l'on trouve sur certaines box Internet représente la manière la plus commode pour connecter des périphériques au réseau Wifi. Il existe pourtant un risque réel de piratage entre le moment où vous lancez l'opération d'appairage sur la box et celui où vous associez votre appareil. N'importe qui se trouvant à portée et se montrant plus rapide que vous peut se connecter à votre réseau. Pour minimiser les risques, préférez l'option de vérification par code PIN, proposée sur la box Fibre SFR, au bouton d'association WPS.

8. Relevez les adresses MAC de vos appareils...

N'importe qui peut se brancher sur votre Wifi dès lors qu'il en connaît la clé de sécurité. Il est possible de restreindre l'accès aux matériels dont vous aurez établi la liste au préalable. Vos visiteurs n'auront qu'à se rabattre sur le réseau invité *(voir p. 42)*. Relevez d'abord les adresses MAC de vos terminaux. Sur votre smartphone Android, par exemple, l'info figure dans la section ***À propos du téléphone***, ***État des paramètres***. Si vous êtes sous iOS, ce sera dans ***Réglages***, ***Général***, ***Informations***, ***Adresse Wi-Fi***. Sous Windows, ouvrez une fenêtre d'Invite de commandes et tapez ***ipconfig/all***.

9. ... et donnez-leur un accès exclusif

Allez à présent dans les réglages Wifi de la box et repérez la section ***Filtrage MAC*** (Livebox 4, Freebox 6) ou ***Filtrage par MAC adresses*** (SFR). Renseignez le nom du premier appareil, saisissez son adresse MAC (du genre ***00:1B:44:11:3A:B7***) et spécifiez l'adresse IP que vous souhaitez lui attribuer. Cliquez sur le bouton ***Ajouter*** et répétez l'opération avec les autres matériels. La Livebox 4 autorise la sélection des appareils depuis une liste s'ils sont connectés au réseau, ce qui évite d'avoir à entrer les adresses MAC... avec les risques d'erreurs inhérents.

10. Sécurisez l'accès à l'interface de gestion

Il serait dommage qu'un indélicat vienne ruiner votre travail et modifier les paramètres que vous venez de définir. Il faut donc protéger l'accès à la console d'administration de la box Internet. Changez sans tarder l'identifiant et le mot de passe par défaut en allant dans le menu ***Sécurité***, ***Identifiant & mot de passe*** (SFR) ou ***Configuration avancée***, ***Administration*** (Livebox 4).

ADMINISTRATION

PARAMÉTRER UNE BOX ? SIMPLE COMME UNE PAGE WEB !

Les réglages relatifs aux fonctionnalités réseau des box s'effectuent depuis une interface Web, comme c'est le cas pour les routeurs Wifi. Pour accéder à cette console d'administration, il suffit de saisir l'adresse IP de la box (***192.168.0.1*** pour la box Fibre de SFR, ***192.168.1.1*** pour la Livebox 4 d'Orange) ou son URL (***http://livebox***, ***http://momodem*** pour SFR ou encore ***mafreebox.freebox.fr*** pour Free), puis de s'identifier avec le nom d'utilisateur et le mot de passe par défaut. Une fois l'accès à distance configuré, il est même possible d'intervenir sur la Livebox 4 et la Freebox 6 sans être chez soi !

DIFFICULTÉ
Élevée
TEMPS
20 min

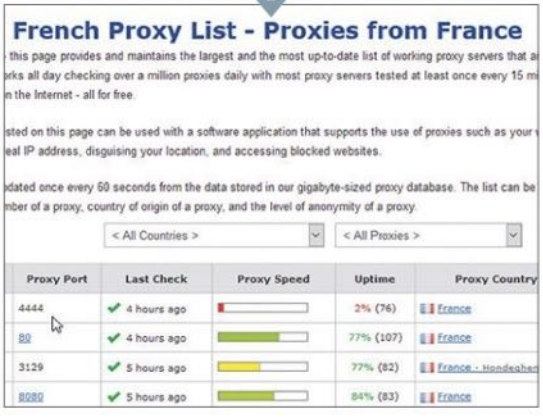
Cachez votre PC derrière un proxy pour parer aux menaces

Un proxy est une passerelle entre votre ordinateur et Internet. Grâce à lui, vous pouvez surfer à vitesse grand V et anonymement, mais aussi filtrer les contenus Web dangereux ou encore les logiciels malveillants.

Trouvez le proxy qui vous convient

Avant toute chose, vous devez choisir un proxy adapté à vos besoins. Il existe des annuaires spécialisés qui répertorient les meilleurs services. Connectez-vous, par exemple, au site Web ***Free-proxy.fr*** pour dénicher des proxy facturés moins de 5 € par mois (la plupart de ces outils sont payants). Sur ***Proxynova.com***, la liste est agrémentée d'une jauge qui renseigne sur le niveau de performance de chaque service.

1



Récupérez les informations de mise en service

Avant de pouvoir utiliser le proxy, il faut vous créer un compte utilisateur et, dans le cas d'un service payant, renseigner un moyen de règlement (carte bancaire, PayPal, etc.). L'étape suivante consiste à configurer l'ordinateur. Sur le site du proxy, notez les informations-clés dont Windows aura besoin pour aiguiller correctement les flux Internet : l'adresse IP du proxy ainsi que le port utilisé.

2

3

Paramétrez Windows en conséquence

Dans la barre des tâches de Windows, cliquez sur l'icône des notifications puis sur ***Tous les paramètres***. Accédez alors à la rubrique ***Réseau et Internet***. Au bas du volet gauche, sélectionnez l'intitulé ***Proxy***. Intéressez-vous ensuite à la section ***Configuration manuelle du proxy***. Activez l'interrupteur ***Utiliser un serveur proxy***, puis saisissez l'adresse IP et le port relevés à l'étape précédente. Enfin, validez à l'aide du bouton ***Enregistrer***.

4

Utilisez un proxy à la demande

Si vous n'avez pas besoin en permanence de la sécurité procurée par un proxy, vous pouvez recourir à un Web proxy de façon ponctuelle. Il s'agit d'un site Internet qui joue le rôle de passerelle virtuelle le temps de votre navigation. Rendez-vous, par exemple, à l'adresse ***Home-biz.info***. Entrez l'URL du site auquel vous souhaitez accéder en toute sécurité, puis faites un clic sur le bouton ***Go***. ■

DIFFICULTÉ
Aucune
TEMPS
10 min

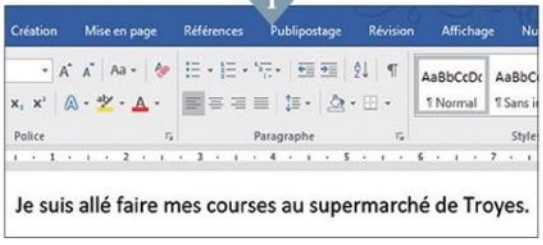
Créez des mots de passe vraiment complexes

Oubliez le prénom de votre épouse ou la date de naissance du petit dernier. Pour disposer d'un mot de passe un tant soit peu sécurisé, il convient de respecter quelques règles de base.

Appuyez-vous sur une phrase type

Un mot de passe doit éviter tout recours à des infos personnelles qui se révéleraient faciles à identifier. L'inconvénient quand on s'interdit les prénoms et les dates de naissance, c'est que l'on se trouve confronté à des combinaisons impossibles à mémoriser ! Une méthode efficace pour se souvenir d'un code sécurisé consiste à s'appuyer sur une réplique culte, un proverbe que vous appréciez ou une phrase usuelle qui compte de huit à dix mots. Pour cet exemple, nous avons retenu le propos suivant : Je suis allé faire mes courses au supermarché de Troyes.

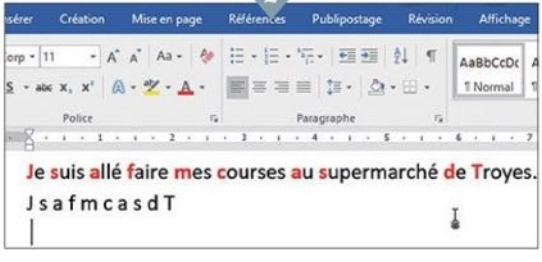
1



Isolez la première lettre de chaque mot

Ouvrez un logiciel de traitement de texte (Word, WordPad...). Saisissez la phrase type que vous venez de choisir. Placez la première lettre de chaque mot en gras ou en couleur afin de ne pas oublier de caractères. Copiez et collez ensuite chacune de ces initiales sur une autre ligne. La suite de dix lettres obtenue (***JsafmcasdT***) va constituer la trame de notre mot de passe. Une astuce pour améliorer le niveau de protection de cette combinaison consiste à modifier la casse de certaines lettres. Amusez-vous, par exemple, à basculer en majuscule un caractère sur deux, ou encore le premier et le dernier de la série.

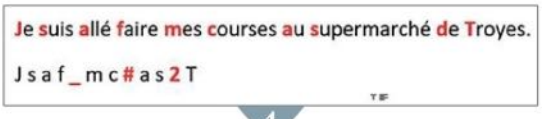
2



3

Combinez des lettres et des chiffres

Pour compliquer encore la tâche d'un individu trop curieux, nous vous conseillons de procéder à des substitutions de certaines lettres. Dans notre cas, nous avons décidé de remplacer le ***de*** par le chiffre ***2***. Vous pouvez également choisir de changer les ***S*** en ***5*** ou les ***E*** en ***3***. L'essentiel est de vous souvenir de la règle mise en place. Notre mot de passe est ainsi devenu ***Jsafmcas2T***.



4

Insérez des caractères spéciaux

Ajoutez maintenant des caractères spéciaux dans le mot de passe. Les symboles -, _, #, $, ou encore * peuvent être employés pour complexifier la combinaison. Placez-les de façon à ne pas avoir de doute au moment de la saisie. Avant les compléments d'objet direct et le complément circonstanciel de lieu, par exemple. Ici, nous insérons un tiret bas (ou ***underscore)*** avant les lettres ***mc*** (pour mes courses), puis le symbole dièse (#) avant les lettres ***as*** (pour au supermarché). Nous obtenons : ***Jsaf_mc#as2T***.

5

Faites appel à un générateur de mots de passe

Si cette méthode ne vous convient pas, recourez à un générateur de mots de passe, tel que celui proposé en ligne par Norton (***bit.do/daNaJ***). Attention, ces services ne reposent pas sur des moyens mnémotechniques ; il vous appartiendra donc de mémoriser les combinaisons obtenues par vos propres moyens. Par ailleurs, quel que soit le code ou la méthode, pensez à changer de sésame au moins une fois tous les deux mois. ■

Ouvrez un réseau Wifi réservé à vos invités

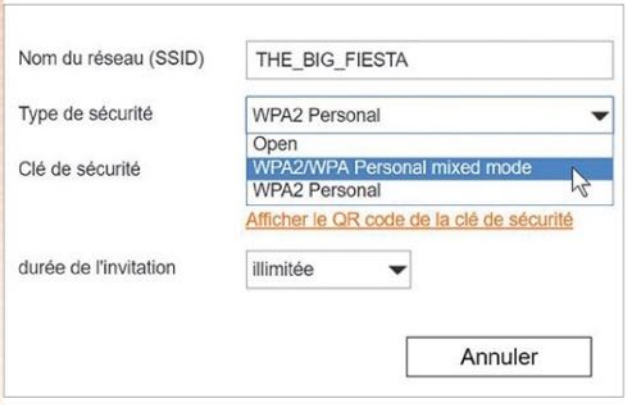
Le code d'accès à votre box Internet n'a pas vocation à être rendu public. Vous n'allez pas pour autant refuser votre connexion à vos amis de passage ! Heureusement, la box Fibre de SFR et la Livebox 4 d'Orange autorisent la création d'un second réseau Wifi, doté de sa propre clé de chiffrement et réservé aux invités. Au travail !

1. Accédez à la console d'administration

L'accès aux réglages avancés de la box s'effectue depuis un navigateur Internet. Saisissez l'URL ou l'adresse IP : ***http://livebox*** ou ***192.168.1.1*** dans le cas d'une Livebox d'Orange ; ***192.168.0.1*** pour la box Fibre de SFR.

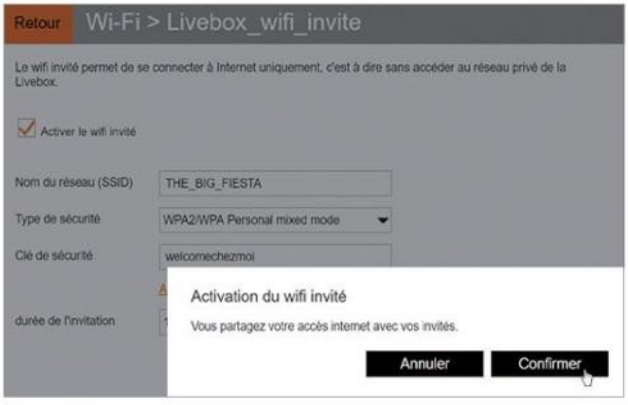
2. Affichez la page des paramètres réseau

Si vous possédez une box Fibre SFR, activez le lien ***Configurer votre modem***, identifiez-vous, puis placez-vous sur l'onglet ***Wifi***. Avec la Livebox d'Orange, cliquez sur l'icône ***Wifi*** du menu principal de l'interface.



5. Personnalisez le mot de passe

Dans la section ***Options de sécurité*** de la box SFR, ou ***Type de sécurité*** pour la Livebox 4, indiquez le mode de chiffrement (WPA-PSK + WPA2-PSK). Modifiez le mot de passe pour une combinaison facile à mémoriser.



6. Ouvrez le réseau invité

Cliquez sur ***Appliquer*** au bas de la page de gestion de la box SFR pour activer le nouveau point d'accès sans fil. Pour la Livebox 4, enregistrez vos réglages, puis faites ***Confirmer***. Il suffira à vos amis de sélectionner ce réseau.

DIFFICULTÉ
Modérée
TEMPS
20 min

© Iko

Le réseau invité offre un accès illimité à Internet. Il dispose en revanche de son propre code d'accès, ce qui évite d'exposer vos données personnelles.

3. Activez le réseau invité

Sélectionnez ***Réseau invité*** dans le menu de la box SFR, puis cochez ***Activer le réseau invité***. Sur la Livebox 4, choisissez ***Livebox Wifi_invité Modifier les paramètres Wi-Fi***, puis ***Activer le Wifi invité***.

4. Rendez ce point d'accès identifiable

Pour faciliter son identification, remplacez le nom par défaut du réseau par un intitulé évocateur: ***THE_BIG_FIESTA*** s'il s'agit d'accompagner une soirée ou ***LES_AMIS_DE_MAX*** dans le cas d'un réseau permanent.

7. Générez un QR Code pour accéder au Wifi

Sur la Livebox 4, cliquez sur ***Afficher le QR Code de la clé de sécurité*** sous le champ ***Clé de sécurité*** de la page ***Wi-Fi, Wifi invité***. Copiez-le et imprimez-le. Vos amis le scanneront avec leur téléphone pour se connecter.

8. Fermez le réseau invité

Une fois la soirée terminée, retournez sur la page des réglages du réseau invité de façon à le désactiver. La Livebox offre la possibilité d'ajuster les horaires de fonctionnement du réseau invité (menu ***Durée de l'invitation***).

DIFFICULTÉ
Modérée
TEMPS
20 min

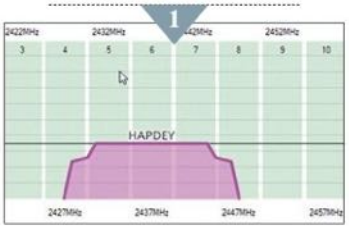
Analysez en direct le trafic sur votre réseau

Malgré toutes les précautions que vous avez prises, vous avez parfois la sensation que votre connexion Wifi se traîne. Pour identifier ce qui consomme de la bande passante, une petite analyse du trafic s'impose.

Détectez les conflits de canaux

Si vous souhaitez disposer d'une solution à la fois simple et gratuite pour mieux comprendre ce qui se passe sur votre réseau sans fil, adoptez la version gratuite du logiciel ***Acrylic Wifi Home*** (***bit.do/demTy***). Une fois installé, ce dernier détecte tous les réseaux Wifi situés à portée de votre ordinateur. Vous bénéficiez ainsi d'un aperçu global des points d'accès ouverts à proximité et voyez si d'autres box utilisent le même canal Wifi que vous.

1



Analysez la couverture Wifi

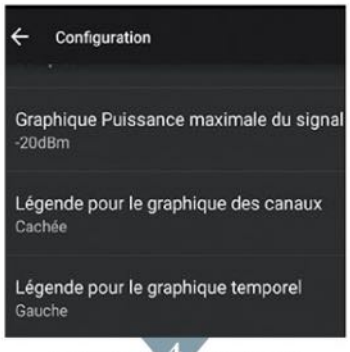
Si les ralentissements ne proviennent pas d'un canal Wifi saturé, il faut procéder à une analyse plus poussée et vérifier, par exemple, que le problème n'est pas lié à une mauvaise couverture Wifi de votre logement. Installez pour cela l'appli ***WifiAnalyzer*** de VREM Software sur votre smartphone Android.

2

3

Visualisez l'activité

Dans l'angle supérieur gauche de l'interface, touchez le bouton ***Menu***, symbolisé par trois lignes horizontales. Activez ensuite la commande ***Graphique par canal*** pour obtenir une cartographie précise et un état de l'utilisation des canaux Wifi.



4

Déchiffrez les données

Si vous éprouvez des difficultés à interpréter les éléments d'analyse générés par l'application, effleurez le bouton ***Menu*** puis l'intitulé ***Configuration***. Faites ensuite défiler les options et activez l'affichage des légendes (graphiques des canaux, graphique temporel, etc.). Vous y verrez ainsi plus clair !

Examinez le trafic depuis un MacBook ou un iMac

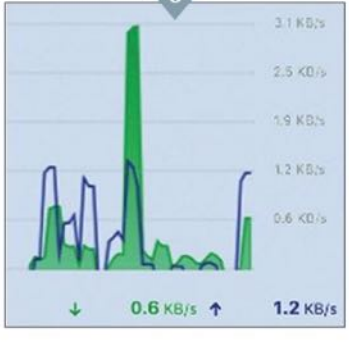
Depuis ***Safari***, connectez-vous au site ***bit.do/dem7z*** et téléchargez l'application ***PeakHour 3***. Si celle-ci refuse de s'installer, ouvrez les ***Préférences Système***, cliquez sur ***Sécurité*** et déverrouillez l'installation. Une fois cette formalité accomplie, procédez à l'analyse.

5

Traquez les anomalies

L'icône de PeakHour 3 prend place dans la barre des menus de macOS. Vous pouvez dès lors suivre le débit des données transitant en réception (download) et en émission (upload), et ce en temps réel. L'actualisation s'avère très utile pour repérer des variations anormales. Cessez toute activité sur votre Mac et vos appareils mobiles. Si des flux de données importants continuent de s'effectuer, tentez d'en identifier la source. ■

6



DIFFICULTÉ
Modérée
TEMPS
5 min

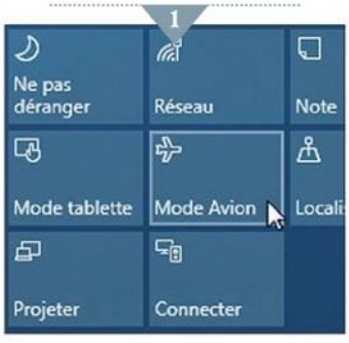
Déconnectez le Wifi quand vous n'utilisez pas Internet

Tant que vous êtes connecté au Net, votre ordinateur et vos appareils mobiles restent exposés aux menaces. Si vous n'êtes pas certain d'être bien protégé, mieux vaut couper le Wifi dès que vos activités peuvent être effectuées hors ligne.

Déconnectez Windows 10

Si vous utilisez Windows 10, placez-vous sur l'icône des notifications dans la barre des tâches, près de l'horloge. Activez ensuite le bouton ***Mode Avion*** au bas du volet. Pour rétablir l'accès à Internet, ainsi que la connexion Bluetooth, il vous suffira de cliquer sur ce même lien.

1



Activez le Mode Avion sur un ordinateur portable

Vous vous servez d'un portable ? Le clavier abrite peut-être une touche de fonction destinée à couper et à rétablir la connexion sans fil. Si ce n'est pas le cas, vous pouvez recourir au raccourci clavier d'activation du Mode Avion (une combinaison variable selon le constructeur). Chez HP, par exemple, ce raccourci se compose des touches ***fonction*** + ***F12***. Chez Asus, il s'agit de ***fonction*** + ***F10***.

2

3

Dotez votre Mac d'un mode off line

Si vous souhaitez disposer de l'équivalent du Mode Avion sur votre Mac, vous devez y installer l'application ***Airplane Setting*** (***bit.do/dbuEE***). Une icône prend alors place dans la barre des menus de macOS. Un clic sur cette vignette suffit pour activer le Mode Avion. Afin d'éviter que votre souris ou votre clavier Bluetooth soient déconnectés lors de l'opération, sélectionnez ***Settings*** et décochez l'option intitulée ***Disable Bluetooth***.

4

"Coupez" iOS

Pour activer le Mode Avion sous iOS, affichez le volet de contrôle en effectuant un mouvement de balayage vertical à partir du bas de l'écran. Lorsque le Centre de contrôle apparaît, touchez l'icône symbolisant un ***avion***. Le tour est joué !

Demandez à l'assistant Siri d'activer le Mode Avion

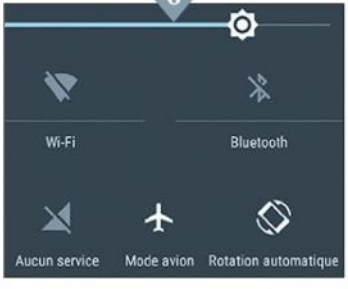
Effectuez un appui prolongé sur le bouton principal de l'iPhone. Quand Siri se manifeste, énoncez la commande ***"Active le mode avion"***. L'assistant vocal vous informe qu'il ne pourra plus fonctionner une fois ce paramètre en place. Confirmez en actionnant l'interrupteur.

5

Déployez le volet des notifications d'Android

Quelle que soit la version d'Android présente sur votre smartphone ou sur votre tablette tactile, la méthode d'activation du Mode Avion est immuable. Faites un mouvement de balayage de haut en bas de l'écran afin de dérouler le volet des notifications, puis touchez l'icône représentant un ***avion barré***. ■

6



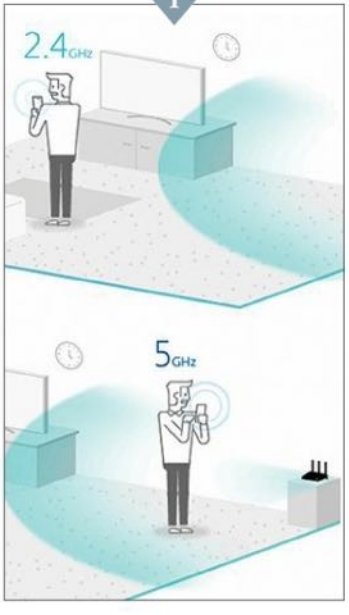
Installez un routeur dédié pour rendre le Wifi plus sûr

La protection de votre réseau dépend de la box Internet mise à disposition par votre fournisseur d'accès (FAI). En confiant la gestion du Wifi à un routeur spécialisé, vous accédez à des options de sécurité étendues, tout en bénéficiant de performances accrues.

Choisissez votre routeur externe

La plupart des routeurs dédiés offrent davantage d'options de sécurité que les box des FAI. Il s'agit, il est vrai, de matériels destinés en général aux utilisateurs experts. Il y est possible de régler le pare-feu de façon à répondre à des besoins particuliers (certains jeux vidéo nécessitent l'ouverture de ports de communication spécifiques, par exemple) ou de gérer avec précision les autorisations d'accès des différents appareils connectés de la famille. Quitte à investir dans un tel équipement, privilégiez un modèle au top de la technologie. Les meilleurs combinent plusieurs réseaux (deux voire trois) et bandes de fréquence (2,4 GHz et 5 GHz) pour atteindre des débits allant jusqu'à 7200 Mbit/s.

1



2

Réservez le nouvel appareil à la gestion du Wifi

Bardé d'antennes, le routeur Synology RT1900AC (170 € environ) que nous avons retenu pour ce pas-à-pas, assure une zone de couverture très large, de quoi profiter d'Internet dans toutes les pièces de la maison. Afin de ne pas compliquer l'installation, nous allons confier à ce matériel le soin de gérer les communications Wifi, le reste des échanges continuant à être pilotés par la box.

3

Libérez un port Ethernet

Ne touchez pas aux appareils connectés en Ethernet à votre box. La mise en place du nouveau routeur n'aura aucun effet sur leur fonctionnement, seuls les équipements et les objets qui communiquent en Wifi devront être reconfigurés. Veillez simplement à garder une prise réseau disponible sur la box.

Accédez à l'interface de gestion de la box Internet

Afin d'éviter tout risque d'interférences, vous devez suspendre le mode routeur Wifi de la box Internet. Ouvrez votre navigateur, saisissez l'adresse IP de la box et indiquez vos identifiants. Si vous n'avez jamais eu recours à cette interface Web, utilisez le nom et le mot de passe par défaut mentionnés dans la documentation de la box. Une fois sur la page d'accueil, accédez aux paramètres réseau et repérez la section relative au Wifi.

4

Coupez le Wifi de la box

Vous pouvez à présent suspendre la fonction de routeur sans fil de la box. La procédure varie d'un FAI à l'autre. Sur la Freebox, il faut positionner les interrupteurs ***Allumer le module Wifi*** et ***Votre réseau Wifi personnel*** sur ***Inactif***. Avec la Box Fibre de SFR ou la Livebox 4 d'Orange, il suffit de décocher ***Activer le réseau Wifi***. Pensez à sauvegarder ces réglages avant de quitter l'interface, sans quoi ils ne s'appliqueront pas.

