N°46

Sept. / Nov. 2020

Casser les codes et décrypter l'info

PIRATE INFORMATIQUE

ANONYMAT

LES SMARTPHONES DE LA MAFIA RÉVÈLENT LEURS SECRETS

TOP 3 DES OUTILS ANTIPLAGIAT

LE GUIDE DU PIRATE

100 % PRATIQUE

VIDÉO

Comment FLOUTER facilement un OBJET ou VISAGE ?

DEEPFAKES AUDIO

IMITER DES VOIX GRÂCE À L'INTELLIGENCE ARTIFICIELLE

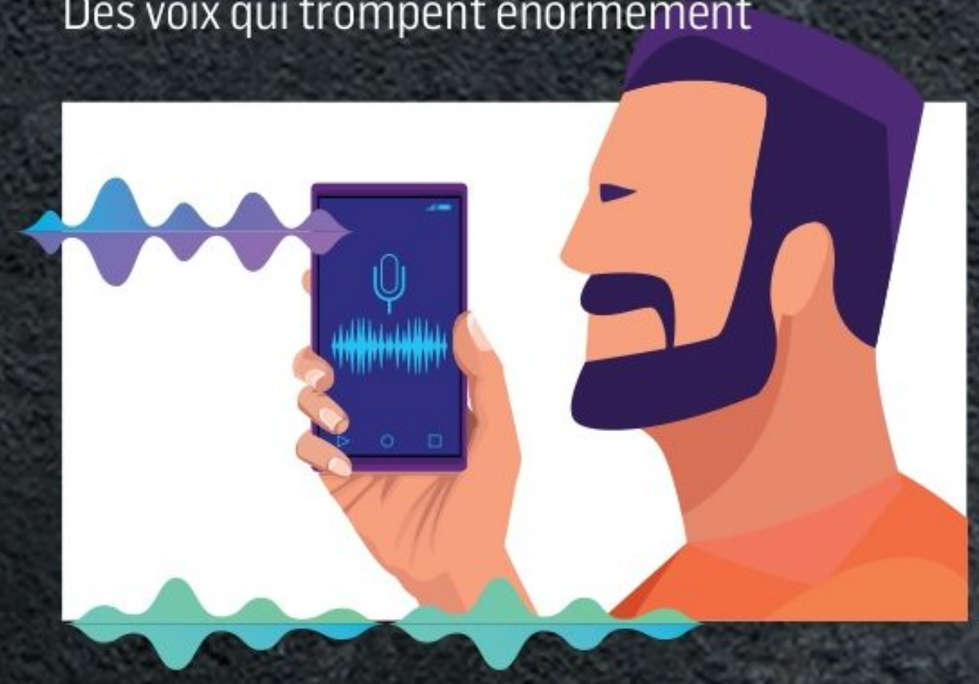
BLACK DOSSIER

Messageries & Réseaux sociaux :

QUI VOUS PROTÈGE ?
QUI SONT LES CANCRES ?

SOMMAIRE

HACKING



ANONYMAT

SOUTENEZ-NOUS !

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

PROTECTION

MULTIMÉDIA

PIRATE INFORMATIQUE

N°46

Septembre / Novembre 2020

Une publication du groupe ID Presse.
Impasse de l'Espéron - Villa Miramar
13960 Sausset Les Pins
E-mail : pirate@idpresse.com

Directeur de la publication :
David Côme

Rédacteurs : Alicia Aloisi, Fabrice Brochain, Marie-Hélène Léon

Maquettistes : Sergei Afanasiuk et Stéphanie Compain

Correctrice : Marie-Line Bailleul

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

Distribution : MLP

Dépôt légal : à parution

Commission paritaire : 0722 K 94236

ISSN : 1969 - 8631

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

Parution : 4 numéros par an.

ÉDITO

BONJOUR AUX HABITUÉS COMME AUX NOUVEAUX VENUS !

Vous ne vous doutez de rien mais beaucoup de choses évoluent en coulisses chez Pirate Informatique. En premier lieu, Benoît quitte la rédaction pour de nouvelles aventures. C'est lui qui apportait ses connaissances et son expertise indispensables, après 10 années passées à travailler pour le magazine. Il était aussi en charge des secrets de sa fabrication, des premières idées de sujets jusqu'à sa livraison chez l'imprimeur. Bons vents à lui !

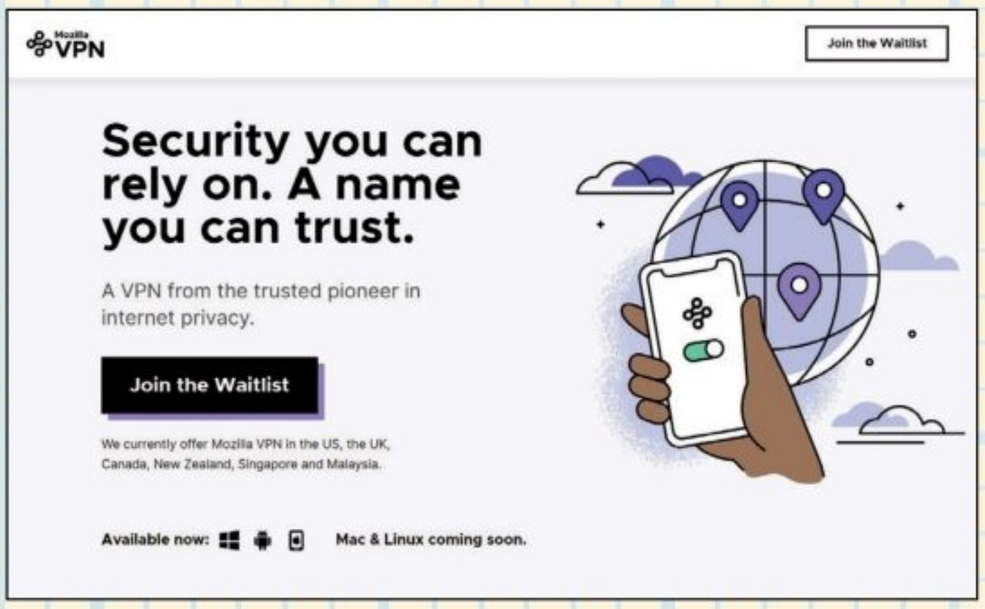
Et puis une surprise est aussi arrivée par la Poste cet été : après 10 ans de refus, Pirate Informatique est enfin reconnu comme un titre de presse à part entière par le Ministère de la Culture (avant, nous n'étions que de dangereux pirates! Comme quoi les mentalités évoluent autour de la culture hacking. À moins que ce ne soit une erreur ??). Un gros enjeu pour nous puisque nous pouvons désormais vous proposer des abonnements à tarifs préférentiels ! Un levier important pour assurer la pérennité et l'indépendance de votre magazine.

Alors, abonnez-vous comme dirait l'autre !

La rédaction

FIREFOX EN DANGER: UN VPN POUR SE RELANCER ?

Le 11 août, Mitchell Baker, la CEO de Mozilla Corporations, annonçait le licenciement prochain de 250 collaborateurs (environ 25 % des effectifs). Le Covid19 et la baisse globale des revenus publicitaires sur le Web pendant le confinement auraient accéléré les difficultés d'un modèle économique déjà fragile (70 employés avaient été remerciés dès janvier dernier).



Firefox espère trouver son salut dans la vente de solutions et services qui s'appuieront sur le savoir-faire et l'image de marque de l'entreprise (sécurité, respect de la vie privée et position de challenger éthique). Ont déjà été présentés : un Mozilla VPN en cours de déploiement (4,99 $ /mois) ; Hubs, un service de discussion en réalité virtuelle ; et le rachat de l'application Pocket. D'autres annonces sont attendues ces prochains mois.

RUMEUR

ENLÈVEMENTS À L'AIDE DE ROSES GÉOLOCALISÉES : NON

Cet été, une rumeur est vite devenue virale chez nos voisins Belges. À Bruxelles, des vendeurs de rue étaient censés s'être spécialisés dans la distribution à des jeunes filles de roses équipées de GPS. L'objectif : pouvoir les suivre à la trace... pour mieux les enlever une fois localisées dans un endroit calme, peu fréquenté et discret. Trafic d'organe, trafic sexuel, etc. Tout y est passé. Bien sûr, cette rumeur ne reposait sur rien de réel mais tous les ingrédients d'une légende urbaine étaient réunis. L'infox est partie d'un simple tweet pas très clair et rapidement effacé.
Les réseaux sociaux ont fait le reste. Avant que la police n'intervienne pour siffler la fin de la récréation en indiquant que jamais un tel mode opératoire n'avait été observé.

LE CHIFFRE

13,7 MILLIONS DE $

De juillet 2019 à juin 2020, Microsoft a versé près de 14 millions de dollars en primes pour ses différents programmes de recherche de failles (appelés « Bug Bounty »). C'est trois fois plus que l'année passée (4,4 M$).1226 vulnérabilités ont été détectées par les hackers participants. La prime la plus élevée s'est montée à 200 000 $. Microsoft a déclaré que la crise du Covid19 avait certainement permis à de nombreux hackers de consacrer plus de temps à ces recherches de vulnérabilités, ce qui expliquerait en partie cette progression.

LE HACKER, L'INVESTISSEUR RUSSE ET LE PORTEFEUILLE CRYPTE

Début août, Michael Stay, ancien expert en cybersécurité de Google, nous racontait une belle histoire sur sa chaîne YouTube. Ce hacker passionné et aujourd'hui directeur technique de Pyrofex Corp se rappelle de sa rencontre avec un investisseur russe.

Un pactole de 300 000 $ en Bitcoin, protégé par mot de passe et devenu inaccessible : l'ancien expert de Google relève le défi

Ce dernier s'adressait à lui en dernier recours après avoir découvert des publications de Stay sur le piratage de fichiers Zip chiffrés. Et on comprend pourquoi : il possédait lui même un fichier Zip protégé dont il avait perdu le mot de passe... et qui contenait 300 000 dollars en Bitcoin !

Michael Stay revient sur sa chaîne YouTube sur un crackage de mot de passe mémorable.

En 2016, cet investisseur avait acheté pour 10 000 $ de Bitcoin. Prudent (il a raison), il décide de protéger son magot dans une archive chiffrée et de laisser fructifier son pécule. Et comme cela arrive parfois, quelques temps plus tard, impossible de se rappeler de son mot de passe. Les mois puis les années passent, la valeur du Bitcoin s'envole et notre investisseur devient fou en lorgnant ce maudit dossier impossible à ouvrir ! Stay accepte le défi.

BELLE RÉCOMPENSE

Pour casser le verrou, le hacker a développé un programme qui injectait différentes combinaisons de mots de passe et a pu bénéficier des ressources techniques de sa société (pour un coût estimé de 7000 $). Heureusement, le logiciel d'archivage n'avait jamais été mis à jour depuis 2016, ce qui a permis à Stay de récupérer les identifiants en seulement quelques jours d'injection. En récompense, l'investisseur anonyme russe a offert 100 000 $ au gentil hacker pour ses services.

En Bref...

DROPBOX TESTE LE CHIFFREMENT DE VOTRE COMPTE

Dans quelques mois, vous devriez sans doute disposer d'un login et mot de passe offrant une

solution native de chiffrement pour votre compte Dropbox et son contenu. Une gestion synchronisée multi-terminaux est prévue. L'entreprise a testé cet été ce dispositif auprès d'utilisateurs Android et iOS (sur invitation uniquement).

CYBERSÉCURITÉ : LE SECTEUR NE CONNAÎT PAS LA CRISE

70% des entreprises manquent de spécialistes en sécurité informatique, indique une enquête mondiale menée par l'ESG, l'ISSA et l'ISC. Cette enquête affirme que 4 millions de postes seraient en souffrance. En cause ? Pas assez de spécialistes formés et des professions mal connues donc mal intégrées par les entreprises. Avec, à la clé, des perspectives de carrières peu claires et un manque de formation continue. En clair, il faudrait commencer par recruter un DRH expert en cybersécurité pour bien identifier les besoins, trouver les bons profils et former en interne !

SITES PORNOS :

BIENTÔT LA GUERRE DES BOUTONS

Empêcher les mineurs d'accéder à du contenu pornographique en ligne. C'est la volonté du président de la République que va tenter de faire appliquer le gouvernement à l'aide d'une nouvelle loi soumettant les sites de charme à un contrôle drastique à l'entrée.

Il va bientôt falloir un peu plus qu'un simple clic sur le bouton « J'ai plus de 18 ans » pour accéder au contenu d'un site porno.
En juin dernier, le Sénat a en effet adopté la loi contre les violences conjugales dans laquelle figure un amendement visant à circonscrire le droit d'entrée aux sites pour adultes… aux seuls adultes, justement. Obligation donc de justifier de son âge d'une manière ou d'une autre avant d'ouvrir la boîte à fantasmes.
Reste à mettre en place les méthodes de filtrage. Et c'est ici que l'on s'aventure en terrain glissant. Première piste envisagée, le recours à la carte bancaire. En France, il est possible de disposer de ce moyen de paiement à partir de 16 ans (c'est mieux que rien). Encore faut-il avoir assez confiance pour livrer ses données sensibles à des sites Web dont on ne connaît que la façade.

Nombre d'entre eux représentent la machine à cash d'entreprises obscures hébergées dans des paradis fiscaux et détenues par des mafias. Décliner son identité et ses données bancaires à des inconnus aux activités douteuses a de quoi calmer les ardeurs.

ET AVEC L'AVAL DE L'ÉTAT ?

Deuxième piste, le recours au système France Connect. Ce dernier, principalement utilisé pour l'accès aux divers sites de services publics comme celui de l'administration fiscale (impots.gouv.fr) ou de la Sécurité Sociale (ameli.fr) affiche de bonnes garanties et est technologiquement au point.
Mais se dressent ici deux obstacles. D'abord, même si l'on certifie que tout ce qui se passe sur le site X reste sur le site X, les cloisons soi-disant étanches recèlent toujours des failles et les dérives sont faciles à envisager. Alors rajouter à la base de données de l'état, déjà bien fournie, des informations sur vos tendances et préférences sexuelles n'a rien de très excitant. Ensuite, on imagine assez mal la Marianne, symbole de la république française, monter la garde à l'entrée d'un site porno et donc, cautionner sa visite.

LES FRANÇAIS PAS SI CHAUDS

Résultat, les français ne sont pas très chauds pour tomber le masque. Dans une étude Ifop pour le magazine « La voix du X » réalisée mi-juin[1], aucune de ces solutions ne semble leur convenir. Et pour 57 %

Notre Marianne montant la garde devant les sites pornos les plus populaires comme sur ce montage ? Le gouvernement n'assume pas et on le comprend.

des interrogés, devoir décliner son identité pour consulter un site porno constitue même une atteinte à la vie privée. C'est mal parti.

À DEUX DOIGTS DE LA RÉUSSITE

Et si la France s'inspirait du modèle britannique sans toutefois commettre les mêmes erreurs ? Car nos voisins d'outre-Manche tentent déjà depuis près de cinq ans de trouver la parade (sans y être encore parvenus). Par exemple, vendre - chez les buralistes ou les supermarchés - un pass certifiant que son possesseur est bel et bien majeur. Avec le risque qu'en peu de temps, le marché noir regorge de ce type de carte. Autre solution : confier la réalisation d'un système d'identification multiplateforme en ligne à une entreprise privée dotée d'un solide savoir-faire en matière de sécurité et de vie privée sur le Web.

YOUPORN PROPOSE SA TECHNOLOGIE : AGEID

MindGeek a proposé ses compétence en faisant la promotion de sa solution AgeID. Un compte, évidemment chiffré, contenant peu d'informations personnelles sur son détenteur (vérifiées au préalable auprès d'un tiers à l'aide d'une pièce d'identité) et surtout la certification qu'il a plus de 18 ans. Proposition alléchante… sauf que MindGeek n'est autre que la holding qui règne sur le marché du porno avec des sites comme YouPorn, PornHub ou encore RedTube. Le manque de transparence de la société, la polémique sur l'origine des vidéos publiées et, surtout, la méfiance de ses petits concurrents ont eu raison du projet.

DORCEL SE FROTTE LES MAINS

Contraignante pour les éditeurs de sites X gratuits, l'obligation de s'identifier fait cependant le bonheur des mastodontes du marché, à commencer par Dorcel. Le spécialiste du porno est dans les clous puisque l'accès à son site est déjà payant à travers l'enregistrement d'une carte bancaire. L'entreprise établie en France depuis 1979 profite d'une bonne notoriété et pourrait séduire les sceptiques de l'identification obligatoire sur des sites moins connus. Une bonne manière d'évincer une concurrence gratuite. Gregory Dorcel, fils de Marc et directeur des productions de l'entreprise, a d'ailleurs été auditionné par la commission des lois du Sénat.

Par ailleurs, parmi les articles concernant la politique de confidentialité d'AgeID, on peut lire : « Nous ne partageons pas vos données personnelles avec des tiers ni ne leur permettons d'y accéder, sauf… dans la mesure où cela est nécessaire pour remplir tout autre objectif non mentionné ci-dessus pour lequel vous avez fourni des données personnelles ». Pas très rassurant.

Sites pornos : comment interdire l'accès au moins de 18 ans sans mettre en danger la vie privée et les données des utilisateurs ?

SECRET DE POLICHINELLE

Néanmoins, le système a de quoi inspirer. En confiant la tâche à une entreprise sérieuse (et sans lien avec le monde du X pour éviter tout conflit d'intérêt) l'État pourrait assurer le filtrage des sites de charme sans pour autant s'impliquer et ne se manifester que lorsque la loi n'est pas respectée. Les sanctions sont déjà prévues. Au Conseil Supérieur de l'Audiovisuel (CSA) de se mettre en branle pour adresser une mise en demeure aux sites qui ne sont pas rentrés dans le rang. Ils auront quinze jours pour se conformer aux nouvelles règles. Passé ce délai, ils pourront se voir déréférencés par les moteurs de recherche et interdits d'accès par les FAI français. Reste que ces mesures pourraient ne pas suffire. Les éditeurs de logiciels de VPN se frottent déjà les mains. Ils imaginent cet âge d'or ou chacun se réfugiera, grâce à eux, derrière une adresse IP fictive, située hors du territoire français, pour accéder comme auparavant à ses sites chauds dans sa région.

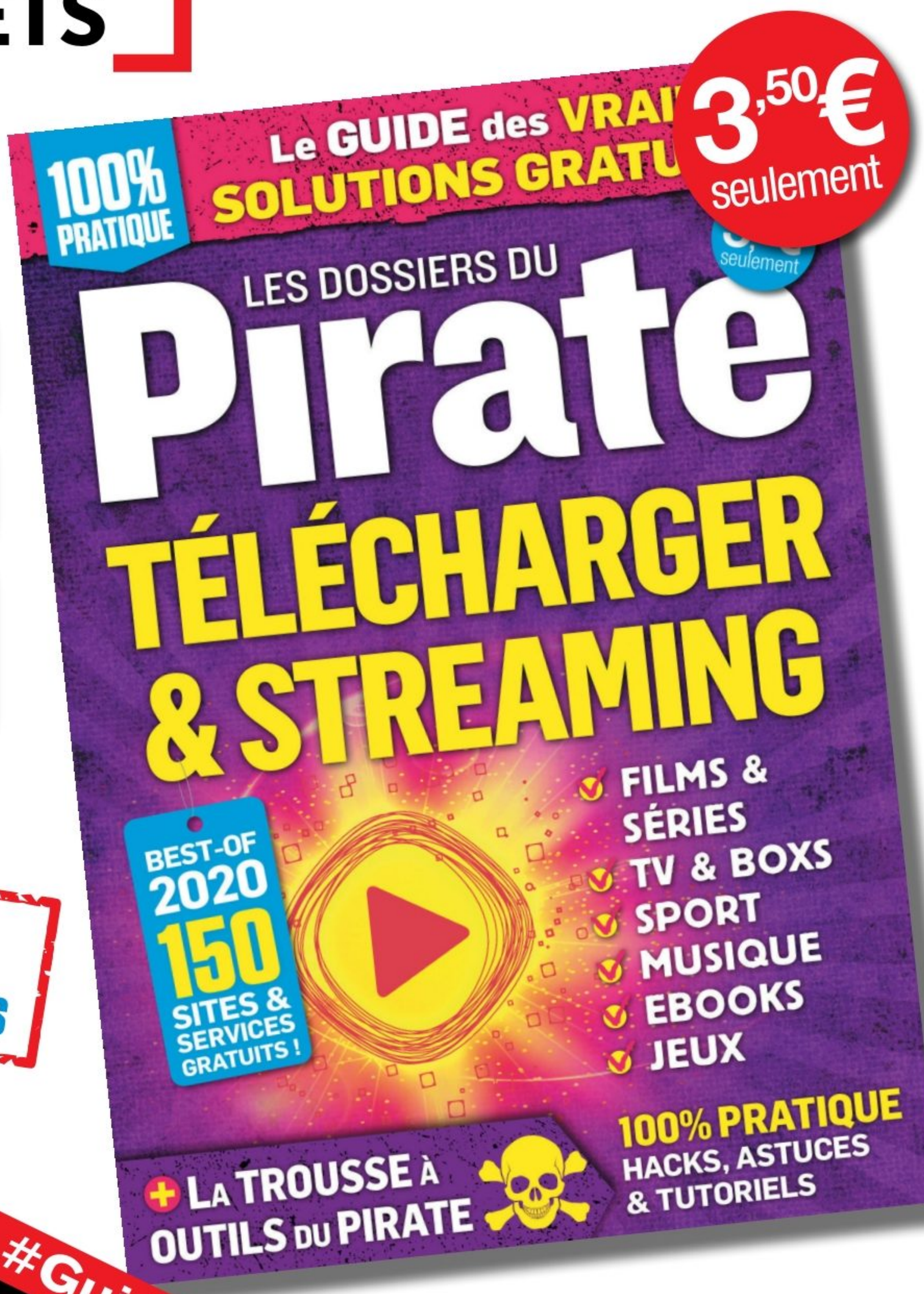
(1) Etude Ifop pour le magazine « La voix du X » réalisée par Internet du 17 au 18 juin 2020 auprès d'un échantillon national représentatif de 1 020 personnes âgées de 18 ans et plus. **https://cutt.ly/FsWwdxT**

LES DOSSIERS DU Pirate

DES DOSSIERS THÉMATIQUES COMPLETS

À DÉCOUVRIR EN KIOSQUES

- PETIT FORMAT
- MINI PRIX
- CONCENTRÉ D'ASTUCES



100% Windows

Actuellement #Guide pratique

BEST-OF 2020

CERTAINES VOUS PROTÈGENT
D'AUTRES SAVENT TOUT DE VOUS

POURQUOI IL FAUT PASSER AUX MESSAGERIES CHIFFRÉES

Vos messages et échanges de contenus disent tout de vous, de vos habitudes et de votre vie privée. Il n'est pas normal que des messageries et réseaux sociaux conservent en clair et aient accès à vos données sur leurs serveurs. Traçage marketing, profilage, surveillance, piratage, danger démocratique : il faut exiger le chiffrement de bout en bout de tous ces services. Comment ça marche ? Quels sont les bons élèves, qui sont les cancres ?

RÉSEAUX SOCIAUX
ET MESSAGERIES

Après le scandale Twitter, IL FAUT GÉNÉRALISER

LE CHIFFREMENT DE BOUT EN BOUT

Twitter traîne les pieds depuis des années pour proposer un chiffrement de bout en bout des échanges et données de ses utilisateurs. Comme d'autres réseaux sociaux et messageries. Et il vient une nouvelle fois d'en subir les conséquences cet été avec un piratage majeur. Un cas d'école qui doit pousser le législateur à imposer cette technologie. Mais demander à un gouvernement d'imposer la protection des échanges entre citoyens ne va pas de soi...

En juillet dernier, Twitter et ses utilisateurs faisaient les frais d'un scandale qui devrait imposer le chiffrement de bout en bout de tous les échanges sur les messageries et réseaux sociaux. L'objectif affiché: récupérer les identifiants de comptes de personnalités influentes et les utiliser pour une arnaque au Bitcoin auprès des autres utilisateurs Twitter.
Des pirates sont parvenus à piéger plusieurs employés de Twitter pour obtenir l'accès à un outil interne à l'entreprise. Si la technique utilisée n'a pas été révélée, on opte bien sûr pour de l'ingénierie sociale. Le profil et l'historique du suspect principal, Graham Clark , diaboliquement doué pour la manipulation et l'arnaque à seulement 17 ans, plaide pour cette hypothèse, en dehors de toute complicité interne.

LES COMPTES DE OBAMA ET BIDEN PIRATÉS

Selon la plateforme Blockchain.com qui inspecte les transferts de cryptomonnaie, ce piratage retentissant n'a pas permis de récupérer des sommes folles, on parle de12,58 bitcoins soit un peu mois de 100 000 euros.

UNE FAILLE HUMAINE. ENCORE.

En novembre dernier, Twitter se faisait déjà taper sur le bec : deux de ses anciens employés, corrompus par l'Arabie Saoudite, étaient parvenus à fournir des informations personnelles sur des utilisateurs du réseau social qui postaient des messages critiques à l'égard du régime saoudien. «*Derrière les machines il y a des humains, qui peuvent avoir accès à nos messages privés et aux informations que l'on y dépose. Ces systèmes ne sont pas clos, tout ce qu'on y échange peut être accessible*», rappelle à l'AFP Gérôme Billois, expert en sécurité. Le chiffrement de bout en bout n'est pas une lubie de paranoïaque : le chiffrement des échanges qu'il implique est aujourd'hui la solution la plus aboutie, simple et maîtrisée pour éviter que le facteur humain ne fasse planer un risque permanent sur la sécurisation de nos comptes et messageries.

Scandale Twitter : « Simple » arnaque au bitcoins ou les élections américaines en ligne de mire?

Mais les hackers sont parvenus à cibler des comptes de personnalités comme Barack Obama, Joe Biden, Elon Musk, Kanye West ou Jeff Bezos parmi une centaine d'autres. Ils ont réussi à en prendre le contrôle et les utiliser pour diffuser leur arnaque. Les messages privés de nombreux comptes ont également été consultés et récupérés par les hackers. Un piratage qui embarrasse donc au plus haut point Twitter et qui démontre une nouvelle fois qu'une technologie, aussi sécurisée soit-elle, présente toujours une faille majeure dès lors qu'un humain peut avoir accès à des données et à des contenus non chiffrés.
Le fait que des personnalités de premier plan, dont l'ancien Président Obama et le candidat démocrate à l'élection présidentielle américaine, Joe Biden, aient pu se faire pirater leurs comptes Twitter si facilement par un gamin de 17 ans semble tout simplement irréaliste en cette année d'élection outre-atlantique.

MESSAGERIES : PRÉSERVER CET ESPACE INTIME

Le grand public a aussi compris que tout le contenu de ses échanges sur Twitter (mais aussi sur Skype, Instagram, Facebook, etc.) est stocké en clair sur les serveurs des GAFA.
Cet intime ne doit pas être marchandé à des fins marketing. Les messageries abritent ce qui est au plus prêt de notre personnalités : envies, espoirs, projets, amours, sexe, famille, ... Il n'est pas sain que ces contenus soient accessibles à des entreprises devenues les plus grandes prédatrices de big datas. Rendez-nous au moins cet espace de liberté protégée. À défaut du reste.
Et si nous vivons aujourd'hui sous un régime étatique relativement protecteur et peu intrusif, cela ne dure jamais pour l'éternité. Pour notre avenir proche, pour ceux qui - déjà à l'étranger - sont persécutés et traqués sur les réseaux sociaux et messageries, il faut passer au chiffrement de bout en bout. C'est aussi un devoir démocratique essentiel.

GRAHAM CLARK RATTRAPÉ PAR LA POLICE DU KARMA

Graham Clark, un jeune homme de 17 ans issu de Floride, est l'accusé principal dans l'affaire du piratage de Twitter. Pas son coup d'essai puisqu'il a démontré tous ses talents en ingénierie sociale depuis ses... 15 ans. Arnaques sur Minecraft, vols de comptes Bitcoins, etc. Pas besoin de matériel espion, pas besoin de coder : le lycéen est doué pour convaincre la bonne cible de prendre la mauvaise décision. Très doué.
Et ironie, quand tu nous tiens : c'est sous requête des enquêteurs que des preuves ont été récoltées contre lui sur Discord. La plateforme ne chiffrant pas ses contenus (!!!), les logs et échanges de Graham avec ses complices ont pu être récupérés sous demande du FBI sur les serveurs de l'entreprise. L'œuf, la poule, tout ça. Débat compliqué, n'est-il pas ?

SI OBAMA ET KANYE WEST TE PROPOSENT DES BITCOINS PAS CHERS PRÈS DE CHEZ TOI ET QUE TU Y CROIS, TU ES SOIT TRÈS NAÏF, SOIT TRÈS CUPIDE, SOIT UN PEU LES DEUX.

SIGNAL, WHATSAPP, TELEGRAM, ETC.

ÊTES-VOUS PROTÉGÉ ?

Messageries chiffrées : comment ça marche, ce qui est protégé, ce qui ne l'est pas… et ce que l'on ne vous dit peut-être pas.

En pratique, lors d'une conversation chiffrée de bout en bout entre utilisateurs, toutes les données sont chiffrées entre l'émetteur et le récepteur. Si un tiers réussissait à intercepter ou à accéder à ce contenu entre les deux machines communicantes (PC, smartphones, serveur, etc.), il ne « verrait » qu'une suite de caractères incohérente, chiffrée généralement en 128, 192 ou 256 bits. Le standard AES256, hier réservé à des usages militaires (!) est aujourd'hui le système d'encryption le plus répandu. Théoriquement, ces chiffrements de haut niveau rendent impossible à reformuler « en clair » ces données. Cela peut être vrai pour du texte, des documents, des appels ou des vidéos.

SECRETS PARTAGÉS

Comment ces informations peuvent-elles alors être reçues « en clair » justement par le récepteur, simplement et quasi simultanément ? Dans une conversation chiffrée de bout en bout, les utilisateurs disposent d'une clé automatiquement générée qui leur est propre

> Seuls restent souvent enregistrés en clair les pseudos des utilisateurs et les dates de leurs échanges. Mais rien sur le contenu

LEXIQUE

***BACKDOOR**

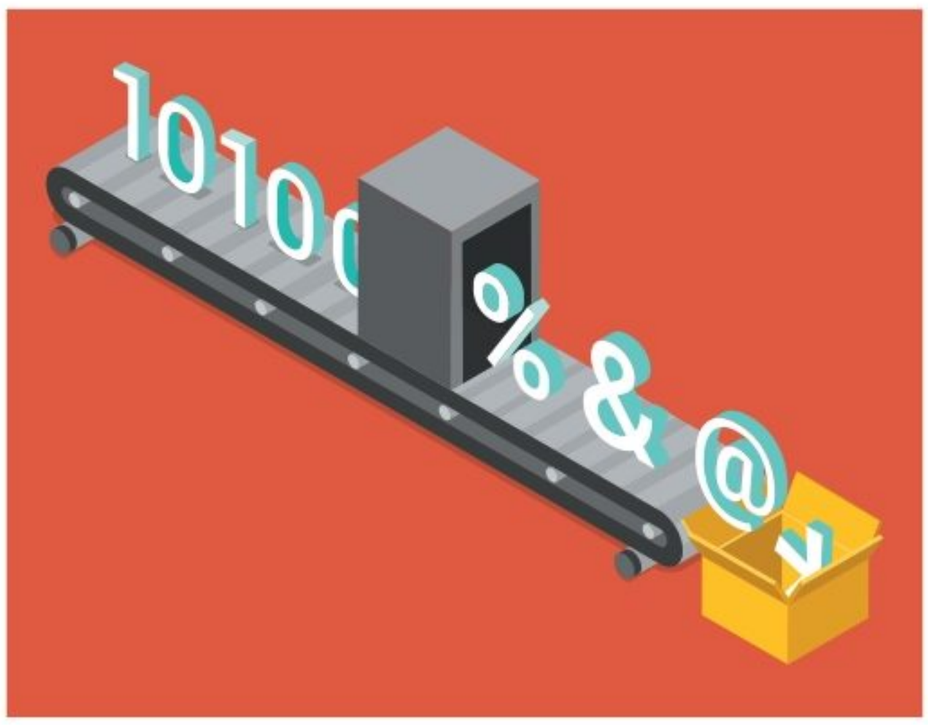
Une porte dérobée (de l'anglais « Backdoor », litt. « porte de derrière ») est une fonctionnalité, souvent inconnue de l'utilisateur final, qui permet à l'éditeur du logiciel ou de l'application d'accéder secrètement à des données ou fonctions sur le terminal de l'utilisateur. Soit pour consulter des informations ou contenus produits par ce dernier, soit pour activer des tâches ou fonctions non sollicitées, jusqu'à la prise de contrôle à distance d'un ordinateur par exemple.

Les États les plus hostiles au chiffrement sont aussi les plus « control freaks »

(fixe, aléatoire ou changée régulièrement). Cette clé intègre un ou plusieurs « secrets » uniques qui, seuls, vont autoriser le chiffrement et déchiffrement du contenu transmis.

CHARABIA ET GLOUBIBOULGA EN 256 BITS

Quand vous acceptez un utilisateur sur un service chiffré de bout en bout, vous reconnaissez sa clé de sécurité unique comme autorisée à déchiffrer les données que vous lui enverrez. Sans posséder la



clé émettrice (la vôtre) et la clé réceptrice (celle de votre contact), les données qui transitent entre vos deux terminaux ne sont que du charabia pour un tiers. Même stockées sur les serveurs du service, elles restent ainsi illisibles par l'entreprise. Cette technologie empêche l'écoute électronique par votre FAI, un spyware scannant vos données, un service marketing trop intrusif, un régime répressif ou votre voisin geek qui aurait piraté votre WiFi. De la même manière, une attaque qui permettrait à un hacker d'accéder aux serveurs d'une messagerie chiffrée n'y trouverait que du gloubiboulga informe. Seuls restent enregistrés en clair les pseudos des utilisateurs et les dates de leurs échanges. Mais rien sur le contenu.

LES LIMITES

Par contre, le terminal qui possède votre clé (votre ordinateur ou smartphone) est la porte d'accès à ces données et à votre historique ! Que l'on regarde par dessus vos épaules, que vous laissiez votre compte ouvert et accessible à un tiers qui l' « emprunterait », ou qu'un logiciel malveillant fasse des captures d'écran de vos échanges puis les récupère (sans accéder donc aux données numériques).

L'on soupçonne également certains services de s'être réservé la possibilité d'utiliser une backdoor* (porte dérobée) pour, en cas d'absolue nécessité (mais laquelle ?), pouvoir accéder et déchiffrer ce contenu. Cela serait notamment possible en copiant les

clés de sécurité de leurs utilisateurs de telle manière qu'il soit possible, au moment opportun, d'utiliser une « clé maître », possédée par l'entreprise, qui puisse s'y substituer. Comme la clé de votre facteur qui peut ouvrir toutes les boîtes aux lettres homologuées La Poste !

LE CITOYEN EST SUSPECT PAR DÉFAUT

Ceux qui défendent l'existence d'une clé maître estiment qu'en cas d'enquête judiciaire, de risque terroriste ou de tout autre besoin impérieux, le gouvernement et les autorités d'un État doivent pouvoir accéder aux informations échangées entre des citoyens potentiellement suspects ou mis en cause. Il s'agit d'un débat compliqué mais l'on remarque aussi que les états les plus demandeurs de telles mesures sont les plus « control freaks », adeptes pathologiques d'une surveillance de masse déviante et parfois les plus répressifs en termes de libertés publiques et d'expression : Indonésie, Iran, Chine, Russie, Grande-Bretagne ou États-Unis par exemple.

Pénétrez les SECRETS de chiffrement made in WHATSAPP

La technique de chiffrement de bout en bout chez WhatsApp utilise une cryptographie asymétrique (classique) pour initier une conversation : lorsque vous créez votre compte, ce dernier génère pour vous deux types de clés, un groupe de trois clés privées et un de trois clés publiques. Cette multiplication des clés offrirait un avantage inattendu à la messagerie...

TROIS CLÉS PUBLIQUES

Sans rentrer dans les détails, sachez que ces clés publiques ont chacune un rôle différent :
Une vous permet d'être identifié par WhatsApp de façon permanente (pour se connecter aux serveurs) jusqu'à réinstallation de l'application, changement de téléphone ou d'ordinateur par exemple ; une sert aux besoins d'identification pour vos usages quotidiens ; et une dernière est créée à chaque nouvelle discussion.

Identity Key Pair > Paire de clés sous protocole de chiffrement Curve25519 (128 bytes) de durée longue > Générée lors de l'installation de WhatsApp sur votre terminal.

Signed Pre Key > Paire de clés sous protocole de chiffrement Curve25519 (128 bytes) de durée moyenne > Générée également à l'installation et signée par **Identity Key**. Cette clé est changée régulièrement.

One-Time Pre Keys > Série d'identifiants sous Curve25519 fournie pour être consommée à chaque nouvel usage et forcément liée aux deux précédentes. Ces clés à usage unique sont très importantes puisqu'à chaque fois que vous engagez une discussion, vous l'échangez en même temps qu'elle disparaît des serveurs WhatsApp : vous en devenez seul propriétaire. Elle est ensuite détruite pour toujours.

TROIS CLÉS PRIVÉES

Et pareil pour les clés privées qui se partagent les responsabilités et les missions pour plus de sécurité (si une tombe - ce qui est improbable – le pirate aura besoin des deux autres pour accéder à votre contenu). WhatsApp promet ne jamais pouvoir accéder à ces clés personnelles. Elles ne sont reconnues que par les masters clés publiques et par celles de vos contacts sans qu'un humain ne puisse les intercepter.