5

DIFFICULTÉ
Élevée
TEMPS
45 min

6

Branchez votre routeur...

Reliez la box au port Internet du routeur à l'aide d'un câble Ethernet. Branchez ensuite le câble d'alimentation au dos du routeur d'une part, et à une prise électrique murale, d'autre part. Connectez alors un PC à l'une des prises Ethernet du routeur et appuyez sur le bouton de mise sous tension. Patientez jusqu'à ce que les voyants de contrôle lumineux placés en façade passent au vert.

7

... puis attribuez-lui une adresse IP fixe

Retournez dans l'interface d'administration de la box Internet. Ouvrez la page dédiée aux paramètres réseau et rendez-vous dans la section consacrée aux baux DHCP permanents. Sélectionnez le routeur dans la liste des appareils connectés à la box (si vous utilisez un ancien modèle de box, vous devrez sans doute renseigner manuellement l'adresse MAC du routeur), puis indiquez l'adresse IP locale de votre choix. Cliquez ensuite sur le bouton ***Ajouter*** ou sur le bouton + afin d'associer une fois pour toutes cette adresse au routeur. Enregistrez les paramètres avant de quitter l'interface de gestion.

Accédez aux réglages du routeur Wifi

Connectez un ordinateur à l'un des ports Ethernet du routeur. Lancez un navigateur et entrez l'URL du routeur (***192.168.0.1*** par exemple) ou l'adresse indiquée dans le manuel d'utilisation. Vous disposez ainsi d'une console d'administration très complète. La première opération consiste à faire en sorte que la box et le routeur ne se marchent pas sur les pieds en générant, par exemple, des conflits d'adresses IP entre les appareils connectés. Recherchez et activez l'option ***Point d'accès sans fil***.

8

Neutralisez la fonction de serveur DHCP

Sur le Synology RT1900AC, cette fonction est appelée ***AP sans fil*** et se trouve dans le ***Centre réseau***, sous l'onglet ***Administration***, ***Mode de fonctionnement***. Dès lors, le routeur devient un simple point d'accès qui sert de passerelle entre les appareils que vous y branchez en Wifi ou en Ethernet et la box qui leur alloue les adresses IP, de façon à ce qu'ils aient accès à Internet et aux ressources partagées. La gestion du Wifi s'effectue en revanche sur le routeur. Pour bénéficier d'une bande passante élargie, activez les différents réseaux disponibles. À noter, le Synology RT1900AC en compte trois : 2,4 GHz et 5 GHz.

9

10

Modifiez l'intitulé et la clé du réseau Wifi

Profitez de vous trouver dans l'interface de gestion du routeur pour personnaliser le nom du réseau sans fil (SSID). Définissez également un mot de passe plus facile à retenir que la combinaison par défaut. Combinez lettres minuscules et majuscules, chiffres et symboles, en veillant à respecter la longueur minimale imposée par le mode de chiffrement activé. Sauvegardez ces réglages, puis essayez de vous connecter au nouveau point d'accès depuis un smartphone ou un portable.

11

Ouvrez un réseau Wifi spécifique pour vos invités

Cette option, disponible également sur certaines box Internet récentes *(lire p. 42)*, évite d'exposer le mot de passe de votre réseau Wifi principal lorsque vous recevez des amis. Le routeur Synology RT1900AC sait créer un réseau autonome, disposant de son propre nom et d'un code d'accès spécifique. ■

DIFFICULTÉ
Aucune
TEMPS
10 min

Sécurisez le Bluetooth et le partage de connexion

Les smartphones sont de grands communicants. Wifi, Bluetooth, NFC, partage de connexion 4G, ils multiplient les protocoles d'échange, pour le meilleur et pour le pire. Les connexions Bluetooth et sans contact s'avèrent en effet très vulnérables.

Désactivez le partage sous iOS

La première des précautions à prendre pour éviter de vous faire pirater votre forfait de données mobile via iOS, consiste à couper le Partage de connexion dès que vous n'en avez pas besoin. Pour cela, touchez les boutons ***Réglages*** et ***Partage de connexion***, puis placez l'interrupteur en position inactive.

1

Forcez la mise à jour du mot de passe de connexion partagée

Que vous activiez et désactiviez le Partage de connexion sous iOS, le code d'accès généré à la première activation reste toujours le même. Il s'agit d'une vraie lacune de sécurité. Cette combinaison doit être régulièrement changée (idéalement à chaque nouvelle session) pour jouer pleinement son rôle et protéger l'accès à l'iPhone. Pour le modifier, effleurez ***Réglages***, ***Partage de connexion***. Touchez le précieux sésame et saisissez-en un nouveau.

2

3

Cachez-vous autant que possible

Vous utilisez sans doute le Bluetooth pour écouter de la musique avec votre casque sans fil ou en voiture pour téléphoner en mode mains libres. Si cette connexion vous est inutile le reste du temps, prenez l'habitude de la désactiver lorsqu'elle n'est pas requise. Sous iOS, déployez le centre de contrôle d'un mouvement de balayage du bas vers le haut de l'écran et sélectionnez l'icône ***Bluetooth***.

4

Activez le Bluetooth à la carte sous Android

Agissez de même si vous ne vous servez pas du Bluetooth en permanence sur votre mobile Android (vous gagnerez ainsi en autonomie !). Faites apparaître le volet des paramètres rapides d'un mouvement de balayage depuis le haut de l'écran, puis effleurez l'icône ***Bluetooth***.

Empêchez l'activation des connexions sans fil

Installez l'appli gratuite ***AppLock*** sur votre mobile de façon à sécuriser le partage de connexion et l'activation du Bluetooth. Une fois le programme téléchargé et en place, dessinez sur l'écran le mouvement qui commandera le déverrouillage des applis et des outils d'Android. Confirmez ce schéma et validez.

5

Verrouillez le Bluetooth

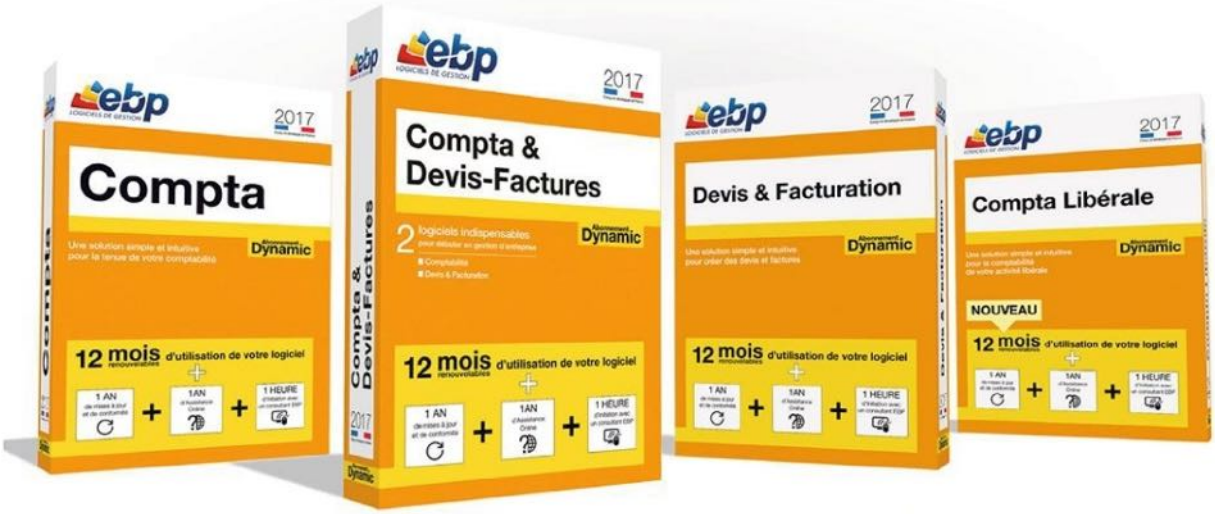
Dans la liste des fonctionnalités gérées par AppLock, repérez la section ***Bouton de verrouillage***. Touchez le ***cadenas*** grisé à droite de la ligne ***Bluetooth***. L'icône devient verte. Désormais, pour suspendre ou rétablir la connexion Bluetooth, il faudra dessiner le mot de passe. ■

6

LOGICIELS DE GESTION

Abonnement Dynamic

Découvrez l'offre tout inclus



Retrouvez ces logiciels et toute la gamme EBP dans votre magasin :

Bureau Vallée
Le discount est dans notre nature

Les logiciels Dynamic : conformité et tranquillité pour votre entreprise.

Licence en ABONNEMENT 1 AN

+

1 AN de mises à jour et de conformité	+	1 AN d'Assistance Online	+	1 HEURE d'Initiation avec un consultant EBP

VERROUILLER

Peut-on vraiment faire confiance à la biométrie ?

© Sergey Nivens

SOMMAIRE

Au rythme où évoluent les smartphones, peut-être y trouverons-nous, dans un futur proche, des systèmes d'identification reposant sur l'analyse ADN de l'utilisateur. En attendant, de plus en plus de modèles embarquent un capteur d'empreintes digitales, sollicité pour déverrouiller l'accès à l'appareil, mais aussi pour s'authentifier auprès de plateformes de paiement. Si la biométrie simplifie notre vie en nous évitant de passer notre temps à saisir des mots de passe, qu'en est-il de la fiabilité des technologies mises en œuvre par les fabricants de mobiles ? Peut-on vraiment leur faire confiance pour protéger nos données personnelles ?

Les chances que deux individus présentent les mêmes empreintes digitales sont environ de 1 sur 64 milliards. Il n'existe donc pas le moindre doute quant à la pertinence de ce marqueur en tant qu'identifiant. En revanche, certaines réserves apparaissent au sujet de la capacité des capteurs implantés sur les smartphones à traiter ces informations de façon pertinente et fiable. Plusieurs expériences menées par des spécialistes de la sécurité ou des laboratoires de recherche ont mis en lumière la faillibilité de ces dispositifs. Le concepteur de systèmes biométriques Vkansee est ainsi parvenu à tromper le capteur TouchID de l'iPhone à l'aide d'un moulage d'une empreinte digitale réalisé... avec de la pâte employée par les dentistes pour effectuer leurs moulages. D'autres sont parvenus au même résultat en prélevant des empreintes à l'aide de colle forte ou, même, à partir de la photo d'une main publiée dans un magazine et d'une imprimante destinée à produire des prototypes de circuits imprimés, valant quelques milliers d'euros !

Courbes et reliefs. Pour contrer ces techniques, plutôt simples, qui pourraient faire le bonheur des cybercriminels, les fabricants travaillent à renforcer l'effi-

Certains appareils Nexus, Microsoft ou Nokia savent déjà identifier l'iris.

cacité de leurs capteurs. Qualcomm a ainsi présenté un procédé combinant reconnaissance optique et ultrasons, capable de prendre une image en relief du doigt. Outre les crêtes et le dessin des sillons papillaires, le capteur mémorise également les courbes et le relief, rendant bien plus difficile une reproduction fidèle. Un autre axe de progrès passe par l'amélioration de la résolution des capteurs et la puissance de calcul accrue des smartphones. Ainsi, davantage de points de concordance seraient pris en compte afin d'éviter toute erreur d'identification. Car actuellement, les mobiles se contentent de quelques points de similitude pour valider une empreinte, là où la police et la justice en exigent 12.

Top secret ? Autre question sensible : les infos biométriques sont-elles à la portée des hackers ? Qu'il s'agisse des empreintes digitales ou de dispositifs basés sur la reconnaissance faciale ou la lecture de l'iris intégrés sur certains smartphones (Lumia 950 de Microsoft, Nexus de Google, Galaxy Note 7 de Samsung), quid du stockage de ces données sensibles ? Pour des raisons de confidentialité, celles-ci sont enregistrées sur le téléphone, après chiffrement, dans une zone de la mémoire seulement accessible par le système. Du moins en théorie, puisque des chercheurs sont parvenus à récupérer des empreintes sur un Galaxy S5 en profitant de failles de sécurité. Il semble donc que rien ne vaille encore un solide mot de passe pour éviter les intrusions sur votre téléphone ! ■

Les données biométriques sont stockées sur le téléphone

BIOMÉTRIE

Quatre technos pour les mobiles de demain

1 Le réseaux veineux Cette cartographie, qui s'avère propre à chaque individu, n'évolue plus une fois la croissance achevée. Difficile à falsifier, elle peut être identifiée à l'aide d'une caméra infrarouge analysant les veines de la paume ou du doigt (en association avec un capteur d'empreintes).

2 L'iris La partie colorée de l'œil présente un dessin unique, défini par près de 200 variables. Sa reconnaissance nécessite l'utilisation d'un capteur photo haute résolution. Pour éviter au smartphone d'être dupé par une image fixe placée devant la lentille, les fabricants ajoutent un dispositif capable de détecter les réactions de l'iris à la lumière.

3 La rétine La membrane qui tapisse le fond de l'œil est parcourue par un réseau très complexe de vaisseaux sanguins, de veines et d'artères. Le tout forme un motif spécifique à chaque individu, et virtuellement impossible à dupliquer. Très efficace, cette technique de reconnaissance rétinienne impose d'illuminer brièvement le fond de l'œil et de placer la caméra assez près.

4 L'oreille Voici une piste étonnante explorée en matière de biométrie : l'authentification liée à la géométrie de l'oreille ! En effet, cette caractéristique physique ne change plus une fois que nous avons fini de grandir. Du coup, ce procédé offrirait un taux de fiabilité supérieur à 99 %.

Adoptez un coffre-fort

Avec une appli comme LastPass, il est facile de conserver mots de passe, données bancaires, copies de papier d'identité et cartes de paiement à portée de main, sans les exposer.

Installez la version gratuite de l'appli

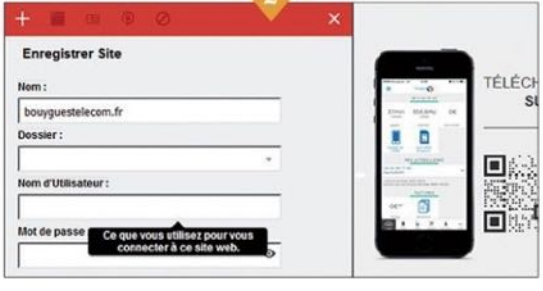
LastPass (comme son concurrent Dashlane) ne se contente pas de mémoriser vos données sous une forme chiffrée. Il les synchronise également sur vos différents appareils. Une fonctionnalité désormais intégrée à sa version gratuite (Dashlane la réservant à ses abonnés Premium). Récupérez ***LastPass*** sur votre ordinateur (***bit.do/daF3a***). Sélectionnez ***Obtenir LastPass Free*** et autorisez l'ajout du module complémentaire au navigateur (Chrome, Firefox). Créez un compte, puis mémorisez un mot de passe maître (le seul à retenir).

1

Répertoriez tous vos sésames

Cliquez sur l'icône de l'appli dans la barre d'outils du navigateur. Entrez le mot de passe précédemment défini pour activer l'extension. Ne cochez pas l'option ***Mémoriser le mot de passe*** si vous partagez votre ordi, sinon n'importe quel utilisateur accéderait au coffre-fort. Connectez-vous à l'un de vos sites Web favoris requérant une authentification (e-commerce, messagerie en ligne, etc.). À droite de la zone de saisie de l'identifiant, choisissez l'icône **...** puis **+**. Tapez le nom d'utilisateur et le mot de passe de ce site et validez avec ***Enregistrer***.

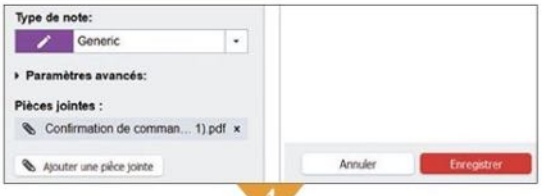
2



3

Générez des mots de passe forts

Connectez-vous à un site cybermarchand et accédez à la page servant à redéfinir le mot de passe. À droite du champ de saisie du nouveau code, activez le ***cadenas*** afin de solliciter LastPass. Le volet ***Générer un mot de passe*** s'affiche. Rendez-vous sur ***Afficher les options avancées***. Ajustez la longueur de la combinaison, optez pour ***Utiliser ce mot de passe*** et confirmez le nouveau code.



4

Protégez vos documents sensibles

Rendez-vous à présent sur l'icône ***LastPass*** du navigateur Web, puis sur ***Mon coffre-fort***, ***Notes sécurisées***, ***Ajouter une note sécurisée*** et, enfin, sur ***Ajouter une pièce jointe***. Pointez vers le document à protéger et lancez ***Ouvrir***. Déroulez ensuite le menu ***Type de note*** et sélectionnez une catégorie. Donnez-lui un nom et terminez avec ***Enregistrer*** pour chiffrer le document et l'envoyer dans votre coffre-fort numérique.

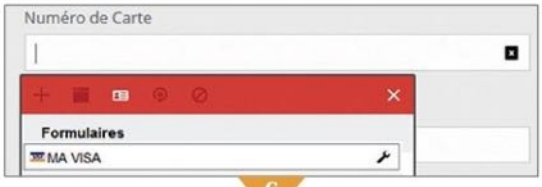
5

Créez des dossiers de rangement

Activez ***Notes sécurisées***. Passez le curseur sur le bouton **+** et ouvrez ***Ajouter un nouveau dossier***. Saisissez un nom, puis optez pour ***Enregistrer***. Le dossier est dorénavant accessible dans le menu ***Folder***.

DIFFICULTÉ
Aucune
TEMPS
45 min

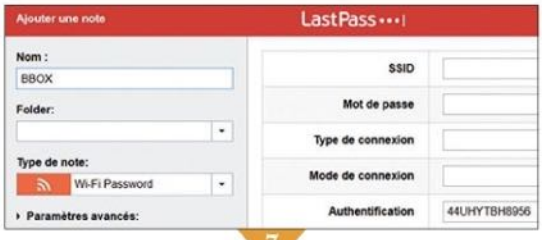
numérique sécurisé



6

Mémorisez vos coordonnées bancaires

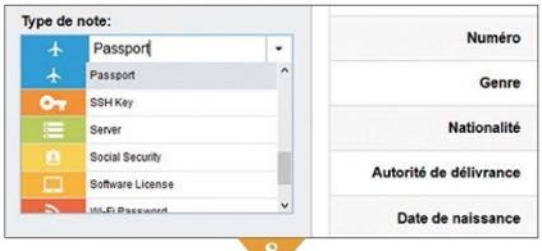
LastPass peut remplir à votre place les formulaires de paiement des sites marchands. Il suffit pour cela d'enregistrer au préalable vos coordonnées bancaires. Reprenez l'étape 4 mais en optant, cette fois-ci, pour ***Formulaires***, ***Add Form Fill***, ***Carte de crédit***. Remplissez les champs et validez à l'aide du bouton ***Enregistrer***.



7

Sauvegardez le mot de passe Wifi

Si vous avez du mal à vous rappeler le mot de passe Wifi de votre box Internet, sauvegardez-le dans LastPass pour l'avoir toujours sous la main. Accédez au coffre-fort, rendez-vous sur ***Notes sécurisées***, **+**, puis déroulez le menu ***Type de note***. Choisissez alors ***Wi-Fi Password***. Dans la section ***Authentification***, entrez le mot de passe WPA ou WEP figurant au dos de la box. Indiquez le nom du réseau dans le champ SSID et activez ***Enregistrer***.



8

Mettez vos papiers d'identité à l'abri

Dans ***Notes sécurisées***, sélectionnez **+**, déroulez le menu ***Type de note*** et précisez la nature de votre document (Driver's Licence, Health Insurance, Passport, etc.). Remplissez les champs associés, puis allez sur ***Ajouter une pièce jointe*** pour enregistrer une copie numérisée.

Partagez des éléments en toute confidentialité

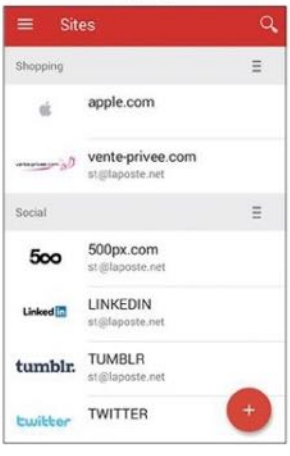
LastPass offre la possibilité d'associer vos contacts à certains formulaires de manière sécurisée. Placez-vous sur ***Centre de partage*** dans la colonne gauche, puis sur ***Ajouter un dossier partagé***. Avec la version payante, vous inviterez jusqu'à cinq personnes à accéder à vos mots de passe et à vos notes. Si vous ne voulez pas passer en mode Premium (13 € par an), il existe un moyen de partager une note gratuitement. Rendez-vous dans le menu ***Notes sécurisées*** et pointez sur le document que vous souhaitez mutualiser. En bas à gauche de la fenêtre, activez l'icône ***Partager***. Renseignez ensuite la ou les adresses mails des individus concernés et validez avec le bouton ***Share***. Ces contacts seront en mesure d'afficher le contenu de la note, mais sans être autorisés à télécharger les éventuelles pièces jointes associées.

9

10

Emportez votre coffre-fort avec vous

L'intérêt de LastPass réside dans sa fonction de synchronisation. Pour en bénéficier, installez l'appli sur votre smartphone depuis le ***Google Play Store*** ou l'***App Store***. Démarrez le programme et renseignez vos identifiants de connexion LastPass. Déroulez le menu puis pressez ***Notes sécurisées*** afin de retrouver vos documents. Pour vous connecter à un site dont vous avez mémorisé les identifiants, effleurez l'intitulé ***Sites***, sélectionnez une adresse, puis appuyez sur le bouton ***Lancer***. Le navigateur intégré à LastPass vous conduit directement sur le formulaire d'identification et remplit automatiquement les champs. ■



DIFFICULTÉ
Aucune
TEMPS
20 min

Doublez la sécurité grâce à la validation en deux étapes

Qu'adviendrait-il si vos identifiants tombaient entre de mauvaises mains ? Rien de grave, à condition d'avoir activé le dispositif de double authentification via SMS que proposent de plus en plus de services en ligne.

Paramétrez les deux authentifications de votre compte Dropbox

Les principaux cybermarchands, les géants du Web ou encore les hébergeurs ont désormais tous intégré ce dispositif de validation en deux temps. Une fois activé, il entre en action dès que vous tentez de vous connecter depuis un nouvel appareil. Pour sécuriser l'accès à votre espace Dropbox, par exemple, allez sur la page des ***paramètres*** de votre compte et affichez l'onglet ***Sécurité***.

1

Activez l'option de réception d'un code de sécurité par SMS

À la rubrique ***Validation en deux étapes***, pointez les liens ***Cliquer pour activer***, ***En savoir plus*** afin d'obtenir une présentation détaillée du fonctionnement de cette option. Choisissez à présent ***Commencer***. Saisissez votre mot de passe Dropbox habituel et cochez l'option ***Utiliser des SMS***, puis ***Suivant***. Précisez votre numéro de mobile et sélectionnez ***Suivant***.

2

3

Indiquez un numéro de mobile de secours

Entrez la combinaison de six chiffres reçue par SMS, puis optez pour ***Suivant***. Ajoutez un second numéro de portable qui sera utilisé en cas de perte de votre mobile pour vous faire parvenir le code de sécurité. À l'étape suivante, mémorisez l'un des codes de sauvegarde affichés à l'écran (il vous sera utile pour débloquer le compte en cas de problème). Terminez avec ***Activer la validation en deux étapes***.

4

Sécurisez votre compte Facebook

Le réseau social Facebook est particulièrement concerné par le vol de comptes et le phénomène d'usurpation d'identité. Pour éviter que l'on s'approprie votre profil, allez dans les ***Paramètres*** de votre compte, cliquez sur ***Sécurité***, ***Approbations de connexion***, puis sur l'option ***Ajouter un téléphone***.

5

Confirmez la validation à deux étapes

Notez votre numéro de mobile dans le champ ***Numéro de téléphone***. Validez (***Continuer***). Réceptionnez le code envoyé par SMS, saisissez-le dans la zone prévue à cet effet et terminez avec ***Confirmer***. Pour ne pas divulguer votre numéro de portable, un élément-clé de la double sécurité, pointez sur ***Amis***, ***Moi uniquement***. Afin d'activer le dispositif, actionnez le bouton ***Enregistrer les paramètres***. ■

DIFFICULTÉ
Aucune
TEMPS
45 min

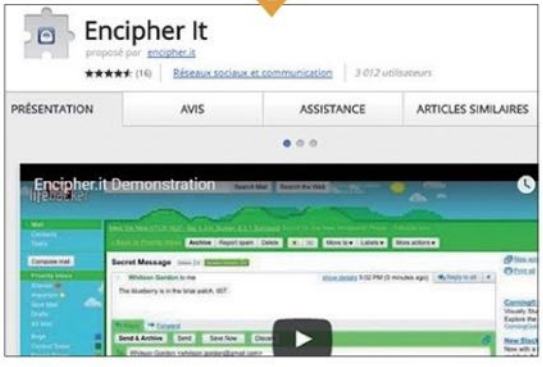
Ne courez pas le risque de voir vos courriels interceptés

Votre correspondance est censée demeurer confidentielle. Le service en ligne Encipher It chiffre vos mails et s'assure qu'ils ne peuvent être lus que par leurs destinataires. Sans la clé de sécurité, le contenu des messages ne s'affiche pas.

Intégrez l'extension Encipher It dans Chrome

Si vous utilisez le navigateur Google Chrome et un webmail comme Gmail, Yahoo Mail ou Outlook, vous avez la possibilité de chiffrer vos messages à l'aide de l'extension Encipher It (***bit.do/daGLL***). Sélectionnez ***Ajouter à Chrome***, puis ***Ajouter l'extension*** pour installer le programme. Accédez ensuite à votre messagerie, rédigez un nouveau mail, puis pointez sur l'icône ***Encipher It*** qui s'affiche en haut à droite de la barre d'outils du navigateur.

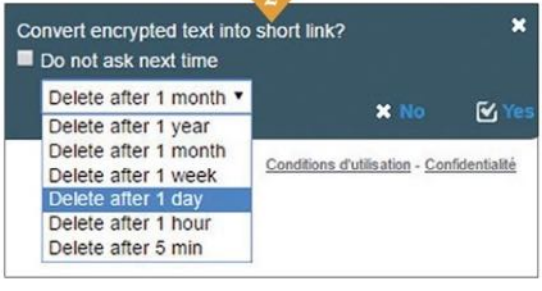
1

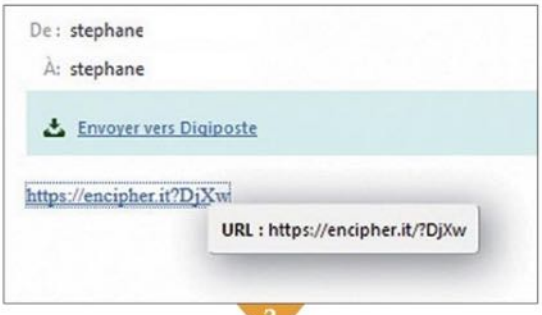


Chiffrez votre message

Activez l'icône bleue représentant un ***cadenas***. Entrez le mot de passe de votre choix dans la zone de saisie et optez pour le lien ***Encipher It*** en bas à droite de la fenêtre de l'extension. Le message Gmail devient alors illisible, le texte étant remplacé par une suite de chiffres. Déroulez le menu ***Delete after 1 year*** et ajustez le délai de suppression du message. Validez par ***Yes***.

2





3

Communiquez le mot de passe

Pour lire le courriel, les destinataires doivent cliquer sur le lien ***encipher.it*** contenu dans le corps du mail. Ils sont alors dirigés vers le site Web du service et invités à saisir le mot de passe défini lors du chiffrement des données. N'oubliez donc pas de leur transmettre cette information. Pour éviter tout risque, n'utilisez pas pour cela votre messagerie électronique. Joignez plutôt vos contacts par Skype, SMS ou téléphone.

4

Composez un texte chiffré en ligne

Il reste aux invités à entrer le mot de passe dans le champ ***Enter the decryption password*** et à activer ***Decrypt***. Le message apparaît alors en clair dans le volet droit de la fenêtre. Il est également possible d'envoyer des courriels chiffrés directement depuis le site Encipher It. Tapez votre texte dans la zone de saisie, cliquez sur ***Encipher It*** et indiquez un mot de passe. Sélectionnez ensuite ***Encipher It***, puis ***Copy*** afin d'effectuer le chiffrement. Enfin, copiez le message dans un mail (***Ctrl + V***). ■

Protégez vos données, vos disques et vos clés USB

Des infos personnelles ont pour vocation de demeurer... privées ! C'est pourquoi il convient de les protéger des regards indiscrets en les chiffrant, en les masquant ou encore en élevant des barrières autour des fichiers.

Récupérez Renee File Protector

La solution la plus évidente consiste à utiliser un programme capable de verrouiller l'accès aux dossiers de Windows. Ouvrez votre navigateur et accédez au site ***bit.do/daJUM***. Repérez le logiciel ***Renee File Protector*** et cliquez sur le bouton ***Version Win*** afin de lancer le téléchargement. Installez l'application, puis redémarrez votre ordinateur. Une fois sur le Bureau de Windows, cliquez sur l'icône ***Renee File Protector***, puis sur ***Essai***.

1

Définissez le mot de passe maître

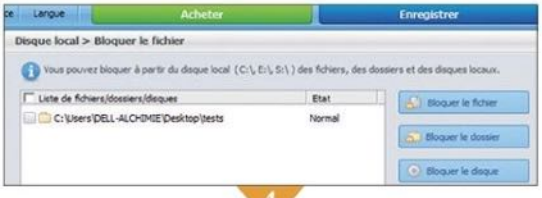
La version gratuite de l'utilitaire n'autorise qu'une faible sécurisation pour vos données. Préférez la version payante (35 € environ) afin de l'améliorer. Entrez le mot de passe indiqué par le logiciel ainsi que votre adresse mail pour recevoir le code sur votre messagerie. Cochez la case ***J'ai copié ce mot de passe*** et cliquez sur ***OK***. Vous accédez alors à l'interface du programme.

2

3

Rassemblez vos contenus dans un dossier

Dans la colonne gauche, exécutez la commande ***Bloquer le fichier***, puis dans celle de droite, optez pour ***Bloquer le dossier***. Définissez l'emplacement à protéger et validez à l'aide du bouton ***OK***. Vous pouvez aussi choisir un nouveau dossier verrouillé pour déposer vos documents sensibles. Ce dernier s'affichera au cœur de la fenêtre, accompagné de la mention ***Bloqué*** en rouge. Fermez ***File Protector***, ouvrez l'***Explorateur de fichiers*** et double-cliquez sur le dossier. La mention ***Accès refusé*** apparaît.



4

Annulez le verrouillage d'un doc sensible

Si vous voulez supprimer ce verrou, faites un double clic sur l'icône de ***File Protector***. Entrez le mot de passe maître défini à l'étape 2, sélectionnez ***Essai***, puis ***Bloquer le fichier*** en colonne gauche. Cochez l'élément à déverrouiller et validez avec ***Débloquer***. La mention ***Normal*** s'affiche alors dans la colonne ***État***. Ouvrez le dossier afin d'être sûr que vous pouvez de nouveau y accéder.

5

Chiffrez un dossier ou un fichier

Revenez à File Protector. Parcourez le volet gauche et activez la commande ***Crypter le fichier***, ***Ajouter un fichier ou dossier***. Pointez vers l'élément que vous souhaitez chiffrer et optez pour ***OK***. Sélectionnez alors le type de chiffrement : glf (File Protector sera alors nécessaire pour le décryptage) ou exe. Double-cliquez sur le dossier et saisissez le mot de passe.

6

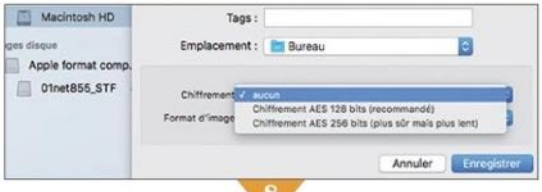
Protégez un disque externe

File Protector sait aussi sécuriser les contenus sauvegardés sur un disque dur externe ou une clé USB. Optez pour ***Disque externe*** en colonne gauche, puis activez la commande ***Bloquer le dossier*** (ou ***fichier***). Désignez le support amovible et l'élément à préserver. Terminez avec ***OK***. Entrez le mot de passe sans ajouter de code invité et choisissez ***Bloquer***. Le dossier est désormais protégé. Pour le déverrouiller, insérez la clé, sélectionnez le dossier et saisissez le mot de passe File Protector.

7

Faites disparaître provisoirement des éléments avant de prêter votre ordi

Autre possibilité offerte par cette protection : rendre momentanément invisible certains fichiers ou dossiers. Une fonction appréciable lorsqu'on prête son ordinateur. Cliquez sur ***Disque local***, ***Cacher le fichier***. Dans la colonne droite, activez la commande ***Cacher le dossier*** (ou ***fichier***). Sélectionnez ensuite l'élément à faire disparaître et validez (***OK***). Pour le faire réapparaître, rendez-vous sur ***Afficher*** en colonne droite.



8

Réalisez un chiffrement sur un Mac

Recherchez et lancez l'***Utilitaire de disque*** de macOS. Cliquez sur ***Fichier***, ***Nouvelle image***, ***Image d'un dossier***. Pointez vers l'emplacement à protéger, puis choisissez ***Ouvrir***. Déroulez le menu ***Chiffrement***, sélectionnez l'option ***AES 128 bits***, entrez un mot de passe, confirmez-le et activez ***Choisir***, ***Enregistrer***. Le chiffrement démarre. Validez avec ***OK*** une fois l'opération terminée. Un dossier portant l'extension .dmg est créé. Double-cliquez dessus et saisissez le mot de passe pour le déchiffrer. ■

Compressez vos documents avant de les envoyer

L'appli 7-Zip sert à créer des dossiers d'archive autoextractibles protégés par un mot de passe. Idéal pour sécuriser les envois de fichiers par mail.

ÉTAPE 1

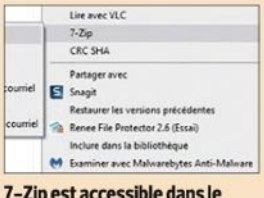
Installez 7-Zip

Connectez-vous au site ***bit.do/daKb9***. Allez sur ***Download*** et sélectionnez la version adaptée à votre édition de Windows (32 ou 64 bits). Mettez en place 7-Zip puis redémarrez l'ordinateur. Ouvrez ensuite l'***Explorateur de fichiers*** (***Windows+E***). Pointez vers le fichier ou le dossier que vous souhaitez compresser.

ÉTAPE 2

Paramétrez la compression

Effectuez un clic droit sur l'élément concerné. Déroulez le menu ***7-Zip*** et choisissez ***Ajouter à l'archive***. Dans le menu ***Format de l'archive***, préférez ***ZIP***, qui garantira une meilleure compatibilité. Vous pouvez modifier le niveau de compression de ***Plus rapide*** (légère) à ***Ultra*** (extrême, afin de gagner le plus de place possible).



7-Zip est accessible dans le menu contextuel de l'Explorateur de fichiers de Windows.

ÉTAPE 3

Compressez et chiffrez les fichiers

Cliquez sur le bouton... situé à droite du nom de l'archive. Désignez ensuite le répertoire de destination. Dans ***Options***, vous pouvez décider de supprimer les fichiers originaux en cochant la case ***Effacer les fichiers après compression***. Il est temps de penser à sécuriser l'archive. Entrez un mot de passe dans le champ ***Chiffrement***, déroulez le menu ***Méthode de chiffrement*** et optez pour ***AES-256***. Validez avec ***OK***. La compression commence. Cette opération dure plus ou moins longtemps en fonction du type de fichier et de sa taille.

ÉTAPE 4

Générez une pièce jointe compressée

Si les fichiers compressés doivent être envoyés par mail, retournez dans le menu contextuel de l'appli, puis activez l'option ***Compresser et envoyer par courriel***. La messagerie définie par défaut dans Windows (Thunderbird ou Outlook, par exemple) se lance automatiquement. L'archive Zip est alors attachée comme une pièce jointe. Au moment de la réception, le destinataire devra cliquer sur son icône avec le bouton droit de la souris, choisir la commande ***Extraire tout***, saisir le mot de passe et, enfin, définir le dossier de destination. ■

Renforcez les défenses autour de votre cloud

S'il est plaisant de pouvoir accéder à ses données depuis n'importe quel appareil connecté à Internet, il ne faut pas négliger la sécurité. Voici comment protéger efficacement l'accès aux fichiers stockés sur OneDrive, Dropbox, Google Drive ou HubiC.

ONE DRIVE

1 Activez les options de sécurité de base

Le principal intérêt des services de stockage en ligne est de pouvoir récupérer des fichiers que l'on utilise sur son ordinateur ou un smartphone. Mais que faire en cas de vol de son mobile ? Si vous n'avez pas pris de précautions, le voleur accédera à vos documents. Quel que soit le service cloud que vous utilisez, rendez-vous dans les ***Paramètres*** du téléphone. Sous Android, appuyez sur ***Sécurité***. Activez le verrouillage automatique, choisissez un mode de protection (code PIN, par exemple) et réglez le délai de mise en veille sur trois minutes. Ouvrez l'appli ***OneDrive*** et connectez-vous à l'aide de vos identifiants de compte Microsoft.

2 Décidez des éléments à charger systématiquement

OneDrive demande s'il peut télécharger les photos et vidéos du smartphone de manière automatique. Touchez ***OK*** ou ***Pas maintenant*** si vous souhaitez garder ces éléments sur le téléphone. Vos dossiers OneDrive s'affichent à l'écran. Déroulez le menu de l'appli, touchez l'icône en forme d'***engrenage***. Désactivez ***Secouer l'appareil pour envoyer un commentaire***.

3 Définissez un code secret

Effleurez ensuite ***Code secret*** dans la section ***Options*** des ***Paramètres*** et activez le curseur associé. Tapez un code à quatre chiffres et confirmez-le. Quittez l'appli ***OneDrive***, ouvrez-la de nouveau : la combinaison que vous venez de définir est indispensable pour continuer. ■

DROPBOX

1 Ne confiez pas trop d'informations à Dropbox

Lancez l'appli ***Dropbox*** sur votre appareil mobile, puis entrez vos identifiants de connexion. Le contenu de votre espace en ligne s'affiche. Pressez l'icône des ***Paramètres***, en haut à droite du volet de menu, puis ***Effacer l'historique de recherche*** et ***Vider le cache***. Désactivez l'option ***Synchroniser les contacts*** et le chargement automatique des photos.

Ajoutez un code de sécurité

Comme OneDrive, Dropbox peut être sécurisé par mot de passe. Dans la partie ***Fonctionnalités avancées*** des ***Paramètres***, touchez ***Configurez le code secret***, ***Activez le code secret***. Entrez une combinaison à quatre chiffres. Cochez ***Effacer les données après 10 authentifications infructueuses***. ■

2

DIFFICULTÉ
Aucune
TEMPS
30 min

GOOGLE DRIVE

1

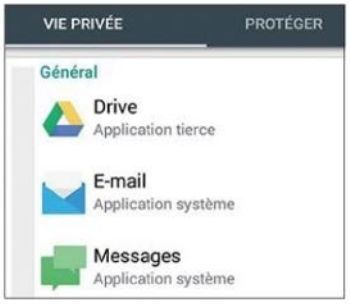
Retrouvez le contenu de votre cloud Google Drive

Google Drive est préinstallé sur la plupart des mobiles Android. Pour vous en assurer, accédez au ***Play Store***, recherchez l'appli et appuyez sur le bouton ***Ouvrir*** ou ***Mettre à jour***. Drive est automatiquement associé au compte Google du téléphone. Il n'est donc pas nécessaire de s'authentifier au démarrage.

2

Forcez la saisie d'un mot de passe au lancement de l'appli

Si Dropbox ou OneDrive propose une option pour sécuriser l'ouverture de l'appli, Google Drive fait l'impasse sur cette fonction. Quiconque a accès au smartphone peut donc lire et copier vos documents enregistrés sur le cloud. Pour y remédier, récupérez l'appli gratuite ***Serrure (AppLock)*** dans le ***Play Store***. Définissez un schéma de déverrouillage en traçant un dessin à l'écran, puis confirmez-le. Activez l'onglet ***Vie privée***, descendez jusqu'à la ligne ***Drive***. Touchez le ***cadenas*** situé en face du nom de l'appli et accordez les autorisations nécessaires au fonctionnement d'AppLock.



Accédez à vos dossiers et à vos documents

Quittez ***AppLock*** et appuyez sur l'icône de ***Google Drive***. Un écran d'authentification apparaît. Tracez le schéma de déverrouillage défini un peu plus tôt pour forcer l'accès à l'appli et retrouver vos fichiers. Ouvrez ensuite les paramètres de ***Drive***, et assurez-vous que l'option ***Chiffrement*** est bien activée.

3

Dissociez le compte Google du mobile

Vous vous êtes fait voler votre smartphone ? Pour protéger l'accès à vos données confiées à Google Drive, connectez-vous à votre compte Google à partir d'un ordinateur. Cliquez sur l'icône ***Applications Google*** en haut à droite, puis sur ***Plus***, ***Mon compte***. Dans ***Connexion et sécurité***, choisissez ***Activité sur les appareils et notifications***. Sous ***Appareils utilisés récemment***, optez pour ***Examiner les appareils***. Sélectionner le nom du téléphone en cause, activez ***Vous avez perdu cet appareil*** et déconnectez-le de votre compte.

4

5

Rendez l'authentification en deux étapes opérationnelle

Il n'est pas nécessaire d'avoir accès à l'un de vos appareils pour s'immiscer dans votre cloud. Cette opération peut être effectuée depuis n'importe quel ordi ou mobile pour peu que les identifiants de votre compte soient connus. Pour éviter cela, rendez-vous sur le site ***bit.do/dfCXu***, faites-vous reconnaître et suivez la procédure de double validation. Une fois celle-ci terminée, un code de vérification sera envoyé par SMS sur votre smartphone à chaque tentative d'accès depuis un nouvel appareil. ■

HUBIC

1

Sécurisez l'accès à l'application mobile Hubic

Ce (généreux) service de cloud français propose 25 Go de stockage gratuit. Mieux vaut protéger ce volume de données. Installez l'appli ***HubiC*** sur votre mobile, puis touchez ... en bas de l'écran, ***Paramètres***, ***Paramètres et configuration*** et ***Verrouillage***. Définissez et confirmez un code à quatre chiffres. ■

Créez votre cloud personnel pour plus de confidentialité

Si vous souhaitez accéder à vos fichiers de n'importe quel endroit sans pour autant confier ces données privées à des services "étrangers", mettez en place votre propre service cloud ! Une opération plus simple qu'il n'y paraît, puisqu'elle ne demande qu'un disque dur réseau (NAS) et un peu de temps pour le configurer.

1. Reliez le disque dur réseau à la box

Tout d'abord, il vous faut un disque dur réseau (ou NAS) que vous raccorderez à une prise Ethernet de votre box Internet. Choisissez un modèle doté d'un logiciel de gestion évolué comme ceux de Synology ou Qnap.

2. Autorisez le NAS à communiquer via la box

Une fois le disque réseau configuré, utilisez la box comme intermédiaire. Le logiciel de Synology intègre un outil très pratique (EZ-Internet), qui se charge d'effectuer tous les réglages à votre place.

5. Créez le dossier pour les données partagées

Toujours depuis l'interface Web, accédez au gestionnaire de fichiers du NAS. Enregistrez vos données dans un dossier spécifique. Allez ensuite dans l'appli de synchronisation et activez le partage de cet emplacement.

6. Utilisez une appli de synchronisation

Installez l'appli mobile sur votre téléphone (DS Cloud de Synology ou Qfile de QNAP). Indiquez l'adresse ou le QuickConnect ID du NAS, les identifiants du compte utilisateur, puis sélectionnez le dossier de partage.

DIFFICULTÉ
Élevée
TEMPS
45 min

DR

Connecté à votre box Internet, le disque dur réseau remplace les serveurs de Dropbox ou Google Drive.

3. Générez un identifiant de connexion rapide

Pour accéder à votre cloud, vous devrez fournir l'URL du serveur et indiquer vos identifiants. Synology peut créer un QuickConnect ID, c'est-à-dire un raccourci (MonCloudPerso, par exemple) facile à mémoriser.

4. Installez l'appli cloud sur votre NAS

Comme Dropbox ou OneDrive, votre stockage en ligne doit assurer la synchronisation des fichiers entre vos appareils. Cette tâche incombe à une petite appli : Cloud Station chez Synology, MyQNAPcloud chez Qnap.

7. Liez les autres appareils à votre cloud

Faites de même sur votre tablette et vos ordinateurs (il existe une version Mac et Windows de Synology Cloud Station). Les éléments ajoutés au dossier partagé depuis un appareil seront dorénavant dupliqués sur les autres.

8. Communiquez votre lien de partage

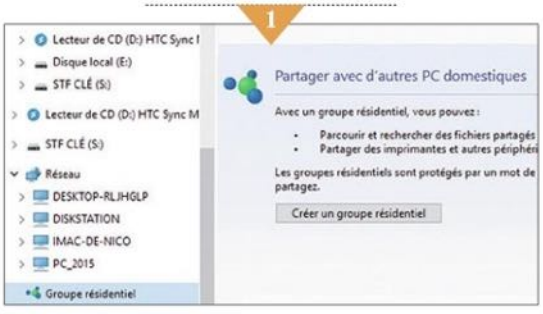
Comme Dropbox ou OneDrive, les applis cloud des NAS offrent une fonction de partage de documents. Cloud Station de Synology génère ainsi un lien qu'il suffit d'envoyer par courriel ou SMS à vos contacts.

Mettez de l'ordre dans le

Grâce aux groupements résidentiels de Windows, vous pouvez partager l'imprimante branchée sur votre PC ou le contenu de votre bibliothèque musicale en toute sécurité.

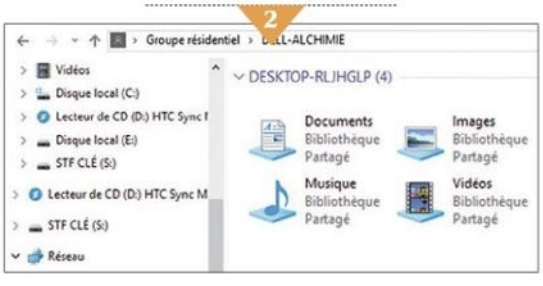
Créez le groupe résidentiel

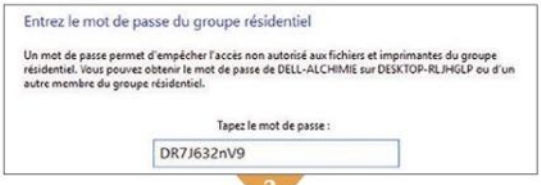
Pour lancer le partage, ouvrez l'***Explorateur de fichiers*** en appuyant sur les touches ***Windows*** + ***E*** du clavier. Dans le volet de navigation, sélectionnez ***Groupe résidentiel***, ***Créer un groupe résidentiel***, ***Suivant***. Décidez des ressources qui seront accessibles aux autres membres de la famille en déroulant les différents menus. Si l'icône du groupe résidentiel n'apparaît pas, tapez son nom dans le champ de recherche de Windows. Activez son intitulé dans la liste des résultats, puis les commandes ***Modifier l'emplacement du réseau***, ***Oui*** et, enfin, ***Fermer***.



Désignez les emplacements partagés

Si l'imprimante familiale est connectée à votre ordi, déroulez le menu ***Imprimantes et périphériques*** et choisissez l'option ***Partagé***. Rendez-vous ensuite sur le bouton ***Suivant***, au bas de la fenêtre de l'assistant de configuration du groupe résidentiel. Un mot de passe est alors généré. Notez-le soigneusement ou optez pour ***Imprimer le mot de passe et les instructions***. Validez (***Terminer***) afin de finaliser la création du groupe. Dans l'***Explorateur de fichiers***, pointez sur ***Groupe résidentiel***, puis sur votre nom pour afficher les éléments partagés.



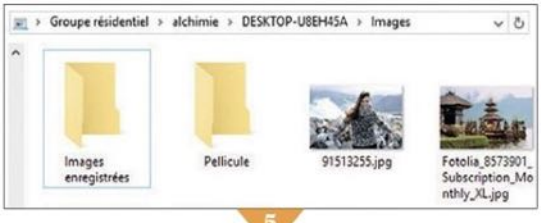


Intégrez un nouveau PC dans la liste

Accédez à un ordinateur relié au réseau familial. Ouvrez l'***Explorateur de fichiers*** de Windows. Choisissez ***Groupe résidentiel*** dans le volet de navigation, puis ***Rejoindre*** et ***Suivant***. Indiquez les contenus du PC qui seront accessibles aux autres membres du groupe et validez. Saisissez alors le mot de passe obtenu un peu plus tôt et enregistrez ces réglages (***Suivant***, ***Terminer***). La nouvelle machine a rejoint le groupe résidentiel.

Évitez les déconnexions

L'Explorateur de fichiers de ce second PC affiche désormais deux icônes de partage dans la section ***Groupe résidentiel***. L'une donne accès aux ressources du PC maître (le vôtre), l'autre aux dossiers partagés par cet ordinateur. Pour que les contenus mutualisés soient accessibles, les machines du groupe résidentiel doivent rester allumées et ne pas basculer en mode veille, sans quoi les tentatives de connexion se solderont par un message d'erreur.

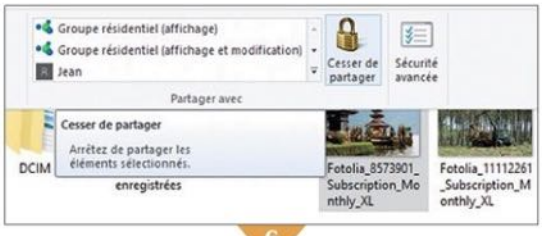


Accédez aux bibliothèques partagées

Ouvrez le dossier partagé dans lequel le fichier a été déposé. Faites glisser celui-ci sur le Bureau afin de le copier sur le PC maître, ou double-cliquez sur son icône. Si toutes les bibliothèques des deux PC ont été partagées, toutes les données sont accessibles.

DIFFICULTÉ
Modérée
TEMPS
40 min

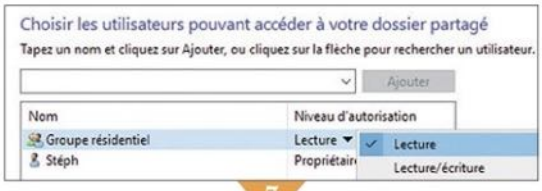
partage de vos fichiers



6

Maîtrisez le partage au fichier près

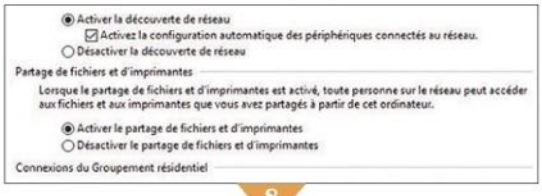
Si vous ne souhaitez plus partager un élément enregistré dans l'une des bibliothèques du groupe résidentiel, ouvrez l'***Explorateur de fichiers***. Sélectionnez le document ou le dossier, puis l'onglet ***Partage*** dans le menu supérieur. Activez l'icône ***cadenas*** pour cesser le partage. L'élément désigné ne sera plus visible sur les autres PC.