Root Key > Votre identifiant unique et personnel correspondant à votre terminal maître. Sous chiffrement de 32 bytes, elle servira a créer vos Chain Keys.

Chain Key > Également sous 32 bytes, elle sera demandée à chaque nouvelle création de contenu. Root Key et Chain Key sont générées sur votre terminal uniquement après vérification de vos clés publiques et la transmission des « secrets ». Elles restent donc en « local ».

Message Keys > Passées à 80 bytes, ces clés serviront à encrypter vos messages après validation de vos clés publiques, identification des « secrets » et attribution personnelle de clés Root et Chain. Grâce aux 80 bytes des Messages Keys, 32 bytes s'appuieront sur une clé AES-256 key, 32 bytes sur une clé HMAC-SHA256 key et les 16 derniers moulineront sous un protocole dit « VI » (Vecteur d'initialisation)... ayant besoin des deux précédents (ouf!).

VOUS ÊTES PERDU ? SIMPLIFIONS

Nous n'allons pas vous proposer une matrice complexe pour comprendre quelle clé fait quoi selon quels usage et situation (Le magazine entier n'y suffirait pas) : mais sachez

> WhatsApp passerait d'un chiffrement asymétrique à un chiffrement en partie symétrique lors de la discussion. Une recette « fait maison » économe pour la messagerie et qui ne semble pas remettre en question la sécurité des échanges

que, là-encore, WhatsApp possède des « formules » à six clés différentes selon que vous êtes deux, un groupe ou passez une visio.
Pour simplifier, nous résumons ci-dessous une situation où nous considérerons que l'utilisateur ne possède qu'une seule clé publique et qu'une seule clé privée. Ce n'est déjà pas si simple à suivre et surtout suffisant pour comprendre le principe de chiffrement de bout en bout chez WhatsApp (comme chez la plupart des autres messageries).

Ces groupes de clés sont donc changés à intervalles réguliers pour plus de sécurité. Lorsque vous (Utilisateur A) entrez en contact avec un autre utilisateur WhatsApp (Utilisateur B), vous échangez automatiquement vos clés publiques via les serveurs de WhatsApp qui vous reconnaissent. Ces clés permettent d'appeler et de rapatrier les « secrets » (protocoles) de chiffrement utilisés par chacun d'entre vous (et bien sûr fournis par WhatsApp). Ce sont ces secrets qui codent vos messages en une suite de caractères incompréhensible. Ainsi, B reçoit le secret de A (il pourra déchiffrer ses messages) et A reçoit le secret de B (et pourra donc les lire).

Le fait que chacun possède aussi une clé privée garantit que tous les messages échangés via l'application ne sont accessibles qu'à A et B (et non aux serveurs de WhatsApp puisque les données en clair et les secrets ne peuvent être connus que sur les terminaux des utilisateurs A et B identifiés par ces clés privées). Ainsi, eux seuls ont le droit d' échanger leurs secrets et de déchiffrer leurs données dans ce canal de discussion unique. Chez WhatsApp, une fois la conversation initiée, il semble que la communication passe alors en chiffrement symétrique : seules les clés privées Message Keys (peut-être avec le concours de la clé publique One-Time Pre Key) sont nécessaires pour déchiffrer les messages en temps réel et gagner ainsi en fluidité. L'utilisation permanente d'une clé publique solliciterait en effet énormément les serveurs et les capacités de calcul de WhatsApp. Ici, c'est votre ordinateur en local qui offre ces ressources. Mais lors d'une nouvelle conversation, vous repasserez en mode asymétrique pour vous identifier à nouveau et échanger vos secrets (les clés peuvent avoir changé) avant de discuter à nouveau en symétrique sur ce canal protégé.

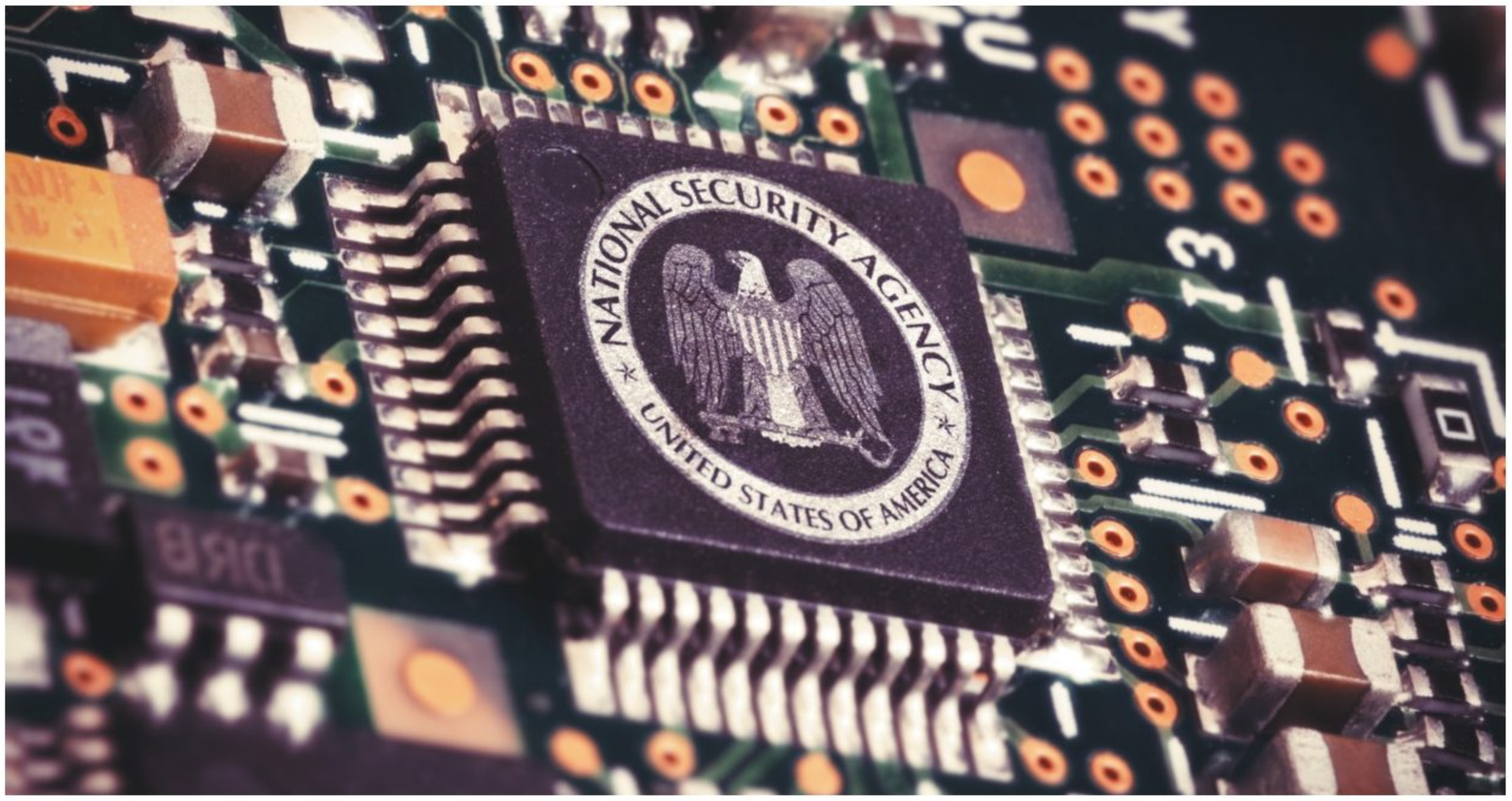
LES ÉTATS-UNIS VEULENT DES BACKDOORS !

Loin d'imaginer une généralisation du chiffrement des échanges au nom de l'intérêt général, l'ambiance est plutôt à la reprise de contrôle par les autorités de l'autre côté de l'Atlantique.

Des représentants du Sénat et du Department of Justice des États-Unis veulent reprendre le contrôle sur les messageries utilisant le chiffrement de bout en bout. Le procureur général William Barr entend criminaliser les messageries qui ne prévoiraient pas de backdoor (porte dérobée) ou de clé maître à leur technologie. En clair, l'État et l'autorité judiciaire américaine doivent pouvoir accéder aux contenus de nos conversations en cas de besoin. Et nous savons tous que les Américains n'abusent jamais de ce type de « permis de surveiller » ! Surveillance intérieure et extérieure, espionnage de personnalités privées et politiques dans le monde entier, collecte d'informations stratégiques et technologiques : L'Oncle Sam utilise tout cet arsenal et n'entend pas qu'on lui ferme la porte au nez avec le chiffrement de bout en bout !

LA BONNE CAUSE, LA LOI ET LA PORTE DÉROBÉE

Comme d'habitude, c'est une noble cause qui est avancée pour exiger la mise en place de backdoors : cette fois-ci, la protection de l'enfance. Avec le soutien des sénateurs Lindsey Graham et Richard Blumenthal, Barr souhaite présenter aux Chambres du Congrès la loi « EARN IT Act » qui, traduite en français, est l'acronyme de « Loi pour éliminer la négligence abusive et généralisée des technologies interactives ».
Si cette loi était votée et appliquée, elle rendrait les messageries et réseaux sociaux pénalement responsables dans des affaires d'abus et d'exploitation d'enfants si elles ne disposaient pas de backdoor ou de clé maître permettant aux autorités d'accéder aux contenus d'utilisateurs suspects.



LE PROCUREUR GÉNÉRAL WILLIAM BARR UTILISE LE CHEVAL DE TROIE DE LA PROTECTION DE L'ENFANCE POUR OBTENIR SES PORTES DÉROBÉES. HABILE WILL !

Crédits :
Reuters – Erin Scott

Les bons et mauvais élèves

Parmi les plus grand publics, quels sont les services de messagerie proposant un chiffrement des échanges par défaut, ceux qui font des efforts et les derniers de la classe ? Attention, n'oubliez pas que l'absence de backdoor et le chiffrement absolu ne reposent que sur la déclaration de ces entreprises.

LES BONS

- **WhatsApp >** Chiffrement de bout en bout
- **iMessage >** Chiffrement de bout en bout
- **Signal >** Chiffrement de bout en bout
- **Telegram >** Chiffrement de bout en bout
- **Zoom >** Après avoir annoncé en mars que le chiffrement de bout en bout ne serait proposé qu'aux abonnés payants, Zoom a rectifié le tir et commence à déployer ce protocole pour tous ses utilisateurs depuis juillet.

PEUT MIEUX FAIRE

- **Snapchat >** Les messages entre utilisateurs ne sont pas chiffrés mais doivent être détruits après 30 jours par l'entreprise. Les « Snaps » photos et vidéos, eux, sont chiffrés de bout en bout et détruits après ouverture.
- **Skype >** Pas de chiffrement par défaut mais possibilité de créer des « Conversations privées » chiffrées de bout en bout, y compris les appels et documents. Attention, les appels vidéo ne sont pas pris en compte. ***(Lire page 19)***
- **Facebook Messenger >** Pas de chiffrement par défaut mais nouvelle possibilité de créer des « conversations secrètes » chiffrées de bout en bout et qui peuvent même s'autodétruire ! ***(Lire page 18)***

LES MAUVAIS

- **Twitter >** Aucun chiffrement
- **Instagram >** Aucun chiffrement
- **Tik Tok >** Aucun chiffrement
- **Tinder >** Aucun chiffrement
- **Discord >** Aucun chiffrement

Obliger les messageries à prévoir une backdoor permettant de lire le contenu des messages chiffrés

Ainsi, ces services devraient tous prévoir par défaut ce type de porte dérobée. Alors même que ces dernières sont pourtant considérées par les experts comme une faille majeure pouvant être exploitée par des pirates, des organisations privées ou puissances étrangères.

DES CONSÉQUENCES BIEN AU-DELÀ DES ÉTATS-UNIS

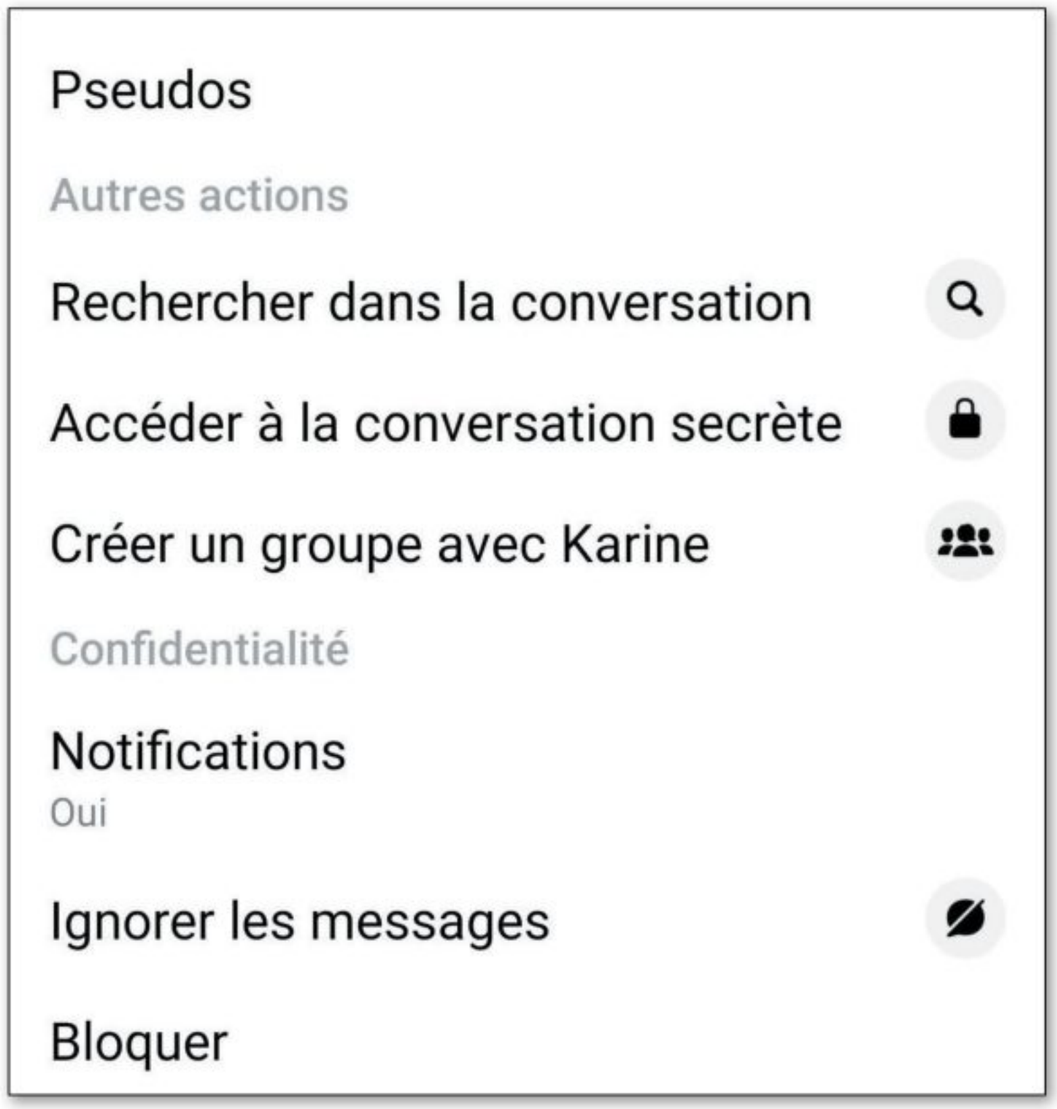
La pression sur les messageries serait aussi terrible dans de nombreux pays. Jusqu'à présent, lorsqu'un État répressif demandait l'accès aux comptes de dissidents par exemple, des messageries comme WhatsApp ou Telegram pouvaient se réfugier derrière un argument imparable : « Nous ne pouvons pas y accéder, nous n'avons pas la clé ! ». Demain, la justice de tel ou tel pays pourrait les criminaliser si elles refusaient de se plier à leur demande. Quant aux états-Unis, parions que, une nouvelle fois, cette loi destinée à la protection de l'enfance sera rapidement étendue à la défense de l'imparable « Sécurité nationale ».

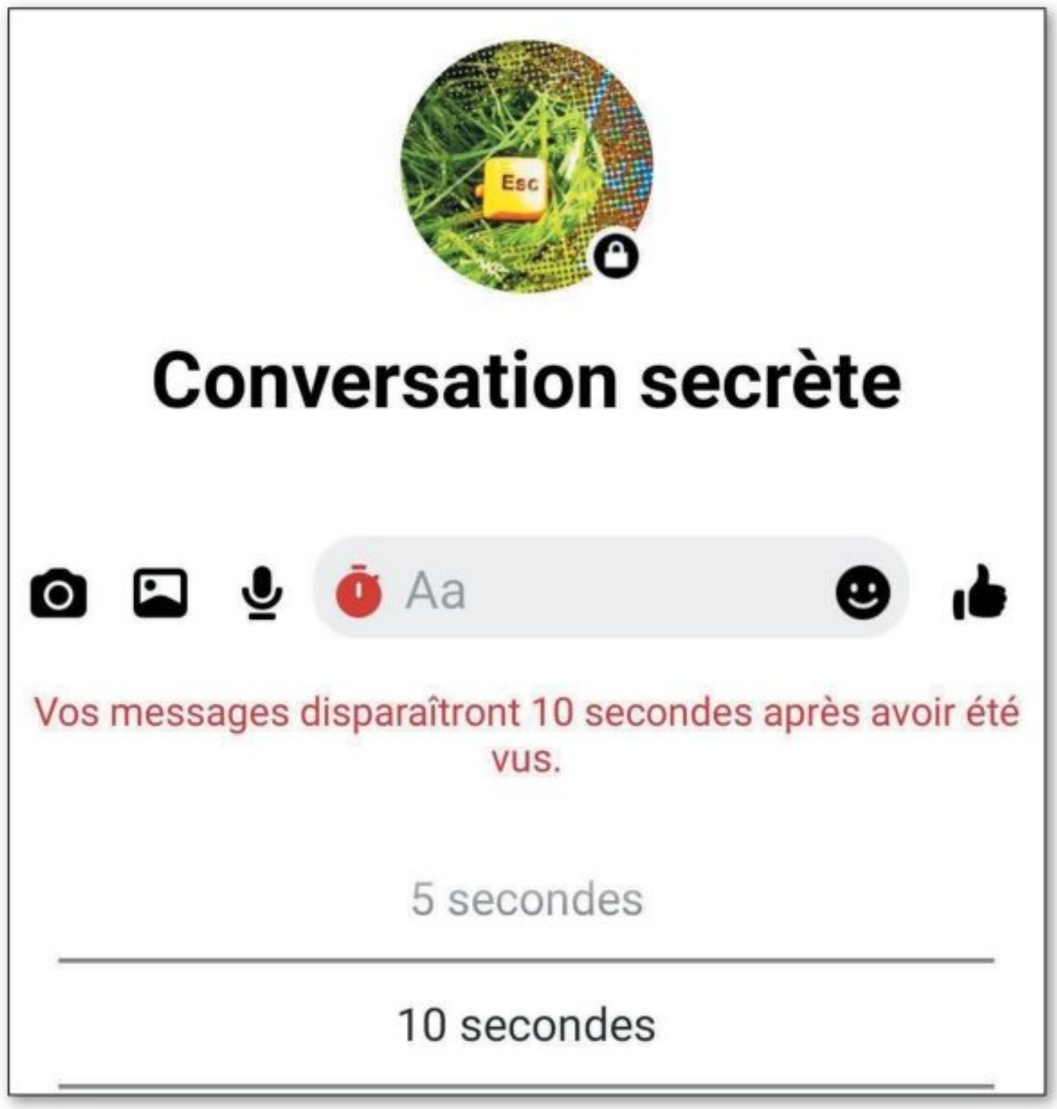
ÉCHANGER DES MESSAGES SECRETS SUR FACEBOOK MESSENGER

PRATIQUE

Sur smartphone, exploitez le mode secret de Facebook Messenger pour que vos messages s'autodétruisent après lecture .

INFOS [Facebook Messenger]
Où le trouver ? [Android & iOS]
Difficulté : ☠☠☠





01› ACTIVER LE MODE SECRET

Sur Android, lancez l'appli puis choisissez le contact avec qui communiquer en mode secret. Appuyez sur l'icône bleue **i** en haut à droite et sélectionnez l'option **Accéder à la conversation secrète**. Sur iOS, pressez l'icône en haut à droite de l'écran en forme de crayon, appuyez sur **Secret** et indiquez enfin le contact souhaité.

02› PROGRAMMER L'AUTODESTRUCTION

Sur Android comme sur iOS, figure à gauche du champ de saisie du message une icône de chronomètre. Appuyez dessus et définissez le temps de lecture souhaité. À l'issue du compte à rebours (de 5 sec à 24h), le message disparaîtra. Attention : rien n'empêche votre contact d'effectuer une capture d'écran et de garder une trace de votre échange.

CRÉER DES DISCUSSIONS PRIVÉES SUR SKYPE

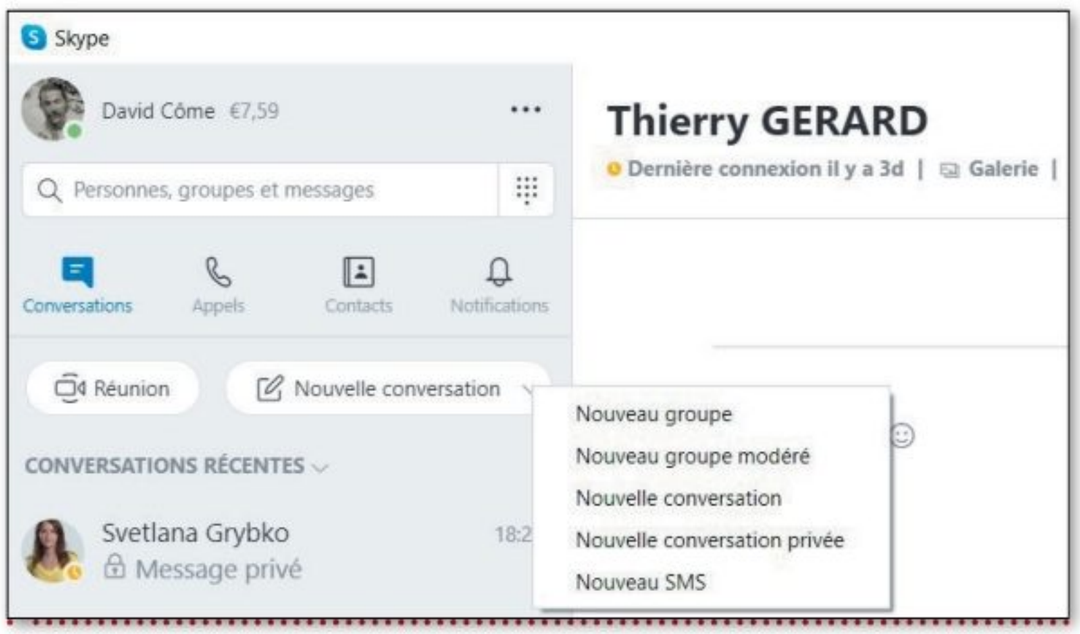
PRATIQUE

Contrairement à WhatsApp, Signal ou Telegram, Skype ne propose pas de chiffrement par défaut. Vous pouvez cependant engager des conversations privées et chiffrées de bout en bout avec certains de vos contacts.

INFOS [**Skype**]
Où le trouver ? [**www.skype.com**]
Difficulté :

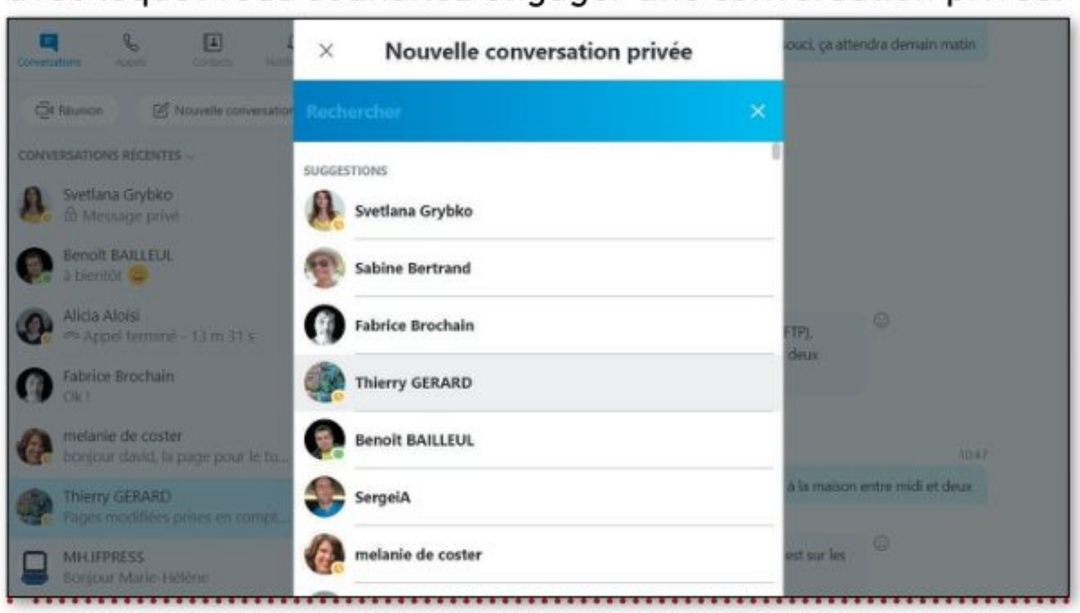
01› ACCÉDEZ AU SERVICE

Nous sommes ici sur la version desktop de Skype. Passez par le menu déroulant, en haut à gauche, **Nouvelle conversation,** et choisissez **Nouvelle conversation privée**.



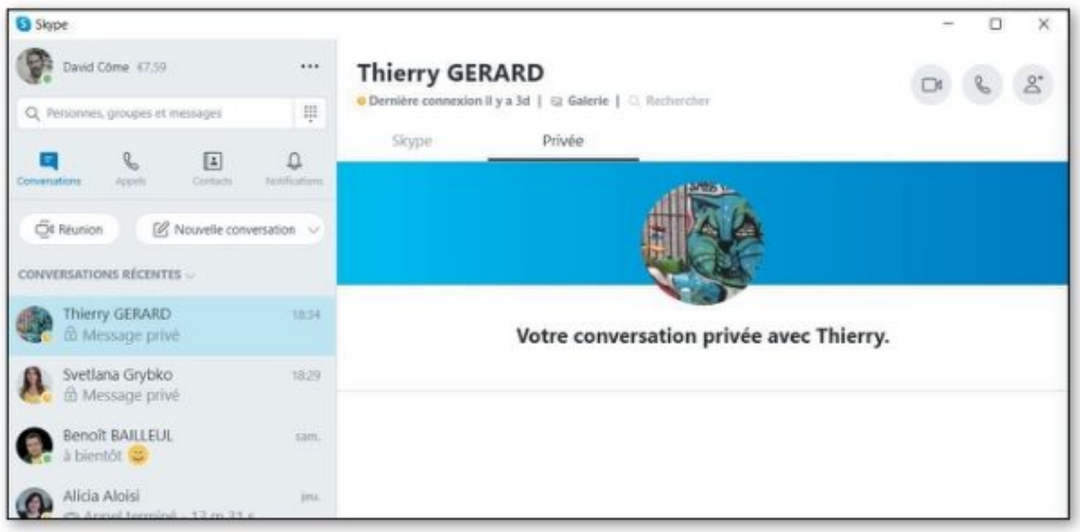
02› CHOISISSEZ UN CONTACT

La liste de vos contacts apparaît. Choisissez celui avec lequel vous souhaitez engager une conversation privée.



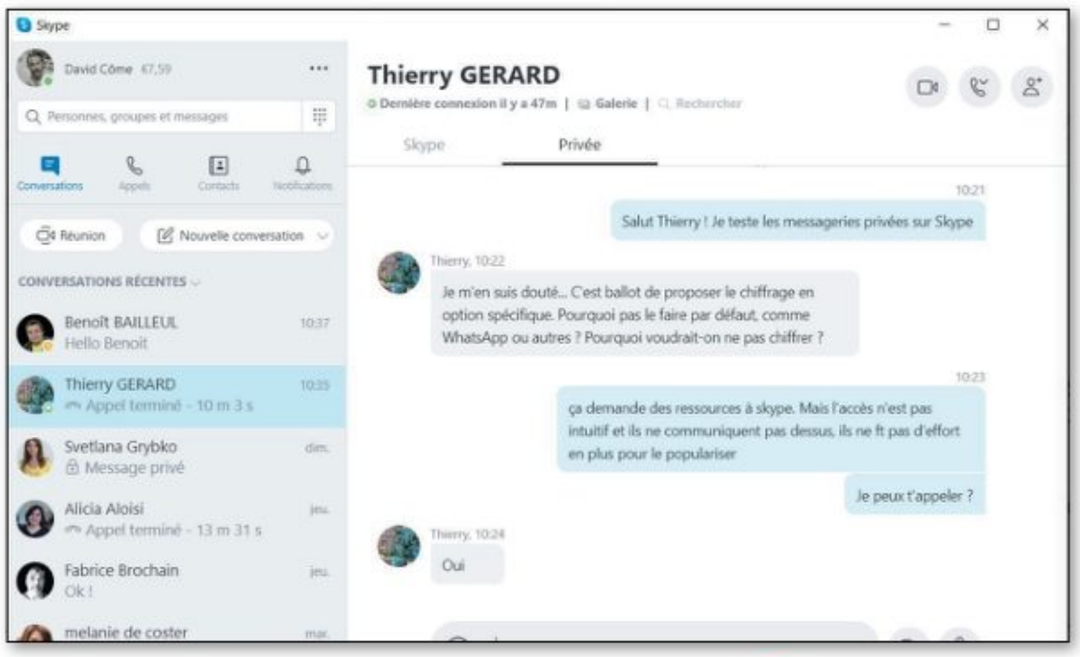
03› INVITEZ-LE

Vous envoyez alors automatiquement une demande de conversation privée que votre contact peut accepter ou refuser. En l'acceptant, vous passez tous les deux en mode chiffré de bout en bout.



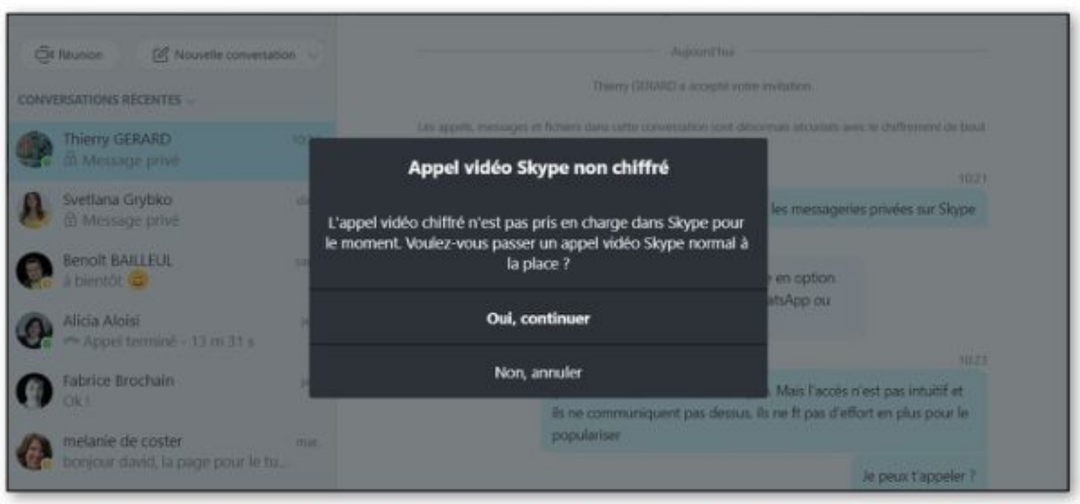
04› HISTORIQUE MAINTENU

Ces discussions privées se retrouvent sous l'onglet **Privé** de Skype. Vous en gardez l'historique. Messages, documents et appels audio bénéficient du chiffrement. Vous pouvez revenir à une discussion « normale » en basculant sur l'onglet **Skype**.



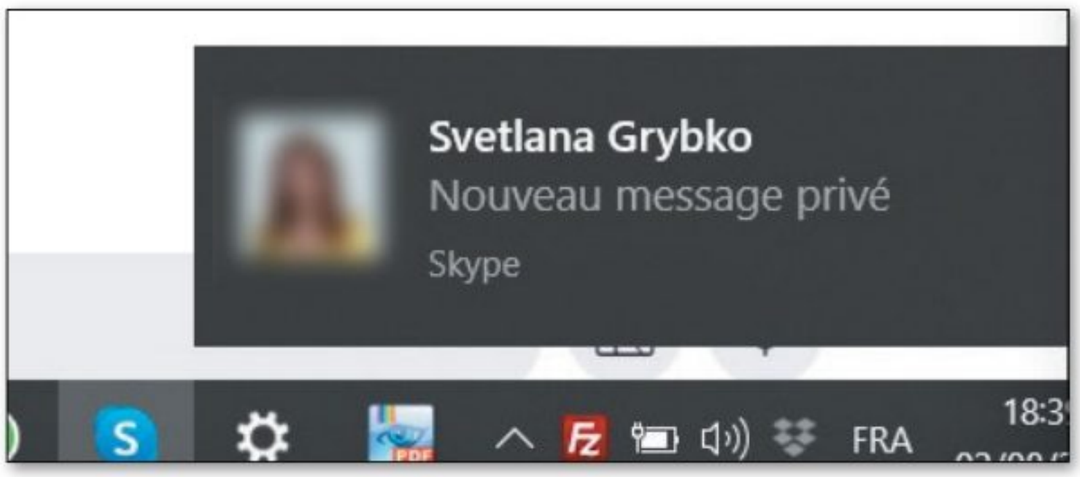
05› PAS DE VISIO PRIVÉE

Par contre, Skype n'a pas intégré les appels vidéo à son système de chiffrement par défaut. Vous êtes alors obligés de repasser en mode non protégé pour une visio.



06› NOTIFICATIONS DISCRÈTES

Lorsque l'un de vos contacts vous envoie un message en conversation privée, la notification Skype que vous recevez reste discrète avec son nom/pseudo comme d'habitude mais sans prévisualisation du message.



TUTO

TESTEZ LA PUISSANCE DE VOTRE SIGNAL WIFI avec Ekahau HeatMapper

POUR QUI ?

Pour ceux qui ont des soucis de réception

POUR QUOI FAIRE ?

Pour cartographier le signal WiFi et repérer les points faibles du signal chez vous

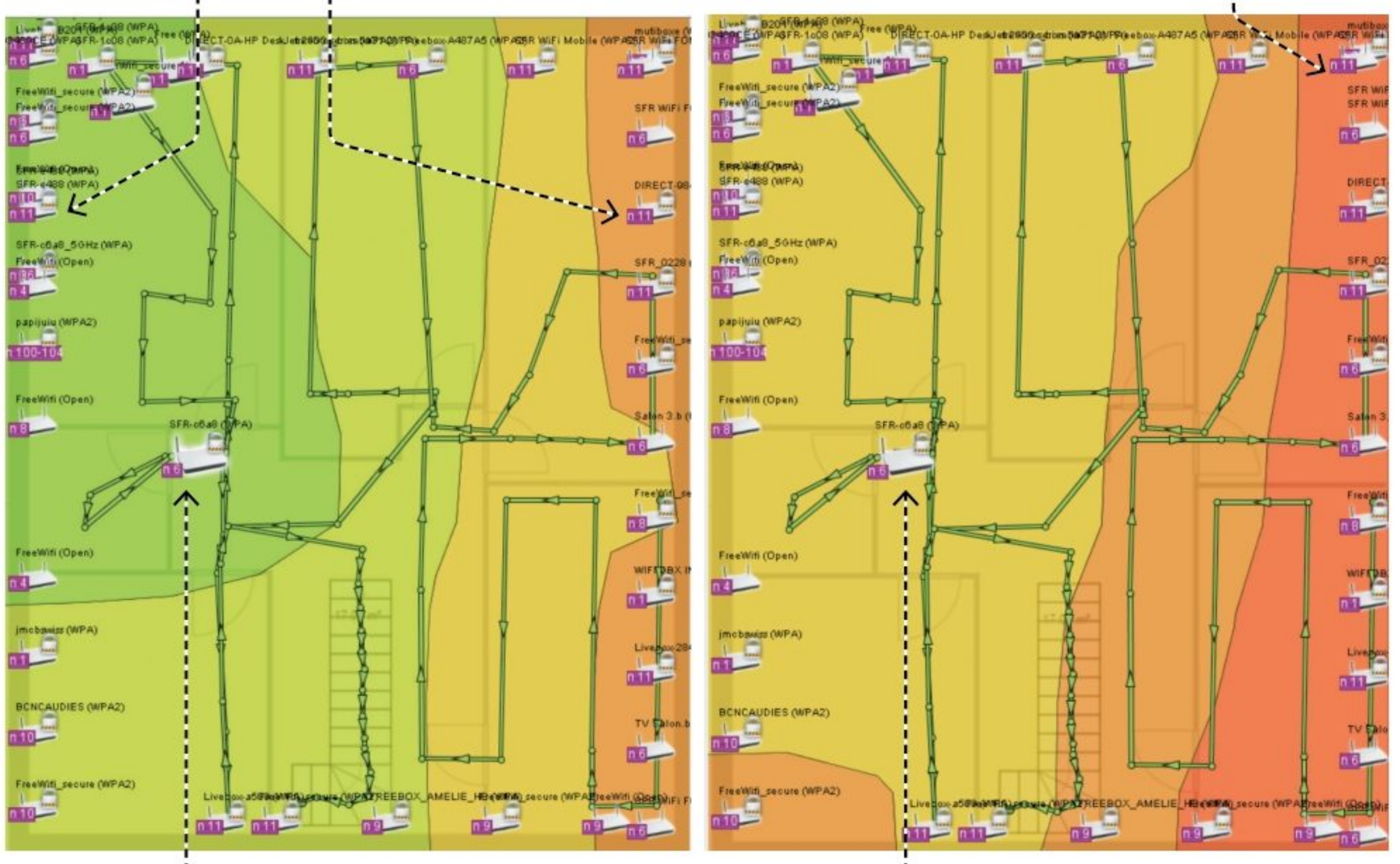
Après une balade de 5 minutes chez vous, le logiciel Ekahau HeatMapper cartographie le signal WiFi. Vous allez enfin pouvoir vérifier quels sont les points chauds de votre logement et éventuellement changer de place votre box internet pour optimiser votre réseau. Ekahau HeatMapper est aussi utile en voyage pour choisir le meilleur réseau auquel se connecter.

PUISSANCE DU SIGNAL WI-FI

La puissance mesurée du signal de votre box en différents points de votre habitation est symbolisée par des zones colorées, du vert (Très fort) au rouge (Très faible).

LES AUTRES WIFI

Sur le bord de la map on peut voir tous les réseaux WiFi des voisins (voire du quartier). Une preuve, s'il en fallait, que nous vivons entourés d'ondes. De quoi faire peur à ceux qui les présument dangereuses et réjouir les fans de technologies... L'avantage est que si vous remarquez que le signal WiFi de votre voisin est de meilleure qualité que le vôtre, vous pouvez toujours essayer de lui demander de partager.



LOCALISATION DE LA BOX

L'image de gauche est la cartographie du signal WiFi au premier étage alors que la box est au rez-de-chaussée. Ekahau HeatMapper ne peut pas tenir compte de ce paramètre et il a donné une localisation de la box... juste au-dessus de sa position réelle ! Lorsqu'on s'éloigne de la box, la connexion faiblit assez vite, notamment en entrant dans les pièces à gauche de la carte. Ces cloisons là, en particulier, stoppent une partie des ondes.

5 GHZ VS 2.4 GHZ

L'image de droite représente la cartographie du même signal WiFi que sur l'image de gauche mais pour la fréquence 5 GHz et non pas 2.4 GHz, qui est la fréquence la plus classique. En théorie, la bande à 5 GHz est plus rapide. Mais sa portée est plus faible et elle est plus facilement arrêtée par les obstacles. Comme cette cartographie a été enregistrée à l'étage et que la box est au rez-de-chaussée, le signal à 5 GHz est plus faible car stoppé par le plafond du rez-de-chaussée. Mieux vaut tester par vous-même la différence entre 2.4 GHz et 5 GHz si vous avez une box qui propose les deux options.

LEXIQUE

*** FRÉQUENCE :**
Certaines box émettent leur signal WiFi sur deux bandes de fréquence : 2,4 GHz et 5 GHz. En théorie, la bande à 5 GHz est plus rapide et moins encombrée car moins utilisée. Cependant, la fréquence 5 GHz s'atténue plus vite que la 2,4 GHz, de la même façon qu'une voix aiguë porte moins loin qu'une voix grave.

CARTOGRAPHIEZ VOTRE WIFI AVEC EKAHAU HEATMAPPER

PRATIQUE

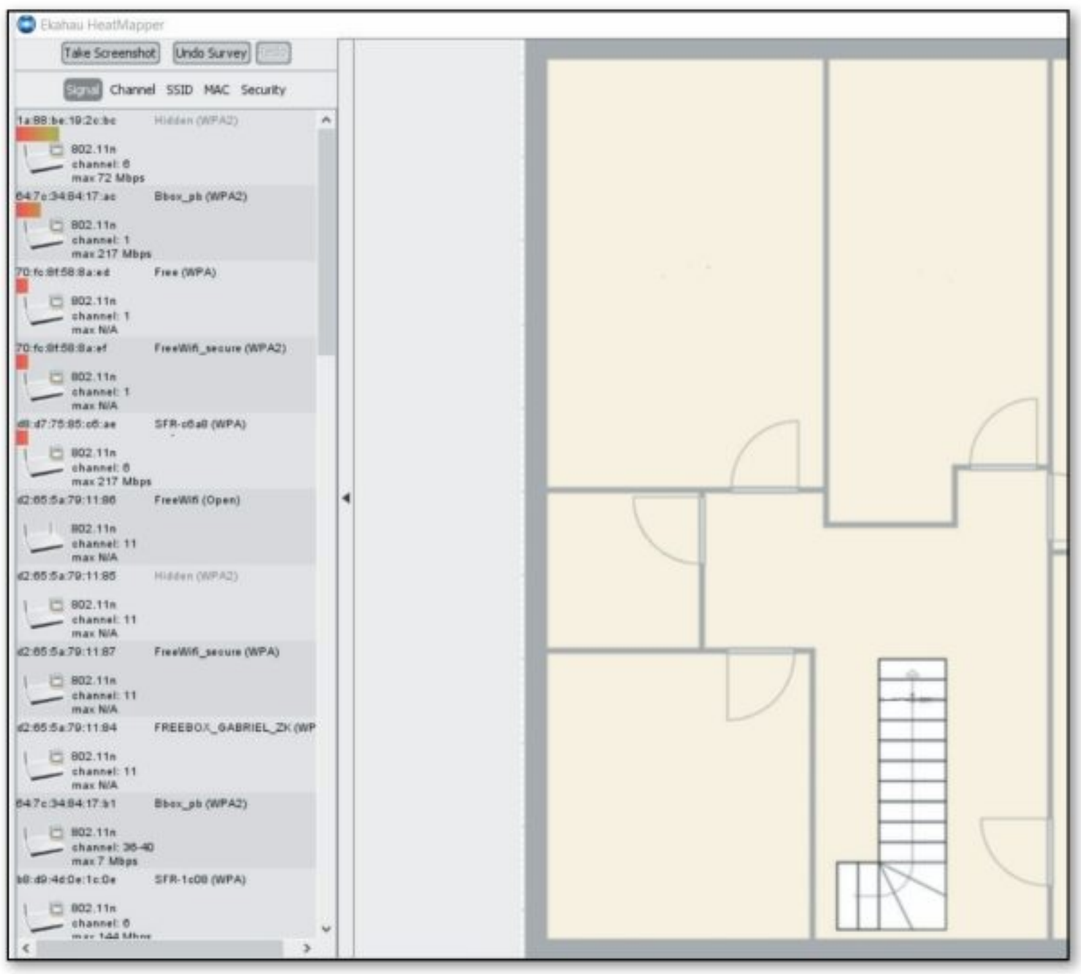
01› CHARGER LE PLAN

Deux modes sont possibles : avec ou sans plan de chez vous. Se repérer sur un plan est plus simple que

sur un quadrillage, nous vous conseillons donc de choisir la première option. Une fois que vous avez cliqué, il vous suffit de sélectionner l'image de votre plan. Même si vous n'avez pas de plan de votre appartement, vous pouvez quand même suivre ce tuto.

02› SE REPÉRER

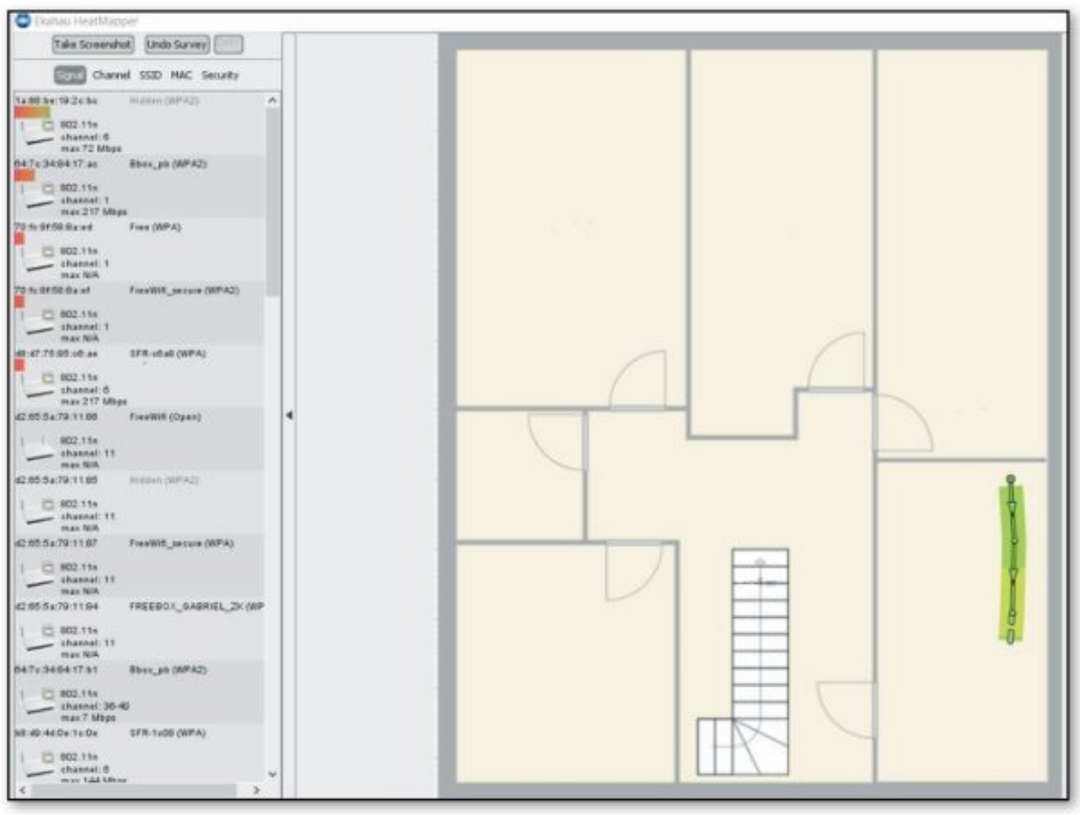
Une fenêtre s'ouvre avec, à gauche, tous les réseaux WiFi que repère le logiciel et, au centre, le plan ou le quadrillage ainsi qu'une aide. Situez-vous sur celui-ci et



levez-vous avec votre ordinateur portable. Pour commencer, faites un clic gauche à l'endroit où vous êtes et commencez à avancer en cliquant régulièrement sur le plan pour signaler votre changement de position.

03› FINIR LA MAP

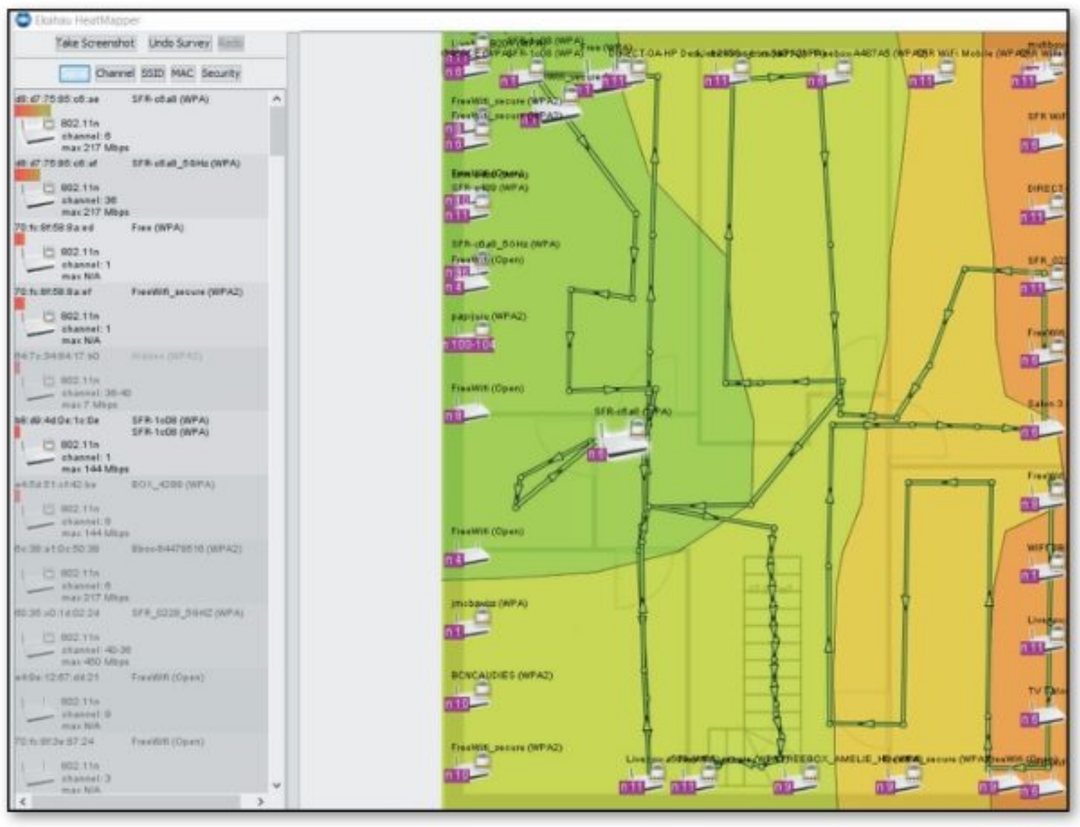
De temps en temps (lorsque vous changez de pièce par exemple), nous vous conseillons de faire un clic droit. Ainsi, vous arrêtez l'enregistrement. Si votre chemin vous convient, reprenez l'enregistrement par un clic gauche.



Si ce n'est pas le cas, cliquez sur **Undo Survey**. Cette action effacera votre enregistrement depuis le dernier clic droit.

04› EXPLORER LA MAP

Lorsque vous cliquez sur le bouton droit de la souris, une carte en couleur s'affiche sur laquelle sont représentés tous les WiFi que vous captez. La vôtre se situe normalement à l'endroit où se trouve votre box. Passez votre souris dessus (inutile de cliquer). Les couleurs qui s'affichent indiquent la force du réseau dans les différentes pièces



de votre logement. Le vert signifie une bonne réception alors que le rouge prouve une mauvaise qualité du signal. Impossible d'enregistrer la carte, donc n'oubliez pas de cliquer sur l'option **Take a screen shot** !

DEEPFAKES AUDIO

DES VOIX QUI TROMPENT ÉNORMÉMENT

Tous les regards sont tournés vers les vidéos deepfakes et la lutte contre les fausses infos a commencé. Mais les criminels ont une longueur d'avance grâce aux deepfakes audio.

Jim Carrey est l'acteur principal de Shining. Bien sûr, c'est faux ! Mais la vidéo existe. Il y a un an, dans Pirate Informatique, on vous expliquait le fonctionnement des deepfakes vidéo. Grâce au deep learning, il est possible d'utiliser des vidéos existantes pour changer le visage d'une personne par une autre de façon toujours plus réaliste. Aujourd'hui, les intelligences artificielles se perfectionnent pour franchir une nouvelle étape : imiter la voix de quelqu'un. Car, contrairement à ce que nous pensons souvent, réussir à parfaitement imiter une voix grâce à l'intelligence artificielle est encore considéré comme plus complexe que réaliser une vidéo deepfake convaincante. Mais le principe est le même : fournir au programme de deep learning des enregistrements de la personne – parfois moins d'une minute suffit, de taper un texte, et l'IA le lira avec la voix voulue. De cette manière, on peut littéralement faire dire n'importe quoi à n'importe qui.

ESCROQUER GRÂCE AUX DEEPFAKES

Évidemment, une telle technologie attire les pirates criminels, en particulier ceux adeptes de vishing*. La société de conseil en sécurité NISOS explique avoir analysé une arnaque employant une deepfake audio. Des hackers ont copié la voix du PDG d'une entreprise et ont demandé à un employé « une assistance immédiate pour finaliser un accord commercial urgent ». L'enregistrement est d'ailleurs disponible sur Internet. Chez Pirate, on l'a écouté et le moins qu'on puisse dire c'est que la voix paraît robotique. Mais dans l'urgence, on peut l'imputer à une mauvaise réception ou à un téléphone de piètre qualité. Rob Volker, un chercheur de NISOS affirme que « ça ressemblait plus à un humain qu'à un robot ». Dans ce cas, l'employé ne s'est pas fait avoir et a signalé ce coup de fil au service juridique de son entreprise.

LEXIQUE

***VISHING**

Pour « voice phishing » : il s'agit d'une technique d'ingénierie sociale souvent utilisée contre des grandes entreprises. Celui qui appelle sa cible espère obtenir en urgence des informations, données sensibles ou des virement bancaires à son profit en se faisant passer pour un responsable, un client ou un prestataire important. Avec les deepfake audio, l'imitation des voix pourrait rapidement devenir parfaite... et donc encore plus dangereuse.

D'après Rob Volker, la voix ne ressemblait tout simplement pas assez à celle du PDG.

DES DEEPFAKES À SUCCÈS

Cependant, certaines arnaques ont bel et bien fonctionné. En 2019, un chef d'entreprise britannique reçoit un coup de téléphone du PDG d'un de ses fournisseurs qui lui demande un virement urgent de 220 000 euros. Plus d'un an après, les hackeurs n'ont pas été retrouvés. Symantec, une entreprise de cybersécurité, comptabilise trois arnaques réussies à l'aide d'une deepfake audio et un total de plusieurs millions d'euros volés. Il est facile pour des hackers d'entraîner des intelligences artificielles à imiter la voix de cadres haut placés grâce aux heures de discours disponibles en ligne – comme des films d'entreprise ou des conférences. Si l'imitation n'est pas assez réaliste à certains endroits, il suffit aux hackers de rajouter un bruit de fond pour dissimuler les faiblesses de leur enregistrement.

UNE SÉCURITÉ À RENFORCER

« Je ne pense pas que les entreprises soient prêtes à affronter un monde où il n'est plus possible de croire la voix d'un collègue », prévient Henry Ajder, un expert de chez SensityAI, une start-up spécialisée dans la détection de deepfakes. Pour l'instant, il n'existe que très peu d'outils pour repérer ces derniers. De plus, l'enjeu dans le cas d'arnaque est de les repérer rapidement voire en temps réel. Un challenge aujourd'hui pour les entreprises de cybersécurité.

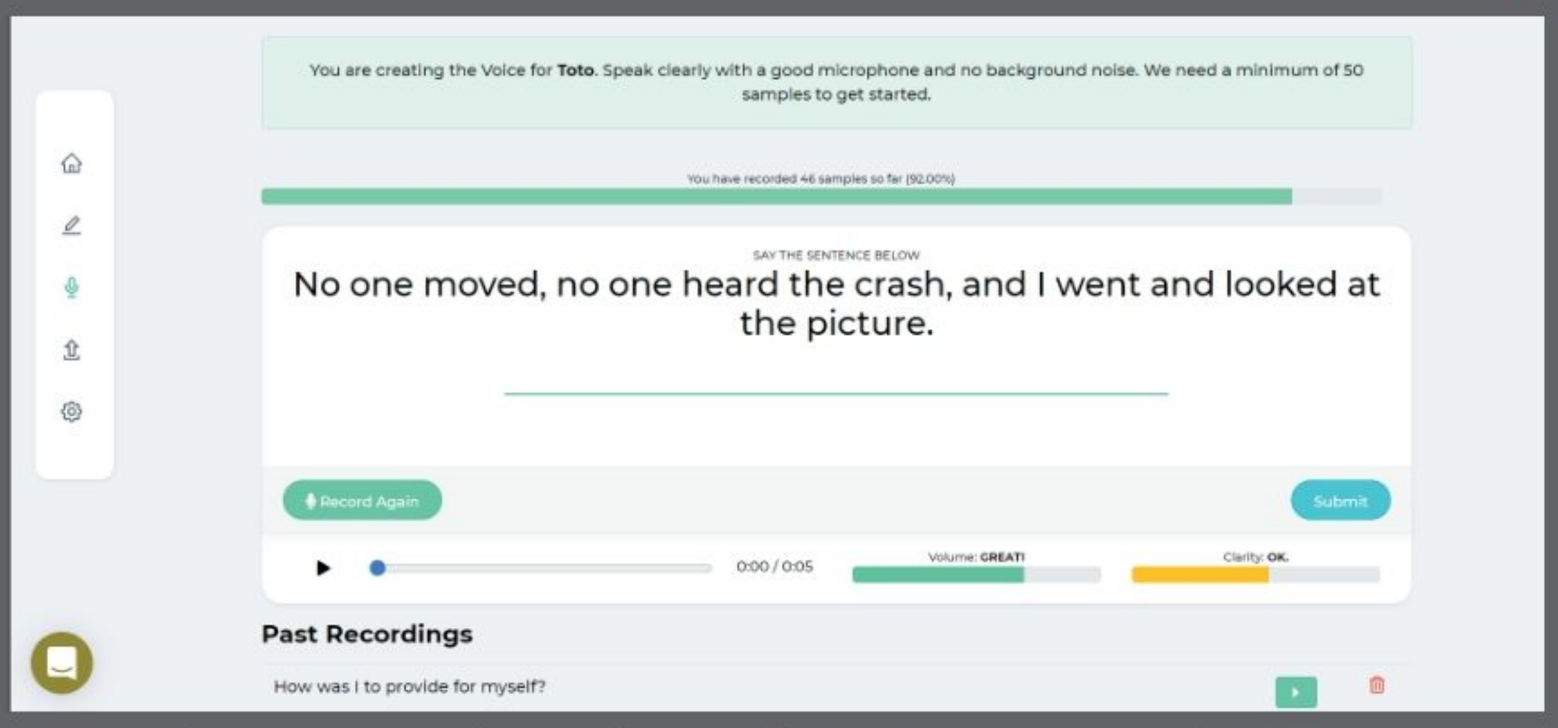
RETROUVER SA VOIX

Au fur et à mesure que les deepfakes audio s'améliorent, on peut imaginer des applications positives. John Costello, directeur du programme « Amélioration de la communication » à l'hôpital des enfants de Boston, affirme que les deepfakes pourraient être d'un grand secours pour les patients qui perdent leur voix. Ainsi, si des enregistrements de leur voix existent, l'intelligence artificielle pourrait être mise à contribution pour recréer une version synthétique au rendu très réaliste qui leur permettra de communiquer avec leurs propres intonations et timbre.

> Symantec comptabilise trois arnaques réussies à l'aide d'une deepfake audio et un total de plusieurs millions d'euros volés

CRÉER DES DEEPFAKES AUDIO, PAS SI SIMPLE !

Alors que les applications capables de créer des deepfakes vidéo sont nombreuses sur la toile, La création de deepfakes audio n'est pas aussi accessible. Nous avons repéré seulement quatre applications : Lovo, Descript, Microsoft's Custom Voice et ResembleAI. Toutes sont en anglais et les deux premières sont payantes. ResembleAI propose une version gratuite pour imiter seulement sa propre voix.



Même si l'intérêt semble pour le moins limité, on l'a quand même testé. Il est nécessaire d'enregistrer 50 phrases courtes pour que l'intelligence artificielle essaie de reproduire notre voix. Mais, pour nous, l'IA n'a jamais réussi. Un échec potentiellement imputable à notre accent anglais… approximatif.

Cependant, le créateur de ResembleAI a posté son premier programme de création de deepfake audio sur Github, une plateforme ou chacun peut publier du code en open source. Pour l'utiliser il faut de solides connaissances en Python et du temps à perdre !

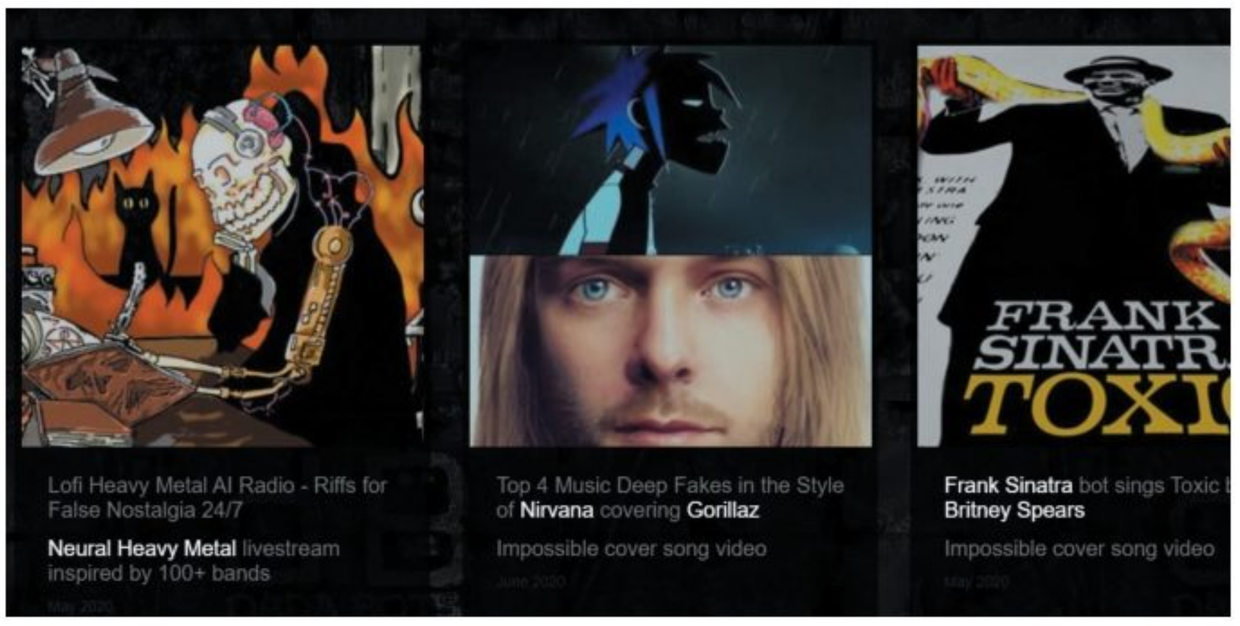
LES DEEPFAKES AUDIO AU SERVICE DE LA CRÉATIVITÉ

Jouer avec les deepfakes vidéo c'est so 2019. Aujourd'hui, les hackers font preuve de créativité en bidouillant les voix de personnalités.

Si vous lisez ces lignes, vous savez bien que tous les pirates ne sont pas mal intentionnés. Certains hackeurs produisent des deepfakes audio pour le fun et avec créativité. Vous êtes toujours affecté par la mort de Kurt Cobain ou de John Lennon ? Le site Internet Dadabots reproduit leur voix et les fait chanter à nouveau grâce au deeplearning. Ces programmeurs se décrivent eux-mêmes comme un mélange entre un groupe, une équipe de développeurs et un laboratoire de recherche. Dadabots crée des covers, Nirvana chante un morceau du groupe Gorillaz, par exemple. Mais ils proposent aussi des musiques dans le même style qu'un mash-up, entièrement générées par une intelligence artificielle. Ce n'est pas encore parfait car les musiques et chants manquent d'une certaine fluidité, pour l'instant, propres à l'être humain.

DES REPRISES IMPROBABLES

La créativité des hackeurs ne s'arrête pas là. Jamais on n'aurait imaginé entendre la Reine d'Angleterre réciter sobrement Wannabe des Spices Girls. Vocal Synthesis l'a réalisé. Depuis un an environ, cette chaîne YouTube poste des deepfakes audio. Elle en compte aujourd'hui plus de 200. Sur le blog Waxy, le youtubeur s'est confié sur les raisons de la création de ses deepfakes : « J'ai créé cette chaîne parce que je voulais montrer que les deepfakes ne sont pas exclusivement conçus à des fins malveillantes. Je pense que cette technologie cache actuellement un fort potentiel en termes d'amusement et de divertissement. » Et, effectivement, il est assez drôle d'écouter Sinatra chanter Dancing Queen de ABBA ou Bob Dylan reprendre Baby One More Time de Britney Spears. Au risque de vous décevoir, on tient quand même à vous prévenir, les enregistrements sont de qualités variables.



Quand la Reine récite Lucy in the Sky des Beatles, certaines intonations ne sont pas au rendez-vous. Selon nous, le deepfake le plus réussi est celle de Jay-Z rappant le célèbre monologue de Hamlet, « To be or not to be ». Ce succès est probablement dû au ton haché très particulier du rap et de Jay-Z. Le trucage était tellement bien fait qu'il a même valu une plainte à Vocal Synthesis (voir encadré). La rançon de la gloire !

À QUI APPARTIENT UNE VOIX ?

Jay-Z n'a pas apprécié s'entendre réciter du Shakespeare. Il a demandé à YouTube de retirer les vidéos des deepfakes audio de sa voix. La plateforme accède à la requête de Jay-Z et les supprime. Mais YouTube revient rapidement sur sa décision en les remettant en ligne. Dans cette affaire difficile de savoir à qui appartient le rap : à Jay-Z, à Shakespeare ou à Vocal Synthesis, le propriétaire de la chaîne YouTube ? C'est d'autant plus complexe que tous les pays n'ont pas la même juridiction. Si le message véhiculé par la voix d'une personnalité nuit à son image il est évident que le deepfake est alors illégal. Mais, pour les cas qui ne concernent que le divertissement, la justice n'a encore jamais tranché. Les plateformes doivent aujourd'hui s'adapter à ces questions... Et vite !

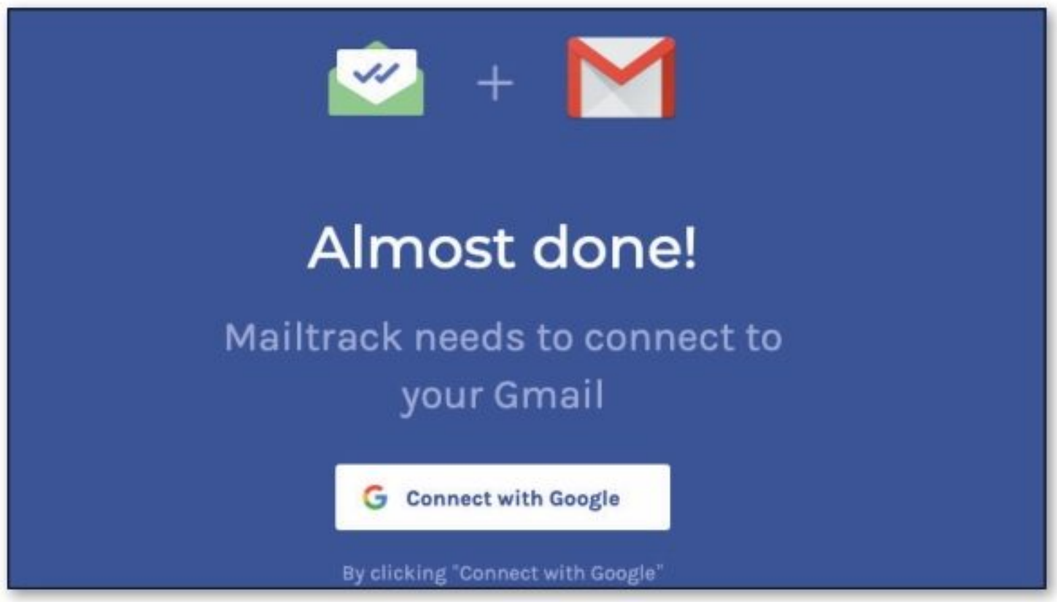
SUR LE SITE INTERNET JUKEBOX TOUTES LES MUSIQUES SONT GÉNÉRÉES GRÂCE AU DEEPLEARNING. ON PEUT RETROUVER QUELQUES REPRISES DE CHANSON PAR DES VOIX CONNUES MAIS IL S'AGIT SURTOUT DE CRÉATION DE NOUVELLES MUSIQUES. LA PAGE D'ACCUEIL VOUS PRÉSENTE LES MORCEAUX LES PLUS RÉUSSIS ET ILS SONT BLUFFANTS !

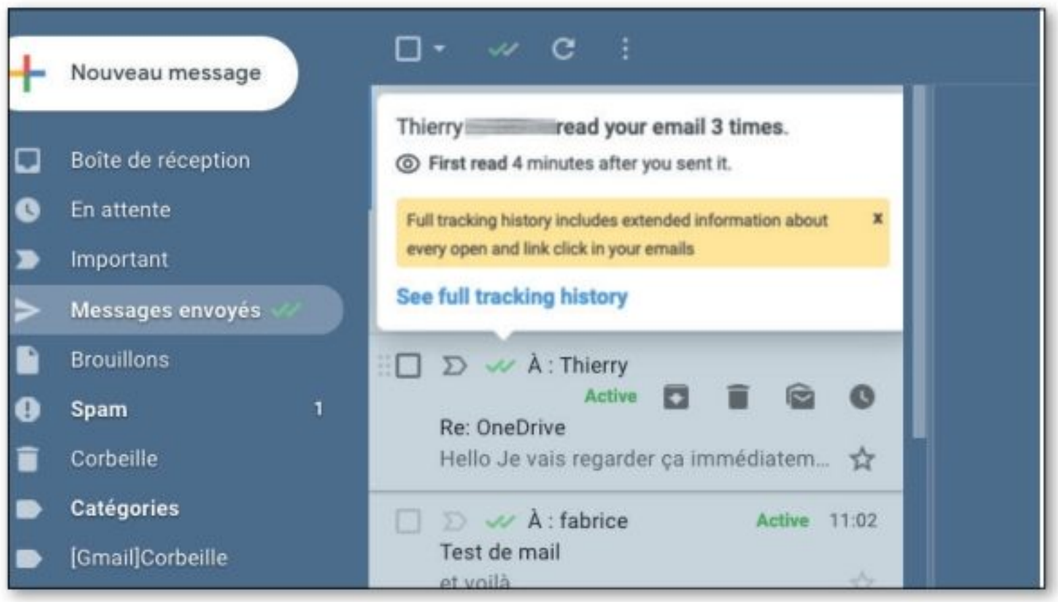
SURVEILLEZ LA LECTURE DE VOS MAILS PAR VOS DESTINATAIRES

PRATIQUE

Cette extension gratuite pour Chrome ajoute une fonction bien utile à votre boîte Gmail en vous informant si votre contact a ouvert et lu votre mail... Il n'en saura rien.

INFOS [MailTrack]
Où le trouver ? [https://mailtrack.io/en/]
Difficulté : ☠☠☠





01› INSTALLER MAILTRACK

Depuis le navigateur Chrome, rendez-vous sur le site de Mailtrack et cliquez sur le bouton **Install for free**. Arrivé sur la page du Chrome WebStore, activez le bouton **Add to Chrome** et cliquez enfin sur **Connect with Google**. Accordez les autorisations nécessaires pour que l'extension accède à votre boîte Gmail.

02› ÉPIER LA LECTURE DES MISSIVES

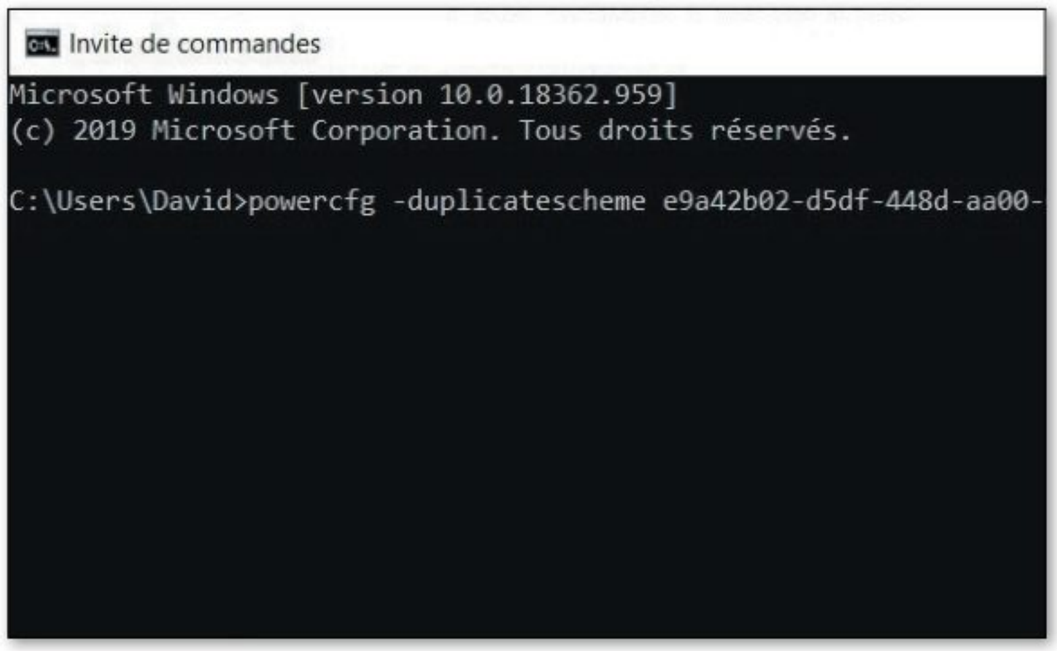
Désormais, les messages que vous expédiez s'accompagnent d'une double coche verte visible dans **Messages envoyés** sitôt que votre correspondant les a ouverts. La version payante de l'extension (jusqu'à 59 €/an) offre quelques fonctions supplémentaires comme la surveillance des clics sur les liens inclus dans vos mails.