7

Modifiez les autorisations d'accès

Par défaut, tous les membres du groupe résidentiel sont autorisés à manipuler les docs placés dans les bibliothèques partagées. Pour intervenir sur les privilèges, pointez sur le document en question dans l'***Explorateur de fichiers***. Ouvrez l'onglet ***Partage***. Cliquez sur la ***flèche*** pointant vers le bas à droite de la fenêtre ***Partager avec***, puis sur ***Des personnes spécifiques***, ***Groupe résidentiel***. Réglez le niveau d'autorisation sur ***Lecture*** afin d'interdire les modifications de ce contenu.



8

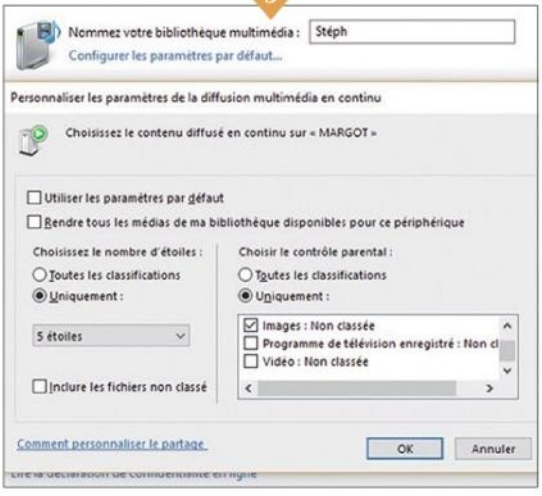
Changez le type de partage

Effectuez une recherche sur le terme ***Partage***. Allez sur ***Gérer les paramètres de partage avancés***. Pour éviter que l'on ne tente de se connecter à votre PC, cochez l'option ***Désactiver la découverte du réseau***. Si vous voulez suspendre le partage de votre imprimante, optez pour ***Désactivez le partage de fichiers et d'imprimantes***.

Gérer les contenus multimédias

Déroulez le menu ***Tous les réseaux***. Sélectionnez le lien ***Choisir les options de diffusion de contenu multimédia***. La liste des appareils (ordinateurs, box TV, etc.) reliés au réseau local s'affiche. Pour interdire à un matériel de s'y connecter, passez le curseur sur son nom et cliquez sur ***Supprimer***. Si vous avez besoin d'activer le contrôle parental afin d'éviter que vos enfants n'aient accès à tous vos films, déplacez le pointeur sur le nom du PC et optez pour ***Personnaliser***. Décochez la case ***Utiliser les paramètres par défaut***. Dans la section ***Choisir le contrôle parental***, validez ***Uniquement*** et décochez les éléments qui ne seront pas accessibles (en excluant les fichiers non classés par le contrôle parental, par exemple).

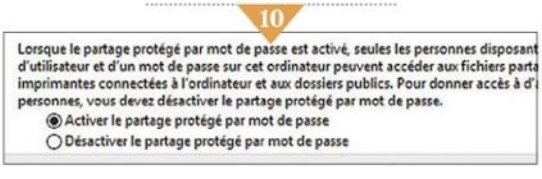
9



Limitez l'accès aux utilisateurs référencés

Vous pouvez conditionner l'accès aux contenus partagés à la saisie des identifiants de compte utilisateur des membres du groupe résidentiel. Cochez l'option ***Activer*** dans ***Partage protégé par mot de passe sur l'intégralité des PC reliés au réseau***. Sélectionnez ***Enregistrer les modifications***. Pour désactiver le réseau partagé, activez ***Groupe résidentiel*** dans l'***Explorateur de fichiers***, puis, sous l'onglet ***Groupement résidentiel***, pointez ***Modifier les paramètres du groupe résidentiel***, ***Quitter le groupe résidentiel***. ■

10

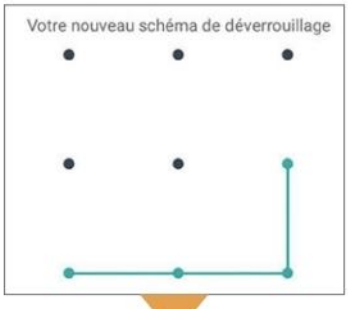


Blindez l'accès à vos PC, smartphones et tablettes

La sécurité de vos données repose pour une bonne part sur les dispositifs de verrouillage déployés sur vos différents appareils. Code PIN, mot de passe, capteur d'empreintes, reconnaissance faciale, à vous d'adopter la méthode qui vous convient !

1. Définissez un code PIN pour déverrouiller votre téléphone

Allumez votre mobile. Si l'écran d'accueil s'affiche aussitôt, aucune protection n'est en place. C'est comme si vous laissiez la porte ouverte en priant pour qu'aucun voleur n'ait l'idée de franchir le seuil de la maison ! Rendez-vous dans les ***Paramètres*** d'Android, appuyez sur ***Sécurité*** et ***Verrouillage écran*** (le nom de la commande peut changer en fonction des appareils). Vous avez le choix entre plusieurs types de protection. Effleurez ***Code PIN***. Entrez un code à quatre chiffres, que vous confirmerez. Au prochain démarrage ou en sortie de veille, cette combinaison sera exigée. Touchez la commande ***Verrouiller le téléphone après*** et optez pour un délai court.

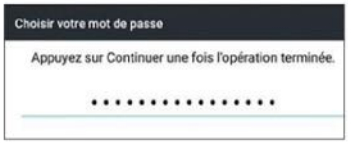


2. Utilisez un schéma

Vous pouvez remplacer le code PIN par un dispositif plus original et qui offre une meilleure sécurité : le tracé d'un motif sur l'écran tactile du mobile. Activez l'option ***Schéma*** sur la page ***Sécurité***, puis tracez un dessin connectant au moins quatre des neuf points. Pressez ***Continuer*** et confirmez le schéma. Décochez ***Faire apparaître le schéma*** afin d'éviter qu'on puisse le voir lorsque vous déverrouillez l'appareil dans un endroit public.

3. Optez pour un code d'accès impossible à deviner

Les paramètres de sécurité autorisent l'ajout d'un mot de passe. Si vous choisissez cette option, ne vous contentez pas de quelques chiffres. Évitez les dates de naissance et associez chiffres, mots et caractères spéciaux afin de former une combinaison sûre comme une banque suisse.



4. Laissez votre smartphone reconnaître votre visage

Certains modèles de téléphone, comme les Nexus et Pixel de Google intègrent une option de sécurité basée sur la reconnaissance des visages, nommée Face Unlock. Le principe est simple : vous regardez le mobile bien en face et si votre visage est reconnu, l'appareil est aussitôt déverrouillé. En cas de difficultés, liées par exemple à la pousse récente d'une barbe, il est possible de se rabattre sur le code PIN pour accéder au terminal.

5. Activez la double sécurité Face Unlock

Touchez ***Face Unlock***. Dans un endroit éclairé, placez votre visage au centre de l'ovale et attendez la confirmation de l'analyse de votre trombine. Si vous portez parfois des lunettes, enregistrez-vous également avec cet accessoire afin d'optimiser la reconnaissance.

DIFFICULTÉ
Aucune
TEMPS
30 min

6. Déverrouillez l'appareil quand vous le portez

Les terminaux Android fonctionnant sous Lollipop (5.0) ou version supérieure bénéficient de Smart Unlock, un système de déverrouillage qui tient compte de l'endroit où vous vous trouvez. Dans ***Sécurité***, rendez-vous sur ***Smart Lock***. Si l'option est grisée, définissez un code PIN. Touchez ***Détection de l'appareil lorsqu'il est porté***.

7. Suspendez la sécurité chez vous ou au bureau

Effleurez le curseur pour maintenir l'écran déverrouillé lorsque vous avez votre mobile en main ou quand vous le transportez dans un sac. Mais vous devrez faire cette opération une première fois pour que cette option s'active. Lorsque vous poserez le téléphone, il se verrouillera de nouveau. Revenez en arrière, touchez ***Lieux vérifiés***, ***Ajouter un lieu vérifié***. Appuyez sur ***Sélectionner cette position***, ***OK***. Votre smartphone sera automatiquement déverrouillé lorsque vous serrez près de la position que vous venez d'enregistrer.

8. Exigez une protection sous Windows

Il est temps de s'intéresser à la sécurité de votre PC. Ouvrez le menu ***Démarrer*** de Windows et activez ***Paramètres***, ***Comptes***, ***Options de connexion***. Déroulez le menu sous ***Exiger une connexion*** et optez pour ***Lorsque le PC sort du mode veille***. Choisissez ensuite la protection par code PIN ou par mot de passe. Pointez sur ***Écran de verrouillage***, ***Paramètres de l'écran de veille*** et définissez un délai de mise en veille assez court.

9. Composez un mot de passe image

Dans les paramètres d'options de connexion, sélectionnez maintenant ***Ajouter***, ***Mot de passe image***. Dans la colonne gauche, optez pour ***Choisir une image*** et désignez une photo. Validez avec ***Ouvrir***, ***Utiliser cette image***. Vous êtes ensuite invité à effectuer trois mouvements sur le cliché (ligne droite, cercles, etc.) au moyen de la souris. Confirmez ces tracés et allez sur ***Terminer***. L'image s'affichera à l'écran au démarrage de Windows ou en sortie de veille. Il vous suffira alors de reproduire les tracés de référence pour déverrouiller l'ordinateur.

10. Préservez votre vie privée

Lorsque l'écran est verrouillé, il peut néanmoins continuer d'afficher des infos personnelles. Afin d'éviter d'exposer ces données, telles que votre adresse mail, accédez aux ***Paramètres*** de comptes. Rendez-vous dans ***Options de connexion***, ***Confidentialité***, ***Afficher les détails du compte***, ***Écran de verrouillage***. Désactivez le curseur ***Personnaliser l'écran de verrouillage à partir de Windows***. Votre vie privée sera ainsi préservée en votre absence.

11. Optimisez la sécurité de l'iPhone

Les iPhone sont généralement protégés par un code à quatre chiffres (six chiffres depuis iOS 9). Si le vôtre ne l'est pas, placez-vous sur l'icône ***Réglages***, puis sur ***Code***. Entrez une combinaison et touchez ***Exiger le code***. Optez pour un délai court et pressez ***Retour***. ■

Ne tombez pas dans le

Le phishing, ou hameçonnage, a pour but de vous dérober vos données personnelles en douceur, au moyen d'un simple courriel ou d'un faux site Web. Ne vous laissez pas attraper si facilement.

Ayez le bon sens chevillé au corps !

Pour éviter de se faire voler ses données personnelles sur le Net par le biais de sites Web contrefaits, il suffit souvent d'un peu d'attention. Avant de cliquer sur un lien qui semble provenir d'un portail gouvernemental ou bancaire, demandez-vous pourquoi vous recevez un tel courriel. Scrutez son intitulé et l'adresse de l'expéditeur. Le message que nous avons reçu du ministère des Finances était ainsi envoyé via free.fr ! De manière générale, ne suivez pas les liens contenus dans les mails émanant des impôts, des fournisseurs d'accès à Internet ou des banques.

1

Activez l'option antiphishing de l'antivirus

La plupart des antivirus bénéficient de protections antihameçonnages, capables d'identifier et de bloquer les messages douteux. Attention, cette option n'est pas toujours activée par défaut. Rendez-vous dans les paramètres de votre antivirus. Repérez la section intitulée ***Messagerie*** ou ***Courrier indésirable*** et mettez en place la reconnaissance du phishing. Si votre logiciel de sécurité ne propose pas ce type d'outils, n'hésitez pas à en changer. Adoptez, par exemple, la version gratuite d'Avast, disponible à l'adresse ***bit.do/dbuEt***.

2

3

Contactez votre banque en cas de doute

Si vous doutez de l'authenticité du message reçu de votre banque ou d'un organisme officiel, prenez le temps d'appeler un conseiller. Sinon, connectez-vous à votre compte comme vous le faites habituellement. Si un changement de mot de passe ou l'ajout de données personnelles sont vraiment nécessaires, n'effectuez l'opération qu'à partir du site officiel. Ceux d'hameçonnage sont de plus en plus réalistes, comme le démontre la capture reproduite ci-dessus.

4

Informez-vous auprès de la DGCCRF

La Direction générale de la concurrence, de la consommation et de la répression des fraudes publie un site Web spécifique au phishing (***bit.do/dbuCF***). Vous y trouverez des infos sur les différentes formes de ces menaces et comment s'en protéger. Vous pourrez aussi y dénoncer une tentative d'hameçonnage dont vous avez été victime.

5

Tenez-vous au courant des menaces

Le service Stop Phishing de Verifrom s'appuie sur la communauté des internautes pour établir une base de données actualisée des menaces d'hameçonnage. L'extension Stop Phishing pour Firefox (***bit.do/dbuHv***) ou pour Google Chrome (***bit.do/dbuHB***) sert à signaler des tentatives de phishing et à être prévenu en retour.

DIFFICULTÉ
Aucune
TEMPS
30 min

piège du phishing

6

Surfez avec Adblock Browser

Les professionnels du phishing utilisent également des sites Web infectés transformés en pièges à internautes. Pour éviter ces pages sur votre mobile, prenez l'habitude de recourir à un navigateur sécurisé comme Adblock Browser (***bit.do/dbuMz***). Accédez aux ***Paramètres*** de l'appli, touchez ***Blocage de publicités***, ***Davantage d'options de blocage*** et cochez toutes les options.

7

Dotez votre mobile d'un filtre antiphishing

Certains antivirus pour mobiles et tablettes proposent des protections spécifiques contre le phishing. À l'image de Kaspersky Antivirus & Security, disponible sur le Play Store. La version d'essai offre la possibilité d'évaluer gratuitement l'appli pendant trente jours. Vous êtes protégé efficacement contre les tentatives d'hameçonnage grâce au blocage des liens et des sites dangereux. L'outil s'appuie sur des listes de filtres. Kaspersky bloque par ailleurs les SMS non désirés et ceux à caractère publicitaire.

8

Évitez les spams grâce à Outlook.com

Le webmail Outlook.com offre un paramétrage spécifique des filtres d'indésirables. Si vous souhaitez qu'il fasse le ménage dans votre courrier plus en amont, cliquez sur la roue crantée ***Paramètres*** en haut à droite, puis sur ***Options***. Activez ***Filtres et rapports*** dans la section ***Courrier indésirable***. Cochez ***Exclusif*** dans ***Filtres et rapports*** puis ***Bloquer les pièces jointes*** dans ***Bloquer le contenu des expéditeurs inconnus***.

Ajustez les paramètres de votre navigateur

Sur PC comme sur mobile, les navigateurs disposent de paramètres antihameçonnage intégrés, pas toujours activés ni très accessibles. Pour vérifier que Firefox est correctement protégé, déroulez le menu principal, puis placez-vous sur ***Options***, ***Sécurité***. Cochez alors l'option ***Bloquer les contenus dangereux ou trompeurs***. Profitez-en pour vérifier que le navigateur (et ses outils de sécurité par la même occasion) est mis à jour régulièrement en pointant sur ***Avancé***, ***Mises à jour***, ***Installer automatiquement les mises à jour***. Avec Chrome, déroulez le menu ***Personnaliser*** et cliquez sur ***Paramètres***, ***Afficher les paramètres avancés***. Dans la section ***Confidentialité***, cochez ***Assurer la protection et celle de votre appareil contre les sites dangereux***. ■

9

MESSAGERIE ET PARAMÈTRES AVANCÉS

OPTIMISEZ LES FONCTIONNALITÉS DU FILTRAGE DANS THUNDERBIRD

Développée par la fondation Mozilla, à l'origine du navigateur Firefox, la messagerie Thunderbird, dispose de paramètres avancés en matière de filtrage. Pour y accéder, déroulez d'abord le menu ***Outils***. Cliquez ensuite sur les intitulés ***Paramètres des comptes*** et ***Paramètres des indésirables***. Sélectionnez l'option ***Se fier aux en-têtes des indésirables***, puis choisissez le module ***SpamAssassin*** dans la liste qui s'affiche à l'écran. Enfin, cochez tour à tour les options ***Déplacer*** et ***Supprimer automatiquement les courriels***.

VOTRE SÉCURITÉ EST LEUR PRIORITÉ !

Ces accessoires malins vous aident à protéger vos mots de passe et vos données, mais aussi à empêcher que l'on ne dérobe votre PC portable.

CÂBLES DE SÉCURITÉ KENSINGTON

Le garde du corps des portables

Rien de tel qu'un solide antivol pour éviter que l'on n'embarque votre ordinateur portable lorsque vous le laissez sur un bureau. Ce modèle à combinaison signé Kensington, un spécialiste à qui l'on doit l'encoche antivol présente sur presque tous les PC, utilise un câble torsadé en acier renforcé de carbone et un dispositif de fixation anti-arrachement breveté. Efficace.

Kensington.com/fr/fr/home – 56 €

MOOLTIPASS MINI

Un coffre-fort pour vos mots de passe

Ce petit boîtier garde vos codes d'accès à l'abri derrière un chiffrement en mode AES 256 bits. Pour les déverrouiller, il faut insérer une carte à puce spécifique, fournie avec le Mooltipass Mini, et saisir un code PIN à quatre chiffres. Une fois connecté à un PC, une tablette ou un smartphone (un câble micro-USB vers USB est livré), le boîtier déverrouille automatiquement l'identification sur des sites et des services en ligne.

Themooltipass.com – 75 €

RAZER STARGAZER

La plus physionomiste des webcams

Voici le premier modèle de caméra équipé de la technologie de reconnaissance Intel RealSense. Capable d'analyser les contours et le relief du visage, la Stargazer est compatible avec l'option de reconnaissance faciale Windows Hello de Windows 10. Plus besoin de mot de passe, un simple regard suffit pour accéder au PC.

Razerzone.com/fr-fr – 170 €

TICATAG TIFIZ

Suivez vos biens les plus précieux à la trace

Là où les porte-clés antivol Bluetooth ne sont efficaces que dans un rayon restreint, cette petite balise GPS (8 x 7 cm pour 45 g) s'affranchit des distances. Que vous soyez tout prêt ou à des centaines de kilomètres, vous pouvez la localiser avec précision sur l'écran de votre smartphone grâce aux signaux émis toutes les dix minutes environ sur le réseau Sigifox.

Ticatag.com – 99 € (hors abonnement) + 3,60 €/mois

3M GOLD

Un bouclier contre les regards indiscrets

Une fois ce filtre appliqué sur l'écran du portable, il devient impossible à quiconque ne se trouvant pas parfaitement dans l'axe de vision, de déchiffrer ce qui s'y affiche. Un moyen infaillible de préserver la confidentialité de votre travail dans le train ou un lieu public. Si les curieux n'ont droit qu'à un écran noir, vous profitez, vous, d'une image parfaitement nette et lumineuse !

Solutions.3mfrance.fr – À partir de 60 €

ISTORAGE DATASHUR PERSONAL 2

Cette clé est un verrou !

Cet accessoire n'est pas une clé USB comme les autres. Dotée de performances correctes (elle est compatible USB 3.0) et d'une capacité de stockage confortable (jusqu'à 64 Go), la Datashur personal 2 intègre un algorithme de chiffrement des données et un clavier. Le contenu n'est visible qu'après avoir saisi un mot de passe composé de 7 à 15 chiffres.

Istorage-uk.com – 100 € (64 Go)

UPEK EIKON II USB

Déverrouillez votre PC du bout des doigts

Associé à Windows 10, ce lecteur d'empreintes digitales ne nécessite ni pilote ni logiciel spécifique puisqu'il est compatible avec les technologies d'identification biométriques de Windows Hello. Enregistrez une ou plusieurs empreintes et le tour est joué ! Il s'accompagne également d'une suite logicielle pour sécuriser l'accès à vos programmes et aux sites Internet.

Amazon.fr – 60 €

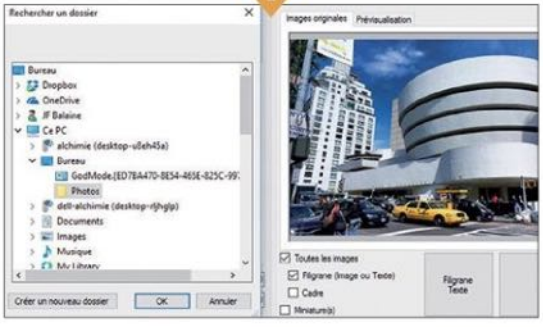
DIFFICULTÉ
Aucune
TEMPS
20 min

Tatouez vos photos pour ne pas qu'on vous les vole

Lorsque vous publiez des clichés sur un réseau social ou un blog, ceux-ci sont téléchargeables par tout un chacun. Utilisez un logiciel de tatouage (ou watermark) pour signaler que vous en êtes l'auteur ou pour interdire leur reproduction.

Chargez votre image dans Watermark Magick

Ouvrez votre navigateur Internet, saisissez l'adresse ***bit.do/dfEeF*** et enfoncez la touche ***Entrée*** du clavier pour télécharger Watermark Magick. Installez l'appli, déroulez le volet ***Démarrer*** de Windows et cliquez sur l'icône ***Watermark*** dans la section ***Récemment ajoutées*** de la liste des programmes. Activez le bouton surmonté de ***trois points*** qui figure à droite du champ ***Source*** et désignez la ou les prises de vue à protéger.

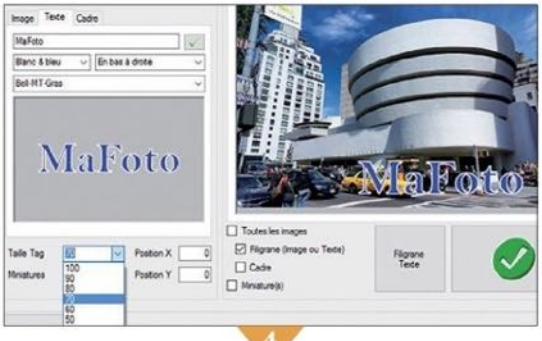


Sélectionnez un logo ou un texte

De la même façon, choisissez l'emplacement où seront enregistrées les versions modifiées des photos. Placez-vous ensuite sur le bouton ... à droite de l'onglet ***Image***, de façon à sélectionner le logo de votre société ou l'une des images proposées par défaut. Enfin, déroulez la liste ***En bas à droite*** pour définir l'emplacement du filigrane.

Ajustez la mise en forme du filigrane

Si vous préférez utiliser un nom ou une formule en guise de marquage antivol, choisissez l'onglet ***Texte*** et saisissez l'intitulé dans le premier champ. Faites un clic sur le bouton surmonté d'une coche grisée pour valider. Sélectionnez ensuite la police de caractères et la mise en forme (transparent, blanc & bleu, blanc et noir) en vous servant des listes déroulantes au bas de l'onglet ***Texte***.



Affinez la position et la taille du tatouage

Pour appliquer le marquage à l'ensemble des photos du dossier d'origine, cochez l'option ***Toutes les images*** sous la fenêtre de prévisualisation. Cette dernière offre un aperçu du filigrane. Vous le trouvez un peu trop petit ou, au contraire, trop présent ? Déployez le menu ***Taille Tag*** et testez différentes configurations. Une fois satisfait du résultat, cliquez sur l'icône de validation en bas à droite de la fenêtre pour lancer l'opération de tatouage. ■

DIFFICULTÉ
Modérée
TEMPS
20 min

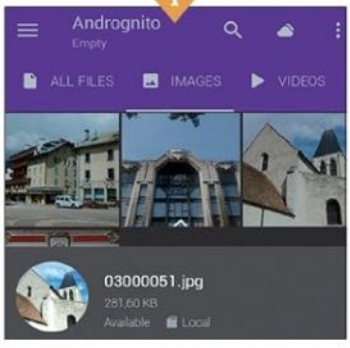
Protégez des applis et des documents sensibles

Il vous arrive sans doute de prêter votre smartphone à un ami ou à un parent. Pour avoir l'esprit tranquille et être certain qu'ils ne tomberont pas sur des informations confidentielles, faites disparaître les fichiers les plus sensibles ou interdisez-en l'accès.

Verrouillez des images

Installez l'appli ***Andrognito*** (***bit.do/dbviA***) sur votre mobile Android. Activez ensuite ***Sign me Up*** et créez un compte gratuit. Touchez ***Continue*** puis définissez un code PIN afin de protéger l'accès à l'appli. Pressez l'onglet ***Images***, le symbole **+** puis ***Images***, sélectionnez une photo et validez. Effleurez l'icône ***cadenas***.

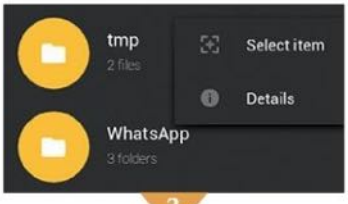
1



Sécurisez vos vidéos

Les images sont désormais à l'abri dans le coffre-fort numérique d'Andrognito. Pour restaurer l'emplacement d'origine d'un cliché, appuyez sur ***Images***, puis sur le fichier de la photo et sur ***Decrypt & Export***. De la même façon, vous pouvez escamoter les films enregistrés sur le téléphone depuis l'onglet ***Videos***.

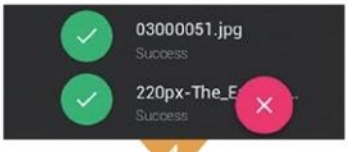
2



3

Profitez de l'explorateur de fichiers

Lorsque Andrognito verrouille un élément, il le fait disparaître de la vue des utilisateurs. Il est possible d'en faire de même avec n'importe quel fichier (des PDF par exemple). Activez pour cela l'onglet ***Documents*** et appuyez sur **+**, ***All files***. Un explorateur de fichiers s'affiche. Si vous disposez d'une carte SD, effleurez son icône dans le menu supérieur afin d'accéder à son contenu.



4

Interdisez l'accès aux documents

Pointez vers l'élément à dissimuler. Il peut s'agir d'un fichier ou d'un dossier entier. Dans ce dernier cas, sélectionnez l'emplacement voulu, touchez la ***coche*** en haut de l'écran puis le ***cadenas*** pour activer la protection. Le dossier devient invisible en dehors de l'appli. Pour vous en assurer, lancez un gestionnaire de fichiers ou branchez le téléphone à un PC et ouvrez l'***Explorateur*** de Windows.

Empêchez les appels

Pour aller plus loin et limiter le champ d'action de la personne à qui vous prêtez le smartphone, installez l'appli ***Serrure(Applock)***. Après avoir défini un mot de passe maître, touchez l'icône en forme de ***cadenas*** située en regard des intitulés ***Appel entrant***, ***Téléphone***, mais aussi ***Play Store***, ***Installer/Désinstaller*** et ***Paramètres***. Vous êtes ainsi certain de récupérer votre mobile intact ! ■

5

CHIFFREMENT DE DONNÉES

CHIFFREZ LES DOSSIERS SENSIBLES AVEC ES EXPLORATEUR

Ce gestionnaire de fichiers pour Android offre pléthore de fonctions très pratiques, parmi lesquelles un outil de chiffrement des données. Lancez l'appli, puis effleurez l'icône ***X*** dans le menu supérieur afin d'accéder à la page de démarrage. Déroulez ensuite le menu principal, appuyez sur ***0*** pour parvenir aux dossiers stockés dans la mémoire interne ou sur ***ext_sd*** pour visualiser ceux sauvegardés sur la carte SD. Effectuez un appui prolongé sur le dossier ou le fichier à protéger. Touchez ensuite les ***trois points*** en haut de l'écran de façon à afficher les options. Enfin, pressez ***Chiffrer***, définissez un mot de passe et validez avec ***OK***.

CONTRÔLER

Objets connectés et big data menacent vos données

© zapp2photo

SOMMAIRE

Selon une étude du cabinet de conseil américain Gartner, 26 milliards d'objets dans le monde seront reliés à Internet en 2020. Des appareils pour tous les usages : cabines d'ascenseurs, chaudières industrielles, caméras de surveillance, réfrigérateurs, capteurs sportifs, ampoules, montres, vêtements, cafetières, semelles de chaussures... Tous les domaines sont concernés, en particulier ceux de la vie quotidienne. La plupart de ces objets, pourtant, ne sont pas – ou mal – prémunis contre les cyberattaques. En cause, la négligence des utilisateurs, mais aussi l'insuffisante prise en compte des problématiques de sécurité par les fabricants, plus prompts à peaufiner les fonctionnalités de leurs produits qu'à empêcher les pirates de fouiner dans les données de leurs clients.

Hackers à l'affût. Les attaques résultent en général de l'introduction d'un cheval de Troie dans un appareil insuffisamment protégé. Une menace supplémentaire pèse sur les informations collectées, qui terminent le plus souvent sur les data centers du constructeur, de façon à ce que l'internaute puisse y accéder depuis son smartphone ou son ordinateur. Ces serveurs apparaissent comme une cible de choix. En cas d'agression, tout devient possible, du simple affichage de messages sur les écrans au vol de documents confidentiels, en passant par la reprogrammation d'objets ou l'arrêt total du réseau. Et lorsqu'il s'agit de la gestion à distance d'un stimulateur cardiaque, de la prise de contrôle d'un véhicule ou encore de la compromission d'un capteur de température dans une centrale nucléaire, on ne rit plus du tout ! D'où la mise en garde, en octobre dernier, du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CEET-FR) : *"Les logiciels embarqués dans ces objets peuvent contenir des vulnérabilités ou présenter divers défauts de configuration*

Bardées d'applications numériques, les voitures collectent quantité d'informations personnelles.

permettant d'en prendre le contrôle. Si les objets sont branchés directement sur Internet, ils représentent des proies faciles pour les hackers, qui s'en serviront comme vecteurs d'attaque."

Choc mortel. Si protéger son ordinateur, sa box Internet ou son mobile est devenu un réflexe, nous portons souvent une moindre attention aux ustensiles de la vie courante. Pourtant, les caméras IP auxquelles nous confions la surveillance de nos logements s'avèrent hautement fragiles. En en prenant le contrôle, un assaillant peut désactiver les dispositifs d'alerte et vous espionner en toute tranquillité. D'autres exemples récents pointent les failles de sécurité des objets connectés. Ainsi, la FDA (Food and Drug Administration), l'autorité américaine de régulation du médicament, a mis en garde sur les risques de cyberattaque de certains pacemakers. En trafiquant le module de transmission de ces dispositifs, un chercheur a pu déclencher, de loin, une décharge électrique de 830 volts ! Le cas n'a rien d'isolé. Des actes récents ont également mis en lumière les points faibles des voitures autonomes et des systèmes électroniques embarqués *(lire encadré ci-contre)*. Plus étonnant, une équipe de scientifiques de l'université de la Ruhr, en Allemagne, a profité d'une série d'erreurs dans les langages PostScript et PJL pour s'en prendre à des imprimantes. Une vulnérabilité qui existerait depuis plus d'une trentaine d'années et qui concernerait un très grand nombre de spécimens.

En 2020, un quart des cyberattaques sera lié à l'Internet des objets

CÔTÉ AUTO

Votre voiture, la prochaine cible des pirates

1 De plus en plus d'électronique à bord
À moins d'acheter une Dacia, parmi les dernières marques à n'embarquer qu'un minimum d'électronique, la quasi-totalité des automobiles sont sujettes à des problèmes de sécurité. Certaines ne réclament pas de grandes connaissances techniques et sont à la portée de malfaiteurs bien équipés.

2 L'ouverture à distance
Voilà un an, une faille de sécurité est dévoilée par l'Adac, un club automobile allemand. Elle concerne le signal radio d'ouverture des portes et de démarrage d'une vingtaine de modèles, chez différents constructeurs.

3 Autos connectées : des cibles prioritaires
Le groupe Fiat-Chrysler, en 2016, a dû rappeler près de 1,4 million de véhicules après que deux chercheurs ont réussi à prendre le contrôle à distance d'une Jeep Cherokee puis la faire ralentir.

4 La voiture autonome ? Encore plus vulnérable !
Des ingénieurs sont aussi parvenus à hacker une Tesla et à piloter le véhicule. Ils se sont introduits au cœur du dispositif de conduite autonome du très réputé modèle électrique fabriqué dans la Silicon Valley.

5 Des bugs et des failles de sécurité
Le cerveau numérique des voitures autonomes comporte des millions de lignes de code : l'assurance de dysfonctionnements dont pourraient profiter les voleurs.

SANTÉ CONNECTÉE

Vos données médicales sont-elles en sécurité ?

Les objets de santé connectés recueillent une foule d'infos très intimes. Mais où sont-elles envoyées ? Qui a le droit de les consulter ? Sont-elles suffisamment sécurisées ?

Aucune donnée ayant trait à votre santé n'est anodine. Si le nombre de pas que vous effectuez chaque jour présente en apparence assez peu de valeur, il renseigne néanmoins sur votre forme physique et sur votre hygiène de vie. Il en va de même du rythme cardiaque relevé par un objet aussi banal que votre traqueur d'activité.

Consommateurs protégés. Selon un baromètre Ipsos pour AG2R La Mondiale publié en octobre 2016, l'indice de confiance envers les applications de santé ne dépasse pas la note de 4,7 sur 10. Parallèlement, cette étude révèle que 72 % des sondés appellent de leurs vœux l'instauration d'un label garantissant la qualité et le sérieux des logiciels médicaux. *"Les consommateurs sont très sensibles à la question de la sécurité de leurs données et aux usages qui peuvent en être faits"*, admet Marie-Françoise de Pange, fondatrice du site Buzz-medecin.fr en 2012. Les consommateurs français sont protégés à double titre. D'abord avec la Commission nationale de l'informatique et des libertés (Cnil), qui encadre la collecte et l'utilisation des données informatisées, mais aussi grâce à la loi Évin qui interdit aux assurances de faire fluctuer leurs tarifs en fonction des ennuis de santé des patients. Ainsi, même si une mutuelle venait à découvrir incidemment que vous ne faites pas assez de sport, elle ne pourrait pas augmenter vos cotisations ni vous radier sceance tenante.

À l'heure du big data, votre médecin n'est plus tout seul à connaître votre pression artérielle...

iHEALTH

Industriels responsables. Comme l'indique Marie-Françoise de Pange, *"il est obligatoire que les informations médicales soient conservées sur des serveurs agréés"*. La liste de ces hébergeurs est disponible sur le site E-sante.gouv.fr. Les constructeurs d'objets connectés ont en outre le devoir de garantir l'inviolabilité de leurs data centers. Le fabricant iHealth (tensiomètres et glucomètres) stocke par exemple ses données chez IDS, un hébergeur bourguignon agrée HADS, la norme de certification imposée par les autorités de régulation de la santé. *"Nous devons en permanence adapter nos protocoles pour répondre aux évolutions réglementaires"*, précise Anne Boché-Hiag, directrice marketing et communication chez iHealth.

Logiciels dans le collimateur. La Haute Autorité de santé a publié un référentiel de bonnes pratiques pour les objets connectés et les applications mobiles de santé. Ce document – à retrouver sur le site Bit.do/dhnAC – contient 101 recommandations. Bien sûr, le risque zéro n'existe pas. Mais les failles ne se trouvent pas où l'on croit. *"C'est rarement l'objet de santé ou les serveurs de son constructeur qui sont en cause, mais l'application qui lui est associée"*, rappelle Marie-Françoise de Pange. Un label officiel devrait voir le jour en 2018 pour attester la fiabilité de ces nouveaux dispositifs.

On ne compte plus, aujourd'hui, les films et les séries mettant en scène le piratage des services de sûreté. Un scénario devenu réalité lorsqu'en janvier, une poignée de malfaiteurs a paralysé le système de vidéosurveillance de la ville de Washington. Une opération spectaculaire, menée au cœur de la capitale de la première puissance mondiale !

La voie de la sagesse. De plus en plus, les entreprises qui conçoivent et qui commercialisent des objets reliés à Internet doivent s'allier à des prestataires spécialisés pour assurer leur inviolabilité. C'est le cas d'iHealth, fabricant et distributeur de produits de santé à destination du grand public – tensiomètres, balances... – et des professionnels. Pour préserver la vie privée de ses clients, la firme californienne fait appel à IDS, une PME bourguignonne agréée par l'Agence française de la santé numérique. IDS héberge et protège les flux de données d'iHealth en Europe. Mais toutes les sociétés ne font pas preuve d'autant de discernement... Le cabinet Gartner estime que, d'ici à trois ans, un quart des attaques sera lié à l'IoT (Internet of Things, pour Internet des objets). Comme l'explique Christophe Moret, le vice-président cybersécurité chez Atos, *"bon nombre d'objets connectés sont lancés sur le marché trop vite, ce qui laisse moins de place à la sécurité"*. La situation s'améliore néanmoins avec la création, fin 2016, d'un premier label baptisé IoT Qualified Security. Il définit le niveau de sûreté minimal et sera décerné aux produits ayant réussi une batterie de tests. Dès cette année, les consommateurs pourront identifier les appareils répondant à leurs exigences. Un premier essai encourageant.

Les liaisons sans fil à courte distance, comme le Bluetooth ou le NFC (communication en champ proche), présentent aussi des lacunes. Certains spécialistes jugent en effet qu'il serait possible pour un hacker passant près de chez vous d'intercepter les informations échangées de cette manière. Un point à corriger au moment où le paiement sans contact – par carte bancaire ou avec un smartphone – se généralise, contraignant les acteurs du secteur bancaire à plafonner le montant des transactions par ce biais à 20 euros – à 30 euros dès cet automne. Pas question qu'un bandit du Web en profite pour vider votre compte ! ■

DIFFICULTÉ
Modérée
TEMPS
10 min

Envoyez des messages et des photos éphémères

Pour éviter que vos fichiers ne soient détournés, l'idéal est qu'ils s'autodétruisent après que vos destinataires en ont pris connaissance. Un principe auquel recourt Snapchat pour les images et que nous vous proposons d'étendre à vos mails.

Rédigez un courriel à durée déterminée...

Grâce au service gratuit Privnote (***bit.do/ddoCG***), vous disposez d'une solution ingénieuse pour envoyer des messages personnels à vos proches sur Mac, PC ou vers un smartphone. Très sobre, l'interface se réduit à un champ de saisie dans lequel vous écrivez le texte de votre mail. Vous n'avez ensuite plus qu'à cliquer sur le bouton ***Créer une note***.

1

... et partagez-le sans crainte

Un lien hypertexte est généré. Sélectionnez-le puis copiez-le vers le presse-papiers de votre ordinateur. Vous pourrez ainsi le coller ultérieurement dans une conversation sur Skype ou dans l'application SMS de votre smartphone. Dès que ce lien aura été consulté, son contenu sera détruit. Si vous préférez l'envoyer plutôt par courriel, choisissez ***Lien Email***. Le client de messagerie s'ouvre sur une fenêtre de composition de nouveau message.

2

3

Installez Instagram Direct sur Android et iOS...

Pour expédier des photos éphémères à des amis, le plus simple consiste encore à télécharger l'application ***Instagram*** sur votre smartphone. Cet outil, plébiscité par les adolescents, est disponible sur iOS et sur Android. Après avoir créé votre compte ou associé l'appli à votre Facebook, il vous suffit de recourir à la fonction intitulée ***Instagram Direct***. Pressez enfin l'icône en forme d'***avion en papier*** dans l'angle supérieur droit de l'interface.

4

... et shootez, envoyez, oubliez !

Au bas de l'écran, touchez la commande ***Nouveau message***. Sélectionnez ensuite les destinataires du cliché temporaire. L'appareil photo du smartphone est alors activé. Capturez l'image dont vous avez envie, puis effleurez la ***flèche***, dans le coin inférieur droit de l'appli. Le document est immédiatement envoyé et s'autodétruira dès qu'il aura été visualisé, sans laisser de trace.

Avec votre iPhone, enregistrez une bande-son temporaire...

En détournant une fonctionnalité de l'application ***Messages*** d'iOS 10, vous pouvez envoyer des messages qui disparaîtront au bout d'un temps précis. Il s'agit en fait de réaliser des enregistrements vocaux. Accédez aux réglages de l'appareil et pressez ***Messages***. Dans ***Messages audio***, touchez ***Expiration*** et fixez, par exemple, la durée de vie à deux minutes (***Après 2 minutes***).

5

... puis transmettez-la

Pour adresser un fichier audio à un contact, activez préalablement la fonction ***Messages***, puis le bouton de composition. Saisissez le numéro de téléphone. Énoncez ensuite distinctement votre texte en maintenant la pression avec votre doigt sur le symbole du ***micro***. Une fois votre enregistrement terminé, appuyez sur ***Envoyer***. ■

6

Naviguez sur Internet

Toutes vos visites sur le Web sont consignées dans l'historique. En prenant aussi en compte les cookies et autres fichiers temporaires, surfer incognito relève de la mission commando !

Brouillez les pistes avec Microsoft Edge

La sortie de Windows 10 a sonné le glas d'Internet Explorer. Le vétéran du Web a laissé sa place à Microsoft Edge, un navigateur à l'interface épurée, quoiqu'aux options plus limitées que ses rivaux. Il ne fait pas l'impasse, pour autant, sur la confidentialité et offre un mode de surf furtif ne conservant pas la trace de vos activités en ligne. Déroulez le volet ***Plus*** de ***Microsoft Edge***, d'un clic sur le bouton formé de ***trois points*** dans l'angle supérieur droit de la fenêtre. Activez l'option ***Nouvelle fenêtre InPrivate***. Une session sécurisée s'ouvre alors à l'écran. La mention InPrivate (à gauche du premier onglet) rappelle le caractère anonyme de la navigation. Durant tout le temps de cette session, Edge n'enregistre ni les adresses des pages que vous visitez, ni les cookies, ni les fichiers temporaires.

1

2

Passez un coup de balai derrière vous

Si vous avez omis d'activer le mode InPrivate avant de commencer votre navigation, affichez le volet ***Hub*** en cliquant sur l'icône à droite du champ d'adresse. Actionnez ensuite l'onglet ***Historique***. Sélectionnez le lien ***Effacer tout l'historique*** pour supprimer les entrées ou bien la ***croix*** située au bout de la ligne ***Au cours de la dernière heure*** afin de restreindre l'opération aux pages visitées au cours des soixante minutes écoulées. Pour éliminer les cookies et les autres vestiges de votre visite, rendez-vous sur le volet ***Plus*** et validez ***Paramètres***, ***Choisir les éléments à effacer***. Cochez ce qui doit être éliminé, puis faites ***Effacer***.

3

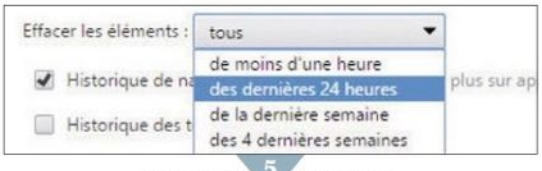
Restez discret grâce à Chrome

Le browser de Google intègre lui aussi un mode secret. Disponible sous Windows et macOS, cette fonctionnalité se révèle très commode si vous devez vous servir d'un autre ordinateur que le vôtre. Pour ouvrir une session sécurisée, déroulez au préalable le menu général de Chrome en cliquant sur les ***trois points***, en haut à droite de la fenêtre. Activez la commande ***Nouvelle fenêtre de navigation privée*** ou utilisez le raccourci clavier ***Ctrl*** + ***Maj*** + ***N***. Une nouvelle fenêtre apparaît à l'écran, avec un onglet gris foncé et la silhouette d'un personnage affublé de lunettes et d'un chapeau.

4

Pensez à purger l'historique

Pour éviter qu'une personne n'en découvre un peu trop sur vos habitudes en naviguant sur votre ordinateur, veillez à vider régulièrement les dossiers de l'historique. Dans le menu principal de Chrome, cliquez sur ***Plus d'outils***, ***Effacer les données de navigation***. Dans la liste ***Effacer les éléments***, activez l'option ***Tous***. Cochez ensuite les éléments à purger : historique de navigation et de téléchargement, cookies, fichiers en cache...

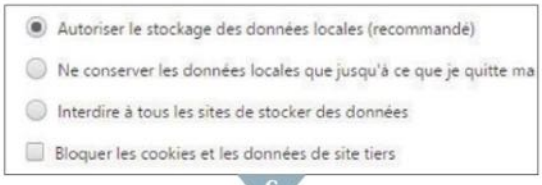


5

Optez pour un ménage ciblé

Chrome vous aide à ajuster le nettoyage. Outre les éléments qui seront effacés, vous pouvez agir sur une période précise. Déroulez la liste ***Effacer les données de navigation*** et indiquez jusqu'où remonter : ***moins d'une heure***, ***les dernières 24 heures***, ***la dernière semaine*** ou ***les quatre dernières semaines***. Confirmez en cliquant sur ***Effacer les données de navigation***.

sans laisser de trace



6

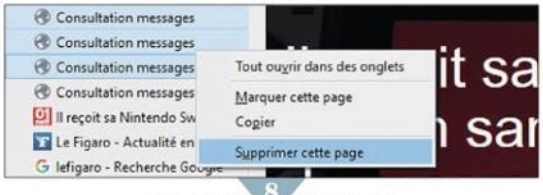
Contrôlez ce que Chrome sait de vous

Pour gérer les cookies, allez dans ***Paramètres***. Cliquez sur ***Paramètres de contenu*** dans la section ***Confidentialité***. Cochez par exemple ***Ne conserver les données locales que jusqu'à ce que je quitte ma session de navigation*** pour tout effacer en quittant le navigateur.

7

Empêchez Firefox de fouiner partout

Comme ses principaux concurrents, Firefox dispose d'un mode de navigation privée qui peut être actionné à discrétion. Pour cela, accédez au menu du navigateur en actionnant le bouton formé de ***trois traits superposés*** (dans le coin supérieur droit de l'écran) et choisissez l'option ***Fenêtre privée***. Vous pouvez aussi recourir au raccourci clavier ***Ctrl+Maj+P***. Le caractère furtif de la session est signalé par un masque de carnaval violet qui s'affiche à droite de la barre de titre et sur les onglets.



8

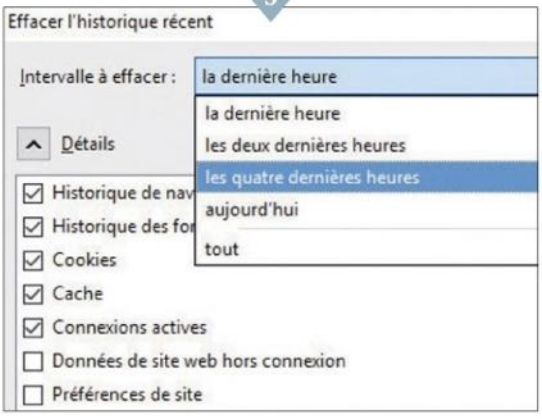
Effacez certaines adresses de l'historique de navigation

Faites apparaître le panneau de l'historique de navigation au moyen du raccourci clavier ***Ctrl+H***. Déroulez la liste ***Aujourd'hui***, faites un clic droit sur l'adresse encombrante et exécutez la commande ***Supprimer cette page***.

Faites le tri quand vous quittez Firefox

Pour procéder à un ménage plus complet – adresses, cookies... –, activez le raccourci ***Ctrl+Maj+Suppr***. Déployez la section ***Détails*** afin de spécifier les éléments à éliminer. Indiquez le point de départ de la purge dans la liste ***Intervalle à effacer*** (la dernière heure, par exemple) et cliquez sur ***Effacer maintenant***. Vous pouvez aussi demander à Firefox que l'historique soit systématiquement effacé quand vous quittez le browser. Dans le volet de menu, allez dans ***Options***, ***Vie privée*** et optez pour ***Vider l'historique lors de la fermeture***.

9



Surfez en mode furtif avec Safari

Sous Mac, vous pouvez aussi surfer incognito. Pour ouvrir une telle session, déroulez le menu ***Fichier***, ***Nouvelle fenêtre privée***. L'unique différence avec une session "normale" tient à la couleur du champ d'adresse, gris foncé et non blanc. Pour effacer vos traces, pointez sur ***Historique***, ***Effacer l'historique***, indiquez la période concernée (***dernière heure***, ***aujourd'hui***...) et approuvez (***Effacer l'historique***). Il est aussi possible de limiter les traces de votre passage sur Internet. Dans les ***Préférences*** du navigateur, activez l'onglet ***Général*** et précisez quand les éléments de l'historique seront effacés (***un an***, ***un jour***...). Placez-vous aussi sur l'onglet ***Confidentialité*** et bloquez l'enregistrement des cookies. ■

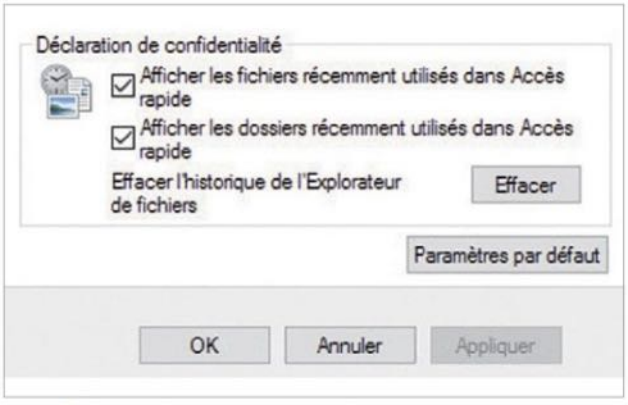
10

Effacez les données qui vous trahissent sur votre PC

Vous avez décidé de céder votre ordinateur ou, simplement, de le partager avec d'autres membres de votre famille ? Alors n'oubliez pas de supprimer les informations personnelles stockées sur le disque dur que vous n'avez pas envie de voir tomber entre de mauvaises mains. Caches, fichiers, activités... Tout doit disparaître !

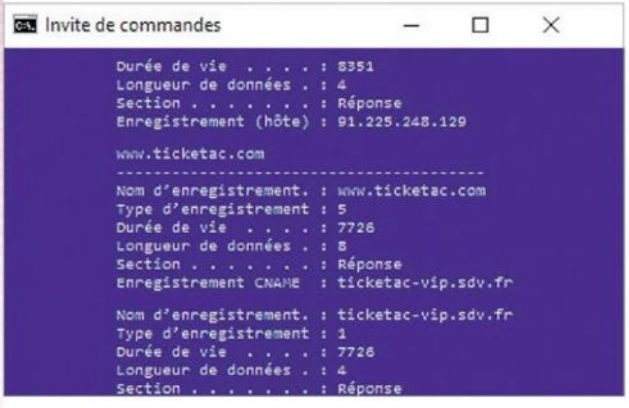
1. Supprimez complètement les fichiers

Servez-vous du ***Broyeur de fichiers*** d'Avast Antivirus ou de l'appli Easy & Secure Eraser. Les derniers fragments de données du disque dur, dans la corbeille de Windows, seront réduits en poussière.