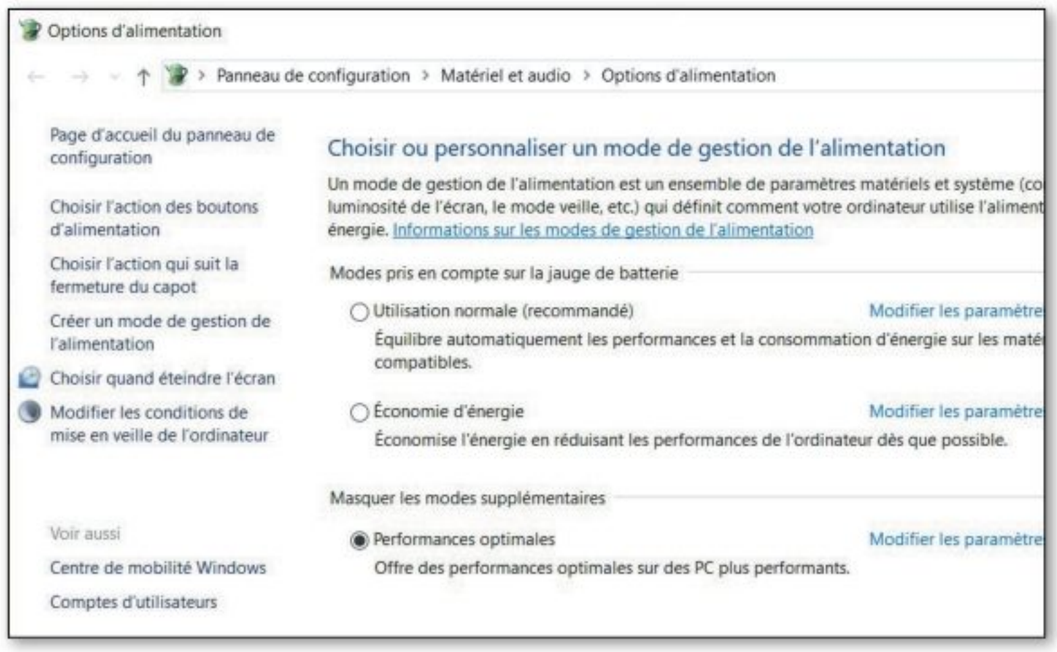
ACTIVEZ LE MODE « PERFORMANCES OPTIMALES »

PRATIQUE

Les dernières versions de Windows Home ne permettent plus de passer en mode « Performances élevées » qui privilégie la puissance à l'autonomie. Cette fonction est en fait cachée...

INFOS [Windows 10]
Difficulté : ☠☠☠





01› FONCTION CACHÉE

Via menu **Démarrer,** recherchez l'**Invite de commande**. Faites un clic droit sur celle-ci et choisissez de l'**Exécuter en tant qu'administrateur**. Entrez cette commande dans la nouvelle fenêtre et Entrée :
powercfg -duplicatescheme e9a42b02-d5df-448d-aa00-03f14749eb61

02› RÉACTIVER !

Vous allez maintenant pouvoir retrouver et choisir cette fonction **Performances Optimales** via **Paramètres > Système > Alimentation et mise en veille > Paramètres d'alimentation supplémentaires > Afficher les modes supplémentaires.** Sélectionnez cette option pour solliciter au maximum les ressources de votre PC.

SÉLECTION

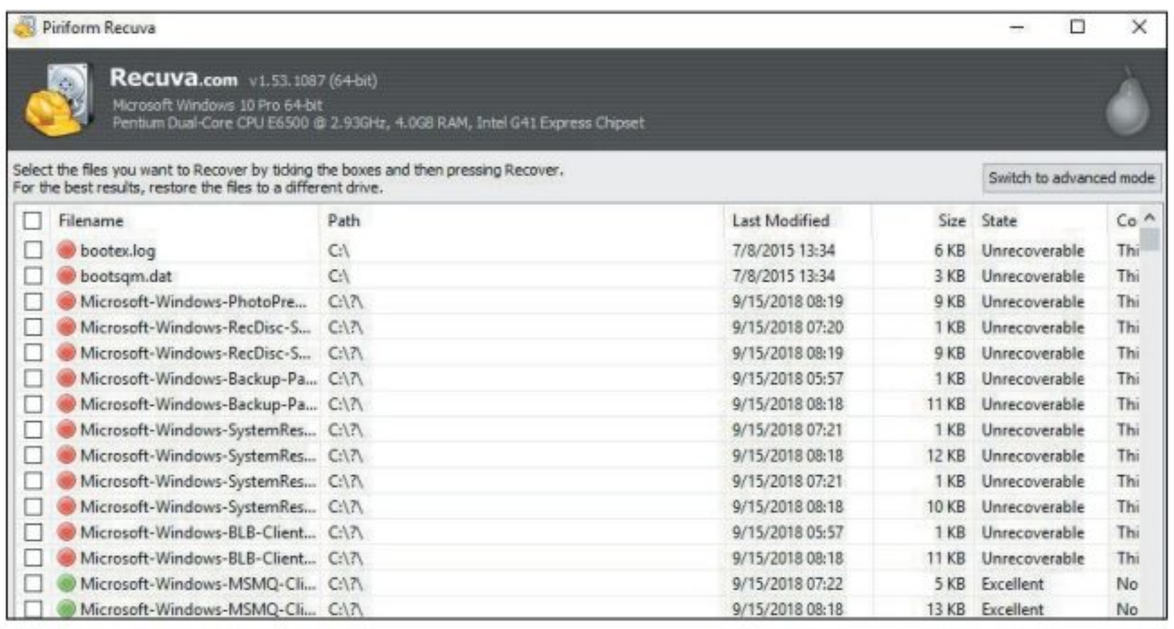
TOP 3 DES LOGICIELS POUR RÉCUPÉRER UN FICHIER EFFACÉ

Une erreur de manipulation et vous pensez avoir perdu un fichier à tout jamais ? Pas d'inquiétude, on vous présente notre sélection de logiciels gratuits pour le retrouver.

RECUVA : PUISSANT ET SIMPLE

Probablement le plus connu des logiciels présentés ici ! Recuva est développé par Piriform, l'éditeur de CCleaner, il vous sera d'ailleurs proposé de l'installer en même temps que Recuva. Beaucoup plus user-friendly que Windows File Recovery et Photorec, avec Recuva vous n'avez qu'à vous laisser guider par le logiciel qui vous demande quel type de document vous recherchez et dans quel dossier vous souhaitez le chercher. Recuva est donc parfait pour les débutants ou comme première approche lorsque vous avez perdu des fichiers. Il possède une option « deep scan » qui permet de récupérer plus de documents mais qui ralentit considérablement l'analyse.

Où le trouver ? **www.ccleaner.com/recuva**



WINDOWS FILE RECOVERY : LA NOUVEAUTÉ MICROSOFT

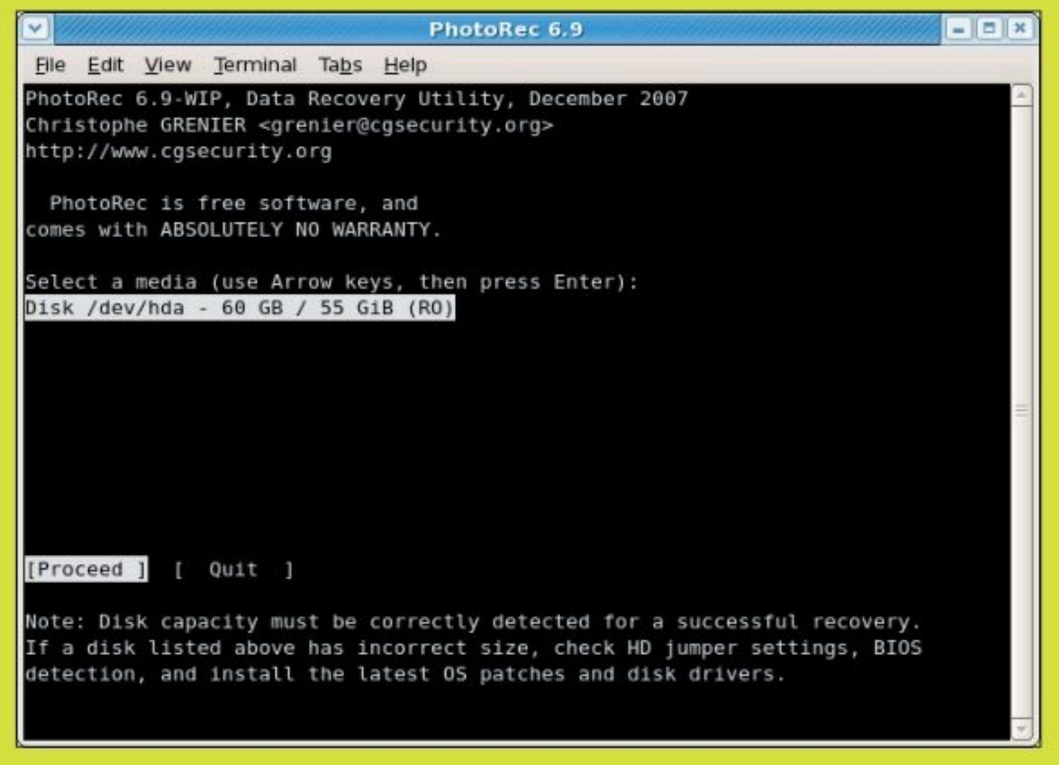
Microsoft lance son récupérateur de fichier qui fonctionne exclusivement sur la dernière version de Windows (à l'heure de l'écriture de cet article) : Windows 10 v2004. Pour télécharger le logiciel, rendez-vous sur le Microsoft Store. Windows File Recovery n'est pas un logiciel à mettre entre toutes les mains. Son absence d'interface graphique peut rebuter à la première utilisation. Cependant, il est capable de récupérer une grande variété de types de dossier comme les jpeg, png, pdf, docx, wma, mp4, mp3 etc. sur plusieurs supports différents (clé USB, carte SD, HDD et SSD). En revanche, il est impossible de récupérer des fichiers qui étaient stockés en réseau, sur un cloud par exemple. Pour apprendre à utiliser ce logiciel rendez-vous à la page suivante !

Où le trouver ? **Sur Microsoft Store à partir de la version 2004 de Windows 10**

PHOTOREC : LE DERNIER RECOURS

Comme son nom l'indique ce logiciel a été conçu à la base pour récupérer des images de carte mémoire d'appareil photo. Mais son champ d'action ne se limite pas aux photos, il est aussi capable de récupérer la plupart des autres fichiers. Photorec fonctionne en binôme avec TestDisk, un logiciel développé pour réparer les partitions de disques corrompues. Photorec a une interface graphique très simple : écrite blanche sur fond noir, mais il nécessite un peu de connaissances pour être pris en main. Cependant, il présente l'énorme avantage d'être capable de récupérer des fichiers même si le disque a été endommagé. Une solution de dernier recours en somme !

Où le trouver ? **www.cgsecurity.org/wiki/TestDisk_Download**

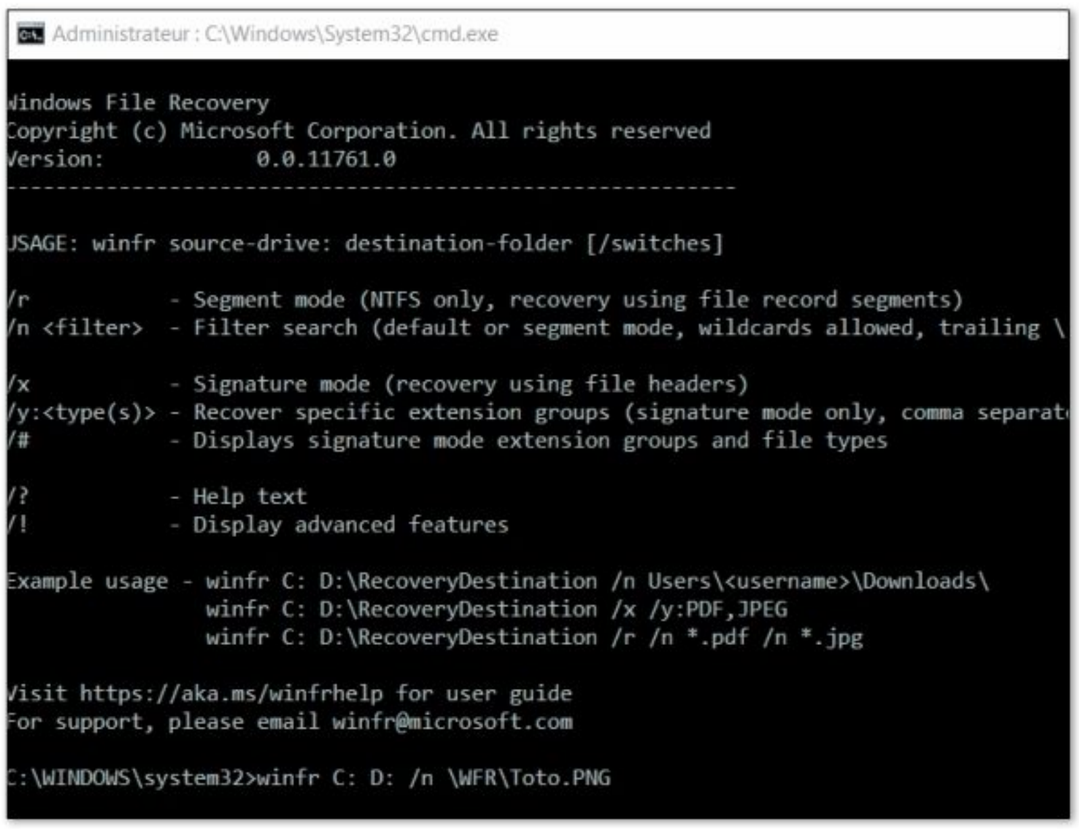


WINDOWS FILE RECOVERY EN ACTION

PRATIQUE

01› CHERCHER UN FICHIER

Lors de l'ouverture du logiciel, il demande les droits administrateurs. Cliquez sur **Oui**. Tapez ensuite la ligne de commande : **winfr** suivi du disque sur lequel était



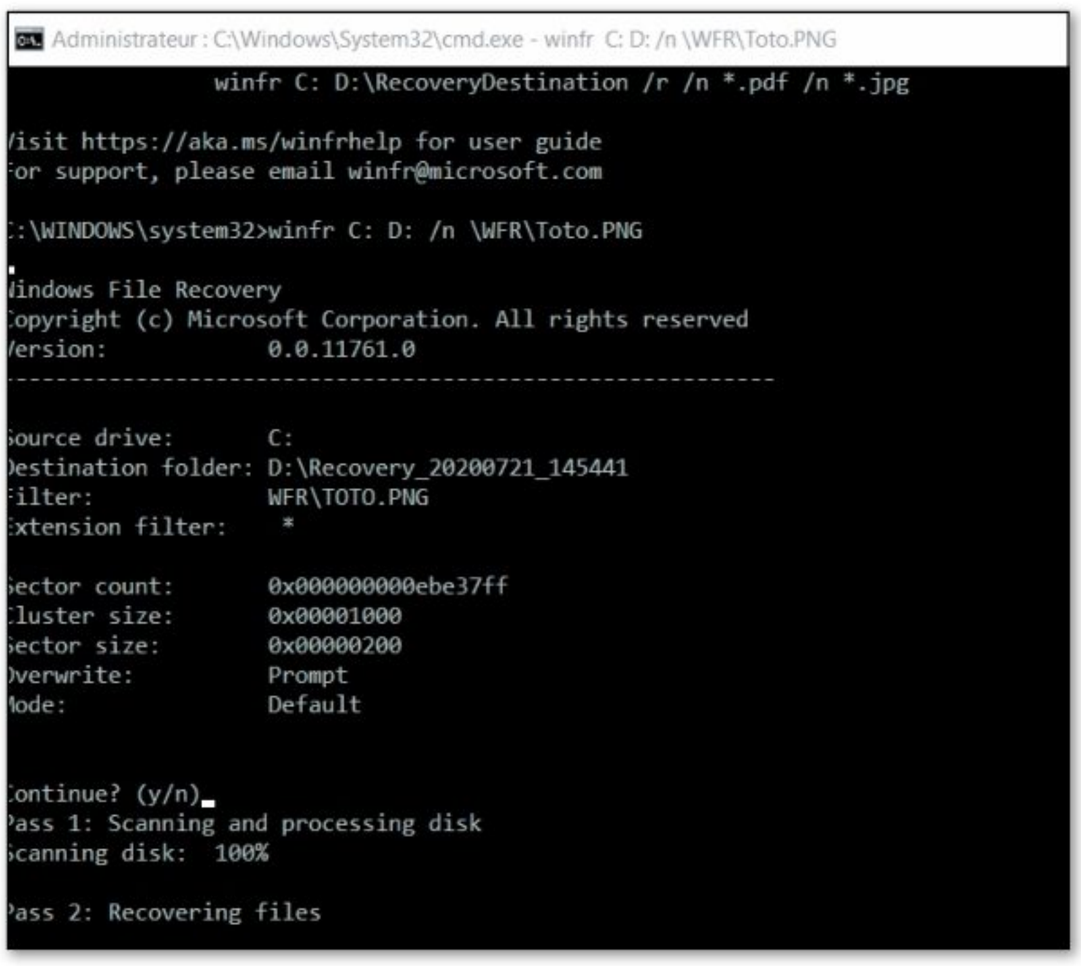
stocké le fichier (C : dans l'exemple) puis du disque sur lequel vous voulez le récupérer (D :), **/n** qui est le mode par défaut et enfin le chemin d'accès au fichier et son nom (\WFR\Toto.PNG). Ainsi vous obtenez la ligne de commande suivante :

winfre C : D : /n \WFR\Toto.PNG.

Appuyez sur **Entrée**.

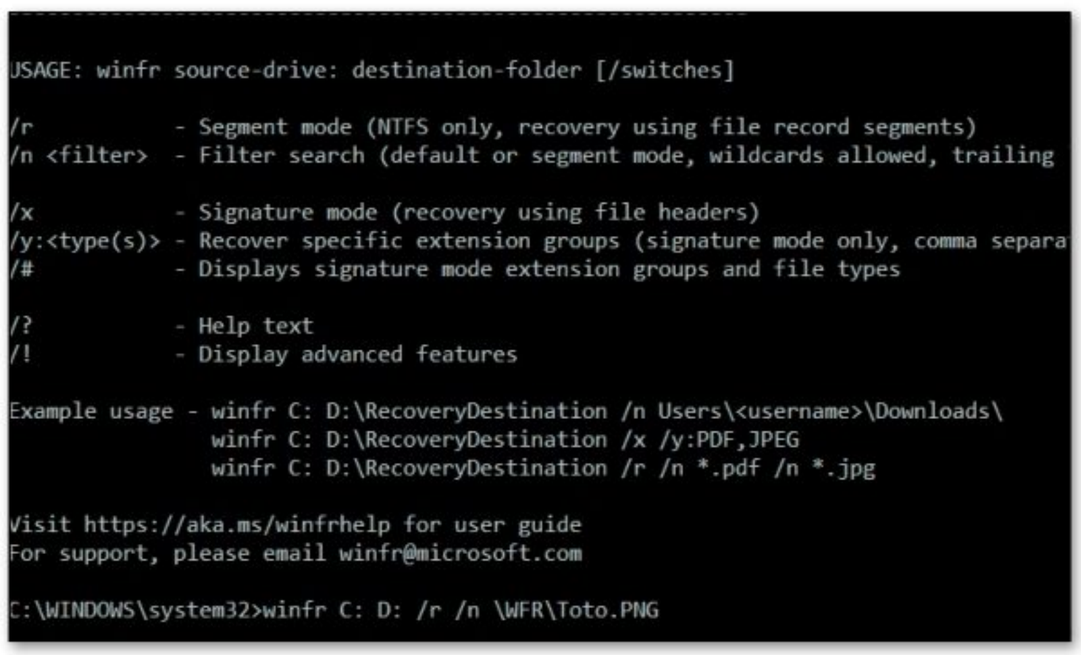
02› RETROUVER SON FICHIER

Windows File Recovery résume votre action et vous demande si vous souhaitez continuer. Appuyez sur **Y**. Il commence par scanner le disque puis récupère votre fichier. Il crée automatiquement un dossier dans lequel il l'enregistre s'il l'a trouvé. Tapez **Y** pour afficher ce dossier.



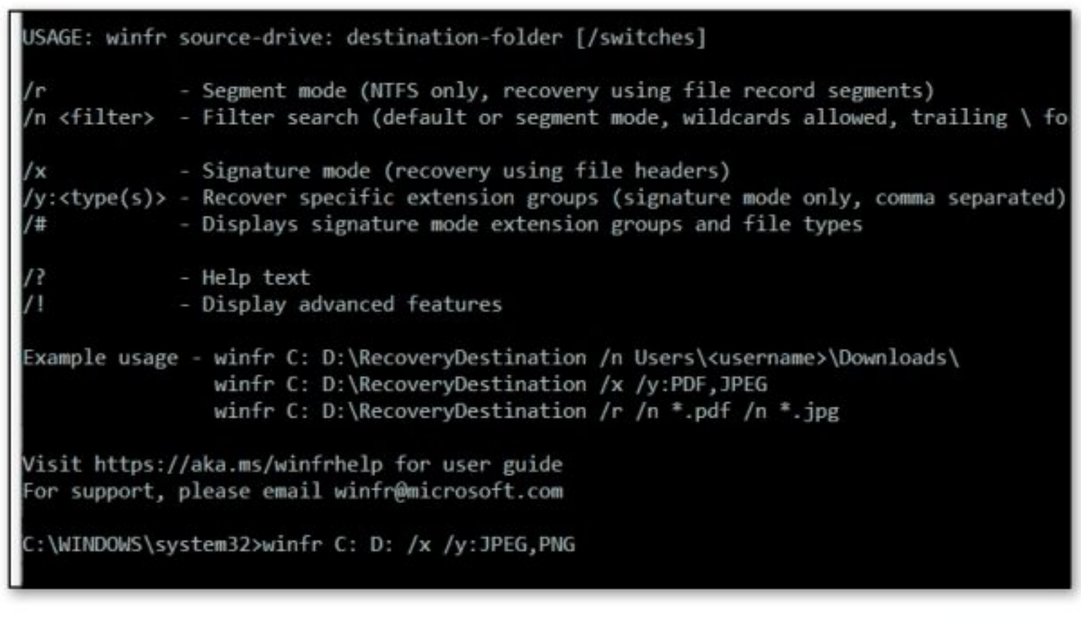
03› RETROUVER UN FICHIER SANS SON NOM

Impossible de vous rappeler du nom exact de ce fichier... Ou alors ce sont toutes vos photos de vacances qui ont disparu ? Il est possible de modifier la ligne de commande ! Le début est le même qu'à l'étape 1 mais à la place d'écrire le nom de votre fichier vous pouvez noter ***.PNG**, par exemple. Dans ce cas le logiciel cherchera tous les fichiers dont l'extension est PNG, peu importe son nom. L'étape 2 reste inchangée.



04› EXPLORER LES AUTRES MODES

L'étape 1, 2 et 3 présentent le mode par défaut du logiciel. Si votre fichier reste introuvable en mode par défaut, testez les autres. Le mode à utiliser ensuite est le Segment. Il est accessible en tapant **/r** juste avant **/n** dans la ligne de commande. Le mode de la dernière chance s'appelle Signature. Dans ce cas à la place de **/n** il faut taper **/x /y :** suivi de l'extension du fichier (JPEG, PNG par exemple). Le mode signature est plus lent que le mode segment lui-même plus lent que le mode par défaut. Si vous voulez arrêter l'analyse pressez **Ctrl + C**



ATTENTION À L'ANTIVIRUS

Vous avez essayé les trois logiciels et aucun ne trouve votre fichier ? Dans certains cas, les antivirus peuvent bloquer la recherche des logiciels, sans même vous prévenir ! Désactivez l'antivirus et retentez le coup.

TUTO

INSTALLEZ UN CLOUD PRIVÉ SUR VOTRE PC

POUR QUI ?

Pour ceux qui veulent une solution en local

POUR QUOI FAIRE ?

Tout transférer, partager, synchroniser

Pour partager facilement documents et médias entre votre PC et votre smartphone, il y a les services de Cloud. Daemon Sync offre une autre solution, avec laquelle vos fichiers restent sur votre disque dur.

Les services de Cloud se multiplient sur Internet, et il peut parfois être difficile de choisir à qui confier ses données. Certains sont payants, d'autres sont gratuits, la plupart ont une limitation d'espace de stockage, c'est une vraie jungle ! Et avec ces services se pose généralement la question de la confidentialité : nous n'avons pas forcément envie de confier nos données à Google, via son Drive, ou à Microsoft, via OneDrive. L'idée de stocker photos et vidéos persos sur Internet peut mettre mal à l'aise.

SÛR ET GRATUIT

Avec Daemon Sync, vous pouvez créer votre propre Cloud privé, avec lequel vos données sont sauvegardées uniquement sur votre ordinateur. La synchronisation avec vos appareils mobiles se fait en Wi-Fi. Pas de stockage en ligne, pas d'abonnement à payer, vous gardez totalement la main sur vos données. Quelques contraintes toutefois : les différents appareils doivent être sur le même réseau Wi-Fi que votre PC, qu'il faut évidemment laisser allumé.

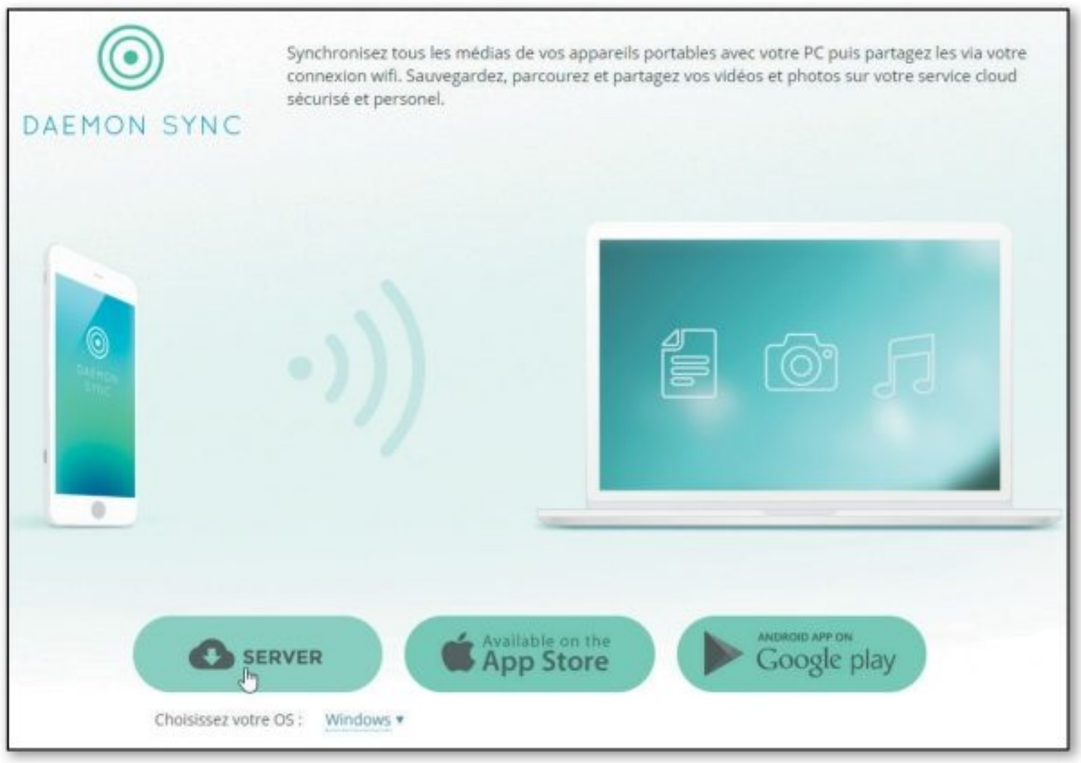
INFOS [Daemon Sync]
Où le trouver ? [https://tinyurl.com/DaemonSyncTA]
Difficulté : ☠☠☠

PARTAGER LES DONNÉES AVEC DAEMON SYNC

PRATIQUE

01› INSTALLER LE LOGICIEL

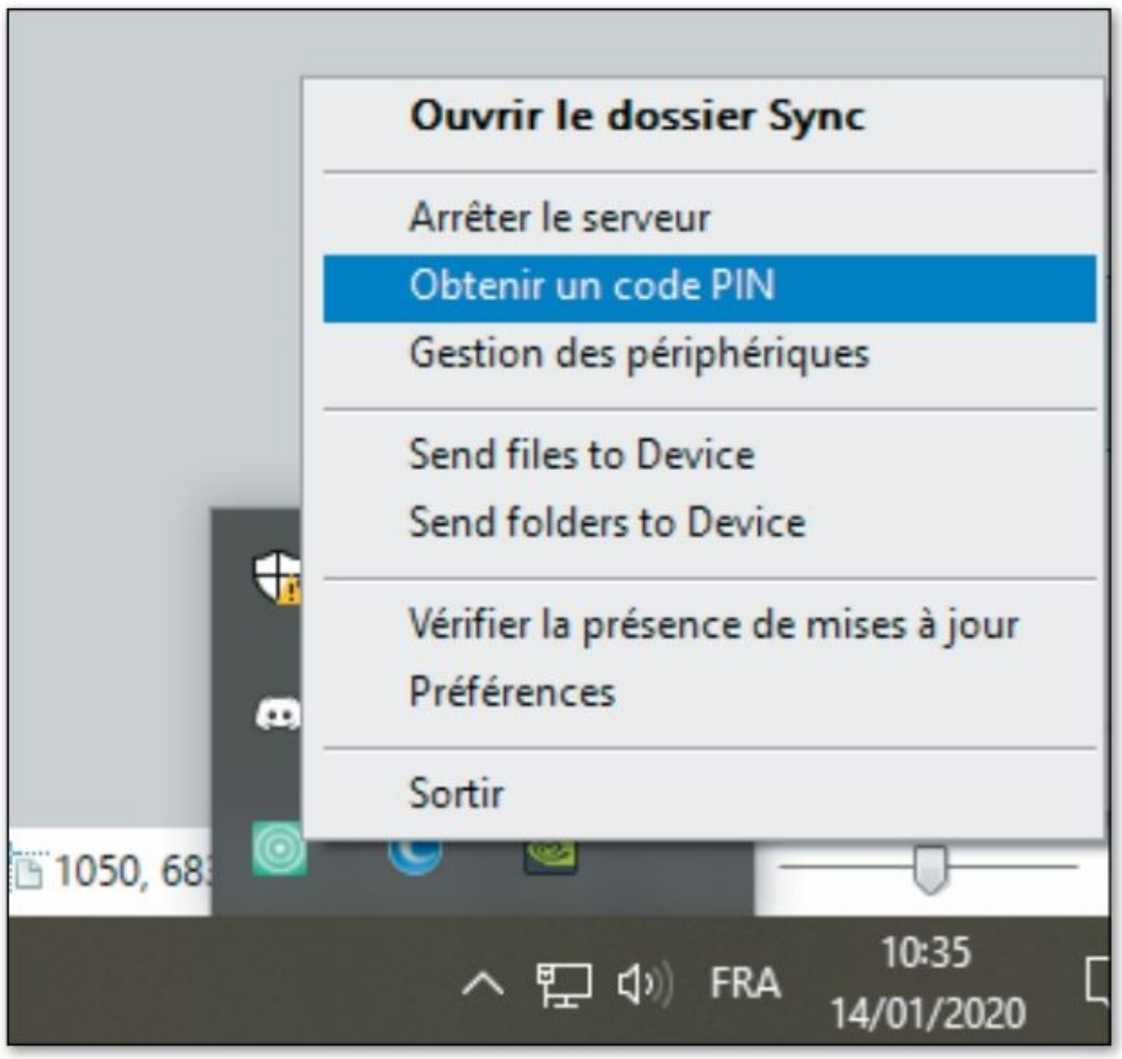
Pour que Daemon Sync fonctionne, il faut installer le logiciel sur votre PC (sur le site, télécharger **Server**),



et installer l'appli sur votre smartphone (via Google Play ou via l'App Store, en recherchant **Daemon Sync**. Tous les appareils doivent être connectés au réseau Wi-Fi de votre box Internet.

02› CONNECTER LES APPAREILS

Lorsque vous lancez Daemon Sync sur votre téléphone, l'appli cherche un serveur. À priori, il n'y aura que votre ordinateur : sélectionnez-le. Un code pin vous est demandé. Sur votre PC, cliquez sur la flèche en bas à droite de votre écran pour afficher les icônes cachées, puis faites un clic droit sur celle de Daemon Sync et **Obtenir un code PIN**. Entrez ce code sur votre téléphone.



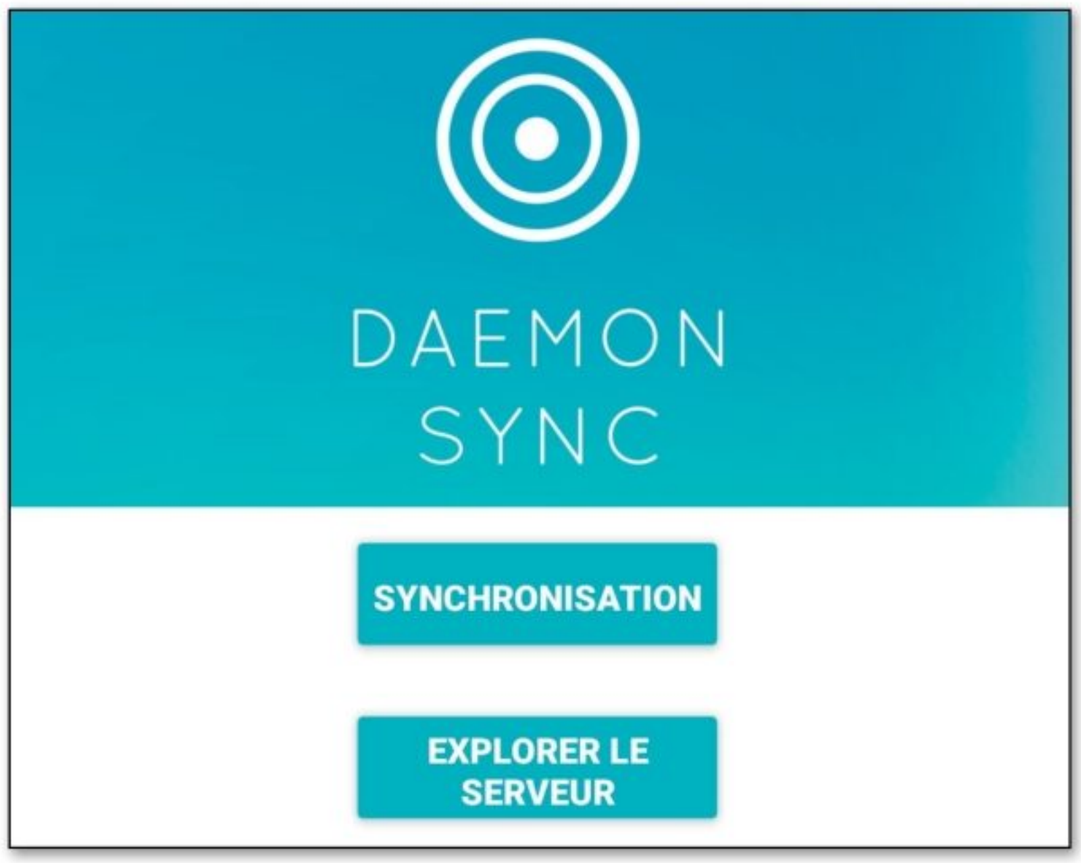
03› CHOISIR LES DOSSIERS

Sur votre téléphone, cliquez sur les 3 points en haut à droite, puis sur **Paramètres**. Sous **Options de sauvegarde**, cliquez sur **Que sauvegarder**. Des dossiers de base vous sont proposés, avec la possibilité de les

décocher si vous n'en voulez pas. Vous pouvez également en choisir d'autres via **Dossiers Personnalisés**, en cliquant sur le **+** vert puis en choisissant les dossiers voulus. Validez avec **Confirmer**.

04› SYNCHRONISER LES DONNÉES

Revenez à la page d'accueil de l'appli mobile, et faites **Synchronisation**. L'opération peut être assez longue. Attention : le Wi-Fi ne doit pas être désactivé pendant la durée de la synchronisation, et l'ordinateur doit rester allumé. Par défaut, la synchronisation se fait toutes les 15 minutes, vous pouvez modifier cette périodicité dans les **Paramètres**.



DECRYPTAGE

HACKINTOSH : ÊTES-VOUS PRÊT À EN CROQUER ?

Se libérer d'Apple et de ses tarifs exorbitants tout en gardant le meilleur ? C'est la promesse des alternatives « Hackintosh » : un PC puissant tournant sous Mac ou une petite beauté design… pour deux fois moins cher.

RÉGULIÈREMENT, DES PME SURFENT SUR LA TENDANCE ET ESSAIENT DE SE LANCER DANS LA VENTE DE PC HACKINTOSH CLÉ-EN-MAIN. ICI, UN MODÈLE DE OPENCORE, LANCÉ EN JUIN 2020. UN MOIS PLUS TARD, LA BOUTIQUE ÉTAIT FERMÉE. LA FAUTE À APPLE (QUI ATTAQUE RÉGULIÈREMENT CE GENRE D'INITIATIVE) OU ESCROQUERIE CARACTÉRISÉE ?

C'est un marronnier : les Mac coûtent (trop) cher. Et en plus, gare à ceux qui voudraient faire durer leur appareil. En matière d'ordinateur comme de smartphone, Apple est le champion de l'obsolescence programmée. Composants soudés et non remplaçables, connectiques spécifiques et non standard, puce T2 qui contrôle et bloque, mises à jour logicielles qui ralentissent, problèmes de batteries… la liste est longue d'événements spécifiquement produits pour encourager l'utilisateur à s'équiper de l'appareil dernier cri.

SYSTÈME DE DÉFENSE CONTRE SYSTÈME PROPRIÉTAIRE

Le problème est financier pour l'utilisateur et environnemental pour la planète. Frédéric Bordage, expert indépendant en numérique responsable et Green IT (www.greenit.fr) précise : « *Apple cherche à handicaper les reconditionneurs et les utilisateurs qui se tournent vers des composants génériques et des réparateurs non officiels. La méthode est simple. Comme le révèle www.ifixit.com sur son blog, si vous changez la batterie de votre iPhone sans passer par ses services, Apple désactive la fonctionnalité de contrôle de l'état de santé de la batterie. Votre iPhone affiche alors le message suivant : impossible de vérifier que cet iPhone dispose d'une batterie Apple authentique. Information de santé non disponible pour cette batterie.* »

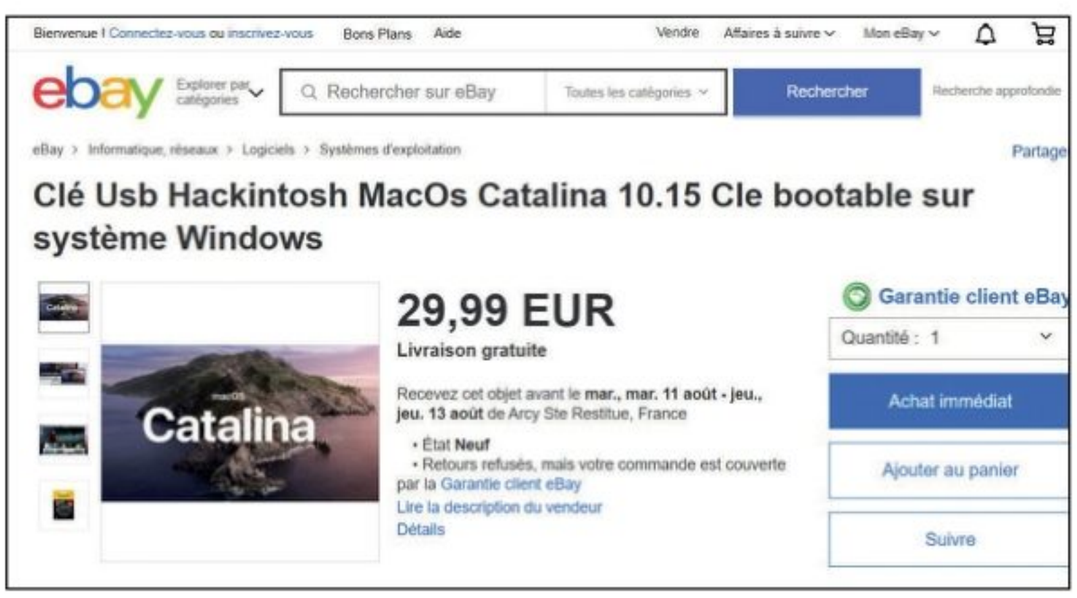
C'est bien pour lutter contre ce genre de pratiques que l'association Halte à l'obsolescence programmée, à l'origine des plaintes contre Apple et Epson, s'est félicitée de la sanction de 25 millions d'euros annoncée le 7 février dernier contre Apple, pour le ralentissement de certains de ses téléphones. Une punition qui représente peu de chose au regard du chiffre d'affaires monstrueux de la firme (plus de 250millards de dollars en 2019).

Etonné ? Pas vraiment quand on voit qu'au dernier salon WWDC, la pomme a présenté un Mac Pro équipé dernier cri à plus de 50 000 $. Pourquoi s'en priver ? Mon grand-père me disait : « Il y a un pigeon qui se lève chaque matin… ». On le sait, quand on choisit Apple, on entre dans le monde fermé et intégré de l'univers propriétaire. Tout l'inverse de l'open source, de la liberté et du choix.

HACKINTOSH : LA POMME CANADA-DRY

C'est pour répondre aux pratiques parfois douteuses d'Apple, que des utilisateurs ont choisi de créer le mouvement Hackintosh. Rejoint par des particuliers, des associations et de petites entreprises, ce dernier tire son nom de la contraction de « hack » et « Macintosh », avec pour but de faire tourner l'OS X (désormais macOS) sur des ordinateurs non conçus par Apple. Ce sera un Canada-Dry, mais on gardera l'ivresse !

Il suffit d'avoir une clé USB bootable, une clé USB vierge d'au moins 8 GO, une copie de Mac OS ou une clé USB préinstallée, des logiciels Unibeast et Multibeast (selon la version de Mac OS), de paramétrer la langue du Mac en anglais... et bien sûr d'un ordinateur compatible. Le processus d'installation est un peu complexe mais le résultat plutôt satisfaisant au regard du prix (selon les configurations autour de 600 euros pour retrouver une configuration Mac de base).
Vous hésitez à ouvrir le capot ? Alors ouvrez bien vos yeux. Des Hackintosh sont régulièrement proposés à la vente sur certains sites, mais leur adresse est parfois éphémère. Attention aux URL qui ne durent que quelques semaines, vous risqueriez de ne jamais recevoir votre précieux ordinateur. Bref, Apple fait encore rêver, mais les réveils sont parfois douloureux.



TOUT S'ACHÈTE, TOUT SE VEND
Y COMPRIS DES CLÉS BOOTABLES
POUR INSTALLER MACOS
SUR VOTRE PC.

QUELQUES ADRESSES UTILES

> **hackintosh.com :** tutos et matériels (en anglais).

> **www.passtech.fr :** trè bon sites avec de nombreuses ressources et projets clés en main (en français).

> **hackintoshfrance.fr :** le forum des passionnés francophones.

> **forum.macbidouille.com :** un forum incontournable. Tout est dit dans l'URL.

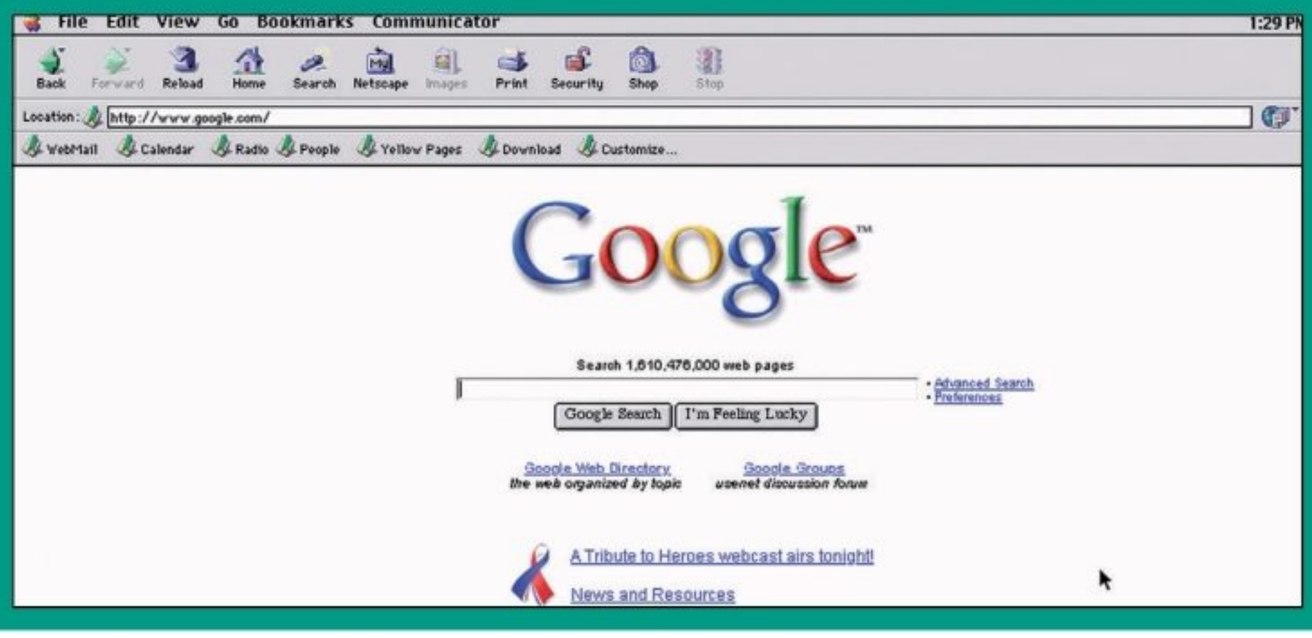
> **www.hackintosh-montreal.com :** ils sont forts ces Québécois.

> **hackintoshfrance :** de nombreux partages et exemples de configs.

Remonter le temps > AVEC OLDWEB.TODAY

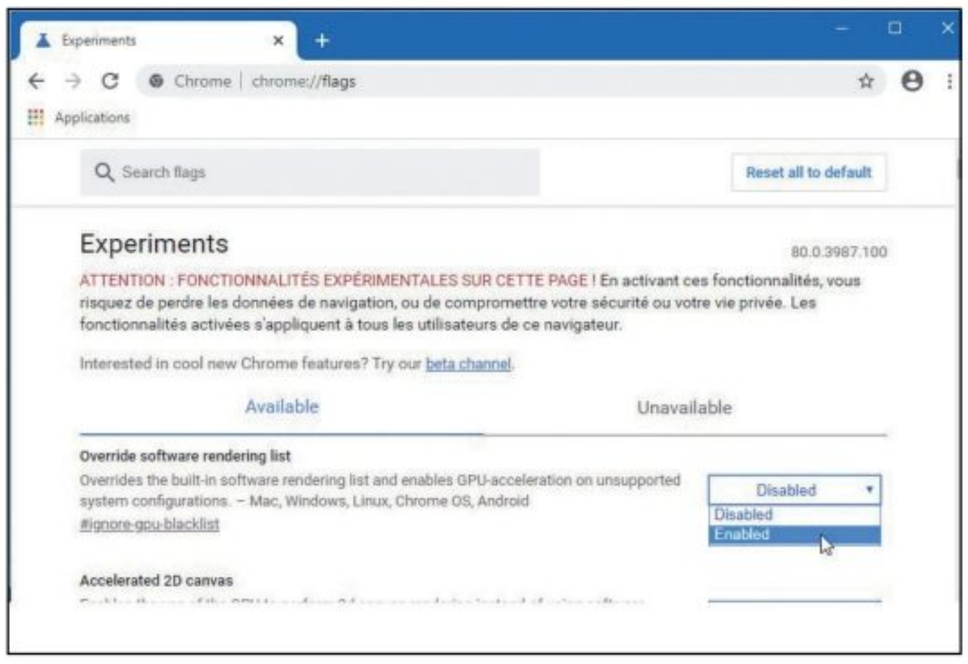
Par curiosité, parce que vous voulez retrouver un site aujourd'hui disparu ou juste pour montrer aux jeunes ce que c'était le Web il y a quelques années, visitez oldweb.today. Choisissez un navigateur (**Browser**),tapez une **URL** et sélectionnez une date. Cliquez sur **Surf the old Web !** et attendez quelques instants. Vous voilàrevenu dans le passé, sur un navigateur d'un autre temps. On saluera le travail d'archivage.

http://oldweb.today



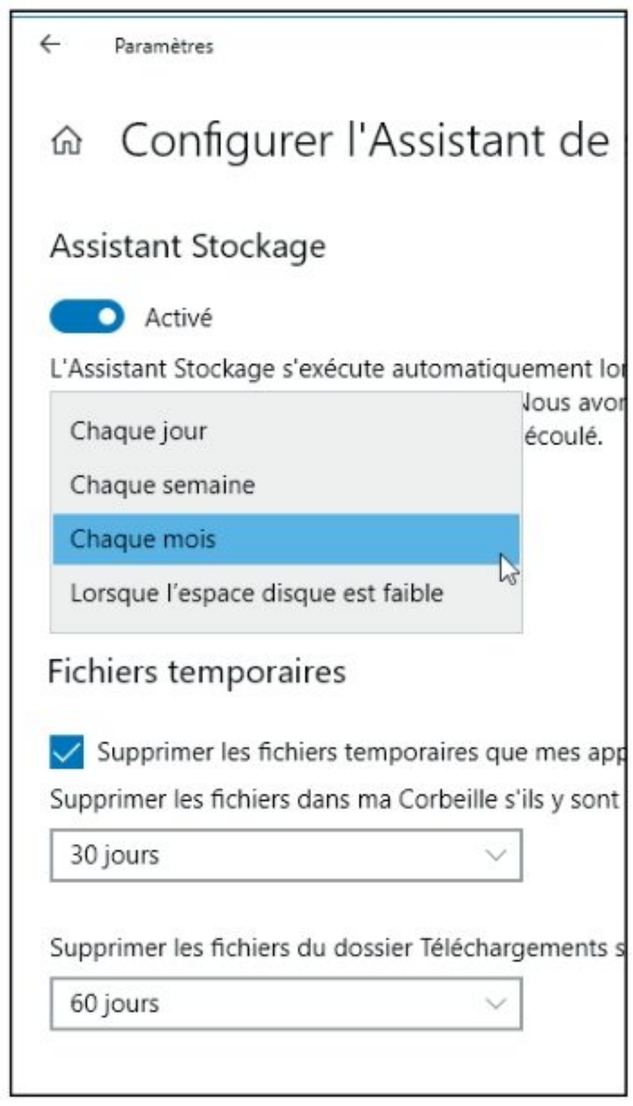
Activer des fonctions expérimentales > AVEC CHROME

Le navigateur Chrome possède des fonctions expérimentales cachées. Pour les voir et éventuellement les activer, tapez **chrome://flags** dans la barre d'adresse. Vous n'avez plus qu'à cliquer sur **Enabled** quand vous voyez une fonction qui vous intéresse. Attention : cela peut entraîner des dysfonctionnements plus ou moins importants.
Soyez prudent.



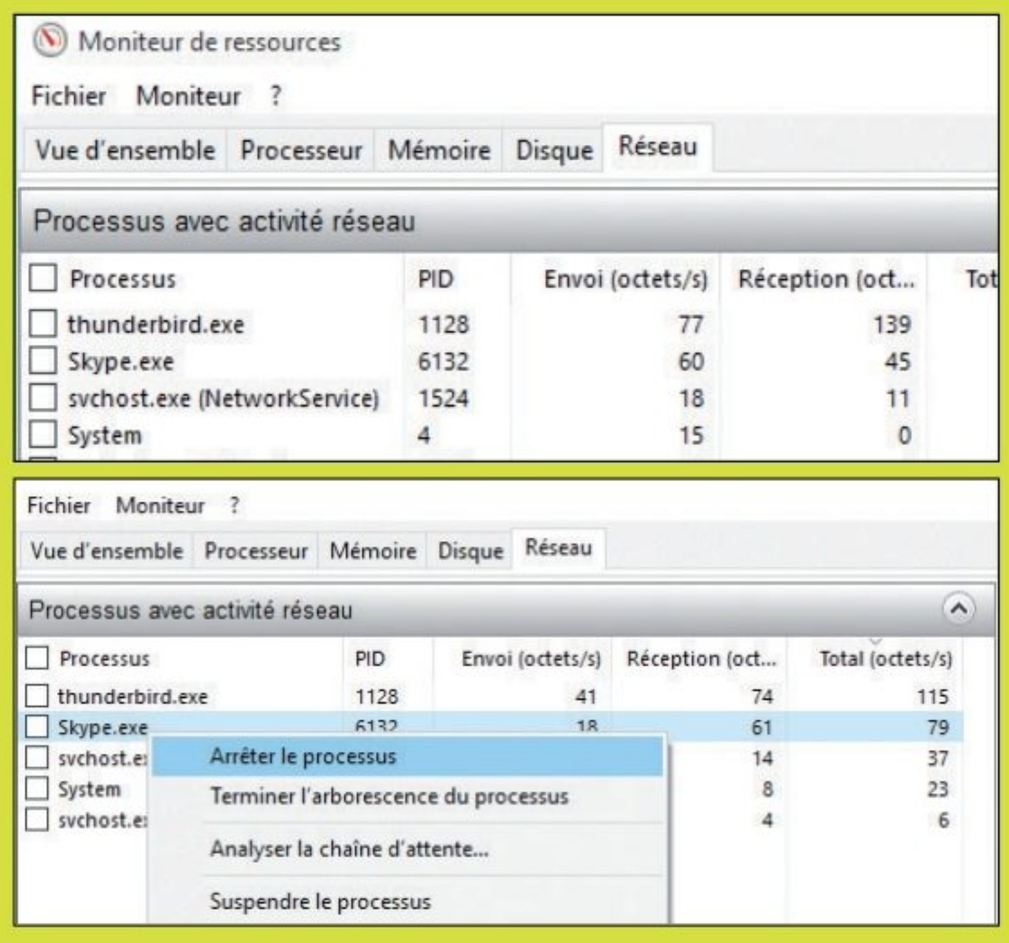
Automatiser le nettoyage du disque
> AVEC WINDOWS 10

Windows 10 s'est doté d'une fonction de nettoyage automatique du disque dur, permettant de supprimer les fichiers temporaires obsolètes, ainsi que les documents qui sont dans la **Corbeille** depuis un certain temps, ou ceux qui ont été oubliés dans le dossier **Téléchargements**. Allez dans **Paramètres > Système > Stockage** et placez le curseur sur **Activé**. Cliquez sur **Configurer l'Assistant...** pour ajuster son fonctionnement.



Arrêter les processus qui monopolisent la connexion
> AVEC MONITEUR DE RESSOURCES

Tapez **resmon** dans la barre de recherche du menu **Démarrer** et ouvrez **resmon.exe**. Basculez sur l'onglet **Réseau**. Notez le(s) programme(s) qui consomme(nt) beaucoup de bande passante sous la colonne **Total**.
Faites un clic droit sur le processus repéré et **Arrêter le processus**.
Vous pouvez aussi **Suspendre le processus** pour le réactiver plus tard. Si vous avez un doute sur son utilité, sélectionnez **Recherche en ligne**.



2€95 seulement

NOUVEAU ! TOUT FAIRE AVEC SON PC > POUR 2,95€ seulement !

L'Officiel PC

100% PRATIQUE

LES

130

MEILLEURS LOGICIELS & SERVICES

GRATUITS

TOUT FAIRE COMME UN PRO

Les GUIDES ESSENTIELS MINI PRIX !

BEST-OF GUIDE

- DOPEZ WINDOWS
- VIDÉOS, AUDIO, PHOTOS
- BUREAUTIQUE FACILE
- VIE PRIVÉE ET SÉCURITÉ

+ 25 TUTOS ESSENTIELS ÉTA

LES GUIDES ESSENTIELS À PRIX MINI

NOUVEAU

Chez votre marchand de journaux

DECRYPTAGE

ENCROCHAT

LES SMARTPHONES DE LA MAFIA RÉVÈLENT LEURS SECRETS

Un vaste réseau de communication censé garantir l'anonymat de ses utilisateurs est tombé dans la nuit du 12 au 13 juin dernier. Près de 60 000 utilisateurs dans le monde (dont 90% de criminels) étaient clients de EncroChat, un entreprise vendant des téléphones chiffrés spécialement conçus pour protéger les échanges et activités d'individus et d'organisations criminelles. Près d'un millier de personnes ont pu être arrêtées grâce à cette opération... et ce n'est qu'un début.

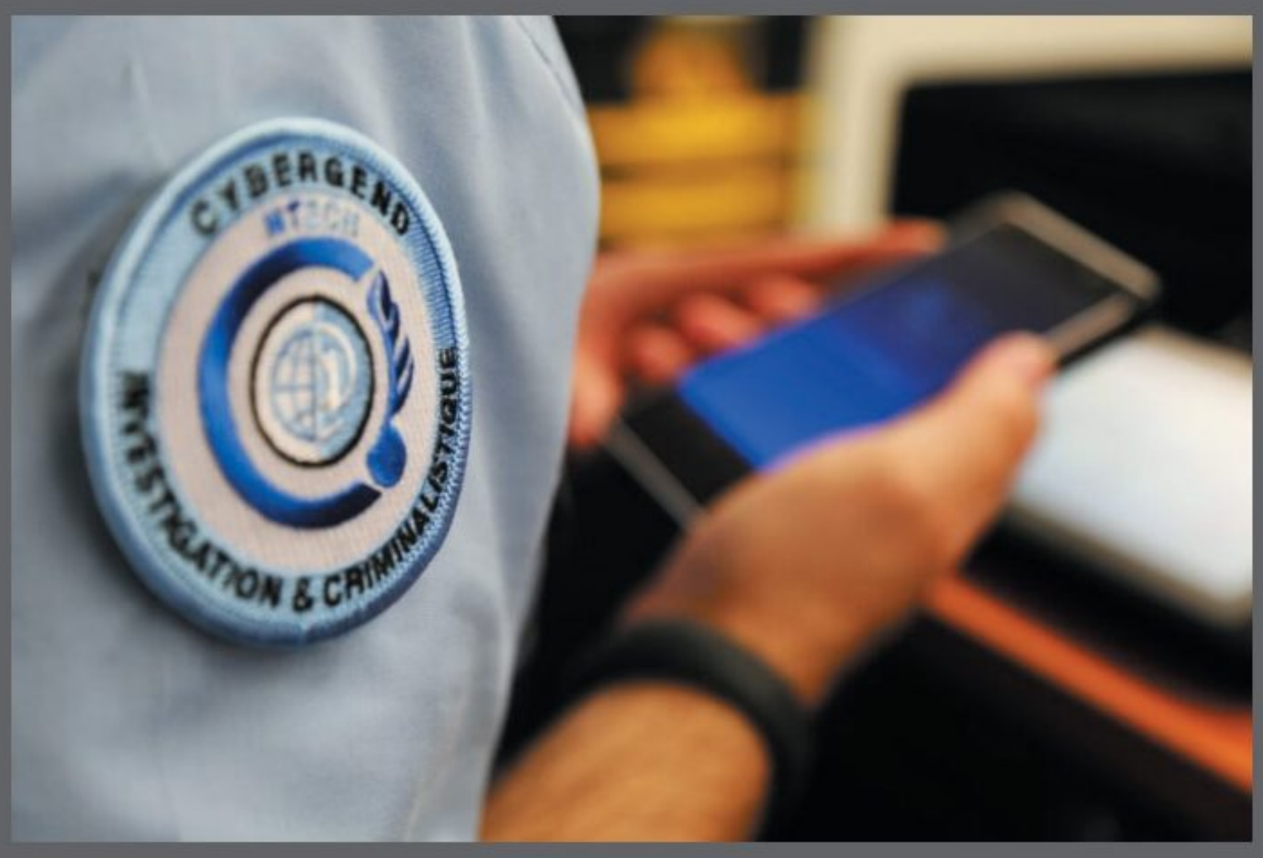
Depuis 2017, la gendarmerie et les autorités judiciaires françaises enquêtent sur les « Encrophones » après avoir observé que ces téléphones, censés garantir l'anonymat de leurs utilisateurs, étaient régulièrement retrouvés dans des opérations visant des groupes criminels organisés. Ils ont senti qu'il y avait un coup à jouer quand ils ont découvert que l'entreprise EncroChat qui les commercialisait fonctionnait à partir de serveurs situés en France. C'est notamment grâce aux serveurs situés à Roubaix (Nord), qu'un malware « made in gendarmerie nationale » a pu être injecté au cœur du réseau EncroChat.

Une fois connecté aux nœuds de ce dernier, il a été possible de mettre en place un dispositif technique permettant de contourner le chiffrement et d'avoir accès à la correspondance des utilisateurs… sans se faire remarquer pendant de nombreux mois ! Cela paraît simple dit comme ça, mais il s'agit d'une véritable prouesse technique qui place à nouveau les cyber-enquêteurs Français dans le « big game ». C'est en coopération avec la police néerlandaise, Europol et Eurojust que les enquêteurs ont pu, petit à petit, dénouer un écheveau européen d'envergure inédite.

> Début juillet, le plus grand coup jamais porté à la criminalité internationale était révélé lors d'une conférence de presse pilotée par les autorités policières et judiciaires françaises et néerlandaises, Europol et Eurojust

LES CYBER-GENDARMES FRANÇAIS DE RETOUR DANS LE « BIG GAME »

Revenus de loin, les techniciens et enquêteurs de la gendarmerie scientifique ont gagné le respect de leurs homologues internationaux ces dernières années. Il y a des compétences sous le capot et quelques succès leur ont offert une petite réputation (hackings Blackberry, Telegram ou lutte contre le rançongiciel Retadup). À la clé, des financements européens leur ont permis de s'acheter des calculateurs plus puissants et ils ont aussi pu intégrer le «Secure communication group», le club très fermé des meilleurs labos de police scientifique du monde. Et c'est notamment en partenariat avec le Netherlands Forensic Institute que les gendarmes Français ont pu mener à bien leur piratage d'EncroChat. Un dernier fait d'armes au retentissement colossal auprès des services de renseignements internationaux.



ANONYMAT

120 MILLIONS DE MESSAGES INTERCEPTÉS

Des millions de messages et de données ont été examinés en temps réel, permettant l'arrestation de centaines de personnes, principalement en Europe (France, Pays-Bas, Royaume-Uni, Suède, Norvège, Italie…). On parle de 120 millions de messages, textes et images au total (1 à 2 millions de messages par jour quand même…).

Beaucoup de ces enquêtes étaient liées au trafic international de drogue et à des activités criminelles violentes.

TROP TAAARD…

L'interception des messages EncroChat a pris fin le 13 juin 2020, lorsque la société a réalisé qu'une autorité publique avait pénétré sa plateforme. Elle a alors envoyé un avertissement en mode panique à tous ses utilisateurs : « Aujourd'hui, notre domaine a été saisi illégalement par des entités gouvernementales et une attaque a été lancée pour compromettre nos unités [...] En raison du niveau de sophistication de cette attaque et du code malveillant, nous ne pouvons plus garantir la sécurité de votre terminal. Nous avons pris une action immédiate sur notre réseau en désactivant le réseau pour combattre l'attaque. Vous êtes avisés d'éteindre et de vous séparer de votre terminal immédiatement ».

> Les criminels tombent comme des mouches depuis 2019… sans savoir que ce sont leurs téléphones qui les trahissaient

CHRONOLOGIE DE L'ENQUÊTE EN FRANCE

> DÈS 2017 : Les téléphones utilisant le moyen de communication sécurisée EncroChat sont détectés par le département Informatique Électronique (INL) de l'Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN). Des travaux de recherches approfondies débutaient, dont l'objectif était d'en comprendre le fonctionnement.

> 15 NOVEMBRE 2018 : Ouverture d'une enquête préliminaire par le C3N (Centre de lutte Contre les Criminalités Numériques) ; Premières investigations techniques.

> DÉBUT 2019 : Le projet CERBERUS, piloté par la gendarmerie et financé par des fonds européens, permettait l'accélération les recherches de l'IRCGN sur ces téléphones.

> LE 15 MARS 2020 : La Sous-Direction de la Police Judiciaire (SDPJ) est décidée la création d'une cellule nationale d'enquête implantée à Pontoise, au sein du C3N. Le code de l'opération devient : EMMA 95. Elle s'articule autour d'un Poste de Commandement (PC) et de différents groupes d'enquête. renforcée par des enquêteurs aguerris des Sections de Recherches (SR) de toute la France et des 4 offices centraux (OCLTI, OCLAESP, OCLDI, OCLCH), elle compte à ce jour 60 gendarmes employés à plein temps et répartis sur les missions d'analyse de la donnée et d'investigations techniques et judiciaires.

> DANS LA NUIT DU 12 AU 13 JUIN 2020 :
Une alerte de sécurité est diffusée par la structure EncroChat à sa clientèle, indiquant notamment que le service était victime d'une « saisie illégale », par des « entités gouvernementales ». Il leur était notamment conseillé de se débarrasser physiquement de leur terminal.

La France n'a quasiment pas communiqué sur les résultats de ses investigations et jouait encore la carte de la discrétion au moment où nous écrivons ces lignes. La Grande-Bretagne, en juillet dernier, parlait déjà de 750 arrestations, de dizaines de meurtres empêchés et de plus de 50 millions de livres sterling saisis. Les Pays-Bas listaient quant à eux 19 labos de drogue synthétique démantelés, 8 tonnes de cocaïne et 20 millions d'euros saisis, plus de 100 arrestations et… une salle de torture découverte. L'Amérique du Nord et surtout l'Amérique du Sud sont également concernées, EncroChat s'y étant largement implanté ces dernières années.

Quant aux fondateurs d'EncroChat, pas de traces aux dernières nouvelles…

LE FONCTIONNEMENT D'UN TÉLÉPHONE ENCROCHAT DÉCORTIQUÉ

1. EncroChat ne fabriquait pas ses propres appareils mais customisait principalement des smartphones de la marque espagnole BQ.

2. Pas d'association de l'appareil ou de la carte SIM avec le compte du client, acquisition dans des conditions garantissant l'absence de traçabilité

3. Carte SIM internationale pouvant appeler et être appelée dans le monde entier sans surcoût. Associés aux protocole de VoIP ZRTP, ces appels étaient chiffrés.

4. Chiffrement de tout l'appareil, des contenus, appels, navigation Web, etc. dès l'ouverture du téléphone.

5. Double système d'exploitation, l'interface cryptée étant masquée pour être non détectable. L'intérêt : lors d'une saisie, le téléphone apparaît comme normal, sans rien de compromettant. Le contenu sensible est présent sur le deuxième système, une version modifiée d'Android, qui ne s'active que si l'on presse une série de touches précise.

6. Les utilisateurs pouvaient demander à ce que le téléphone soit livré sans caméra, microphone, GPS ou USB pour échapper aux techniques habituelles de cyber-surveillance.

7. Suppression automatique des messages sur les terminaux de leurs destinataires.

8. Code PIN spécifique destiné à la suppression immédiate de toutes les données sur l'appareil, suppression de toutes les données en cas de saisies consécutives d'un mauvais mot de passe.

9. L'appareil pouvait aussi être effacé à distance par le revendeur/service d'assistance (24h/24).

EncroChat vendait ses téléphones au prix unitaire de 1000 € et proposait des abonnements avec une couverture mondiale à un coût de 1500 € pour une période de six mois, avec un support 24/24.

LA GUERRE DES TÉLÉPHONES CHIFFRÉS

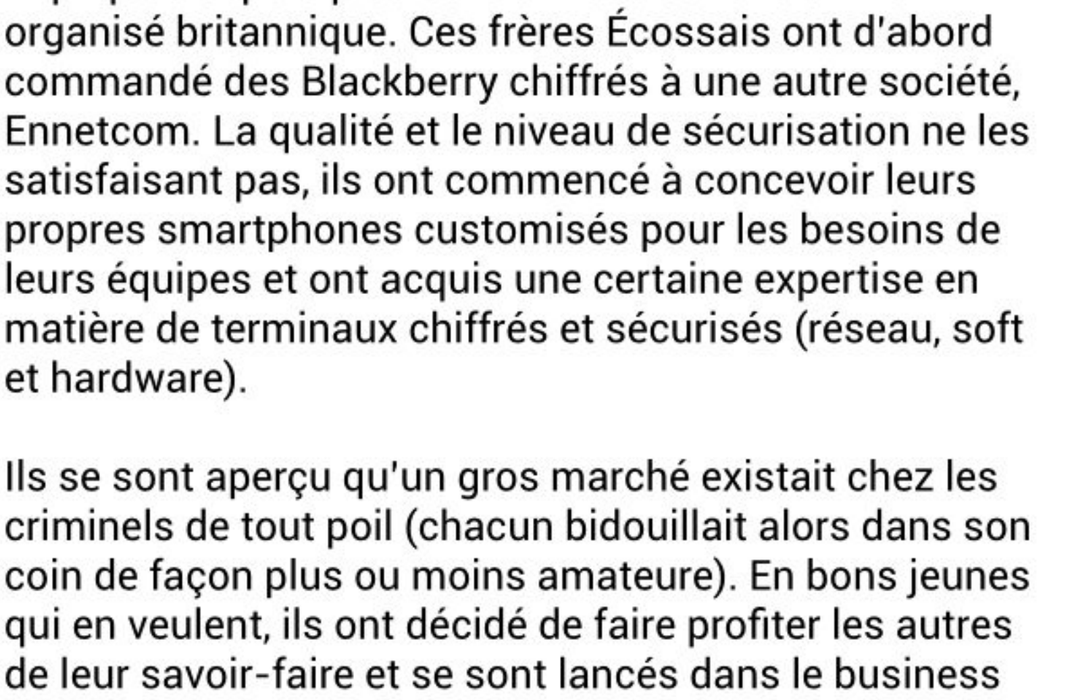
Si Encrochat est désormais mondialement connue, l'entreprise n'est que l'un des principaux acteurs de ce business sous-terrain.

Certains concurrents sont eux-même des groupes criminels. Quant à la clientèle, vous devez traiter avec des organisations parmi les plus violentes et les plus mafieuses au monde. Si on se doute que le SAV doit être parfait, il faut aussi penser au marketing, critiquer discrètement la concurrence sans se faire tromblonner en retour et attaquer de nouveaux segments prometteurs. Un marché juteux… mais stressant. Le mieux qui puisse vous arriver est de vous faire dénigrer par la concurrence.

ASCENSION ET CHUTE DE MPC

L'une des premières marques a avoir atteint une renommée internationale est MPC qui distribuait ses téléphones en Europe mais aussi en Amérique du Sud et du Nord. Il s'est avéré que les fondateurs de cette entreprise, James and Barrie Gillespie, étaient connus dans le milieu sous le patronyme « The Brothers », impliqués depuis plusieurs années dans le crime organisé britannique. Ces frères Écossais ont d'abord commandé des Blackberry chiffrés à une autre société, Ennetcom. La qualité et le niveau de sécurisation ne les satisfaisant pas, ils ont commencé à concevoir leurs propres smartphones customisés pour les besoins de leurs équipes et ont acquis une certaine expertise en matière de terminaux chiffrés et sécurisés (réseau, soft et hardware).

Ils se sont aperçu qu'un gros marché existait chez les criminels de tout poil (chacun bidouillait alors dans son coin de façon plus ou moins amateure). En bons jeunes qui en veulent, ils ont décidé de faire profiter les autres de leur savoir-faire et se sont lancés dans le business des smartphones chiffrés avec MPC en 2015.
Mais comment attirer des clients du monde entier ?



Comme tout le monde, en plaçant des pubs sur des sites spécialisés, en communicant sur les réseaux sociaux et en distribuant des produits dérivés (tee-shirts, mugs, …) !

ÇA DÉRAPE...

Mais MPC n'était pas une boîte comme les autres. Quand un partenaire supposé (Martin Kok) se fait tuer par balle en compagnie de l'un de vos employés (Christopher Hughes) à la sortie d'une maison close fin 2016, quand la concurrence commence à menacer vos revendeurs (et que vous répondez par la violence) dès 2017 puis que la police vient l'année dernière sonner à votre porte pour vous accuser de collusion avec le crime organisé… c'est mauvais signe. Les « Brothers » ont annoncé suspendre l'activité de MPC fin 2019. Ils seraient en fuite en Amérique du Sud.
Comme toute activité mafieuse, la vie de ce nouveau type de start-up qui cible le crime organisé est mouvementée.

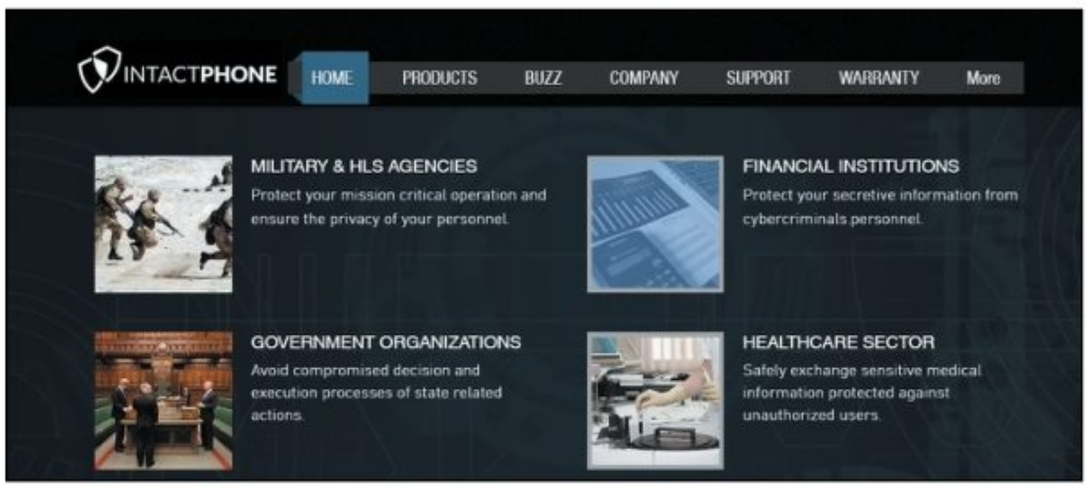
> EN DÉCEMBRE 2017, UNE VIDÉO POSTÉE SUR YOUTUBE PAR SYLAK 88 A TENTÉ DE METTRE EN GARDE TOUS LES CLIENTS DE ENCROCHAT EN ESSAYANT DE DÉMONTRER LA VULNÉRABILITÉ DE LEUR SMARTPHONE. À L'ÉPOQUE, LES OBSERVATEURS Y ONT VU UNE TENTATIVE DE DÉSTABILISATION VENANT D'UN CONCURRENT.

LA RELÈVE EST DÉJÀ LÀ

Les principaux concurrents identifiés de Encrochat et MPC ces dernières années étaient Phantom Secure (tombé en 2018), PGPSafe ou Ennetcom (tombés en 2016 et 2017). Leurs dirigeants, contrairement à ceux de MPC, ont fini derrière les barreaux.

Aujourd'hui, des sites Web ayant pignon sur rue continuent de proposer des services équivalents (en tout cas le garantissent), assurant « travailler pour le renseignement, des gouvernements, l'armée, des organisations humanitaires ou de très grandes entreprises ». Sans préjuger de leurs clientèles, ils proposent des services assez similaires à leurs « illustres » aînés et proposent tous un discours marketing ambiguë, en essayant de se différencier les uns des autres.