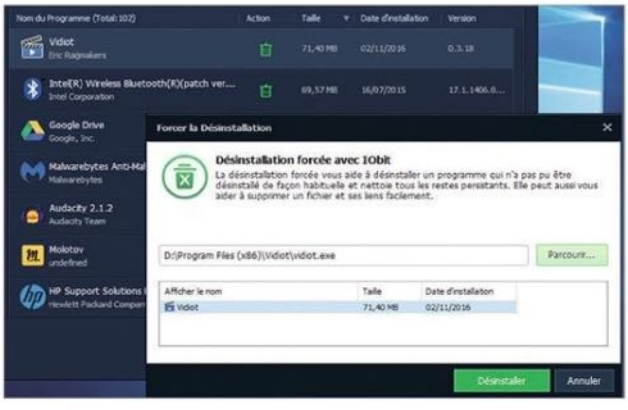
2. Occultez les derniers documents consultés

Ouvrez l'***Explorateur de fichiers***. Opérez un clic droit sur ***Accès rapide***, activez la commande ***Options*** et décochez les deux cases dans la section ***Déclaration de confidentialité***. Sélectionnez ***Effacer***, puis ***OK***.



5. Videz la liste des pages Web visitées

Purger l'historique du navigateur *(lire p. 76)* ne suffit pas. Windows garde en mémoire votre activité sur Internet. Ouvrez une fenêtre d'Invite de commandes et saisissez ***ipconfig /flushdns*** pour tout jeter aux oubliettes.



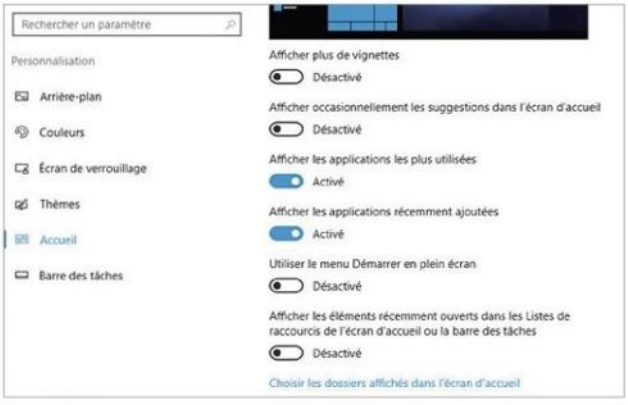
6. Retirez la totalité des logiciels

Le module de désinstallation de Windows ne réussit pas toujours à évincer les fichiers de configuration des programmes. Employez donc l'analyse approfondie d'***IObit Uninstaller*** (***bit.do/ddXfY***).

DIFFICULTÉ
Élevée
TEMPS
45 min

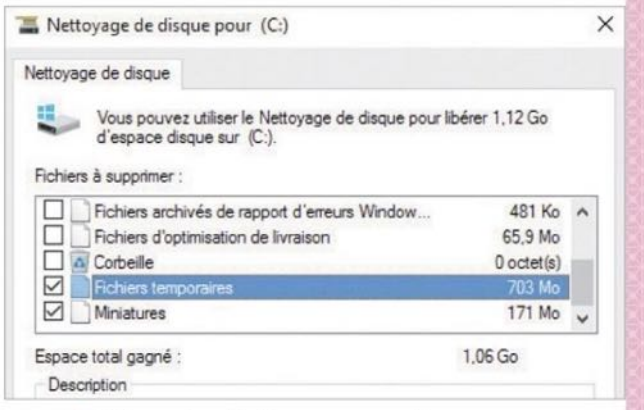
© freshidea

Fichiers temporaires, historique des documents, corbeille... Un petit tour dans Windows en dit très long sur vos habitudes.



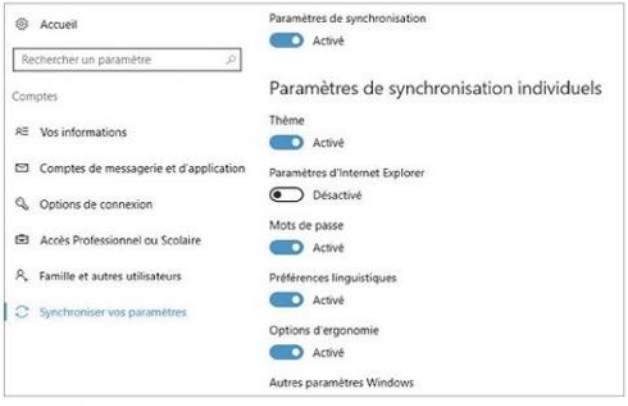
3. Masquez votre activité récente

Le menu Démarrer conserve la trace des derniers fichiers ouverts. Pour éliminer ces informations, rendez-vous dans ***Paramètres***, ***Personnalisation***, ***Accueil*** et fermez l'option ***Afficher les éléments récemment ouverts***.



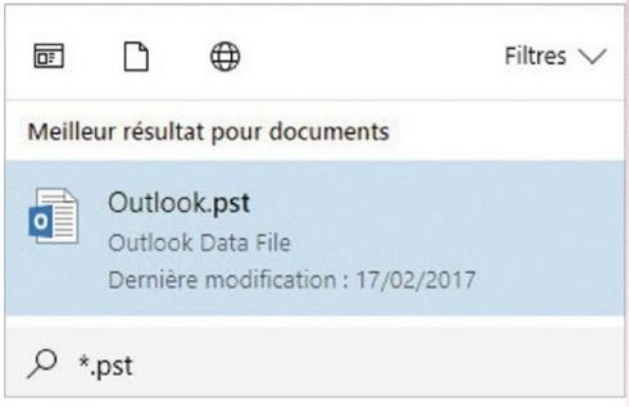
4. Effacez les fichiers temporaires

Dans l'***Explorateur de fichiers***, faites un clic droit sur votre disque dur. Puis dans ***Propriétés***, ***Nettoyage de disque***, cochez ***Pages Web hors connexion***, ***Fichiers Internet temporaires***, ***Fichiers temporaires***. Validez.



7. Suspendez toute synchronisation

Pour éviter que réapparaissent les données que vous venez d'effacer, allez dans ***Paramètres de compte utilisateur***, cliquez sur ***Synchroniser vos paramètres*** et coupez l'option ***Paramètres de synchronisation***.



8. Dites ciao à vos vieux courriels

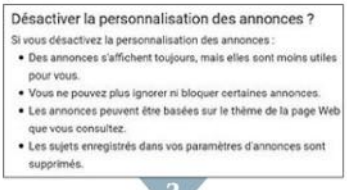
Si vous avez une appli de messagerie, n'oubliez pas de supprimer le dossier où sont archivés vos mails. Pour Outlook, il s'agit d'un fichier portant l'extension .pst regroupant messages, calendriers, contacts et tâches.

Contrôlez ce que les géants du Web savent de vous

Google, Facebook, Microsoft et Apple engrangent des milliers d'informations sur vos activités et sur vos petites habitudes. Faites le point sur ce qu'ils connaissent de vous et reprenez la main sur votre vie privée en coupant l'aspirateur à données.

1 Identifiez les informations que Google utilise

Vous êtes surpris de voir apparaître des publicités dont le contenu semble très lié au dernier message que vous avez reçu sur votre adresse Gmail ? Cela vous étonne que la bannière affichée corresponde exactement au dernier achat que vous avez fait sur un site d'e-commerce ? En vous rendant à l'adresse ***bit.do/dbvkv*** – et après avoir saisi vos identifiants si vous n'étiez pas déjà connecté à votre compte Google –, vous disposerez d'un aperçu global et... effrayant de la façon dont le géant d'Internet cible les réclames qu'il vous adresse. Pour reprendre le contrôle de votre vie privée, utilisez le curseur ***Activer*** situé à droite de l'intitulé ***Personnalisation des annonces sur cette page***.

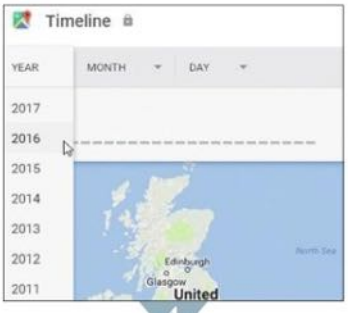


2 Filtrez les publicités

Quand vous désactivez la personnalisation des annonces commerciales, ne pensez pas pour autant vous débarrasser définitivement des pubs en ligne. Vous risquez, au contraire, de ressentir une gêne encore plus grande, puisque les annonces ne seront plus ciblées en fonction de vos goûts et de vos habitudes. Google vous en informe d'ailleurs. Si vous persistez dans votre choix, cliquez sur ***Désactiver***.

3 Rationnez la collecte

Vous pouvez toutefois conserver la personnalisation des publicités, tout en limitant les infos collectées par Google. Pour cela, ne choisissez pas Désactiver, mais décochez l'option ***Utiliser également les informations et l'activité du compte Google pour personnaliser les annonces...*** Enregistrez ce paramètre en sélectionnant ***Exclure***.



4 Évitez les prises en filature

Que vous possédiez un smartphone Android ou iOS, vous vous servez sans doute des services de Google pour gérer votre courrier (Gmail), vos photos ou faire des recherches sur Internet. La firme de Mountain View profite de tous ces accès pour collecter des informations sur votre géolocalisation et vos déplacements. Rendez-vous sur ***bit.do/dbvng*** pour afficher les données enregistrées au cours des derniers jours.

5 Demandez à votre iPhone de vous lâcher la grappe

Sous iOS, empêchez l'accès du smartphone aux données de localisation en touchant l'icône ***Réglages*** et en accédant à la rubrique ***Confidentialité***. Si vous êtes soupçonneux, placez l'interrupteur ***Service de localisation*** en position inactive et confirmez votre choix à l'aide du bouton ***Désactiver***.

6

Contrecarrez Apple

Si vous détenez un iPhone ou un iPad, vous avez la possibilité de visualiser les données personnelles enregistrées par votre appareil, puis envoyées vers les serveurs d'Apple. Des informations qui sont ensuite monétisées, directement par la société ou par ses partenaires. Pressez l'icône ***Réglages*** et ouvrez la rubrique ***Confidentialité***. Là, exécutez la commande ***Publicité*** et placez l'interrupteur ***Suivi publicitaire limité*** en position ***Active***. Vous réduirez ainsi la quantité de renseignements transmis aux annonceurs.

7

Limitez l'accès aux données de votre compte Facebook

Comme une majorité d'utilisateurs, vous suivez l'actualité de votre réseau principalement à partir de votre téléphone. Pour savoir quelles applications et quels services fouinent dans les données de votre compte, effleurez l'icône ***Réglages*** de l'iPhone, puis l'intitulé ***Confidentialité***. Faites défiler la liste des options jusqu'à la section ***Facebook***. Pour restreindre l'accès, mettez l'interrupteur en position inactive. Les données ne disparaîtront pas, mais leur divulgation sera davantage contrôlée.

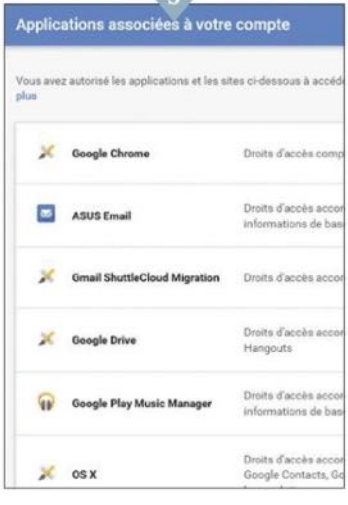
Censurez les applications

Quand vous importez une appli sur un appareil Android, celle-ci sollicite un droit d'accès à moult données. Vous ne prêtez sans doute pas attention à ces demandes. Et pourtant, ces exigences ne sont pas toujours justifiées. Un logiciel photo doit pouvoir accéder à la galerie d'images du téléphone, mais a-t-il besoin de voir vos contacts ? Dans les paramètres, appuyez sur ***Applications*** et choisissez une appli pour découvrir les infos auxquelles elle accède.

8

Obtenez un aperçu global des services associés à Google

Pour faire le point sur les droits d'accès aux données de votre compte Google accordés aux différentes applications présentes sur votre mobile, connectez-vous, depuis un navigateur Internet, sur le site ***bit.do/dbvtP***.



9

10

Empêchez le mouchard de Google Play de vous pister...

Allez dans les ***Paramètres*** d'Android. Appuyez sur ***Applications***, puis recherchez l'intitulé ***Services Google Play***. Vous avez la faculté d'effacer les données liées à vos recherches sur Google Play. Pressez simplement ***Gérer l'espace*** afin d'afficher les différentes options disponibles.

11

... et faites place nette

Plusieurs possibilités s'offrent maintenant à vous. En optant pour ***Gérer les données de recherches***, vous pouvez faire le point sur ce que l'on retient de vos visites sur Google Play. Tout en bas de l'interface, se trouve le bouton ***Effacer les données***. Activez cette commande et confirmez votre choix. Les infos collectées sont alors supprimées. Vous restaurez ainsi un peu de confidentialité, tout en libérant de l'espace sur votre smartphone ! ■

Surveillez vos activités sur les réseaux sociaux

Quand c'est gratuit, c'est vous le produit ! Twitter, Facebook et consorts ont tendance à exploiter et à exposer un peu trop vos informations. À vous de décider de ce que vous partagez. Et avec qui.

Privilégiez vos amis autant que possible

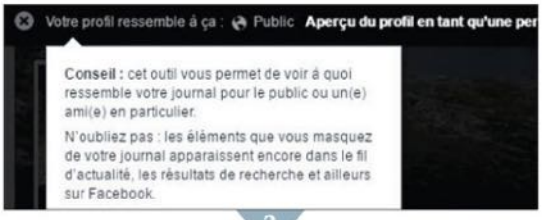
Facebook est évidemment le premier réseau social auquel on pense lorsqu'on évoque les fuites d'informations, l'exposition de son profil et tous les problèmes que cela peut engendrer. Une situation qui repose à la fois sur les fondements de ce service – qui privilégie la visibilité de vos publications – et le manque d'attention porté par les utilisateurs aux questions de sécurité. Pour éviter de montrer des images ou des propos potentiellement embarrassants, assurez-vous d'abord que seuls vos "amis" pourront y accéder. Utilisez pour cela l'icône située à gauche de la commande ***Publier***.

1

2

Changez les règles de confidentialité

Facebook offre de nombreuses options pour ajuster les règles de publication. Cliquez sur le bouton des raccourcis de confidentialité, symbolisé par un ***cadenas***, en haut de la fenêtre, puis sur l'intitulé ***Qui peut voir mes contenus***. Sous ***Qui peut voir mes futures publications***, sélectionnez ensuite l'option ***Amis***. Vous pourrez modifier ce critère pour chaque post. Pour contrôler vos contributions (Like, partages...), choisissez ***Utiliser l'historique personnel***, puis ***Modifier*** afin de supprimer un élément. La section ***Comment empêcher quelqu'un de me contacter*** sert à définir une liste noire.



3

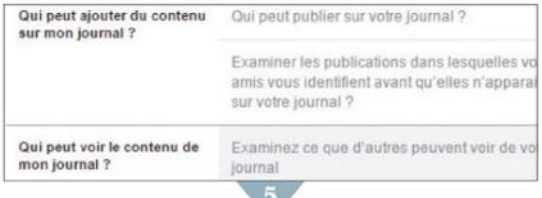
Préservez votre réputation numérique

L'un des points critiques de Facebook est ce que l'on voit de votre profil lorsqu'on ne fait pas partie de vos amis. Un futur employeur ou qui que ce soit d'autre a vite fait d'épier ce type d'informations. Toujours dans la section ***Qui peut voir mon contenu*** des raccourcis de confidentialité, effleurez la commande ***Aperçu de mon profil en tant que***. Effacez toutes les publications qui vous paraissent inappropriées.

4

Gérez les applis qui ont accès à votre profil

Cliquez de nouveau sur l'icône des raccourcis de confidentialité et exécutez, cette fois, la commande ***Affichez plus de paramètres***. Dans la colonne de gauche, activez ***Applications***, supprimez toutes celles que vous n'utilisez plus de façon à ce qu'elles n'aient plus accès à votre profil Facebook et à vos données.



5

Optez pour une diffusion restreinte

Allez maintenant dans ***Journal et identification***. Déroulez la liste ***Qui peut publier sur mon journal*** et sélectionnez l'option ***Moi uniquement***. Réglez les droits des autres sections sur ***Amis*** ou sur ***Moi uniquement***.

6

Protégez vos publications sur Google+

Le réseau social de Google compte bien moins d'utilisateurs que Facebook, ce qui constitue en soi une bonne protection ! Pas question pour autant d'ignorer la sécurité et de diffuser vos publications à tout va. Dans les paramètres du service, réservez vos posts à vos seuls cercles et débranchez les options ***Autoriser les internautes à télécharger mes photos et vidéos*** et ***Autoriser l'affichage de mon profil dans les résultats de recherche***.

7

Épinglez en toute sérénité

Les réseaux sociaux ne se cantonnent pas à Facebook et à Google+. Les images que vous collectionnez sur Pinterest peuvent aussi en dire beaucoup sur vos goûts et sur vos centres d'intérêt. Pour maîtriser la diffusion de vos données personnelles, rendez-vous sur la page de gestion de votre profil. Sur l'icône en forme de ***boulon***, ajustez le paramètre ***Protection contre l'indexation*** sur ***Oui***. Pensez aussi à recourir aux tableaux secrets afin de limiter l'accès à vos collections à vos seuls amis.

8

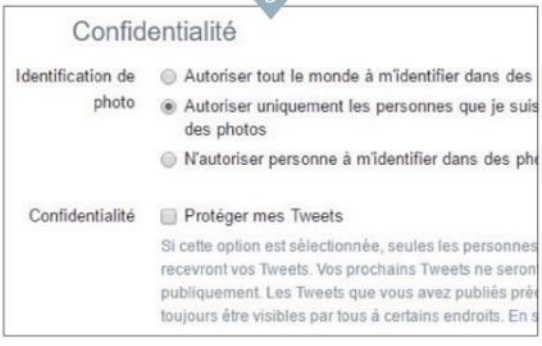
Verrouillez l'accès aux photos de Flickr

Le droit à l'image reste une notion floue sur le Web en général... et sur Flickr en particulier. Pointez sur votre avatar, puis sur ***Paramètres***, ***Confidentialité***, ***Autorisations***. Réglez le type de licence sur ***Tous droits réservés***. Dans la section ***Qui pourra voir, publier (etc.)***, cliquez sur ***Modifier*** et limitez l'accès à votre famille, à vos amis et aux personnes que vous suivez.

Gazouillez tranquille sur Twitter...

Combien de phrases en 140 signes envoyées trop vite et de pensées péremptoires avez-vous déjà répandu sur la Toile ? Pour éviter de nouveaux dérapages, contrôlez votre compte autant que vos propos. Pointez sur votre avatar puis sur ***Paramètres***. Dans l'onglet ***Confidentialité et sécurité***, ***Identification de photo***, choisissez l'option ***Autoriser uniquement les personnes que je suis***. Vous pouvez bénéficier d'un niveau de sécurité plus élevé en optant pour ***Protéger mes tweets***. Vos publications seront ainsi réservées à votre liste d'abonnés et personne ne pourra les retweeter. Vos messages n'apparaîtront pas non plus sur les moteurs de recherche. Attention, vous risquez de perdre des abonnés qui considéreront que vous ne jouez plus le jeu sur le réseau social.

9



... sans oublier de blinder votre mot de passe

Les malwares que nous évoquons tout au long de ce hors-série visent vos adresses mails, identifiants ou mots de passe pour poster à votre place ou revendre des fichiers. Pensez à constituer un code d'accès solide avec chiffres, lettres, capitales et symboles. En associant en plus votre numéro de mobile à votre compte, vous pourrez ainsi le réinitialiser s'il devient inaccessible. Enfin, dans les paramètres de ***Twitter***, activez l'onglet ***Vos données Twitter***, insérez votre précieux sésame, puis vérifiez l'historique d'activité pour vous assurer que personne d'autre n'accède à votre compte et ne tweete en votre nom. ■

10

Larguez vos comptes Google, Facebook et Microsoft

Comme les matières radioactives, les données associées à vos comptes ont une durée de vie longue... très longue ! Une excellente raison pour fermer ceux dont vous ne faites plus usage.

FACEBOOK

1

Désactivez le service

Commencez par vous connecter au service puis, dans la barre située en haut de l'interface, cliquez sur le ***cadenas***. Dans le volet qui se déploie, pointez sur ***Affichez plus de paramètres***. Dans la liste des rubriques à gauche de l'écran, sélectionnez l'option ***Sécurité***. Au bas de la page des paramètres de sécurité, activez ***Modifier*** à droite de la rubrique ***Désactiver votre compte***. Avant de confirmer votre décision, gardez à l'esprit que la fermeture effective du compte n'interviendra qu'après un délai de quinze jours. Durant ce laps de temps, le contenu de votre page reste consultable.

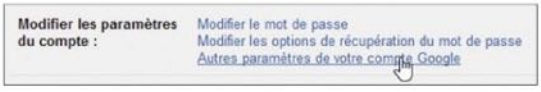
Approuvez la fermeture complète

Certains éléments ne disparaîtront jamais de Facebook malgré la désactivation du compte. Ainsi, les messages que vous avez échangés avec vos amis ne seront pas effacés de la boîte de réception de leurs destinataires. Si vous persistez dans votre volonté de clôturer le compte, cliquez sur le lien ***Désactiver***. ■

2

GOOGLE

1



Accédez aux réglages

Qu'il ait été piraté ou qu'il vous soit devenu inutile, peu importe, c'est vous qui décidez. Pour clôturer un compte Google, connectez-vous d'abord à votre boîte de réception Gmail depuis un navigateur Internet, sur un ordinateur ou une tablette. Cliquez sur la ***roue crantée*** qui figure dans l'angle supérieur droit de la fenêtre, puis sur ***Paramètres***. Activez l'onglet ***Comptes et Importation***. Dans la section ***Modifier les paramètres du compte***, allez enfin dans ***Autres paramètres de votre compte Google***.

2

Gérez vos préférences

Un nouvel onglet s'affiche dans le navigateur Web. Les premières commandes proposées portent principalement sur les options de connexion et de sécurité. Intéressez-vous au volet ***Préférences de votre compte*** situé à droite de l'écran. Pointez sur la commande ***Supprimer votre compte ou des services***.

3

Supprimez le compte

Deux possibilités s'offrent à vous : renoncer au bénéfice de certains services seulement (YouTube, Google+, Gmail ou Orkut), ou effacer tout ce qui concerne le compte Google. Dans ce dernier cas, optez pour ***Supprimer le compte Google et les données associées***. Une nouvelle fenêtre s'affiche. Sécurité oblige, vous êtes invité à vous identifier de nouveau.

4

Récupérez vos données

Si vous n'avez plus l'usage de ce compte, ce n'est pas pour autant que toutes ses données sont devenues obsolètes. Avant de confirmer la suppression, Google vous offre l'opportunité de récupérer les infos associées au compte : les fichiers stockés sur Drive, les messages Gmail, les photos publiées sur Google+, etc. Activez la commande ***Télécharger vos données***. Indiquez les éléments que vous souhaitez sauvegarder et validez. Ils seront enregistrés dans une archive compressée.

5

Personnalisez l'archive

Par défaut, le dossier de sauvegarde est enregistré au format Zip. Si vous utilisez un utilitaire de compression comme 7Zip, vous pouvez toutefois opter pour un format plus compact (TGZ par exemple). Définissez ensuite le mode de récupération des données : la réception d'un mail contenant un lien de téléchargement ou un transfert direct dans votre espace Dropbox.

6

Finalisez l'opération

Avant d'aller plus loin, vérifiez que vous pouvez accéder au contenu de l'archive. Cochez ensuite les cases ***Oui, je reconnais que je suis toujours redevable des frais liés à toutes les transactions financières en attente et je comprends que dans certaines circonstances, mes revenus ne seront pas versés*** et ***Oui, je souhaite supprimer définitivement ce compte Google et toutes les données qui y sont associées***. Pressez enfin le bouton ***Supprimer le compte***. ■

MICROSOFT

1

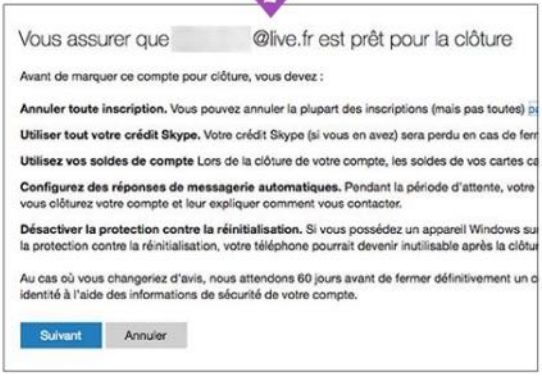
Actualisez vos paramètres de sécurité

Avant de fermer définitivement votre compte Microsoft, assurez-vous que vous ne l'avez pas associé à d'autres services en ligne, faute de quoi vous ne pourrez plus y accéder. Connectez-vous ensuite au site ***bit.do/ddF3u***. Identifiez-vous, cliquez sur ***Sécurité*** puis rendez-vous, en partie droite de l'écran, à la rubrique ***Mettre à jour vos informations de sécurité***. Suivez les instructions pour authentifier votre compte.

Clôturez… et patientez !