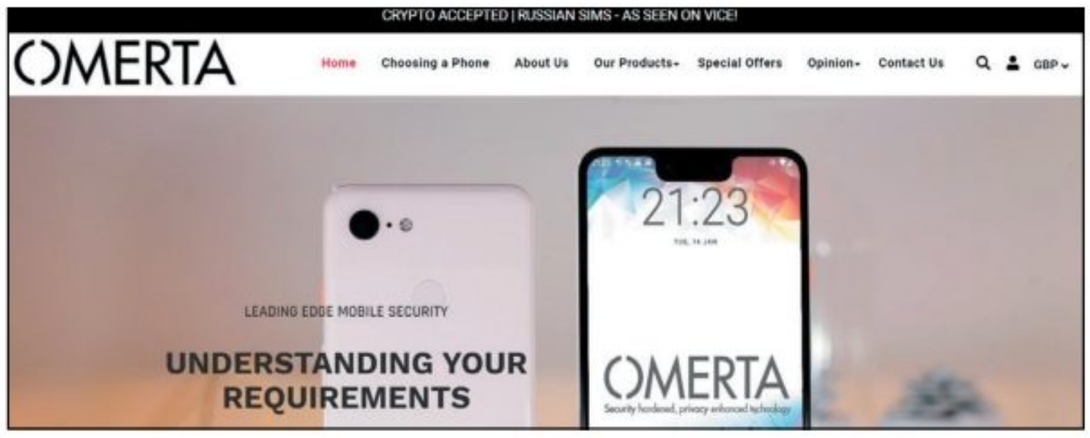
GHOSTECC INSISTE AUSSI SUR L'INTRAÇABILITÉ DES MOYENS DE PAIEMENT POUR IDENTIFIER SES CLIENTS



INTACTPHONE QUI DIT OFFRIR UNE SOLUTION DE HAUT NIVEAU CONTRE LES ÉCOUTES

ANO-PHONE NOUS ACCUEILLE AVEC UN JOLI MASQUE ANONYMOUS

KRYPTOTEL PENSE À TOUS LES FANS D'APPLE EN PROPOSANT UNE CUSTOMISATION DU DERNIER IPHONE SE



ET OMERTA MET EN AVANT LA MISE À DISPOSITION DE « CARTES SIM RUSSES » ! (VOILÀ LES MILITAIRES ET GOUVERNEMENTS DU MONDE ENTIER RASSURÉS !).

BLACKPHONE N'A JAMAIS SÉDUIT LE GRAND PUBLIC ET LES ENTREPRISES

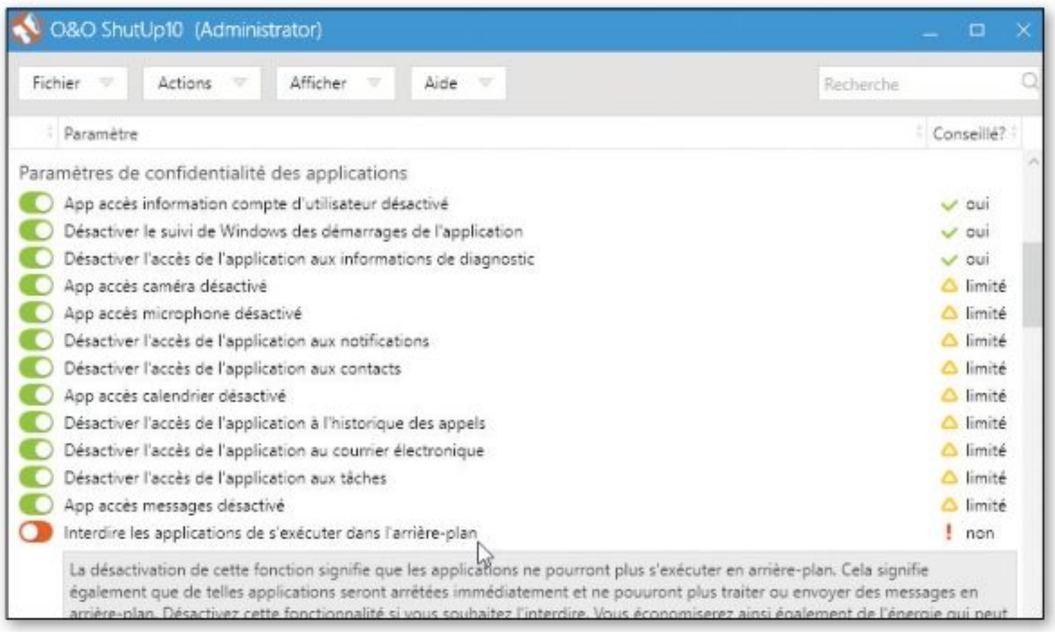
En 2013, nous découvrions le « Blackphone » au MWC de Barcelone. Un smartphone qui concentrait alors tout ce qui permettait de protéger la vie privée et l'anonymat de ses utilisateurs. Conçu par la marque espagnole Geeksphone en partenariat avec Silent Circles, le Blackphone avait même bénéficié de l'expertise et de l'adoubement de Phil Zimmermann , grand défenseur de l'opensource et de la vie privée, et co-créateur du protocole de chiffrement mondialement connu PGP. Proposé à un prix correct (à partir de 550 euros) et plutôt joli (sans plus), les Blackphone 1 et 2 n'ont jamais trouvé leur public malgré deux levées de fonds de 30 millions de dollars en mai 2014 et 50 millions en juillet 2016 ! L'entreprise souhaitant une certaine respectabilité (des banques étaient parmi les investisseurs), il semble qu'elle n'ait pas frayé avec la grande criminalité pour écouler ses stocks. Seule une commande d'un distributeur sud-américain (tiens donc, lui avait peut-être une idée en tête...) avait un temps laissé miroiter une super commande de 250 000 exemplaires. Sans suite. En 2017, la société arrêtait la commercialisation de ses téléphones.
Mais l'ensemble des technologies utilisées, leur combinaison et leur intégration à un OS Android modifié dès 2013, a semble-t-il donné des idées à de nombreuses personnes par la suite...

DÉSACTIVEZ LES ESPIONS DE WINDOWS 10

PRATIQUE

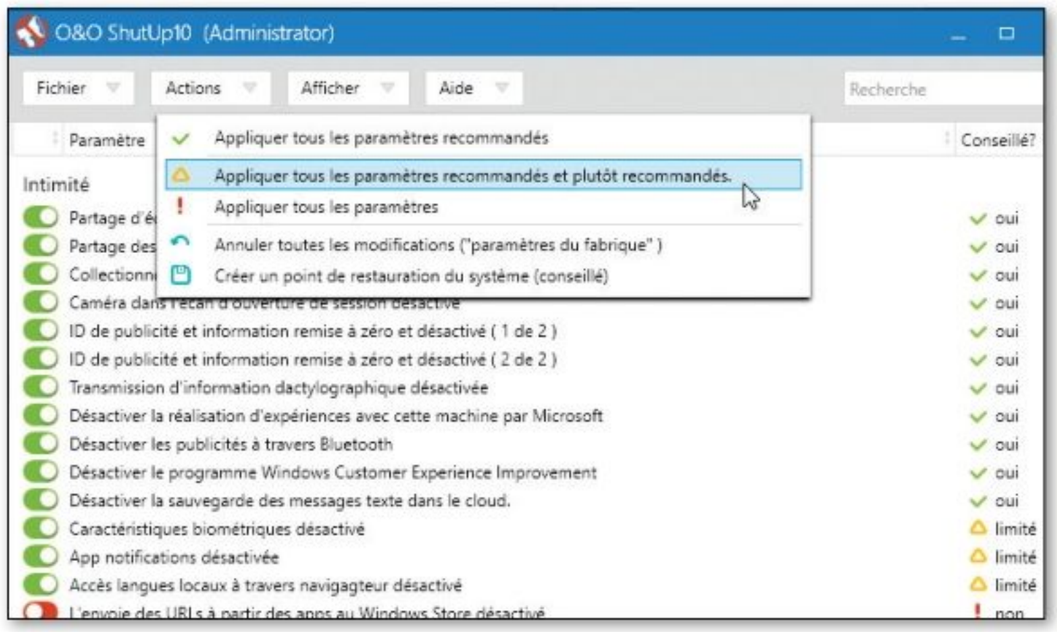
Certaines fonctions indiscrètes ne figurent pas dans les paramètres de confidentialité de Windows 10. Pour les désactiver, utilisez O&O ShutUp10.

INFOS [O&O ShutUp10]
Où le trouver ? [www.oo-software.com]
Difficulté :



01› EXAMINER LES OPTIONS

Téléchargez et lancez le logiciel. Pour chaque option proposée, vous pouvez obtenir des explications en cliquant sur la ligne. Certaines sont recommandées (**oui**), d'autres plutôt recommandées mais pouvant entraîner quelques limitations (**limité**), d'autres déconseillées (**non**).



02› FAIRE VOS CHOIX

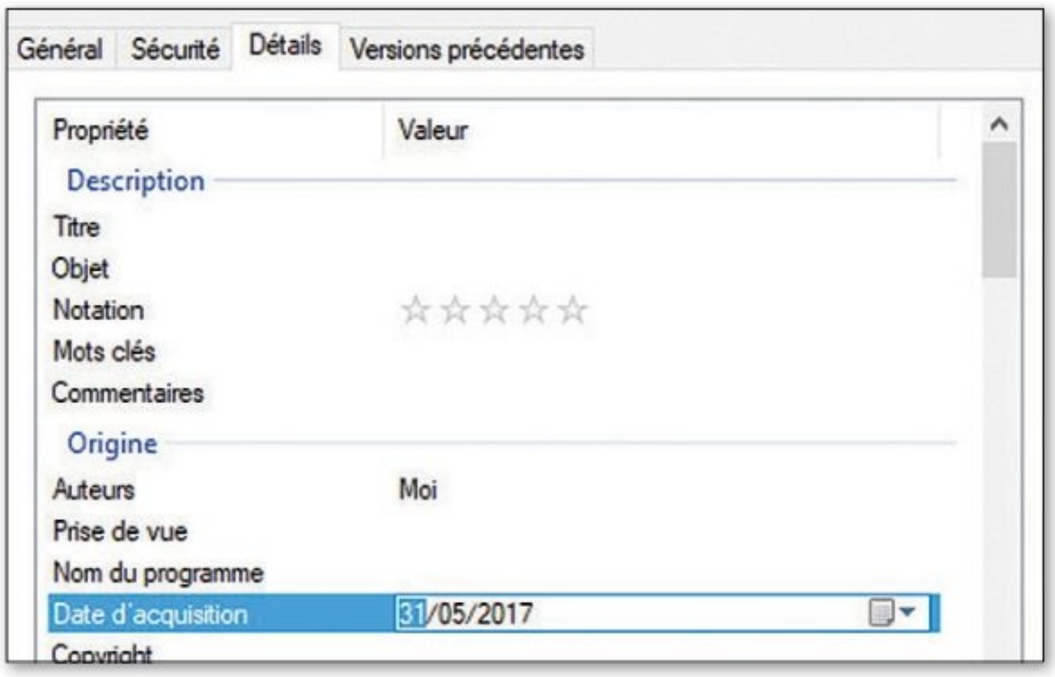
Cliquez sur l'interrupteur, en début de ligne, pour modifier une option. Par sécurité, le logiciel vous propose de créer un point de restauration système : acceptez. Vous pouvez aussi appliquer en bloc certaines catégories de paramètres, via le menu **Actions**. Vos choix faits, refermez le logiciel.

SUPPRIMEZ LES MÉTADONNÉES D'UNE PHOTO

PRATIQUE

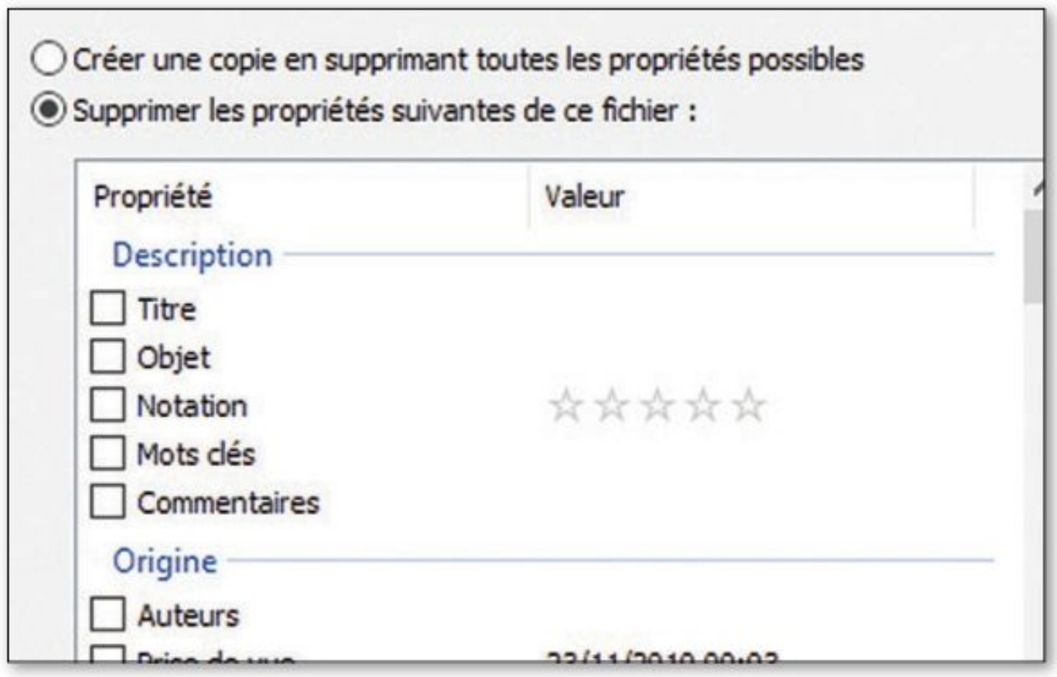
Les données EXIF d'une photo contiennent beaucoup d'informations : date de prise de vue, appareil utilisé, etc. Voici comment les modifier ou les supprimer.

INFOS [Windows]
Difficulté :



01› MODIFIER LES DONNÉES

Faites un clic droit sur une photo et allez dans **Propriétés > Détails**. Cliquez sur une ligne et tapez directement ce que vous voulez écrire, ou effacez son contenu. Notez que tous les paramètres ne sont pas modifiables.



02› SUPPRIMER DES INFORMATIONS

Toujours dans l'onglet **Détails**, cliquez sur **Supprimer les propriétés et les informations personnelles** puis cochez **Supprimer les propriétés suivantes de ce fichier**. Cochez les cases de votre choix et validez avec **OK**.

Disparaître des moteurs de recherche > AVEC FACEBOOK

Pour éviter que n'importe qui puisse facilement vous trouver sur Facebook, allez dans les **Paramètres** (menu en haut à droite), à la section **Confidentialité**. À **Qui peut vous trouver à l'aide de l'adresse e-mail/du numéro de téléphone**, sélectionnez **Amis** (oui, vos amis pourront toujours vous trouver, c'est logique). Dans **Voulez-vous que les moteurs de recherche en dehors de Facebook affichent votre profil**, décochez la case **Autoriser...**.

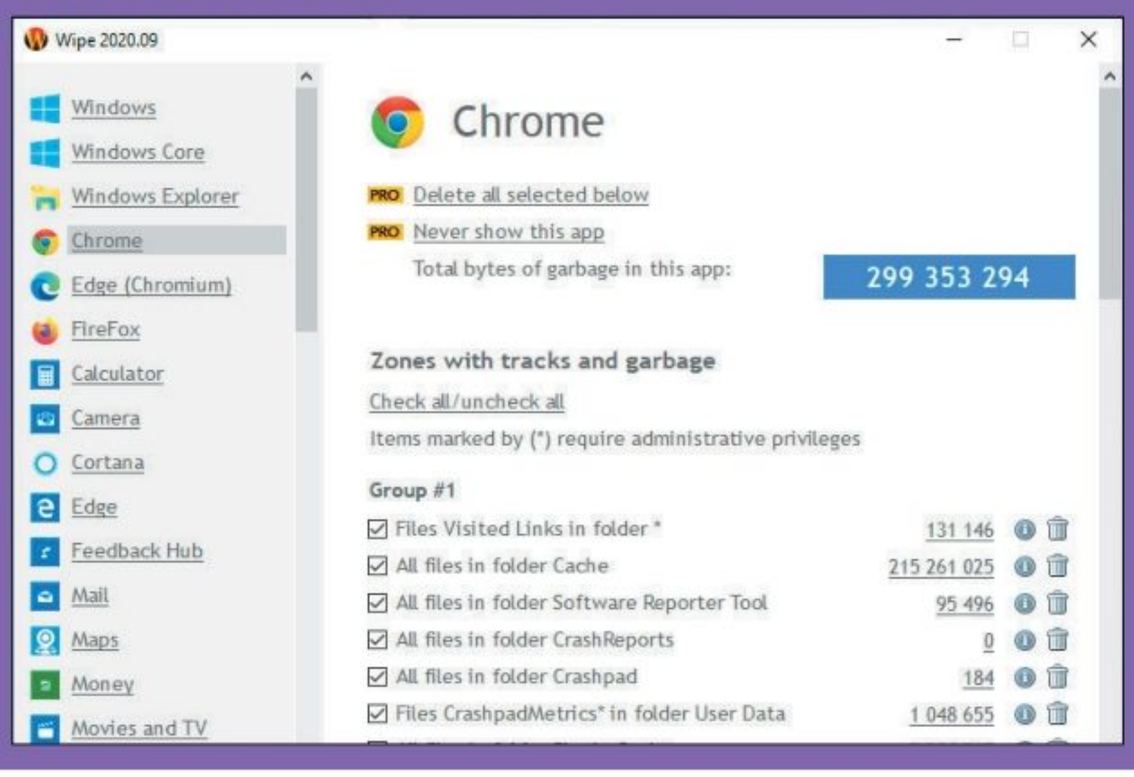
Supprimer la demande de géolocalisation > AVEC CHROME

De nombreux sites demandent d'accéder à votre localisation. Pour ne plus voir ces messages, ouvrez le menu de Chrome (en haut à droite), et cliquez sur **Paramètres**. Cliquez sur **Paramètres avancés**, en bas de la page, puis sur **Paramètres du site**, dans la rubrique **Confidentialité et sécurité**. Cliquez sur **Position**, et déplacez le curseur **Demander l'autorisation avant d'accéder** sur **Bloqué**.

Supprimer ses traces > AVEC WIPE

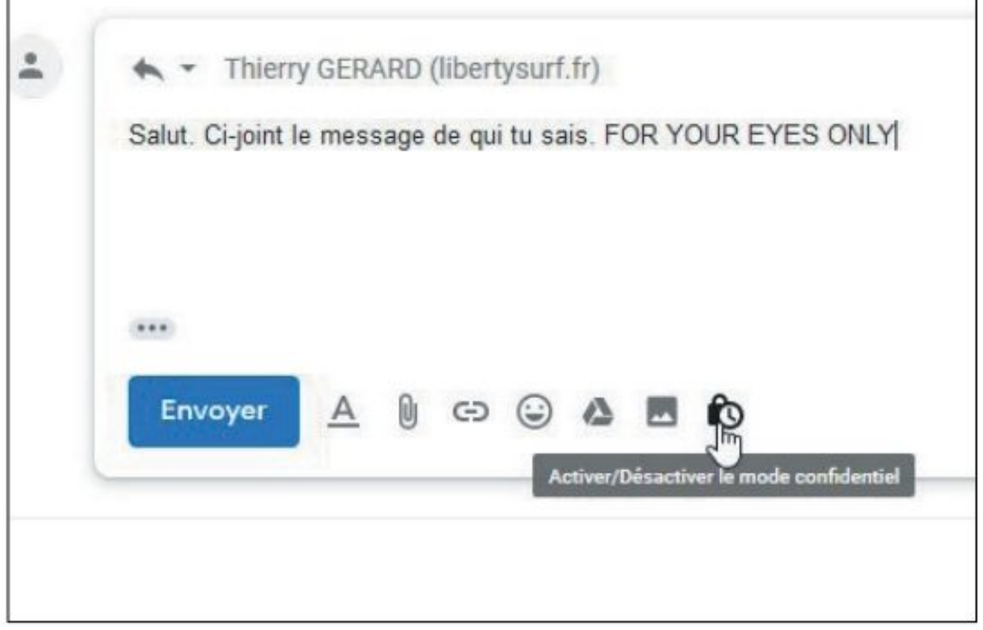
Wipe va faire le ménage dans votre PC en supprimant plusieurs types de fichiers et d'informations issues de votre navigateur ou de vos autres logiciels : documents récemment ouverts, traces de vos activités, journaux, cache, fichiers temporaires, etc. Une fois effacées, les données sont rendues irrécupérables grâce à un algorithme spécifique. C'est aussi l'occasion de gagner un peu de place sur le disque dur... Une fois que le logiciel aura calculé le nombre d'octets «libérables», cliquez sur **Détails** pour ne pas supprimer des éléments que vous voudriez garder. La version Pro propose juste quelques options supplémentaires, mais rien de bien vital.

https://goo.gl/94ldCF



Protéger les mails confidentiels > AVEC GMAIL

En mode confidentiel, il faut un code pour lire vos messages, ils ne peuvent être copiés, transférés ou imprimés, et ils s'autodétruisent quand vous le décidez. C'est dans la fenêtre où vous rédigez le message, parmi les icônes proposées en bas, que vous trouverez le mode confidentiel (la dernière icône). Cliquez dessus pour sécuriser votre mail. Le destinataire reçoit un lien lui permettant de lire votre message. Ce lien expire au bout d'un certain délai, fixé dans **Définir un délai d'expiration**.



TUTO

POUR QUI ?

Pour ceux qui utilisent avidement leur espace cloud

POUR QUOI FAIRE ?

Protéger ses fichiers les plus sensibles

CHIFFREZ VOTRE ESPACE CLOUD AVEC BOXCRYPTOR

Si vous sauvegardez des documents confidentiels dans le cloud, verrouillez-les avec l'outil gratuit BoxCryptor.

On stocke un peu tout et n'importe quoi dans le cloud. Des photos, des documents sans grand intérêt comme des factures, des fichiers texte, etc. Et l'on accorde notre confiance aux géants du cloud comme Microsoft, Google ou encore Dropbox pour garder un œil dessus. Mais qu'adviendrait-il s'ils se faisaient pirater ? Apple se souvient encore avec amertume des photos volées de stars sur iCloud en 2014. Pour éviter ce genre de désagrément, la solution consiste à chiffrer ses données. Ainsi, personne d'autre que vous, ou celui à qui vous aurez donné les droits d'accès, ne pourra ouvrir votre fichier. Et sur ce terrain, vous pouvez vous en remettre à BoxCryptor.

UN SEUL SERVICE DE CLOUD DANS SA VERSION GRATUITE

Ce logiciel, gratuit dans sa version de base, prend l'apparence d'un lecteur virtuel dans Windows. Il est en lien direct avec un espace cloud à choisir parmi plus d'une trentaine de fournisseurs (il faudra s'offrir la version Personal à 36 € / an pour cumuler les services). Il chiffre à la volée ce que vous y déposez suivant un cryptage AES 256. Si bien que vos données se trouvent verrouillées sur votre compte cloud (le nom des fichiers est même brouillé avec la version Personal) sans que vous n'ayez à vous en occuper.

Mais attention : si vous oubliez vos identifiants, c'est fichu. BoxCryptor ne saura pas déchiffrer vos fichiers. Avec la version gratuite utilisée dans ce pas à pas, vous disposez également d'un accès depuis un second appareil (le nombre devient illimité avec la version payante). Pratique pour accéder à tous ses fichiers sensibles même depuis un smartphone.

Attention, si vous perdez vos identifiants BoxCryptor, vous ne pourrez plus retrouver vos fichiers en clair sur votre cloud préféré !

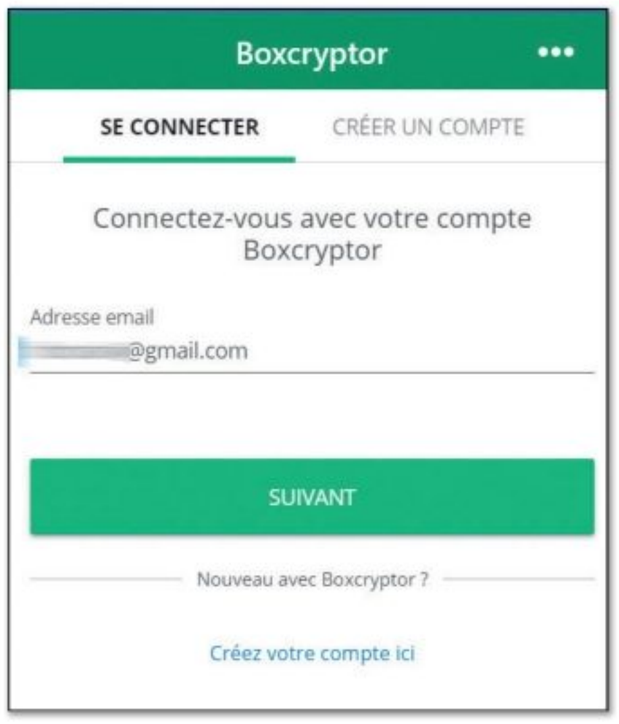
INFOS [BoxCryptor]
Où le trouver ? [www.boxcryptor.com/fr/]
Difficulté :

CHIFFRER GOOGLE DRIVE AVEC BOXCRYPTOR

PRATIQUE

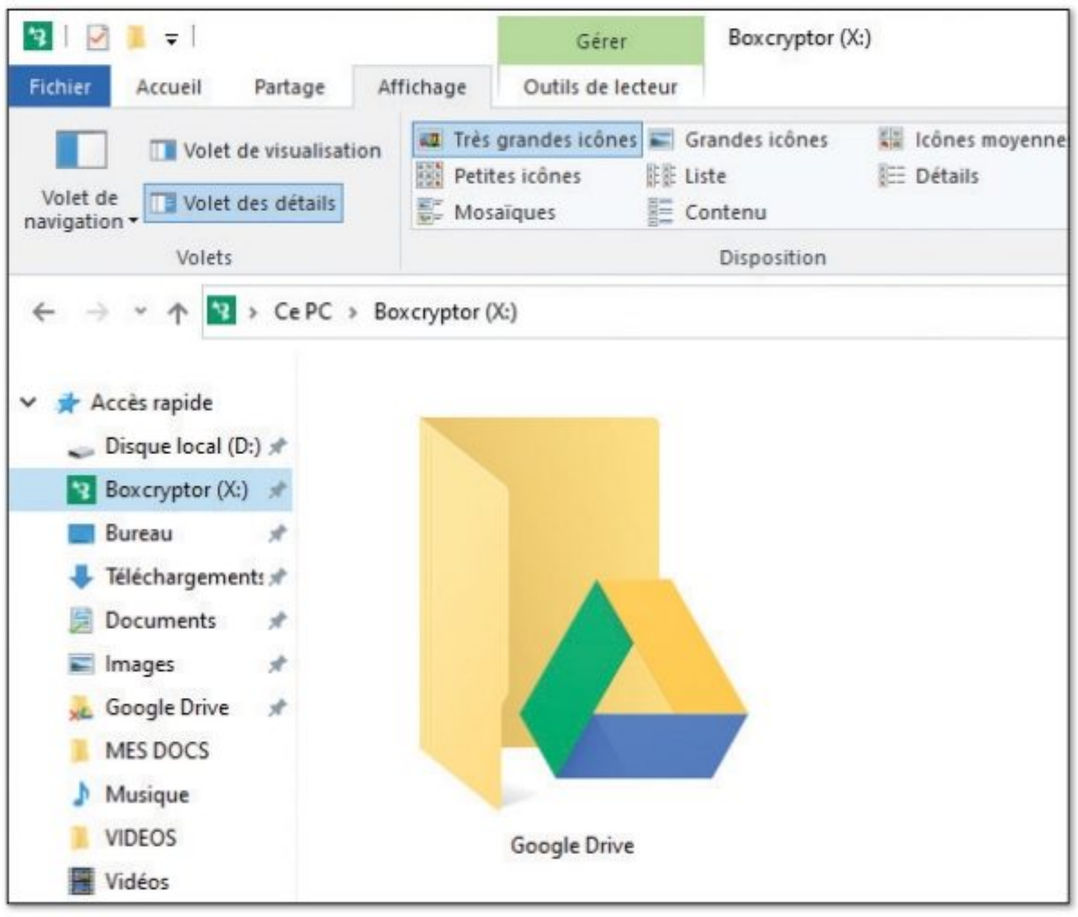
01 › INSTALLER BOXCRYPTOR

Créez un compte (gratuit) sur le site de Boxcryptor et cliquez sur le lien **Je souhaite conserver l'offre gratuite** pour accéder au téléchargement (n'oubliez pas de valider votre inscription d'un clic sur le lien reçu par mail). Lancez l'installation puis saisissez vos identifiants.



02 › ACCÉDER À GOOGLE DRIVE

Fermez la fenêtre d'aide de Boxcryptor. Puis ouvrez l'**Explorateur de fichiers** : un nouveau lecteur **Boxcryptor** y apparaît. Ouvrez-le depuis la colonne de gauche, puis allez dans le dossier **Google Drive** qu'il contient (s'il n'apparaît pas, voyez l'encadré ci-contre). Tous les fichiers qui se trouvent sur votre espace en ligne s'affichent.

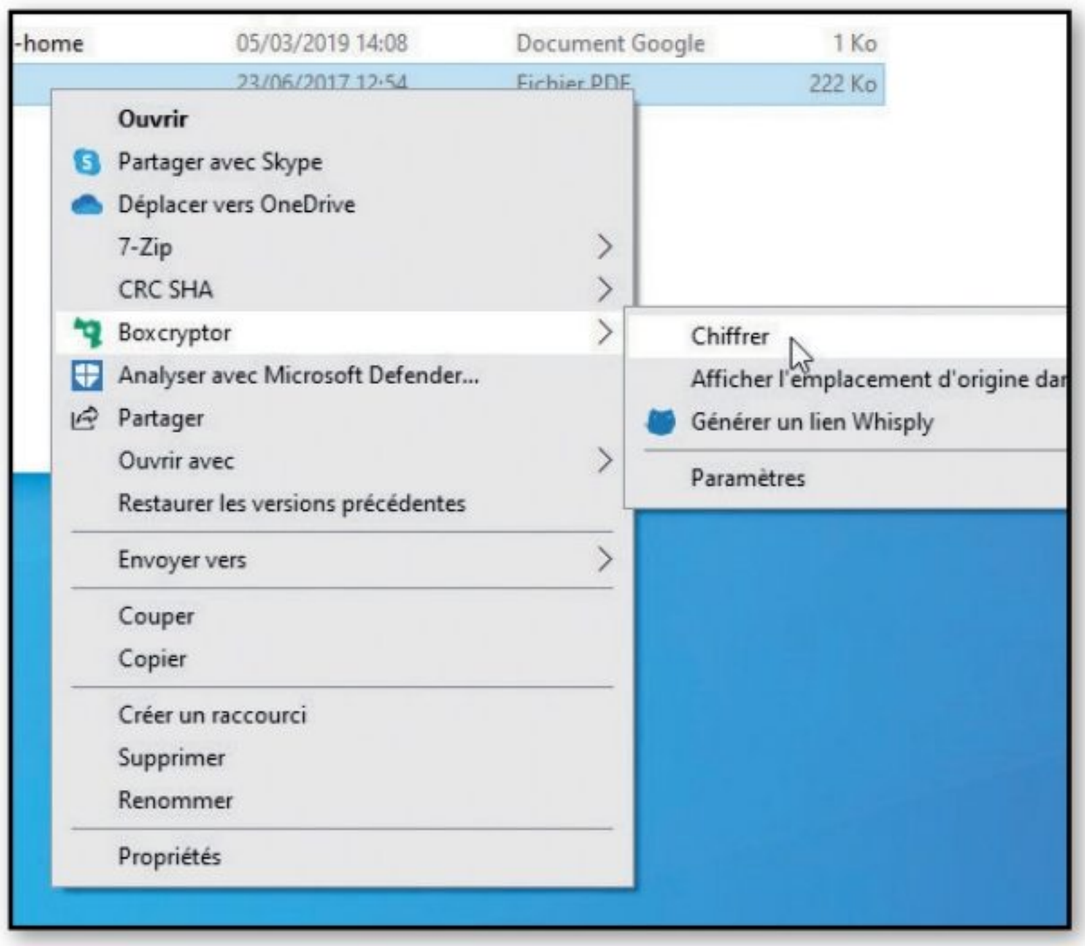


PLUSIEURS CLOUD

Vous exploitez plusieurs services de Cloud ?
En version gratuite, Boxcryptor ne peut en gérer qu'un.
Si Google Drive n'apparaît pas (étape 2), faites un clic droit sur l'icône de Boxcryptor, à l'extrémité de la barre des tâches, choisissez **Paramètres**, et dans **Emplacements**, cochez **Google Drive**.

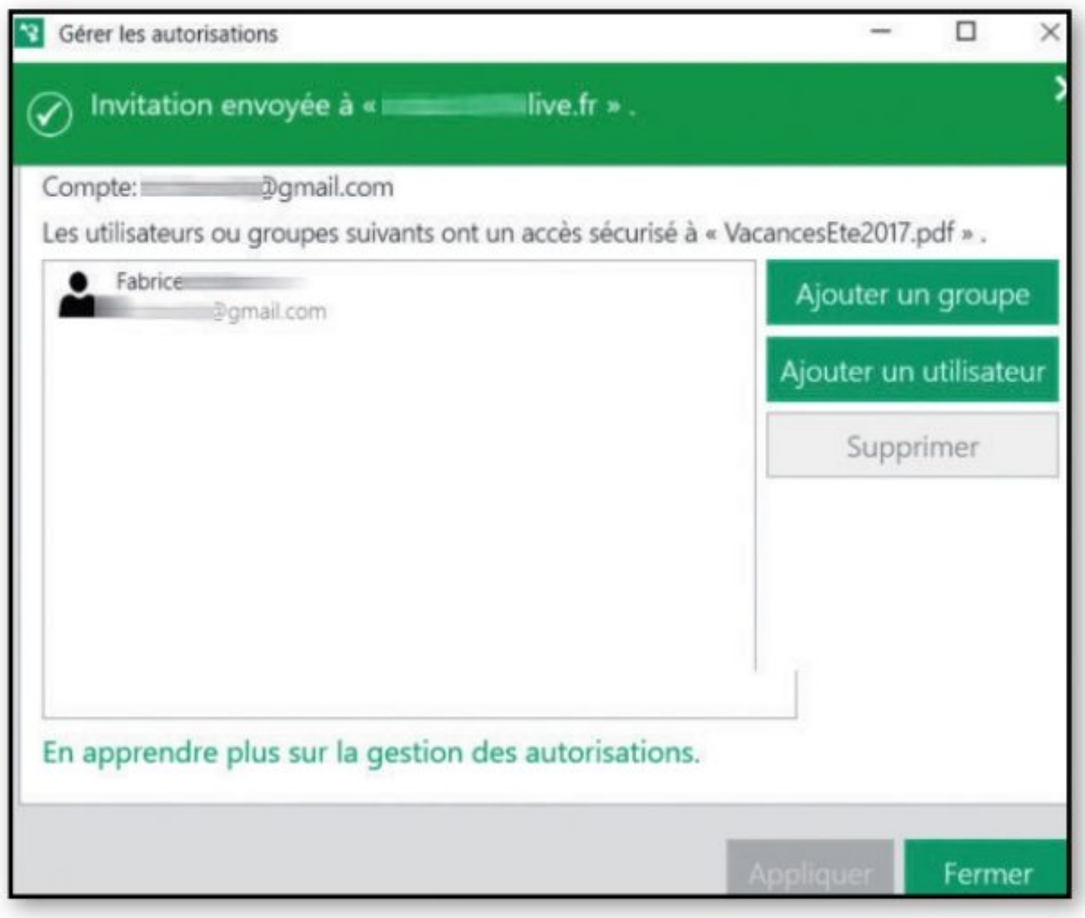
03 › CHIFFRER DES ÉLÉMENTS

Ouvrez l'un des dossiers synchronisés avec votre PC. Sélectionnez le dossier ou le fichier que vous souhaitez chiffrer. Effectuez un clic droit et dans le menu contextuel, choisissez **Boxcryptor > Chiffrer**. Au bout de quelques secondes, l'élément est verrouillé. Un petit symbole vert représentant un cadenas a d'ailleurs pris place en bas à gauche de l'icône.



04 › PARTAGER

Pour partager des éléments chiffrés avec d'autres utilisateurs, effectuez un clic droit sur un fichier ou un dossier verrouillé. Choisissez **Boxcryptor > Gérer les autorisations**. Dans la fenêtre qui s'affiche, cliquez sur **Ajouter un utilisateur**. Saisissez son adresse mail. S'il ne possède pas Boxcrytor, il recevra une invitation à l'installer afin de pouvoir ouvrir l'élément protégé.



SÉLECTION

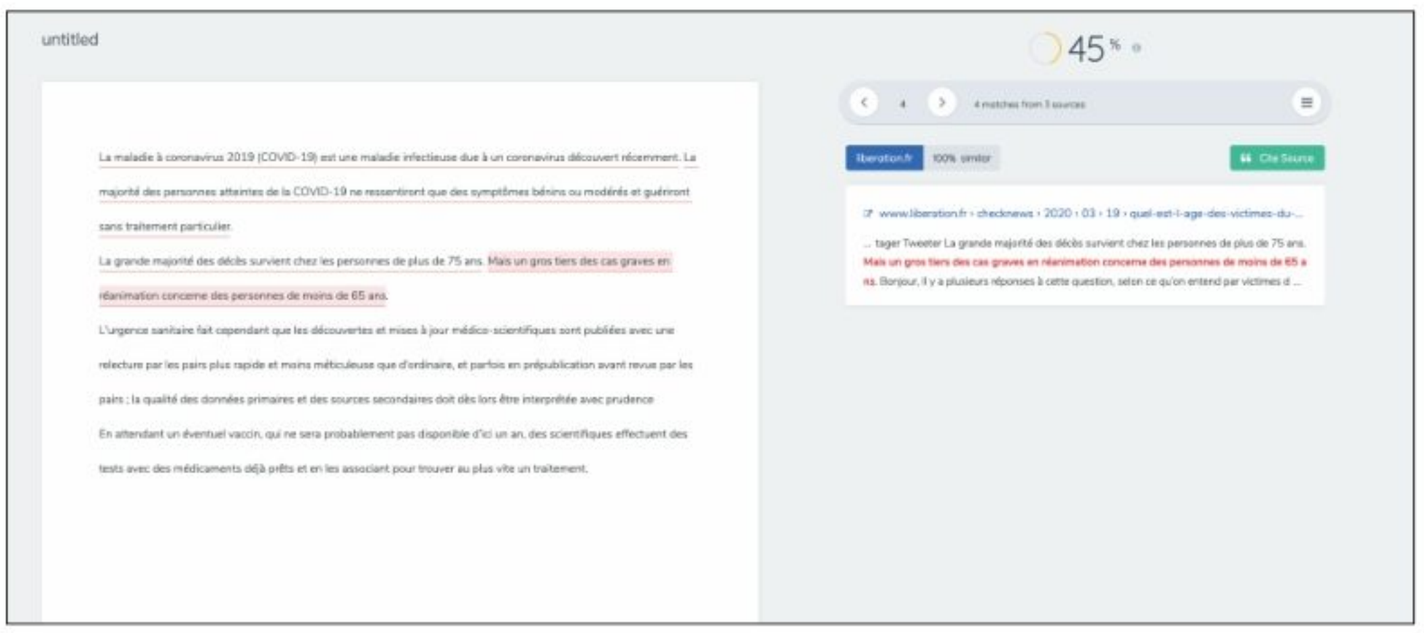
TOP 3 OUTILS DE DÉTECTION DE PLAGIAT

Une thèse, un mémoire ou des articles édités pour un site Web représentent un énorme travail de recherche et d'écriture. Sachez détecter ceux qui s'inspirent un peu trop de vos productions ou des ressources disponibles sur le Web avec ces outils dédiés.

QUETEXT : SIMPLE ET RAPIDE

L'interface de Quetext se résume à un simple cadre au sein d'une page Web où il suffit de copier le texte à analyser. Bien que les menus s'affichent en anglais, le service en ligne se montre tout à fait capable de vérifier les contenus en français. Dans sa version gratuite, il accepte 2500 mots par mois. Comptez 9,99 $ mensuels (environ 8,5 €) pour examiner 100 000 mots. Dans notre document de test, Quetext a su pointer du doigt les éléments récupérés sans modification depuis diverses sources sur le Web. Bizarrement, il n'a pas reconnu certains éléments provenant de Wikipédia. Mieux vaut ne pas l'utiliser pour la vérification de travaux universitaires. Enfin, il est totalement passé à côté des paraphrases.

Où le trouver ? **www.quetext.com**



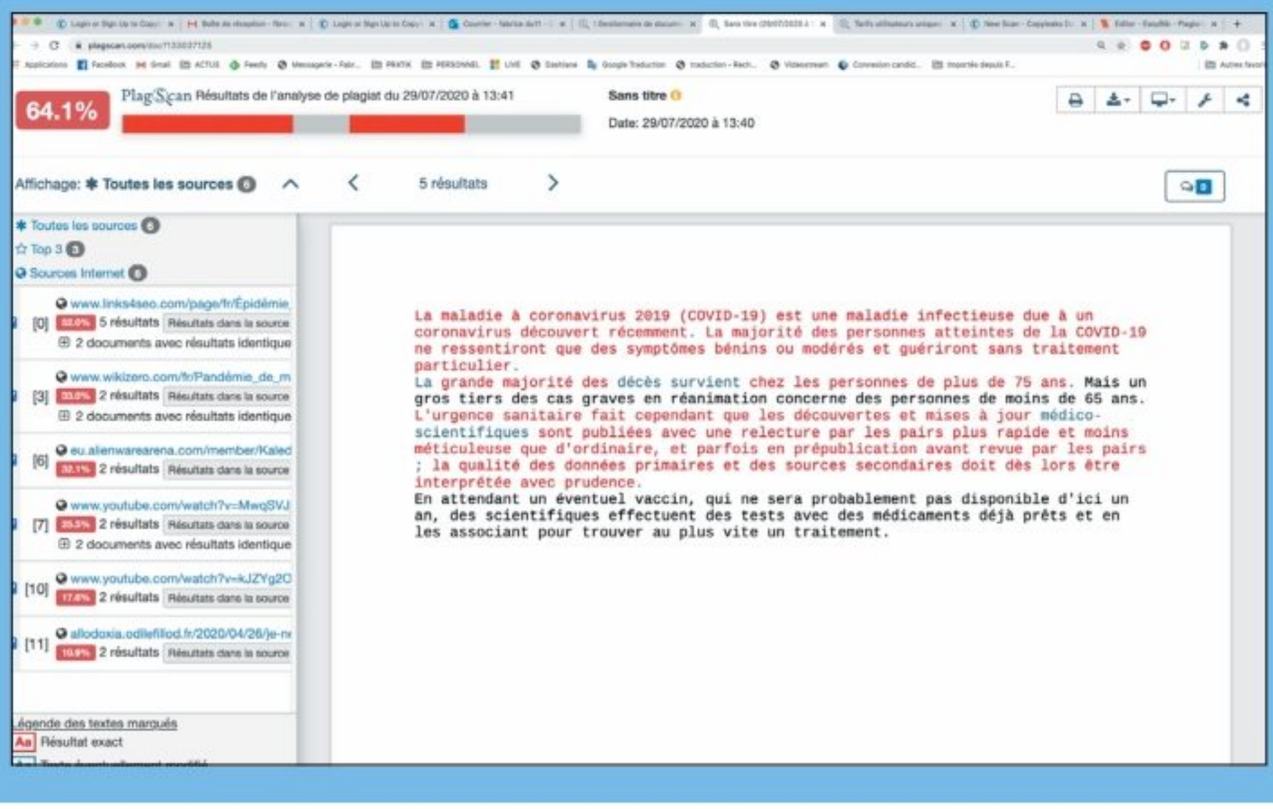
COPYLEAKS : WORD EST SON AMI

Pour utiliser Copyleaks, deux méthodes cohabitent. La première consiste à passer par le service Web afin d'y soumettre un document entier ou un extrait de texte. La seconde convient à ceux qui utilisent Word. L'éditeur fournit une extension pour lancer une analyse sans quitter le traitement de texte, pratique. Gratuit pour les 10 premières pages, l'outil est facturé 9,99 € par mois (8,5 €) pour 100 pages mensuelles ou 99,9 $ par an (85 €) pour plus de 1200 pages dans l'année. Côté détection Copyleaks s'est montré convaincant en dénichant les contenus issus de Wikipédia et des autres sources du Web et en listant les sites ayant repris les mêmes formules. Il a en revanche fait chou blanc sur les paraphrases.

PLAGSCAN : POUR LES UNIVERSITAIRES

Pas de formules d'abonnement mensuel ou annuel ici. L'utilisateur reste libre d'exploiter le service quand il le souhaite selon le volume voulu. Les tarifs s'échelonnent de 4,99 € pour 5000 mots (environ 20 pages) jusqu'à 39,99 € pour 80 000 mots (environ 320 pages). La version d'essai porte sur près de 2000 mots. Si l'outil s'est révélé très efficace avec les contenus provenant de Wikipédia et d'autres sources de connaissances universitaires, il n'a pas su identifier les informations copiées depuis les quotidiens nationaux. En cause, une base de données moins étendue que ses concurrents. Notre paraphrase, provenant d'un article de magazine, n'a donc pas non plus été repérée.

Où le trouver ? **www.plagscan.com**

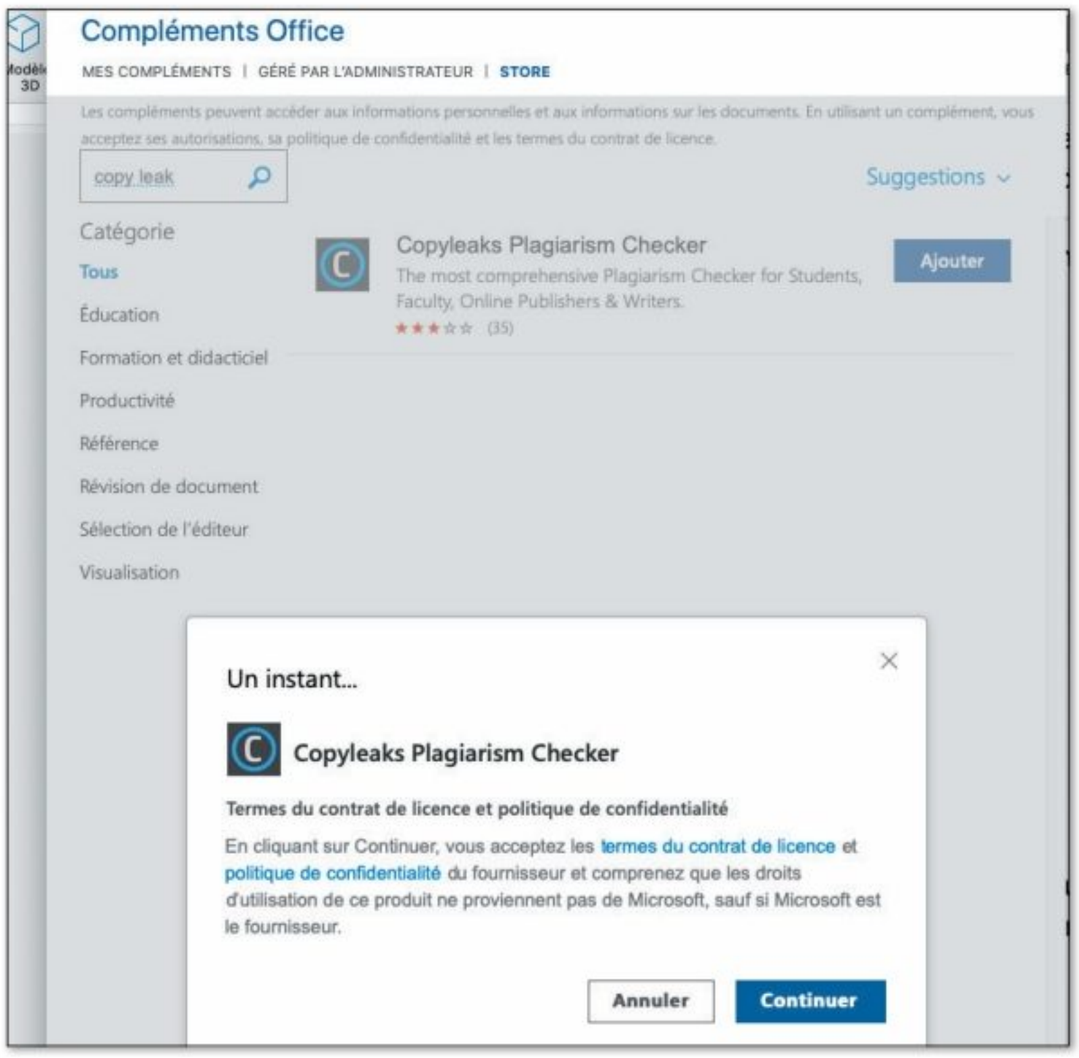


TRAQUEZ LE PLAGIAT DIRECTEMENT DANS WORD

PRATIQUE

01› AJOUTER L'EXTENSION COPYLEAKS

Lancez Microsoft Word puis ouvrez le document à vérifier. Cliquez sur le menu **Insertion** puis, dans le ruban d'outils,



activez l'option **Télécharger des compléments**. Dans le champ de recherche de l'Office Store, saisissez **copyleak** et validez. Cliquez enfin sur **Ajouter** puis sur **Continuer** pour accepter le contrat de licence.

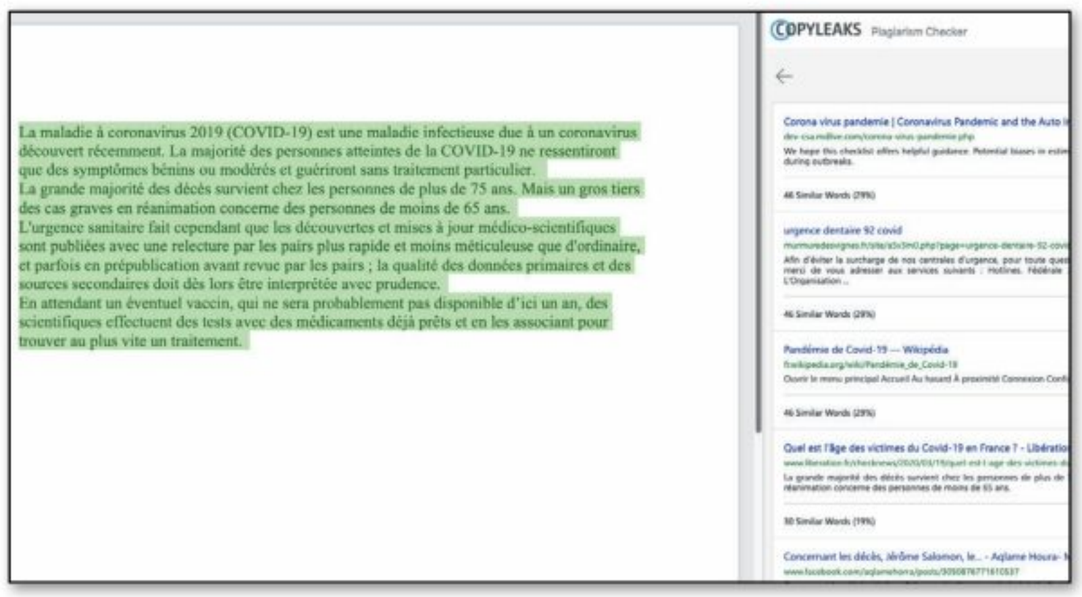
02› CRÉER LE COMPTE ASSOCIÉ

Activez l'onglet **Références** de Word. À l'extrême droite du ruban d'outils, cliquez sur l'icône **Scan** de

CopyLeaks puis sur le lien **Don't have an account yet**. Saisissez une adresse mail valide, un mot de passe, vos nom et prénom et une catégorie d'usage parmi les propositions du champ **Who are you ?** Validez par **Sign Up** puis vérifiez votre boîte mail (y compris les spam) pour activer votre compte.

03› EFFECTUER L'ANALYSE

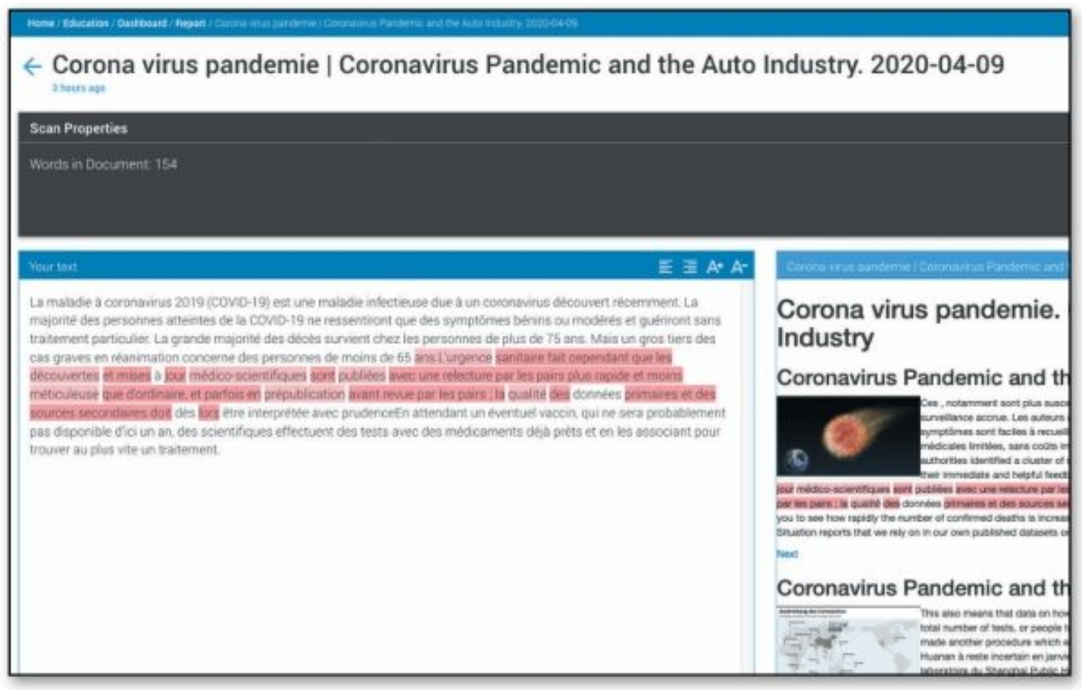
Vous pouvez refermer la page Web qui vient de s'afficher dans votre navigateur et retourner sur Word. Cliquez maintenant sur le bouton **Scan** dans la fenêtre de



CopyLeaks à droite de votre document. L'examen de ce dernier démarre. Il peut durer plusieurs minutes s'il s'avère assez long. À l'issue de l'opération, les premiers résultats tombent et présentent les similitudes repérées avec du contenu déjà sur le Web.

04› ÉTUDIER LE RAPPORT

Cliquez sur le bouton bleu **Launch Report** à droite pour obtenir plus de détails. Votre navigateur Web prend le relais et affiche les éléments du texte dont CopyLeaks a retrouvé des traces sur le Net. Pour chaque phrase, sont



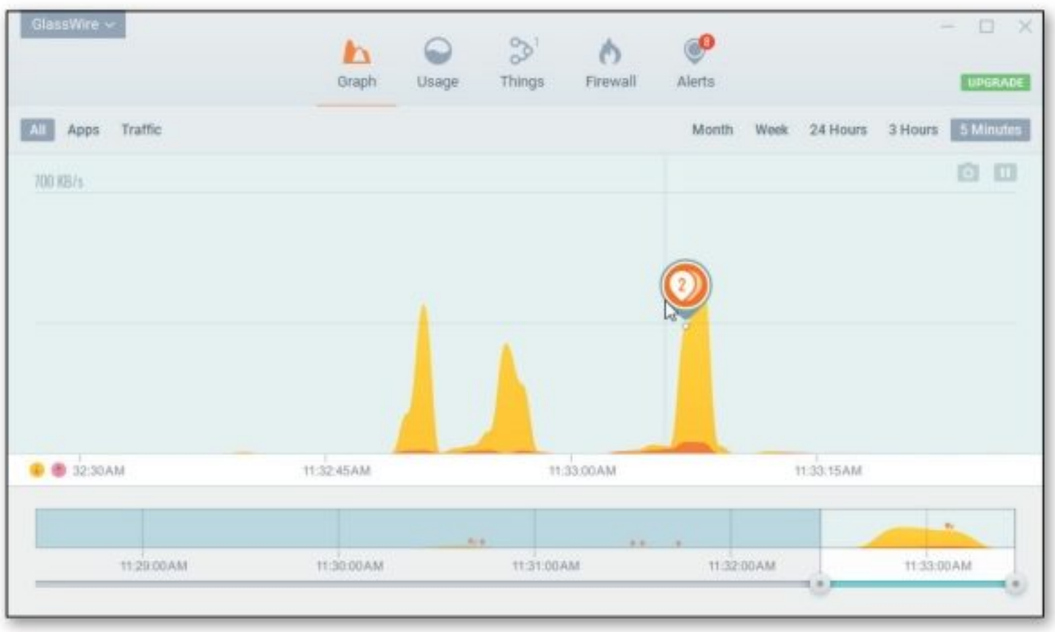
précisés en colonne de droite la source ainsi que le taux de similitude. Un clic sur l'une des sources permet d'ouvrir la page du site plagié en maintenant la mise en forme originale.

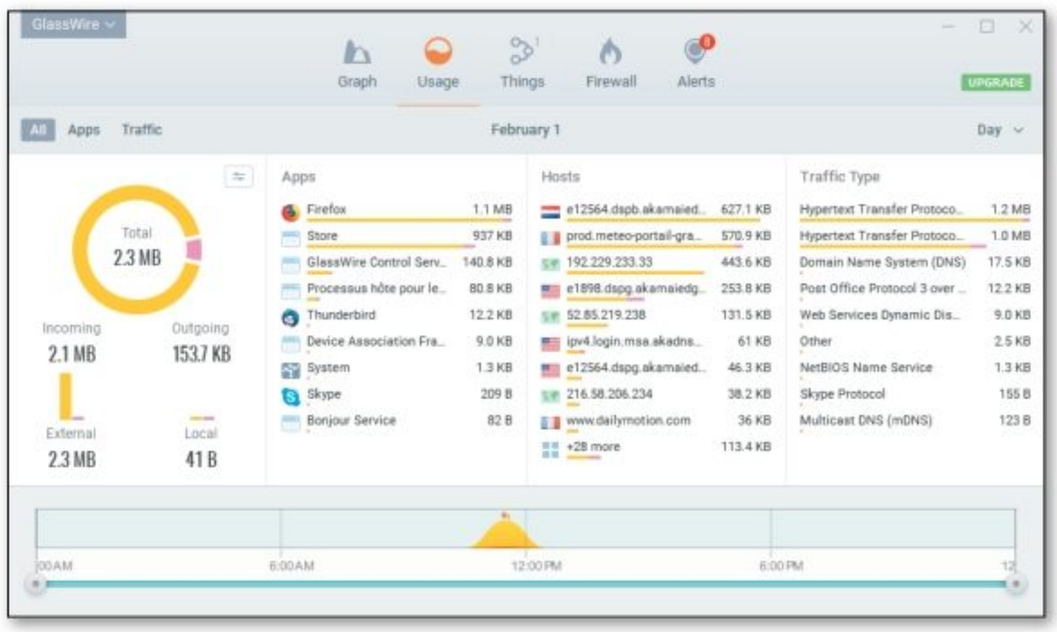
SURVEILLEZ LES ACCÈS À INTERNET

PRATIQUE

Le logiciel GlassWire permet de surveiller l'activité sur votre réseau. Alors que les autres programmes de ce type rivalisent d'austérité, GlassWire s'avère agréable et bien conçu.

INFOS [Glasswire]
Où le trouver ? [www.glasswire.com]
Difficulté :





01› LANCER LE LOGICIEL

Dès son démarrage, GlassWire surveille les activités de vos programmes sur Internet. Depuis l'onglet principal, vous pouvez garder un œil sur l'utilisation de votre bande passante (quel processus consomme le plus de données, etc.), mais aussi sur l'utilisation des ports et le pare-feu (onglet **Firewall**).

02› REPÉRER LES PROBLÈMES

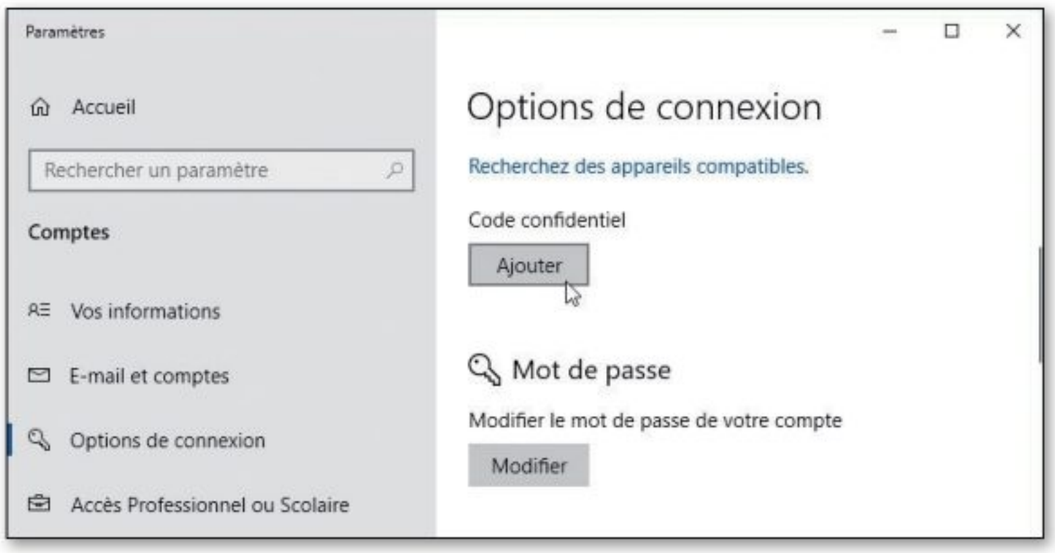
Le logiciel intègre aussi un module de détection des modifications de fichiers et déjoue les attaques type «ARP poisoning». Idéal pour repérer les activités louches ou les programmes un peu trop «bavards». Dans **Usage**, vous voyez toute l'activité de votre ordinateur. En cas de pépin, Glasswire affiche une alerte.

CHANGEZ DE MODE D'AUTHENTIFICATION

PRATIQUE

Votre session Windows est normalement protégée par le mot de passe associé à votre compte. Vous pouvez aussi opter pour un code confidentiel plus rapide à saisir, ou un mot de passe « image ».

INFOS [Windows]
Difficulté :



01› ACCÉDER AUX DIFFÉRENTES OPTIONS

Tapez **options de connexion** dans le champ de recherche de la barre des tâches et sélectionnez **Options de connexion**. Vous pouvez exiger la saisie du mot de passe à la sortie du mode veille, modifier le mot de passe de votre compte (local) ou paramétrer un code confidentiel permettant de déverrouiller votre session plus rapidement, à la façon d'un code PIN.

02› CHOISIR UN MOT DE PASSE « IMAGE »

Mot de passe image demande le tracé de schémas secrets. Choisissez ce mode, faites **Choisir une image** et trouvez une photo dans un de vos dossiers. Faites ensuite **Utiliser cette image** et tracez trois schémas sur l'image avec votre souris (relier des points imaginaires, faire des points ou des cercles, etc.). Ces mouvements seront à reproduire dans le même ordre lors de la prochaine connexion.

TUTO

SCAN AU DÉMARRAGE :

LA SOLUTION QUAND LES AUTRES ONT ÉCHOUÉ

POUR QUI ?

Vous ne comprenez pas pourquoi votre ordinateur rame encore.

POUR QUOI FAIRE ?

Analyser avant le camouflage d'un programme malveillant

Comme d'autres antivirus, Avast propose une fonction Scan au démarrage qui lui permet d'analyser votre disque dur en mode offline et avant que le boot ne soit finalisé. Puissant pour débusquer les intrus adeptes de camouflage.

Par défaut, la **Sensibilité** est réglée sur **Moyenne**. Si vous choisissez **Haute**, le temps de scan sera nettement allongé.

Gardez ces deux cases cochées.

Vérifiez que cette case soit bien cochée et choisissez **Corriger automatiquement.** Avast se chargera d'effectuer les opérations nécessaires sans que ayez à intervenir pendant le scan.

Le disque système est généralement votre disque **C**, celui sur lequel opère Windows 10. Vous pourrez aussi analyser vos autres disques de stockage (**Tous les disques durs**).

INFOS [Avast]
Où le trouver ? [www.avast.com]
Difficulté :

LANCEZ VOTRE SCAN AVAST AU DÉMARRAGE

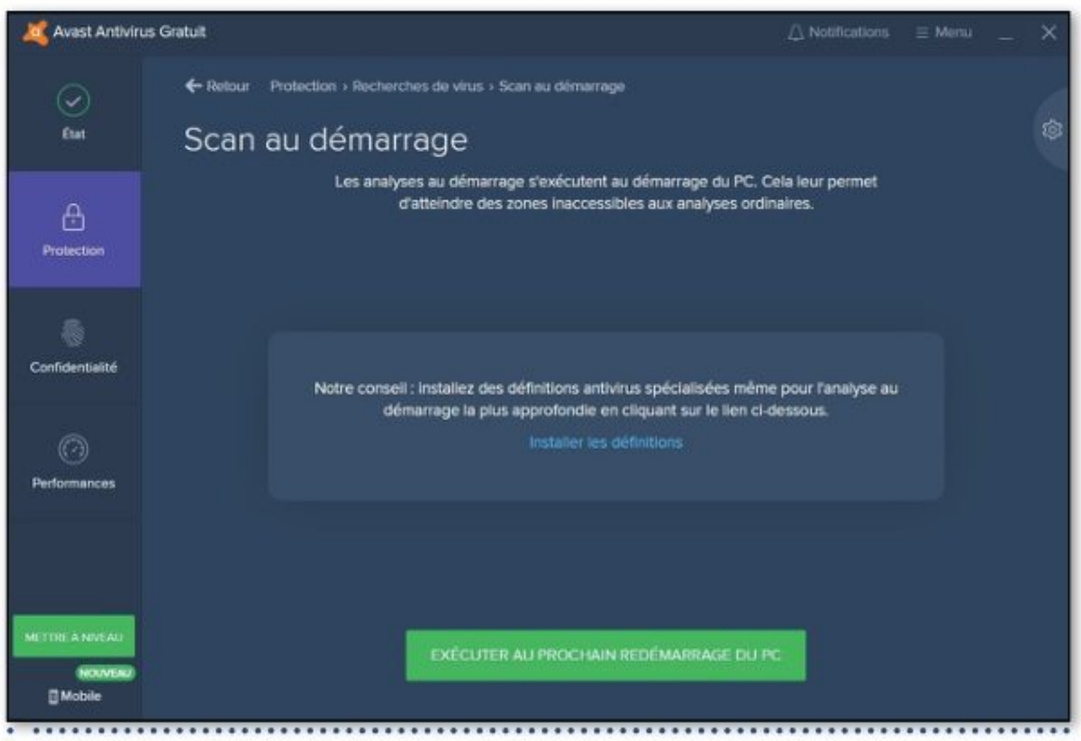
PRATIQUE

01› ACCÉDER AU SERVICE

Ouvrez votre console Avast. Allez dans **Protection > Recherche de Virus** puis ouvrez **Scan au démarrage**, présent en bas de la fenêtre.

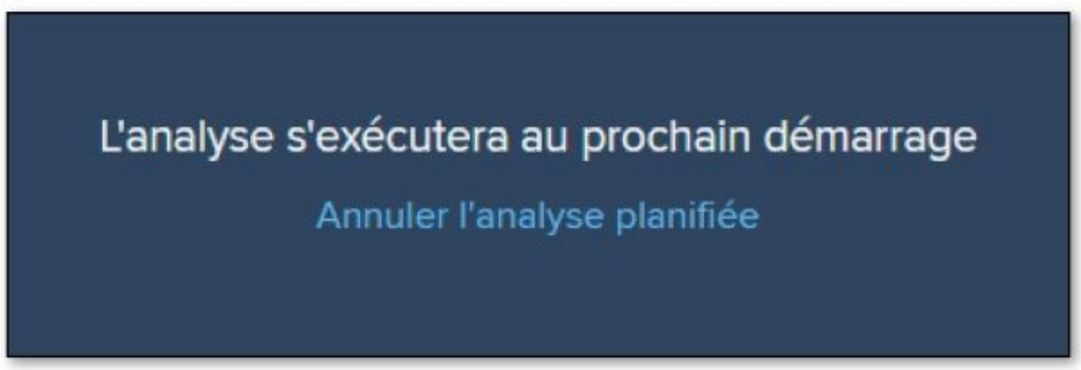
02› METTRE À JOUR

Vérifiez dans la fenêtre suivante que votre base de définitions antivirus soit à jour. Si Avast vous le propose comme ici, lancez le lien **Installer les définitions**. Cette mise à jour prendra quelques secondes ou minutes.



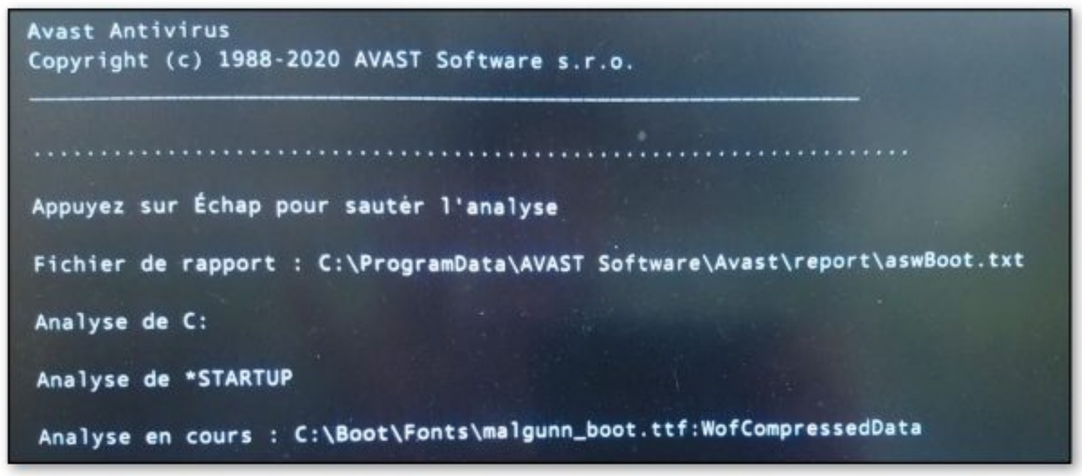
03› PLANIFIER L'ANALYSE

Cliquez ensuite sur **Exécuter au prochain redémarrage PC**. L'analyse se fera la prochaine fois que vous éteindrez et redémarrerez votre ordinateur. Vous pouvez encore annuler ce choix si ce n'est finalement pas le moment (n'oubliez pas qu'une analyse au démarrage peut prendre plusieurs heures selon la taille de vos disques durs !) en cliquant sur le lien **Annuler l'analyse planifiée**.



04› SCAN AU DÉMARRAGE

Au prochain démarrage de votre PC, vous l'aurez compris, l'analyse de Avast se lance et scanne tous les fichiers, dossiers, répertoires et programmes de votre disque dur principal (celui contenant votre système d'exploitation). Et ce avant même que votre session ne soit ouverte, ce qui permet d'accéder à des informations ou problèmes avant que d'éventuels programmes malveillants ou que votre système ne masquent leur existence.

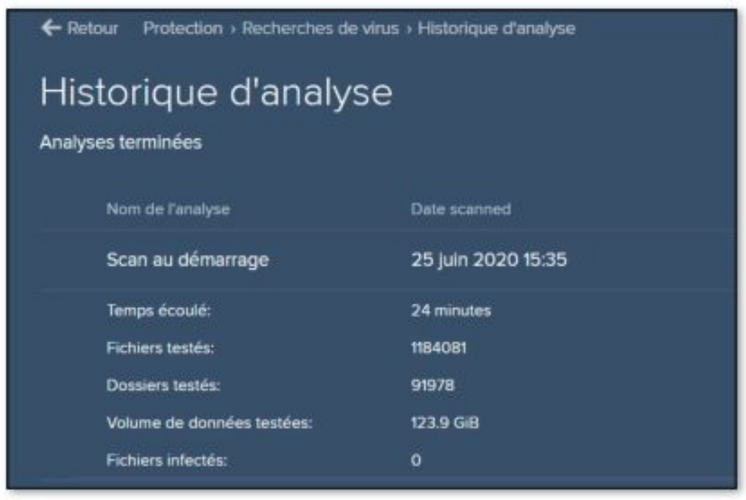


05› CORRECTIFS MANUELS OU AUTOMATIQUES

Pour toute menace détectée, sélectionnez l'action à appliquer (à moins d'avoir précédemment défini des actions automatiques dans les paramètres du Scan au démarrage, ce que nous vous conseillons > lire ci-contre). Une fois l'analyse terminée et les correctifs apportés, votre ordinateur poursuivra son démarrage habituel.

06› RAPPORT

Un rapport d'activité synthétique est disponible via la console Avast en suivant **Protection > Recherche de Virus > Historique d'analyse.** Ici, le scan a mis 24 minutes à tester 1 184 081 fichiers, 91 978 dossiers pour 123,9 Gb de données.



RÉGLAGES DU SCAN AU DÉMARRAGE

Avant de lancer votre scan, voici comment accéder aux réglages préalables. Via la console de Avast, allez sur **Protection > Recherche de Virus.** Cliquez sur l'icône en forme d'engrenage à droite de l''écran pour accéder aux paramètres. Sélectionnez ensuite l'onglet **Scan au démarrage.**

Interview de Martin Zima, , Senior Product Manager chez Avast

POURQUOI UN SCAN AU DÉMARRAGE SERAIT-IL PLUS EFFICACE ALORS QUE L'ANALYSE HABITUELLE N'A RIEN DÉTECTÉ ?

L'objectif est de détecter les logiciels malveillants qui se chargent habituellement au démarrage du système et avant l'initialisation des antivirus. Le scan au démarrage d'Avast supprime ces malwares sans avoir à lutter contre leurs fonctionnalités malveillantes furtives.
En effet, une fois un malware chargé et en cours d'exécution, il peut parvenir à éviter la détection des antivirus de bien des façons. Par exemple, il peut verrouiller ses fichiers pour empêcher le programme antivirus de les ouvrir et de les rechercher ; ou il peut s'exécuter en plusieurs copies, afin que celles toujours en cours d'exécution réinfectent continuellement la machine. L'analyse au démarrage d'Avast empêche que ces cas ne se produisent.