Cliquez à présent sur la commande ***Clôturer votre compte*** qui figure en bas de la page ***Paramètres de sécurité***. Vérifiez que le compte Microsoft affiché est bien celui que vous souhaitez désactiver, puis passez à l'étape suivante. Vous avez un doute sur votre décision ? Pas de panique, vous disposez de soixante jours pour changer d'avis et réactiver le compte (et restaurez les données). ■

2



DIFFICULTÉ
Modérée
TEMPS
20 min

Reprenez le contrôle d'un compte piraté

Si vos amis vous reprochent tout d'un coup de les inonder de messages publicitaires ou de demandes d'aide financière, aucun doute, votre boîte mail a été piratée. Ces quelques conseils devraient vous aider à retrouver la maîtrise de votre compte.

Changez de mot de passe

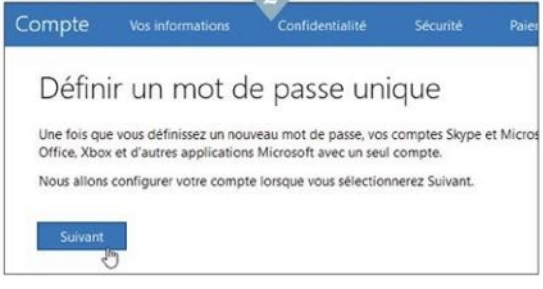
Lorsque vous êtes victime du piratage de votre adresse mail, la première chose à faire est d'empêcher le responsable de se connecter de nouveau sur votre compte. Pour cela, vous devez modifier sans attendre le code associé à l'adresse. Ce principe vaut quel que soit le service de messagerie (Yahoo!, Gmail, Microsoft ou autre) dont vous vous servez. Rendez-vous sur l'interface d'administration de votre compte et identifiez-vous.

1

Saisissez un nouveau sésame

Si vous utilisez une adresse Microsoft (Outlook.com, Live.fr, etc.), cliquez sur votre avatar dans l'angle supérieur droit de l'interface, puis activez la commande ***Afficher le compte***. Dans le volet gauche de la page qui s'affiche alors, sous votre nom et l'adresse mail, sélectionnez l'intitulé ***Modifier le mot de passe***. N'oubliez pas de changer les paramètres d'identification sur tous vos appareils (PC, Mac, smartphone, tablette).

2



3

Agissez sans accès au compte

Le problème devient plus sérieux si l'auteur du piratage a lui-même modifié le mot de passe et que vous ne pouvez plus vous identifier. Dans ce cas, allez sur la page de connexion du service depuis un navigateur Internet et lancez la procédure de récupération du code d'accès. Répondez à la question secrète mise en place lors de l'ouverture de votre compte.

4

Prévenez le fournisseur du service mail

Si les mesures précédentes n'ont rien donné, signalez le problème au fournisseur du service de messagerie. Pour Microsoft, connectez-vous à l'adresse ***bit.do/dc7wJ***. S'il s'agit d'un compte Google, faites un tour sur le site ***bit.do/dc7wQ***. Pour Yahoo!, cap sur la page ***bit.do/dc7w7***. Vous serez alors guidé pas à pas pour votre déclaration. Vous pouvez également déposer une plainte auprès des autorités (***bit.do/dc7xp***). ■

DIFFICULTÉ
Modérée
TEMPS
10 min

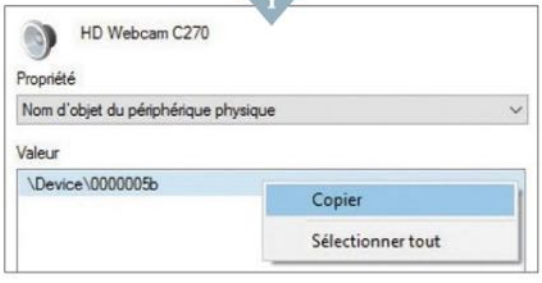
Empêchez la webcam de vous espionner

Et si un malware détournait la caméra de votre ordinateur pour vous épier ? Voici comment contrer ces tentatives et contrôler l'usage de la webcam d'un PC ou d'un Mac.

Identifiez le vrai nom de la caméra

Sur votre PC, effectuez une recherche sur le terme ***Gestionnaire de périphériques*** et ouvrez le lien qui figure en tête des résultats. Explorez la catégorie ***Contrôleurs audio, vidéo et jeux***, puis double-cliquez sur le nom de la webcam. Activez l'onglet ***Détails***, déroulez le menu ***Propriétés***, et sélectionnez ***Nom d'objet du périphérique physique***. Faites un clic droit sur la valeur affichée et exécutez la commande ***Copier***. Ouvrez un document Word ou WordPad et collez-y l'adresse système de la caméra. Puis fermez le ***Gestionnaire de périphériques***.

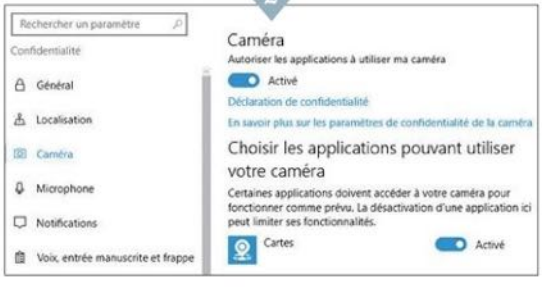
1



Rendez aveugles les logiciels espions...

Depuis le site ***bit.do/ddGaY***, téléchargez et installez ***Process Explorer***. Ouvrez l'archive Zip et lancez le programme ***procexp64.exe*** (ou ***procexp.exe*** pour une version 32 bits de Windows). Enfoncez les touches ***Ctrl+F***, entrez le nom de la webcam et cliquez sur ***Search*** pour afficher la liste des programmes accédant à la caméra. Si vous repérez un inconnu, accédez aux paramètres de Windows, choisissez ***Confidentialité***, ***Caméra*** et basculez le curseur du logiciel en question en position inactive.

2



3

... mais aussi sourds !

La caméra de votre PC ne se contente pas de vous filmer. Elle vous écoute également. Pour interdire l'accès au microphone à une appli, revenez sur la page ***Confidentialité*** des paramètres de Windows et cliquez, cette fois, sur l'intitulé ***Microphone***. Repérez le programme et positionnez son interrupteur sur ***Désactivé***.

4

Soyez averti lorsqu'une application tente d'accéder à la webcam de votre Mac

Le détournement de la caméra est un problème qui concerne également les Mac. Sur le site ***bit.do/ddGgd***, activez le bouton ***Download*** sous le logo de l'appli OverSight. Une fois celle-ci installée, une notification s'affiche à chaque fois qu'un programme essaie d'accéder à la webcam ou au microphone, accompagnée de deux boutons. Cliquez sur ***Allow*** pour autoriser l'usage de la caméra, ou sur ***Block*** pour l'interdire.

5

En dernier recours, pensez au Scotch !

Après une absence, faites un clic sur l'icône d'***OverSight*** (un parapluie) dans la barre d'état de macOS pour savoir si la caméra et le microphone sont actuellement utilisés par une appli. Contrairement à Windows, macOS n'offre pas la possibilité de désactiver la webcam. Aussi, pour éviter que l'on vous filme à votre insu, vous n'avez d'autre choix que d'obstruer l'objectif à l'aide d'un ruban adhésif opaque. Vive le système D ! ■

Floutez les visages sur les photos avant de les publier

Les personnes figurant sur les clichés et les vidéos que vous partagez sur les réseaux sociaux ne souhaitent pas être exposées au regard de tous ? Une seule solution : brouiller leur visage.

Ouvrez l'image dans votre logiciel de retouche

Le floutage peut être effectué avec la plupart des applications de retouche d'images. Pour ce pas-à-pas, nous avons choisi GIMP, un logiciel gratuit doté de nombreuses fonctionnalités. Si vous ne l'utilisez pas déjà, téléchargez-le à l'adresse ***bit.do/ddnNG***. Déroulez le menu ***Fichier***, ***Ouvrir***. Accédez au dossier qui abrite la prise de vue à modifier, puis cliquez dessus et validez. Il n'est pas question de dénaturer le cliché en plaquant un cache ou un flou grossier. Il faut agir de façon à préserver l'image, tout en interdisant l'identification du sujet.

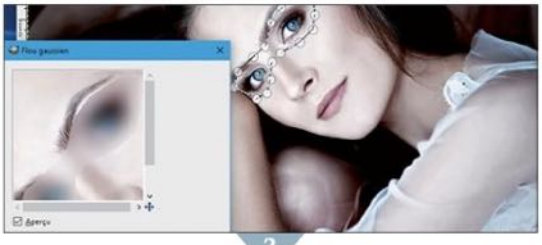
1

39039059_237000001901578285_RELEVE.pdf	62,4 ko	05/01/2016
1484835500988_1771.pdf	263,4 ko	19/01/2017
BDCC161209899.pdf	78,7 ko	11/01/2017
BDCC170109956.pdf	76,8 ko	12/01/2017
facture-EDF-11-15.pdf	123,4 ko	07/12/2015
girl-2032802_1280.jpg	201,4 ko	13:55
IMG_0338.jpg	7,4 Mo	25/06/2014
IMG_0923.JPG	6,1 Mo	11/10/2016
Margareth-DUCHE.jpg	35,9 ko	06/11/2015

Spécifiez la zone à flouter

Sélectionnez l'outil ***Chemin*** dans la palette de GIMP. Celui-ci va servir à délimiter précisément la zone où sera appliqué l'effet de flou. Ce travail s'effectue à l'aide de la souris, par clics successifs. Une série de points s'affiche en surimpression de l'image. Une fois les contours de la zone de sélection définis, faites un clic droit sur l'un des points et exécutez la commande ***Sélection*** dans le menu contextuel. Placez-vous ensuite sur ***Depuis de chemin***.

2



3

Paramétrez la densité du flou

Déroulez le menu ***Filtres***. Cliquez sur ***Flou*** et sélectionnez l'option ***Flou gaussien***. Une nouvelle fenêtre apparaît. Elle présente une zone d'aperçu afin d'évaluer le résultat obtenu. Vous pouvez alors ajuster les propriétés du flou progressivement, en utilisant les curseurs horizontal et vertical. Lorsque vous pensez avoir atteint un niveau satisfaisant, activez le bouton ***Valider***. Le flou est alors appliqué à la photo.

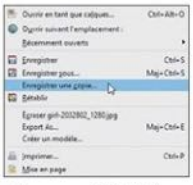
4

Appliquez d'autres effets

Si vous estimez que le flou n'est pas très heureux, annuler l'opération, déroulez le menu ***Filtres*** et cliquez, cette fois, sur ***Artistiques***, puis sur ***Cubisme***. La fenêtre des options de ce filtre répond aux mêmes principes que la précédente. Réglez les paramètres à appliquer à la zone de sélection. Le résultat sera moins grossier qu'un simple flou, mais tout aussi efficace.

5

Sauvegardez la photo modifiée



Pour publier votre cliché retouché sur les réseaux sociaux, n'oubliez pas de l'enregistrer. Par défaut, GIMP suggère l'emploi de son format propriétaire. Si vous souhaitez sauvegarder votre travail tout en conservant la version originale de l'image, allez sur ***Fichier***, ***Enregistrer une copie***, ***Fichier/Export As*** et sélectionnez le format ***JPEG***.

6

Agissez aussi sur vos vidéos YouTube

La problématique de floutage des visages est a priori plus complexe lorsqu'il s'agit de vidéos. C'était sans compter sur l'inventivité de YouTube. La plateforme de partage intègre en effet un module qui détecte automatiquement les visages et peut, si vous le voulez, y appliquer un effet de flou. Connectez-vous au service et identifiez-vous. À droite du champ ***Rechercher***, cliquez sur ***Mettre en ligne*** et glissez votre film dans la zone prévue à cet effet.

7

Affichez les fonctions de retouche

Patientez jusqu'à la fin du transfert de votre fichier (l'opération peut durer quelques minutes s'il s'agit d'une longue séquence en HD). Portez ensuite votre attention sur la barre d'outils figurant au-dessus de la zone d'aperçu. Activez la commande ***Retouches*** pour accéder aux différentes options d'amélioration proposées par YouTube.

8

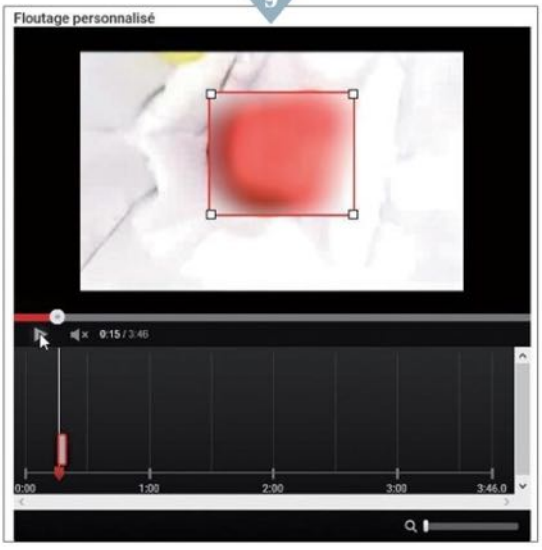
Activez le floutage automatique

Dans l'onglet ***Corrections rapides***, sélectionnez la commande ***Effets de floutage***. Si vous désirez protéger l'identité de tous les sujets apparaissant dans le film, cliquez sur le bouton ***Appliquer*** à droite de l'intitulé ***Flouter les visages***. La vidéo dans son intégralité en bénéficie. Le temps de traitement nécessaire dépend évidemment de la durée et du poids de la séquence.

Ne masquez que certains visages

Tous les visages n'ont pas forcément vocation à être floutés. Il se peut que seuls quelques acteurs de votre film s'opposent à y figurer. Dans ce cas, procédez manuellement. Cliquez sur le bouton ***Modifier*** placé à droite de l'intitulé ***Floutage personnalisé***. Il suffit alors de tracer, à l'aide de la souris, les zones spécifiques sur lesquelles les effets de flou seront appliqués. Vous pouvez définir ainsi plusieurs zones au sein d'une même séquence. Une fois ce balisage réalisé, enregistrez les modifications à l'aide du bouton ***OK***.

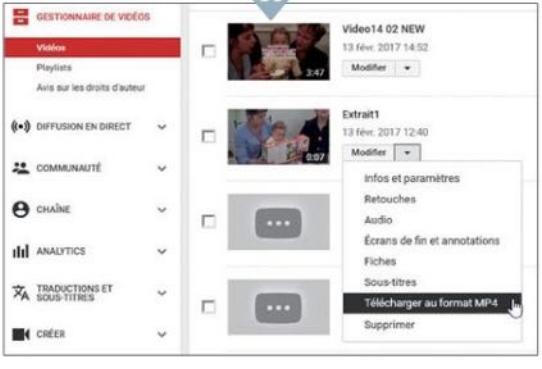
9



Récupérez le film YouTube et publiez-le sur d'autres sites

Les visiteurs verront dès lors la version floutée de votre vidéo. Vous pouvez profiter du travail opéré par YouTube et diffuser la séquence retouchée sur Facebook, par exemple. Pour cela, accédez à la page de gestion de votre compte YouTube. Sélectionnez votre œuvre et cliquez sur ***Télécharger au format MP4***. Une fois le fichier copié sur le disque dur de votre PC, rien ne vous empêche de l'utiliser comme bon vous semble. ■

10



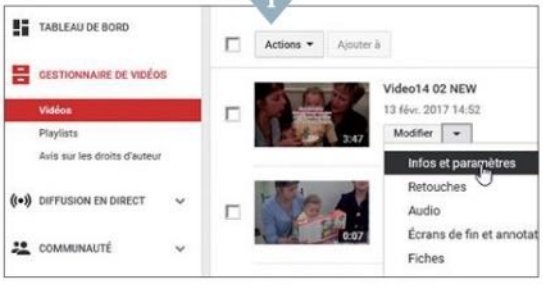
Entravez le téléchargement de vos images et vidéos

Les visiteurs de votre page Facebook et les utilisateurs de YouTube peuvent télécharger les clichés et les films que vous y avez publiés. Découvrez comment protéger ces contenus.

Sécurisez un clip publié sur YouTube...

Il n'existe aucune solution technique susceptible de garantir que les vidéos diffusées sur YouTube ne seront pas utilisées à votre insu. Dès lors, deux possibilités s'offrent à vous : les supprimer de votre chaîne et vous priver ainsi du plaisir de les partager, ou bien limiter la diffusion des fichiers à vos seuls proches. Pour cela, rendez-vous sur le site ***YouTube***. Identifiez-vous à l'aide de votre compte Google. Cliquez sur votre avatar, dans le coin supérieur droit de la fenêtre, puis sur le bouton ***Creator Studio***. Activez alors l'onglet ***Gestionnaire de vidéos***. Repérez la séquence dont vous souhaitez restreindre la diffusion. Placez-vous sur la ***flèche*** à droite du bouton ***Modifier***, puis sur la commande ***Infos et paramètres***.

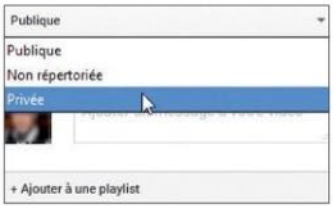
1



2

... et limitez sa diffusion

Une série d'onglets s'affiche sous la fenêtre de lecture. Activez celui intitulé ***Informations générales***. Dans la partie droite de l'écran, déroulez la liste ***Publique*** puis optez pour ***Privée***. Seuls les abonnés à votre chaîne seront désormais en mesure de visionner la séquence. Vous pouvez également inviter les personnes de votre choix. Cliquez pour cela sur ***Partager***, saisissez les adresses électroniques de vos contacts et validez à l'aide du bouton ***OK***. Confirmez à présent les nouveaux paramètres avec ***Enregistrer les modifications***.



3

Signez votre production...

Les protections offeres par YouTube sont hélas imparfaites. Aussi, à défaut de pouvoir interdire le téléchargement de vos œuvres, faites-en sorte que personne ne puisse s'en approprier la paternité. Vous pouvez par exemple incruster un logo de type watermark sur les images. Retournez sur la page d'accueil de ***Creator Studio*** comme indiqué à l'étape 1.

4

... en y incrustant un logo

Dans le volet gauche de la fenêtre, cliquez sur l'onglet ***Chaîne***. Des sous-rubriques apparaissent. Choisissez ***Branding*** puis, dans la partie centrale de l'écran, le bouton ***Ajouter un watermark***. Parcourez ensuite l'arborescence de votre disque dur, sélectionnez l'image qui fera office de logo (attention, le fichier ne doit pas dépasser 1 Mo), puis optez pour le bouton ***Enregistrer***. Votre cliché est alors importé.

5

Marquez ainsi toutes vos œuvres

Le logo sera ajouté aux vidéos publiées sur votre chaîne ainsi qu'aux séquences que vous importerez. Pour que le marquage apparaisse tout au long de la lecture, déroulez la liste ***Affichage*** et jetez votre dévolu sur l'option ***Intégralité de la vidéo***. Un clic sur ***Mettre à jour*** et votre logo s'applique à l'ensemble des contenus de la chaîne.

6

Protégez les images postées sur Flickr

Rien n'empêche un indélicat de copier vos photos présentes sur les réseaux sociaux et de se les approprier. Interdire le téléchargement ne servirait d'ailleurs pas à grand-chose puisqu'il suffit de réaliser une simple capture d'écran. Tout l'enjeu consiste à limiter l'accès à ces contenus aux personnes de confiance. Si vous animez une galerie sur la plateforme Flickr, connectez-vous à votre compte et activez ***Confidentialité et autorisations***.

7

Encadrez la publication

Observez la section ***Paramètres généraux***. Cliquez sur ***Modifier*** à l'extrémité droite de la ligne. Par défaut, Flickr autorise tous les utilisateurs à visionner vos images. Changez ce paramètre. Opter pour la solution la plus restrictive (***Uniquement vous***) n'a pas de sens, puisque personne ne serait en mesure d'admirer vos clichés. Cochez plutôt ***Personnes que vous suivez***. Ces contacts visualiseront vos contenus de la même façon que vous pouvez afficher les leurs. Terminez par ***Sauvegarder***.

8

Réduisez la taille du fichier

Flickr propose une solution astucieuse pour limiter la tentation de télécharger vos clichés. Il s'agit ni plus ni moins de réduire la taille des images que vous partagez afin de restreindre les possibilités d'exploitation. Cela devrait suffire à décourager les indélicats. Cliquez sur ***Modifier*** à droite de la commande ***Taille maximale des photos partagées***. Cochez ***Large 1024*** et validez à l'aide de ***Sauvegarder***.

9

Empêchez les usagers de Flickr d'utiliser vos clichés

Intéressez-vous à présent aux options ***Permettez à d'autres personnes de partager vos éléments***, ***Autoriser l'ajout de vos photos à une expo*** et ***Masquer vos photos lors des recherches publiques***. Interdisez les deux premières et attribuez la valeur ***Oui*** à la dernière. Vous limitez ainsi l'usage qui peut être fait de vos publications sur Flickr et conservez le contrôle de leur diffusion, en contrepartie d'une moindre visibilité.

10

Gérez les prises de vue et les films qui figurent sur votre compte Facebook

Pour accéder aux options de confidentialité, cliquez sur la ***flèche*** située à droite du ***cadenas***, en haut de la page d'accueil, puis sur ***Paramètres***, ***Confidentialité***. Vous pouvez ici définir les conditions d'accès à vos photos et vidéos, et ainsi les réserver à certaines personnes ou à des groupes d'amis. N'oubliez pas de vérifier ces options à chaque publication pour éviter les mauvaises surprises.

11

Limitez l'accès aux contenus de Twitter

Connectez-vous sur votre fil Twitter et faites un clic sur votre avatar afin d'afficher le menu ***Profil et paramètres***. Pointez alors sur ***Paramètres*** puis sur ***Confidentialité et sécurité*** et cochez l'option ***Protéger mes Tweets***. Seules les personnes que vous approuvez recevront vos prochains messages et les images associées. Attention, les anciens tweets restent visibles de tous. ■

DIFFICULTÉ
Élevée
TEMPS
40 min

Surfez en tout anonymat avec un réseau privé virtuel

Connue sous le nom de VPN (Virtual Private Network), cette voie souterraine sert à naviguer sur le Web en toute discrétion et en toute sécurité. Impossible pour quiconque de voir les données qui y transitent, ni même votre véritable adresse IP.

Activez le VPN de votre box

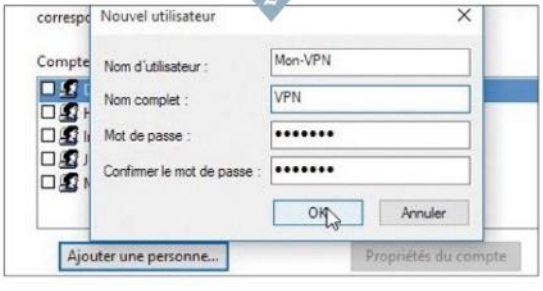
Certains routeurs intègrent une fonction VPN. Pour savoir si c'est le cas du vôtre, accédez à la console Web d'administration. Saisissez pour cela ***http://192.168.0.1*** ou ***http://192.168.1.1*** dans la barre d'adresse de votre navigateur Internet. Recherchez une éventuelle option intitulée VPN. Si votre matériel n'est pas compatible, vous pouvez exploiter les ressources de Windows.

1

Créez un réseau virtuel sous Windows

Le Centre réseau et partage du PC sert de passerelle Internet. Cliquez sur ***Réseau et Internet***, ***Modifier les paramètres de la carte***. Affichez la barre de menu (***Alt***), puis déroulez ***Fichier***, ***Nouvelle connexion entrante***, ***Ajouter une personne***. Définissez un nom et un mot de passe et terminez avec ***OK***, ***Suivant***. Lancez l'ordinateur qui utilisera le VPN. Dans le Centre réseau et partage, sélectionnez ***Configurer une nouvelle connexion***, ***Connexion à votre espace de travail***, ***Suivant***, ***Utiliser la connexion Internet (VPN)***. Tapez le nom du réseau virtuel dans le champ ***Adresse Internet***, validez d'un clic sur ***Créer*** et entrez le mot de passe.

2



3

Configurez Opera VPN sur un smartphone

Le navigateur Opera propose un VPN gratuit pour iOS (***bit.do/dc7BG***) et Android (***bit.do/dc7BT***). Au terme de l'installation de l'appli, touchez la commande ***Installer le profil***. Il suffit ensuite d'appuyer sur le bouton ***Allow*** lorsqu'une alerte s'affiche pour vous informer que l'application souhaite accéder au panneau des réglages d'iOS. Vous êtes ensuite dirigé vers le volet ***Réglages***, ***Général***, ***VPN***. Effleurez la commande ***Ajouter une configuration***. Par mesure de précaution, iOS vous invite alors à confirmer ce choix via TouchID ou votre mot de passe. La procédure est identique sous Android. Une fois l'application ouverte, vous êtes informé que ce réseau est activé. Pressez la commande pour naviguer en mode sécurisé.

4

Servez-vous du VPN sur Android et iOS

L'utilisation du VPN d'Opera est parfaitement transparente. Elle ne donne lieu à aucun message d'alerte et ne provoque pas de ralentissement perceptible. Si vous voulez vérifier que vous communiquez bien en mode sécurisé, lancez le navigateur Internet de votre smartphone. Observez l'angle supérieur gauche de l'interface. Un cartouche ***VPN*** doit s'afficher. Si ce n'est pas le cas, revenez à l'écran des réglages d'iOS et assurez-vous que l'interrupteur ***VPN***, situé entre ***Partage de connexion*** et ***Opérateur***, est bien actif. ■

DIFFICULTÉ
Aucune
TEMPS
5 min

Procurez-vous une adresse mail éphémère

La meilleure arme contre la prolifération des spams ? L'utilisation d'une adresse de courriel jetable, valable le temps de vous inscrire aux sites et aux services en ligne. Mode d'emploi.

Protégez votre messagerie habituelle

Lorsque vous souhaitez accéder à un service gratuit, télécharger un livre blanc ou encore un logiciel, il vous est presque systématiquement demandé de fournir une adresse mail. Et vous ne pouvez pas en inventer une de toutes pièces car, pour profiter du produit ou du service convoité, il vous faudra cliquer sur un lien d'activation envoyé par mail. Inutile de divulguer votre adresse principale et subir ainsi un matraquage publicitaire incessant à travers l'envoi de pourriels. Sachez qu'il existe des services gratuits tels qu'AirMail. Pour en bénéficier, connectez-vous sur ***bit.do/dg884***. Cliquez ensuite sur le bouton ***Get Temporary Email***.

1

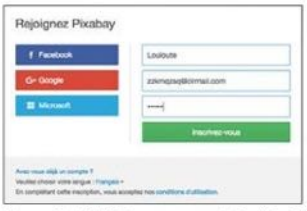
Générez une boîte de réception temporaire

Il ne faut que quelques secondes au service pour vous procurer une adresse mail jetable. Celle-ci s'affiche en surbrillance dans la barre jaune en haut de page. Activez le raccourci clavier ***Ctrl*** + ***C*** (***cmd*** + ***C*** sur macOS) ou choisissez la commande ***Copy to Clipboard*** afin de copier ce lien dans le presse-papiers.

2

3

Utilisez ces coordonnées jetables



Une fois l'adresse temporaire opérationnelle, connectez-vous sur le site qui exige la saisie d'une adresse mail pour finaliser l'inscription, débloquer du contenu premium ou obtenir des liens de téléchargement. Collez l'adresse temporaire générée ainsi. Le message contenant le lien d'activation s'affiche dans la boîte de réception AirMail durant vingt-quatre heures. Passé ce délai, le courriel sera détruit.

4

Obtenez des adresses personnalisées

AirMail n'est pas le seul service de ce genre. Vous pouvez aussi vous tourner vers ***Adresseemailtemporaire.com***. Ce service présente l'intérêt de donner le choix entre plusieurs extensions pour cette adresse provisoire. Sélectionnez celle qui vous convient, puis validez avec le bouton ***Copie*** afin de l'envoyer dans le presse-papiers.

5

Affichez le lien d'activation

Avec Adresse Email Temporaire, vous n'avez même pas de boîte de réception à consulter. Dès que le service auquel vous avez confié cette adresse électronique envoie le message qui abrite le lien d'activation, la page d'accueil qui affiche votre adresse est actualisée. Il ne reste plus alors qu'à activer le lien et à le copier dans la barre d'adresse de votre navigateur Internet. ■

Désactivez votre smartphone à distance

Grâce aux outils de localisation d'Apple et de Google, vous avez une petite chance de retrouver votre téléphone égaré. Dans le cas contraire, il est plus prudent d'effacer les données qu'il contient afin qu'elles ne tombent pas entre de mauvaises mains.

iOS 1

Activez la localisation

Si Apple a conçu tous les outils permettant de retrouver un mobile perdu ou volé, il n'en demeure pas moins qu'il vous revient, en tant qu'utilisateur, d'exploiter au mieux ces dispositifs. En les activant, vous renoncez à la confidentialité de vos déplacements. Quiconque connaît votre Apple ID pourra vous suivre de loin et en temps réel. Il ne faut donc pas agir à la légère ! Si vous vous engagez dans cette voie, prévoyez quelques garde-fous. Accédez à la rubrique ***Confidentialité*** des réglages de votre iPhone. Appuyez alors sur l'étiquette ***Service de localisation*** et placez l'interrupteur en position active.

2

Envoyez ces infos sur iCloud

Une fois la localisation activée, passez en revue l'ensemble des applications susceptibles d'utiliser ces données. Si vous jugez que certaines d'entre elles n'en ont pas l'utilité, n'hésitez pas à les désactiver. Une fois cette opération réalisée, revenez à l'écran d'accueil des ***Réglages***. Touchez l'intitulé ***iCloud*** et activez ***Localiser mon iPhone***, ainsi que l'option ***Envoyer ma dernière position***. Ainsi, en cas de panne de batterie ou d'extinction du mobile, vous obtiendrez au moins une situation récente. De quoi définir un périmètre de recherche.

3

Accédez au suivi de l'iPhone

Vérifiez sur votre ordinateur (PC ou Mac) que tout fonctionne correctement en ouvrant votre navigateur Internet et en vous connectant à ***Icloud.com***. Saisissez vos identifiants Apple puis, une fois sur le service, activez l'icône ***Localiser***.

Lancez la détection

Lorsque vous possédez plusieurs périphériques iOS associés au même compte Apple ID, ils peuvent tous être localisés simultanément. Déroulez la liste ***Tous mes appareils*** pour sélectionner votre iPhone. Ainsi, vous êtes informé du temps écoulé depuis la dernière localisation. Choisissez le bouton ***Actualiser*** afin de rafraîchir les données.

4

Faites sonner le téléphone

Différents modes d'interaction avec l'iPhone volé ou perdu sont envisageables. Ils sont tous réunis dans l'angle supérieur droit de l'onglet du navigateur. La première possibilité consiste à faire sonner le téléphone. Cela paraît étrange, mais si votre iPhone se trouve à proximité, caché sous un coussin, dans une poche ou un sac à main, cela suffira à le repérer. Cette sonnerie se fait entendre y compris si vous aviez activé le mode silencieux. Touchez l'écran du mobile une fois que vous avez remis la main dessus.

5

6

Verrouillez votre appareil où qu'il se trouve

Vous oubliez votre mobile sur la table d'un restaurant et vous n'êtes plus du tout à proximité de ce lieu ? Mieux vaut activer le ***Mode Perdu***. Ainsi, personne ne pourra accéder à ses données ni l'utiliser à des fins personnelles jusqu'à ce que vous le récupériez. Dans le panneau de contrôle d'iCloud, sélectionnez ***Mode Perdu***. Saisissez un numéro de téléphone permettant de vous joindre, lequel s'affichera à l'écran de l'iPhone. Ou alors libellez un message à l'attention de celui qui vous a dérobé le smartphone, afin de le décourager ou même de lui proposer une récompense en cas de restitution. Validez à l'aide de l'intitulé ***Terminé***. L'appareil ne sera ensuite déverrouillé que par votre code PIN.

7

Réinitialisez le mobile pour préserver vos données

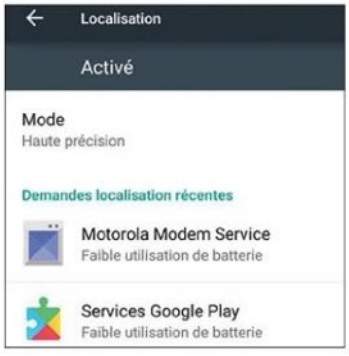
Lorsque vous pensez que les données personnelles stockées sur le téléphone sont en danger, la solution la plus sûre consiste à en effacer le contenu. Sachant qu'il vous sera toujours possible de restaurer l'iPhone (si vous le retrouvez) en récupérant la dernière sauvegarde réalisée avec iTunes ou sur iCloud. Pour procéder à la réinitialisation, optez pour ***Effacer l'iPhone*** et confirmez l'opération. ■

ANDROID

1

Paramétrez la localisation de votre appareil Android

Comme iOS, Android a besoin de votre accord pour pister votre mobile. Assurez-vous d'abord que la fonction de géolocalisation est bien activée. Touchez l'icône ***Paramètres*** sur l'écran d'accueil de l'appareil. Accédez à la rubrique ***Personnel***, effleurez l'intitulé ***Localisation*** et placez l'interrupteur en position ***Active***. Vous êtes désormais paré !



Accédez au gestionnaire de périphériques

Si vous avez besoin de localiser un téléphone ou une tablette Android associé à votre compte Google, il vous suffit de lancer votre navigateur Internet sur un ordinateur et de vous connecter à la page ***bit.do/ddMxf***. Saisissez ensuite vos identifiants (adresse mail et mot de passe). Le processus de localisation est amorcé. La position de l'appareil sera alors épinglée sur une carte avec une marge d'erreur d'environ 20 m.

2

3

Interagissez avec le smartphone

Vous avez plusieurs interactions possibles avec un mobile égaré. Selon la situation, faites-le sonner, verrouillez-le à distance ou effacez son contenu en revenant à la configuration de sortie d'usine. Si vous optez pour la solution du blocage, vous devez définir puis confirmer un nouveau mot de passe, avant de sélectionner ***Verrouiller***. Quand vous voudrez reprendre le contrôle du téléphone, vous entrerez simplement le nouveau code d'accès.

4

Pistez vos proches

Google propose Android Device Manager, une appli mobile dédiée à la gestion de vos appareils. Une fois celle-ci installée, vous localiserez, à partir d'un ordinateur, mais aussi depuis votre téléphone, tout terminal associé à votre compte Google. Un outil très pratique quand vous n'êtes pas chez vous pour vérifier que votre enfant est bien rentré de l'école (via son smartphone). ■

DIFFICULTÉ
Aucune
TEMPS
10 min

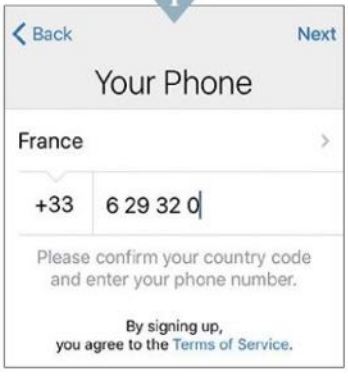
Installez Telegram, l'appli qui chiffre les messages

Vous craignez que vos communications sur Skype ou Messenger soient insuffisamment sécurisées ? Prenez l'habitude d'utiliser Telegram. Cette appli fait transiter vos messages par un tunnel virtuel, rendant ainsi vos conversations impénétrables.

Configurez l'application

Telegram Messenger peut être utilisé aussi bien sur iOS que sur Android. Après l'avoir téléchargé et installé, touchez le bouton ***Start Messaging*** pour la lancer. Indiquez votre pays (pour nous, France) et confirmez votre numéro de mobile. Pressez ensuite le bouton ***Next***. Saisissez le code secret contenu dans le SMS d'activation.

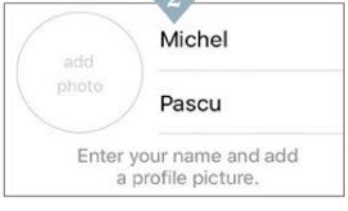
1



Complétez votre profil

L'appli Telegram, conçue pour chiffrer les conversations, oblige toutefois à créer un profil public afin d'identifier des personnes avec qui parler. Saisissez vos nom et prénom, ajoutez éventuellement une photo puis appuyez sur ***Next***.

2



3

Autorisez les notifications

Comme toute messagerie qui se respecte, Telegram Messenger se chargera de vous notifier la réception des nouveaux messages. Afin de bénéficier de ces alertes, effleurez le bouton ***Autoriser*** quand l'appli suggère l'usage des notifications. Si vous vous en servez sur un iPhone, vous pouvez l'associer à Siri. Ainsi, vous dicterez vos messages à l'assistant vocal d'iOS. La configuration est terminée.

4

Lancez une discussion

Pour commencer à converser, activez le bouton ***Contacts***. Sélectionnez le nom de votre interlocuteur (il faut évidemment qu'il recoure lui aussi à cette même application). Si c'est le cas, l'heure de sa dernière connexion au service s'affiche. Il ne vous reste plus qu'à saisir votre message de manière tout à fait classique.

Répondez aux messages et gérez les conversations

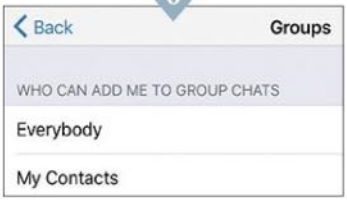
Telegram Messenger s'utilise comme n'importe quelle appli de SMS ou de tchat. Textes et conversations (dans leur intégralité) sont effaçables à tout moment. Pour ce, effectuez un appui prolongé sur le message, puis exécutez la commande ***Delete***.

5

Filtrez les utilisateurs

Si vous êtes habitué à Messenger ou à Message, vous ne serez pas dépaysé. Sachez que n'importe quel utilisateur de l'appli peut vous inviter à rejoindre une conversation. Afin d'éviter les mauvaises rencontres, pressez l'icône ***Settings***. Activez la rubrique ***Privacy and Security***, ***Groups*** et remplacez ***Everybody*** par ***My Contacts***. ■

6



DIFFICULTÉ
Aucune
TEMPS
10 min

Refusez que vos applis fouinent dans vos données

Si nombre d'applications vous sont proposées gratuitement, en contrepartie, leurs éditeurs exploitent vos infos personnelles pour les monétiser. Vous pouvez accepter la règle du jeu, la refuser, ou encore tenter d'y voir un peu plus clair.

Faites le point sous iOS

Pour tenter d'identifier les applications qui tirent parti des informations de votre iPhone ou de votre iPad, touchez l'icône ***Réglages***, puis l'intitulé ***Confidentialité***. Sélectionnez un service ou un type de données (contacts, calendriers, photos, localisation, etc.) afin d'afficher la liste des applis qui vont chercher. Si vous utilisez Voyages-SNCF, par exemple, sachez qu'il va farfouiller dans votre calendrier...

1

Ne laissez pas la marque à la pomme croquer vos infos

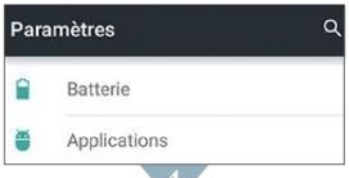
Apple analyse vos activités et collecte des données qui sont utilisées avant tout à des fins d'amélioration. Il n'en demeure pas moins que celles-ci vous appartiennent et que vous avez le droit d'en refuser l'envoi. Dans ***Réglages***, ***Confidentialité***, pressez ***Diagnostic et utilisation***, puis cochez ***Ne pas envoyer***.

2

3

Modifiez les autorisations des applications

Nous n'avons traité que les données et applications propres à iOS. Pour dresser un état des lieux des autres applis installées sur l'appareil, allez dans ***Réglages***, parcourez le volet gauche de l'écran et sélectionnez une app dans la liste. Vous visualisez alors les privilèges qui lui sont accordés. Utilisez les interrupteurs pour révoquer certaines permissions.



4

Effectuez un audit des applis pour Android

Afin de vérifier les autorisations associées aux applications installées sur votre appareil Android, déployez le volet des ***Paramètres rapides*** et activez l'icône en forme d'***engrenage***. Déroulez la liste des rubriques de la page ***Paramètres*** et appuyez sur l'intitulé ***Applications***.

Parcourez les autorisations

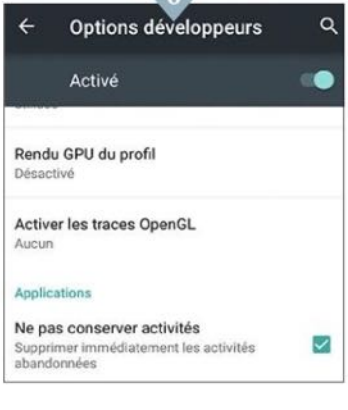
Choisissez une appli dans la liste alphabétique (***Dropbox***, par exemple). Effleurez la ligne ***Autorisations***, pressez les ***trois points*** dans le coin supérieur droit de l'écran puis ***Toutes les autorisations***. L'ensemble des privilèges accordés à cette appli s'affichent alors. Tous ne peuvent pas être révoqués. Revenez en arrière pour découvrir les paramètres modifiables.

5

Rendez Android un peu moins indiscret

Certains éléments sont stockés par Android par défaut, comme l'historique des activités menées sur vos applis. Si vous souhaitez restaurer un peu de confidentialité, touchez ***Options pour les développeurs*** dans le panneau ***Paramètres***. Faites défiler les options jusqu'à ***Applications*** et cochez la case ***Ne pas conserver les activités***.

6



DIFFICULTÉ
Aucune
TEMPS
5 min

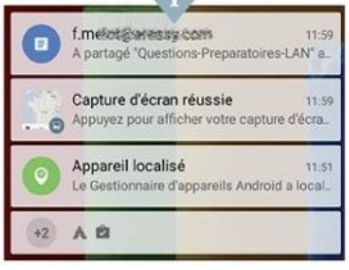
N'affichez pas d'infos perso sur l'écran de verrouillage

Quel confort de pouvoir découvrir les notifications sans avoir à déverrouiller son téléphone ! Mais quel risque également, puisque toute personne à côté de vous a la possibilité, elle aussi, de les consulter. Mieux vaut privilégier la sécurité.

Mesurez l'étendue du problème

Effectuez ce simple test. Laissez votre smartphone dans un coin pendant trente minutes. Lorsque vous revenez, appuyez sur le bouton pour le faire sortir de veille. L'écran verrouillé affiche quelques lignes des derniers mails et SMS reçus, la liste des appels manqués, ainsi que vos rendez-vous. Des données en libre-service pour quiconque passe devant votre mobile.

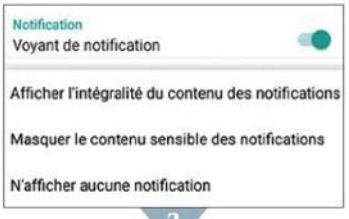
1



Limitez les notifications

Si vous vous servez d'un smartphone Android, vous pouvez modifier la configuration par défaut, qui privilégie trop nettement le confort d'utilisation à la sécurité. Touchez pour cela l'icône des ***Paramètres*** sur l'écran d'accueil du mobile. Parcourez les rubriques jusqu'à ***Appareil*** puis appuyez sur l'intitulé ***Sons et notifications***.

2



3

Réglez les alertes sur la page d'accueil...

Le problème des notifications ne se pose finalement que lorsque l'écran est verrouillé. Dans le cas contraire, on peut supposer que vous avez votre smartphone en main et qu'il y a peu de risques que quelqu'un consulte les informations affichées. Effleurez la commande ***Si l'appareil est verrouillé*** et activez l'option ***N'afficher aucune notification***. Vous pouvez également empêcher certaines applis d'en émettre.

4

... et paramétrez-les vous-même à la place d'iOS

Sous iOS, la personnalisation de l'affichage des notifications en cas de verrouillage répond à la même logique. Sur l'écran d'accueil, choisissez ***Réglages***. Parcourez la liste des intitulés et pressez ***Notifications***. Toutes les applis susceptibles de générer des alertes sont réunies.

Configurez Messages

Avec les SMS, naturellement courts, le contenu de l'alerte suffit souvent à connaître la teneur de la conversation. Pour éviter tout regard indiscret, touchez l'intitulé ***Réglages***, ***Notifications***, ***Messages***, puis placez l'interrupteur ***Afficher sur l'écran verrouillé*** en position inactive. Faites de même avec d'autres applications si besoin.

5

N'oubliez pas d'utiliser le Centre de contrôle

Par défaut, cette fonction est également accessible depuis l'écran de verrouillage d'iOS. Cette dernière offre la possibilité d'accéder à des fonctionnalités comme la recopie vidéo ou l'appareil photo. Elle sert aussi à savoir quelle musique vous écoutiez. Dans ***Réglages***, appuyez sur ***Centre de contrôle*** et désactivez ***Accès sur écran verrouillé***. ■

6

DÉVELOPPEZ 10 FOIS PLUS VITE

WINDEV®

[2017]

922 NOUVEAUTÉS

WINDEV 22 : ATELIER DE DÉVELOPPEMENT PROFESSIONNEL, COMPLET EN STANDARD

Gestion du cycle de vie complet: Idée, Conception, Développement, Génération, Déploiement, Exploitation • Un code multi-plateformes Windows, Linux, Java, Internet, Mobiles • Environnement ALM complet • Toutes les bases de données sont supportées, Big Data • Inclus: HFSQL, base de données locale, Client/Serveur, cluster, embarquée et cloud • Puissant RAD • Intégration continue • Tableau de bord de vos applications • Audit statique & dynamique • Générateur de fenêtres (UI) visuel & intuitif • Utilisation facile de charte graphique • Héritage et surcharge d'interface • Tous les champs (contrôles) sont très puissants et livrés en standard: Champ de saisie, Tableau croisé dynamique (cube), Champ Planning, Champ Diagramme de Gantt, Champ Tableau de bord, Champ Table, Champ Graphe, etc • FAA: chaque application bénéficie automatiquement de Fonctionnalités Automatiques: export vers Excel, vers Word, envoi d'email, etc • Sécurité : Mot de passe de vos applications • Puissant générateur de rapports et codes-barres • Langage de 5ème génération: WLangage • Editeur de code intuitif avec puissant débogueur • Tests unitaires et tests automatiques • Versioning (GDS/SCM) • Webservices SOAP et Rest • Modélisation Merise et UML • .NET, 3-Tier, MVP • Support de tous les standards: XML, USB, Bluetooth, NFC, J2EE, OLE, ActiveX, RPC, SaaS, SMTP, FTP, OPC, DLNA, IoT, Sockets, API, Webservices... • Lien avec Lotus Notes, SAP, Google, Outlook • Multimédia, Domotique • Livré avec des centaines d'exemples et d'assistants • Génère le Dossier technique d'un clic • Télémétrie pour connaître l'utilisation réelle de vos applications • Générateur d'aide • Support de 64 langues étrangères par application • Générateur de procédures d'installation: local, CD, USB, Internet, Réseau, Push... • Gestion des suggestions et incidents utilisateurs • Support Technique Personnalisé Gratuit* • ... • Robot de surveillance: surveillez vos applications

CONSULTEZ PLUS DE 100 TÉMOIGNAGES DE PROFESSIONNELS SUR LE SITE PCSOFT.FR

Elu
«Langage le plus productif du marché»

VERSION EXPRESS GRATUITE
Téléchargez-la !

Windows - Linux - Mac - Internet - iOS - Android

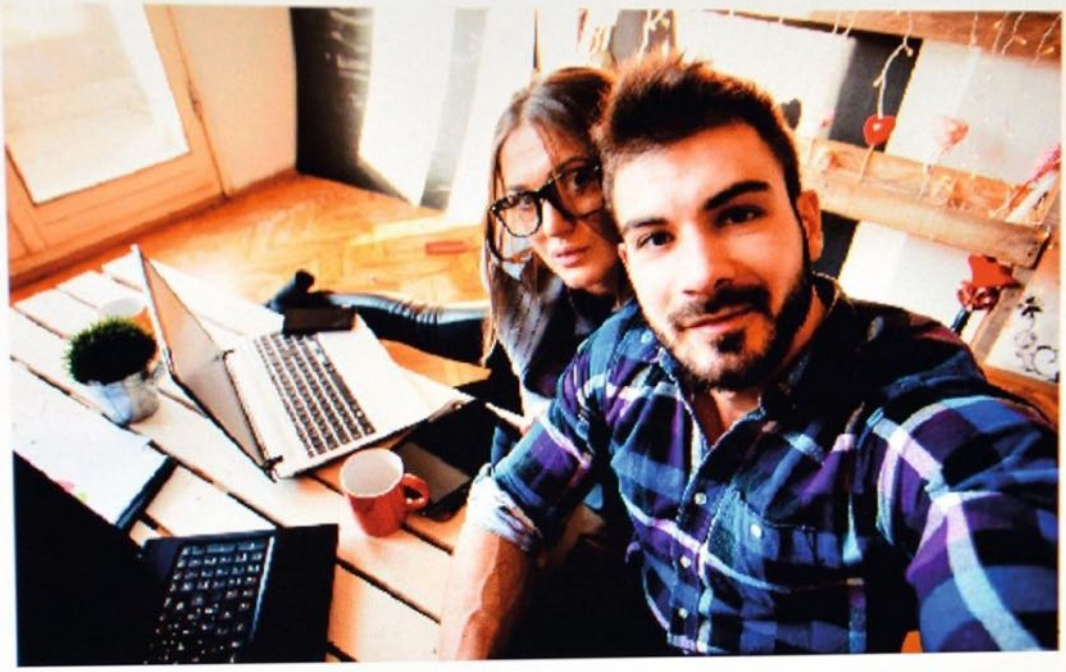
VU À LA TÉLÉ EN 2017
SUR **TF1**, SUR **BFMTV** ET SUR **M6**

Logiciel professionnel. * 15 requêtes gratuites sur la version en cours de commercialisation

Tél Paris: 01 48 01 48 88 *Tél Montpellier: 04 67 032 032*

Plus de 100 témoignages **WWW.PCSOFT.FR**

@bim_x_BadaBim a ajouté 1 nouvelle photo.
il y a 4 minutes



J'ai fini l'install de #Securitoo. Résultat : 2 PC, 2 smartphones et 1 tablette protégés. Merci @NordnetOFFICIEL ! #ProtectionAuTop #SécuritéMultiDevices

#Securitoo

Nordnet, votre expert en sécurité sur Internet…

Virus, hameçonnage, ver, usurpation d'identité, vol de données bancaires… Pour vous prémunir au quotidien contre **les nombreuses menaces sur Internet**, attachez-vous les services d'un expert ! Notre gamme **Securitoo regroupe toutes les protections fondamentales** pour évoluer plus sereinement sur Internet : antivirus, pare-feu, antispam, sécurisation de la navigation et des données privées, etc.

Avec Securitoo, nous vous apportons immédiatement des solutions performantes sur PC, Mac, smartphones et tablettes Android™.

Pour votre protection, nous sommes sur tous les fronts.

3420 (appel non surtaxé)
www.nordnet.com

.nordnet.
nos solutions Internet vous ouvrent le monde

Ce post est fictif. Toute ressemblance avec une personne réelle serait une pure #coïncidence.