TECHNIQUEMENT, COMMENT CELA FONCTIONNE ?

Un scan au démarrage est une application Windows spéciale qui se lance très tôt pendant le processus de démarrage, avant que la plupart des composants Windows eux-mêmes aient démarré et avant même que le sous-système Win32 ne soit chargé. Il s'agit d'une application native qui ne dépend pas du sous-système Win32, et qui est donc très similaire au programme de vérification de disque chkdsk. Son exécution est programmée dans le registre Windows et le système d'exploitation le lance pendant le processus de démarrage. Le scan au démarrage utilise également un accès direct au disque, ce qui limite davantage ses dépendances sur les composants Windows standards, qui pourraient potentiellement être déjà infectés par un malware.
Si un pilote pour les programmes malveillants furtifs (rootkits) est déjà chargé quand le scan au démarrage se met en route, il peut interférer avec le code de traitement du système de fichiers pour se cacher. Cependant, étant donné que le scan au démarrage utilise un accès direct au disque, même les logiciels malveillants protégés par les rootkits restent visibles par ce dernier, qui peut donc les supprimer.

> *« Détecter les rootkits, les bootkits et les logiciels malveillants difficiles à supprimer »*

QUELS TYPES DE MENACES LE SCAN AU DÉMARRAGE IDENTIFIE-T-IL ?

Tous les types de menaces. La base de données virales est identique à celle utilisée localement par notre produit PC. Cependant, le but du scan au démarrage est de détecter les rootkits, les bootkits et les logiciels malveillants difficiles à supprimer.

WINDOWS DEFENDER A DÉSORMAIS UNE ANALYSE HORS LIGNE INTÉGRÉE GRATUITEMENT SUR WINDOWS. QUELLES SONT LES DIFFÉRENCES AVEC L'ANALYSE AU DÉMARRAGE D'AVAST ?

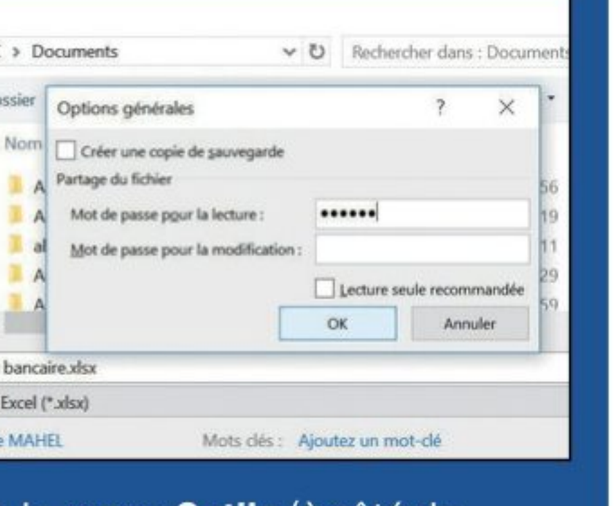
Windows Defender ne fonctionne que sur la dernière mise à jour de Windows 10, tandis que notre analyse au démarrage s'exécute dès Windows7, et sur toutes les versions suivantes. L'analyse au démarrage d'Avast et l'analyse hors ligne de Windows Defender sont très similaires en ce sens que Windows Defender s'exécute dans un environnement de récupération Windows distinct. C'est un bon moyen d'isoler le malware avant qu'il ne puisse se lancer. Le scan au démarrage d'Avast, d'autre part, fait cependant partie du processus de démarrage normal. Une fois programmé, il démarrera automatiquement ; et, une fois terminé, l'utilisateur pourra se connecter normalement. L'approche d'Avast est plus légère et a des exigences plus restreintes, car elle n'a pas besoin d'une image Windows dédiée.

Fermer une session à distance > avec Gmail

Vous n'êtes pas certain d'avoir pensé à refermer votre session Gmail, au bureau ou chez un ami ? Vous pouvez le faire depuis chez vous. Ouvrez votre boîte Gmail, et tout en bas de la fenêtre

principale, sous la mention **Dernière activité**, cliquez sur **Détails**. Dans la fenêtre qui s'ouvre alors, cliquez sur le bouton **Se déconnecter de toutes les autres sessions Web Gmail**.

Générer des mots de passe sûrs > avec Chrome

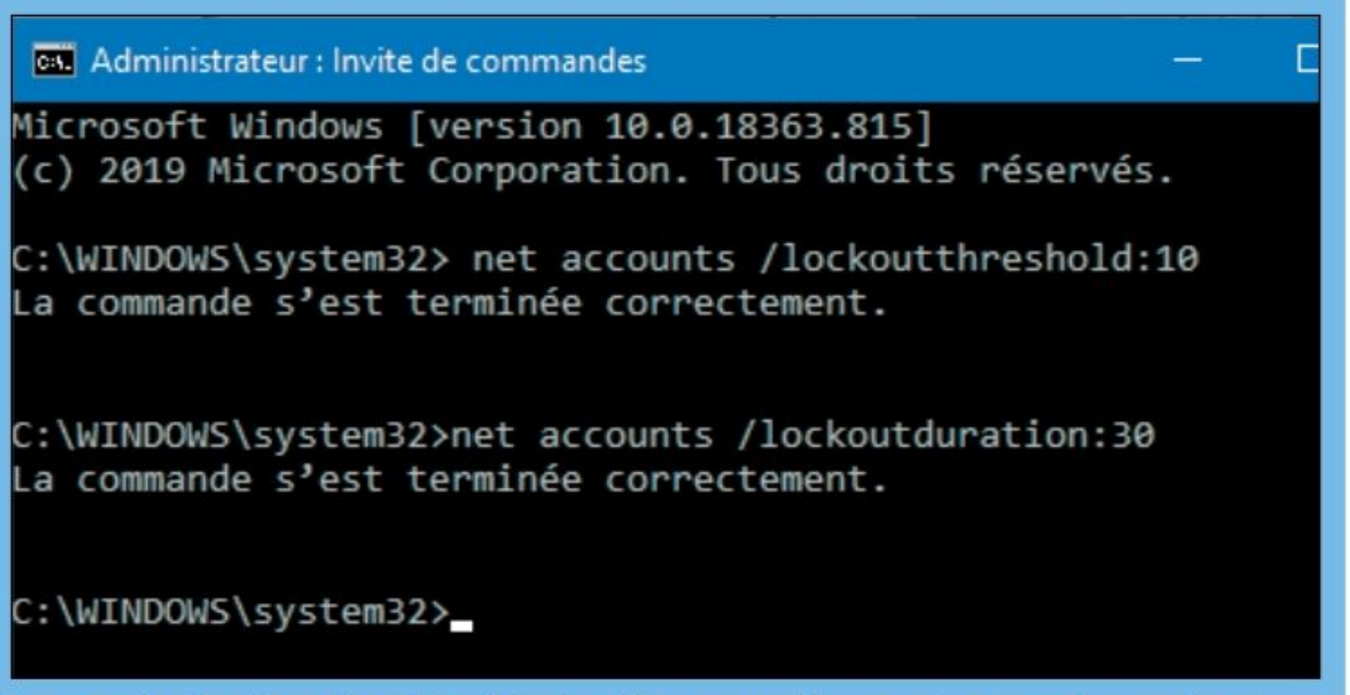


Chrome peut vous proposer des mots de passe sécurisés. Pour cela, activez la synchronisation pour les mots de passe, ces derniers sont alors enregistrés dans votre compte Google (sinon, ils ne sont que sur votre ordinateur). Ensuite, quand vous devrez créer un mot de passe, une fenêtre apparaîtra pour vous en suggérer un. Si ce n'est pas le cas faites un clic droit sur le champ **Mot de passe**, et cliquez sur **Suggérer un mot de passe**.

Protéger un document avec un mot de passe > Avec Microsoft Office

Vous voulez qu'un document (texte, tableau ou présentation) ne puisse pas être lu ou modifié par n'importe qui ? Ouvrez le document en question puis cliquez sur **Fichier > Enregistrer sous > Parcourir**. Dans le menu **Outils** (à côté de **Enregistrer**), choisissez **Options générales** et définissez un **Mot de passe pour la lecture** (demandé pour ouvrir le document) et/ou un **Mot de passe pour la modification** (demandé pour pouvoir modifier le document).

Verrouiller son PC > avec Windows



Pour éviter qu'un pirate ne puisse essayer plein de mots de passe à la chaîne sur votre session Windows, il est possible de verrouiller votre ordinateur pour décourager le «pirate». Après un certain nombre de tentatives infructueuses, il est en effet possible de bloquer l'écran du mot de passe principal pour X minutes... Cliquez sur le bouton **Démarrer** et tapez **cmd** dans le champ **Rechercher**. Faites un clic droit dans le programme **cmd.exe** et choisissez de l'exécuter en tant qu'administrateur. Saisissez **net accounts /lockoutthreshold:10** et validez par **Entrée**. Votre session sera alors verrouillée après 10 tentatives pendant 30 minutes.
Pour changer cette durée, tapez la commande **net accounts /lockoutduration:30** et validez pour bloquer le compte pendant 30 minutes. À vous de choisir la durée que vous souhaitez.

NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC

+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3,50 €

Chez votre marchand de journaux

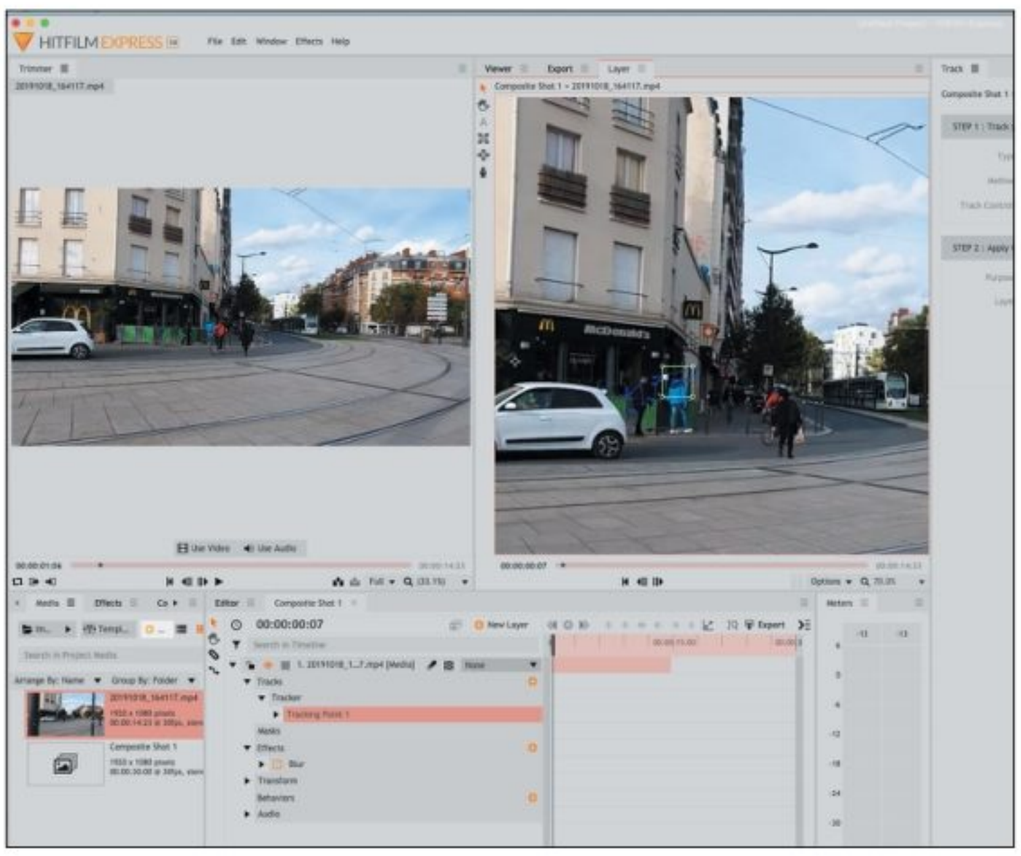
SÉLECTION

TOP 3 DES LOGICIELS POUR FLOUTER FACILEMENT UN VISAGE SUR UNE VIDÉO

Dans les séquences vidéo saisies dans des lieux publics, il s'avère utile de pouvoir masquer des visages ou des plaques d'immatriculation avant toute diffusion. Voici nos trois outils gratuits préférés pour y parvenir.

HITFILM EXPRESS : EFFICACE ET PRÉCIS

Pour ceux qui recherchent la précision,le logiciel de montage HitFilm Express offre des outils assez puissants pour cibler des objets dans une vidéo et leur appliquer l'effet souhaité. Il se montre évidemment bien plus efficace que la fonction proposée par YouTube mais requiert un peu d'apprentissage et de multiples essais pour obtenir un résultat correct et exploitable. Heureusement, les tutos en vidéo ne manquent pas sur le Web pour expliquer la mise en place de l'effet. Disponible pour Windows et MacOS, il ne manque à HitFilm Express qu'une adaptation en français pour se sentir vraiment à l'aise.



Où le trouver ? **https://fxhome.com/hitfilm-express**

YOUTUBE STUDIO : LE PLUS SIMPLE

Les concepteurs de YouTube ont depuis longtemps compris qu'un outil de suivi d'objet dans les séquences (motion tracking) était nécessaire pour éviter aux auteurs d'être confrontés à des problèmes d'atteinte à l'image. Le système se montre assez simple à utiliser. Il faut obligatoirement passer par le navigateur Chrome de Google et se connecter avec son compte Gmail pour accéder à l'éditeur de vidéo. Celui-ci propose de détecter automatiquement les visages (merci l'IA) ou de définir soi-même la zone à flouter. Il faudra se montrer cependant patient pour parvenir à ses fins. La précision n'est pas toujours au rendez-vous.

DAVINCI RESOLVE : COMPLET MAIS COMPLEXE

Si vous n'avez jamais touché un logiciel de montage vidéo, Davinci Resolve n'est pas fait pour vous. Voici un éditeur de vidéo ultra-complet (aussi puissant que Final Cut Pro d'Apple ou Premiere Pro d'Adobe) mais entièrement gratuit. Lui aussi se dote d'un outil de suivi extrêmement précis et assez bluffant mais qui demande de solides connaissances pour être manipulé. Floutage ou pixelisation selon plusieurs niveaux sont de la partie pour un résultat exceptionnel. Encore faut-il dénicher les fonctions qui sont enfouies dans les menus. Une fois maîtrisé, c'est un vrai régal pour les youtubeurs consciencieux.

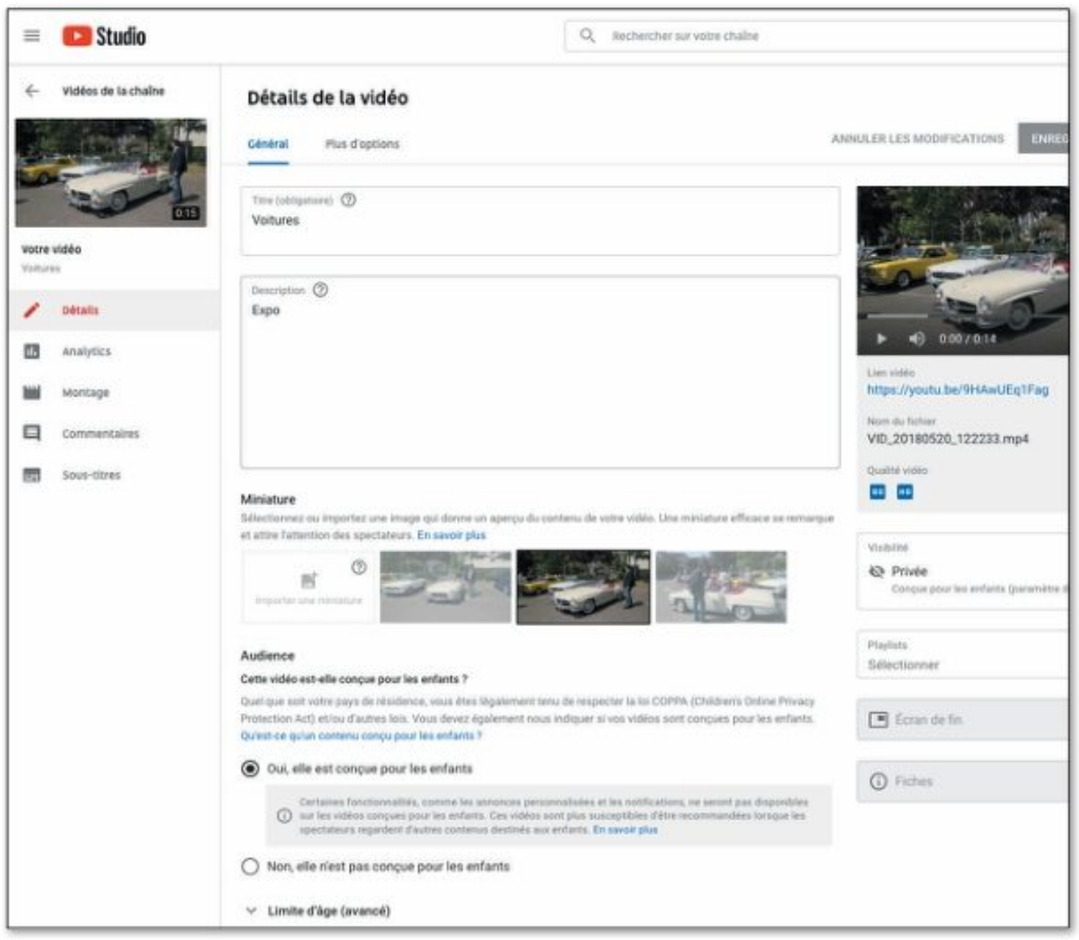
Où le trouver ? **cutt.ly/esb2COq**

FLOUTEZ DES ÉLÉMENTS AVEC YOUTUBE STUDIO

PRATIQUE

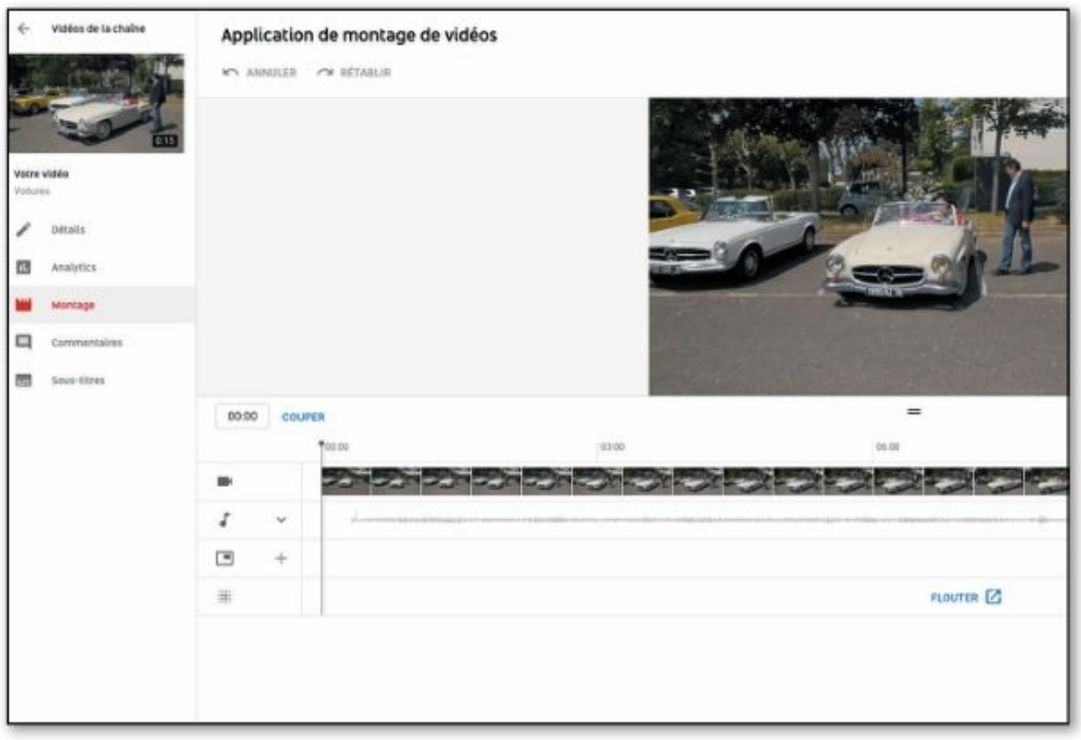
01› IMPORTER LA SÉQUENCE

Envoyez d'abord votre clip vidéo vers les serveurs de YouTube. Rendez-vous sur **studio.youtube.com**, connectez-vous avec votre compte Google puis, depuis l'onglet **Tableau de bord**, cliquez sur **Importer des vidéos**. Choisissez votre fichier et validez. Précisez ensuite un titre, un commentaire, s'il figure des scènes choquantes et indiquez son statut (privé ou public).



02› ACCÉDER AUX OPTIONS DE MASQUAGE

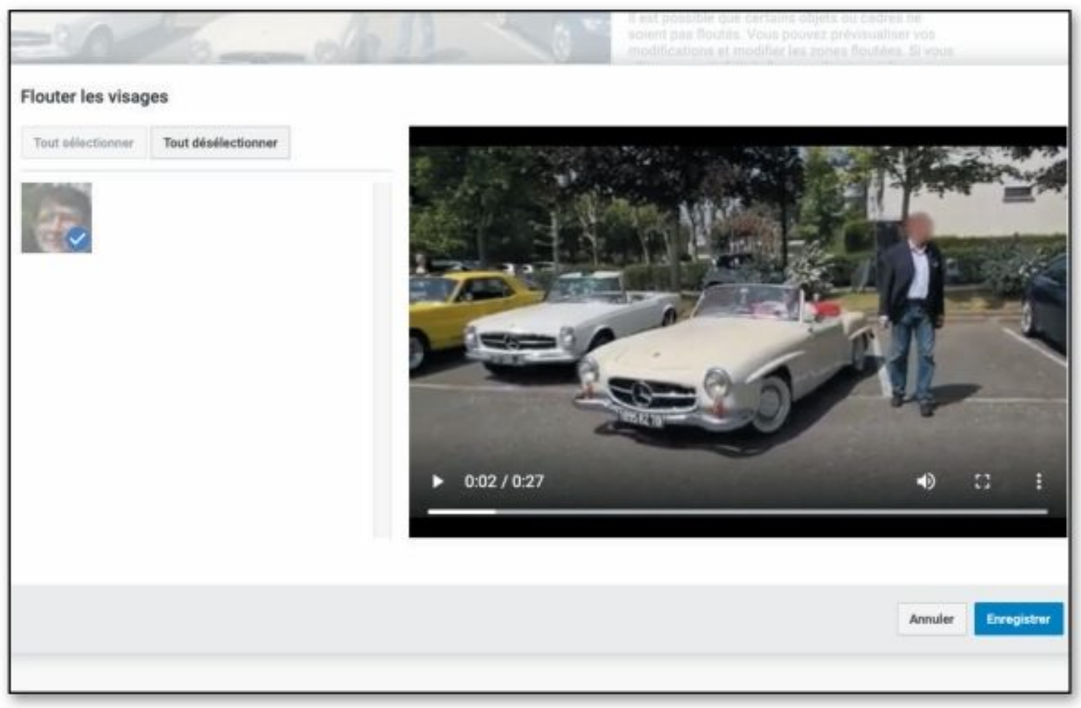
Cliquez maintenant sur l'onglet **Vidéos** à gauche puis sur la vignette de votre séquence et enfin sur l'onglet **Montage** qui a pris place à gauche. Votre clip s'affiche au centre de la fenêtre avec, au-dessous, une timeline des images qui



le composent. Dans celle-ci, à la dernière ligne, figure le bouton **Flouter**. Activez-le pour découvrir les options de floutage.

03› FLOUTER DES VISAGES

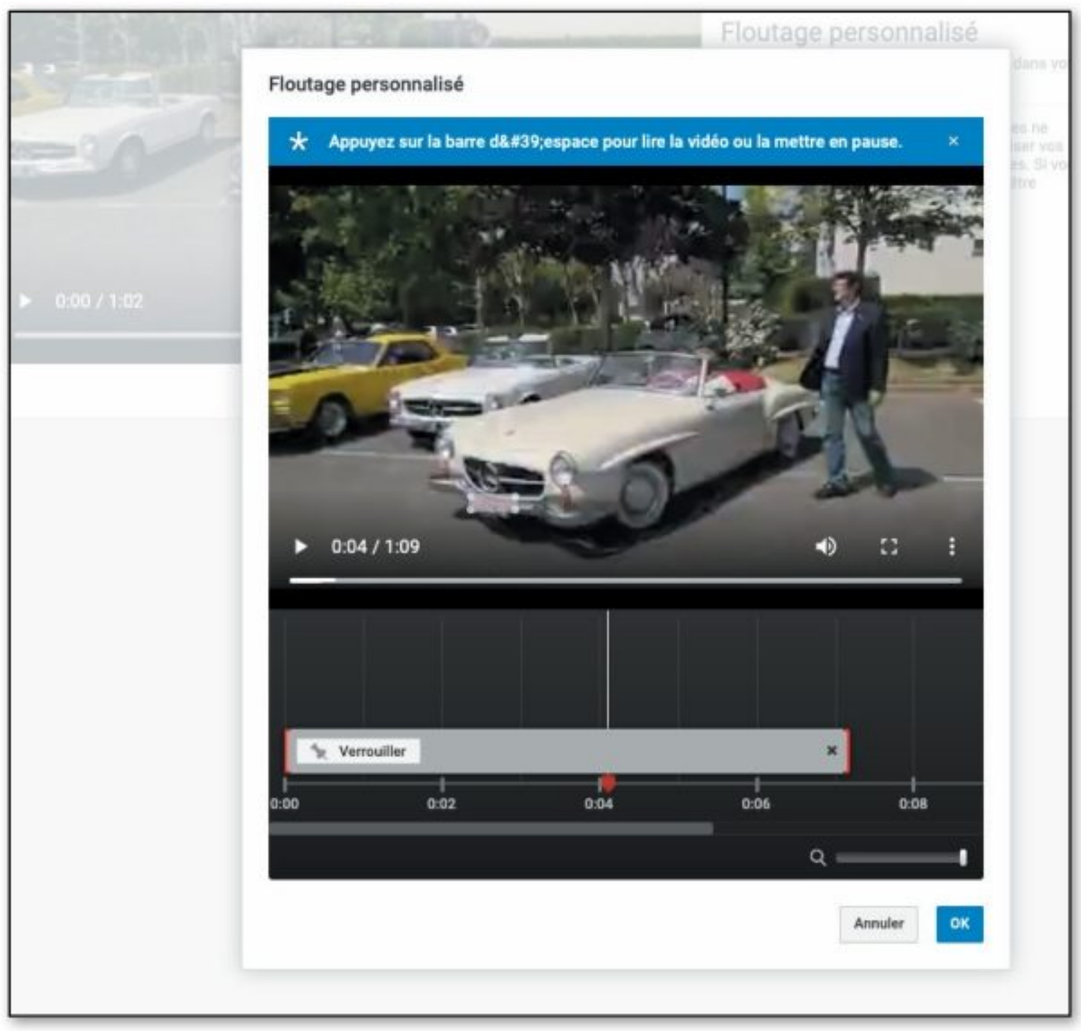
Pour vous simplifier la tâche, laissez les algorithmes de Google détecter les visages présents dans l'image et les masquer. Cliquez sur le bouton **Modifier** de la section **Flouter les visages**. Après l'analyse de la séquence,



se présente en vignettes tous les visages identifiés. Choisissez ceux que vous souhaitez masquer et validez par **Enregistrer**.

04› MASQUER CE QUE VOUS SOUHAITEZ

Pour flouter une plaque d'immatriculation par exemple, cliquez sur le bouton **Modifier** de la section **Floutage personnalisé**. Faites pause dans la vidéo qui défile puis



dessinez à la souris sur l'image la partie qui sera floutée. Relancez la vidéo pour apprécier le tracking et arrêtez l'effet lorsqu'il n'est plus nécessaire en réduisant sa durée dans la timeline. Validez par **OK**.

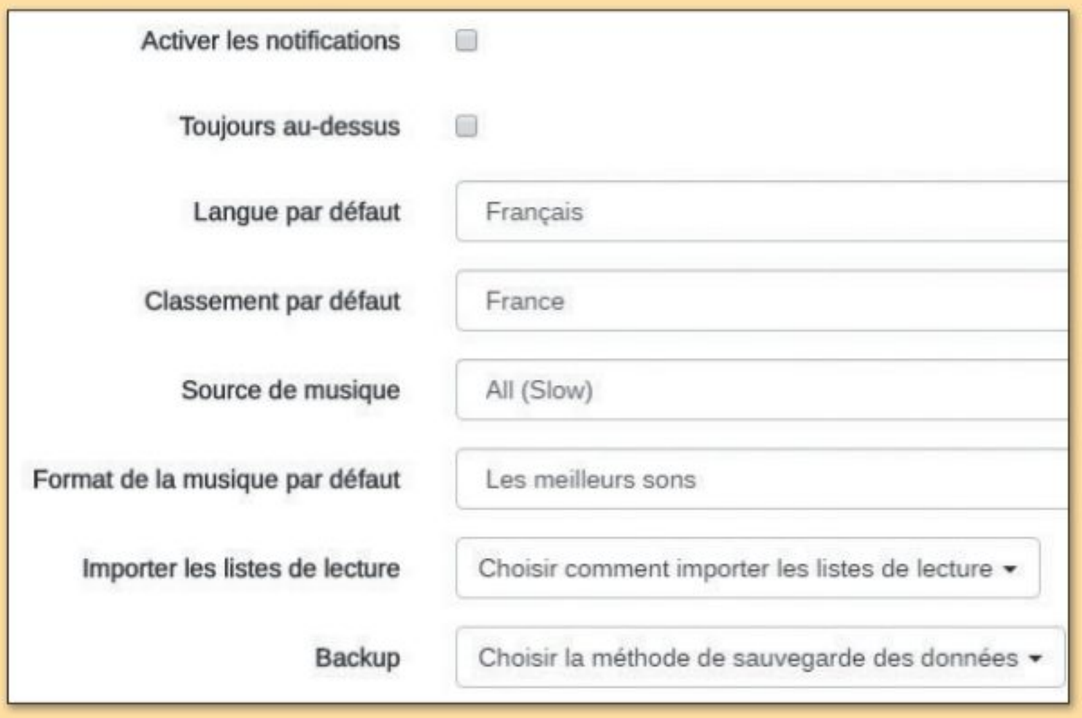
INFOS [KAKU]
Où le trouver ? [http://kaku.rocks]
Difficulté :

ÉCOUTEZ TOUTE LA MUSIQUE DU WEB

Original, Kaku est un lecteur audio open source qui permet d'accéder facilement aux morceaux diffusés sur YouTube, Vimeo et SoundCloud.

01› AJUSTER LES PARAMÈTRES

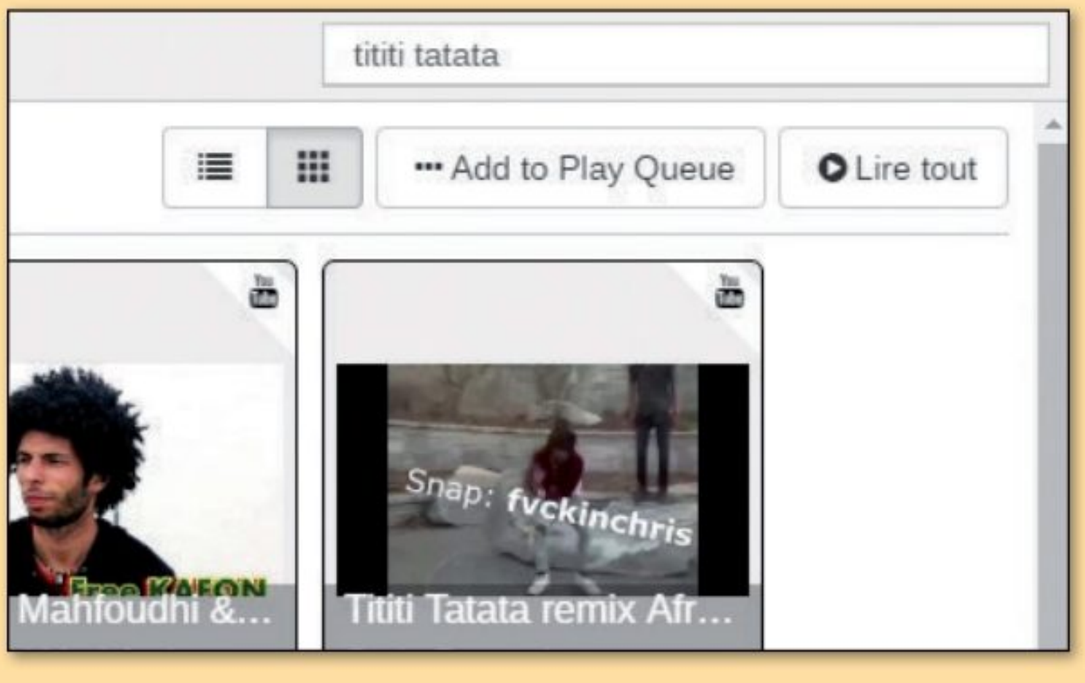
Allez dans **Settings** pour changer la langue en **Français**. Profitez-en pour modifier le **Classement par**



défaut avec un pays dont vous aimeriez connaître les tendances musicales. Sous **Source de musique**, mettez **Tout (lent)** pour afficher un maximum de résultats. Enfin, si les clips vidéo ne vous intéressent pas, sélectionnez **Les meilleurs sons** pour **Format de la musique par défaut**.

02› TROUVER UNE MUSIQUE

Dans le champ **Find something**, entrez votre recherche (titre de chanson, groupe, artiste…) et validez avec la touche **Entrée**. Cliquez sur un résultat pour lancer la lecture. Si vous n'avez pas choisi **Les meilleurs sons** à l'étape précédente, le clip apparaît en bas à gauche. Autrement, le lecteur, toujours au même endroit, affiche un fond noir.



03› CRÉER UNE PLAYLIST

Dans la colonne de gauche, cliquez sur **Ajouter une liste de lecture**, donnez un nom à votre playlist, et validez avec **OK**. Faites un clic doit sur le titre à ajouter dans une playlist : la liste de toutes celles que vous avez créées apparaît. Cliquez sur celle de votre choix pour y intégrer le morceau.

04› PARTAGER SA MUSIQUE

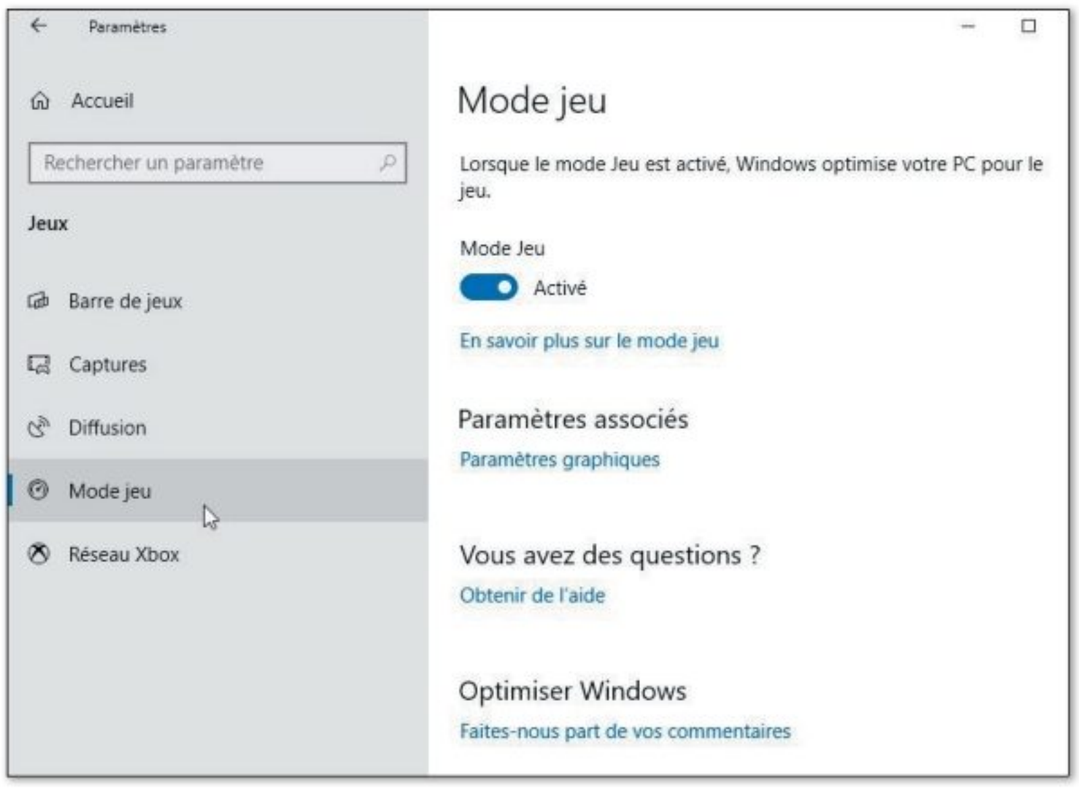
Cliquez sur **Online DJ**, entrez un pseudo et le nom de votre **chan** (canal), en validant avec **Créer une chan**, pour que les utilisateurs de Kaku puissent y entrer et écouter les musiques que vous êtes en train de jouer. Il faudra partager la **Clé du chan** avec les invités, qui pourront alors vous rejoindre et discuter via la fenêtre de chat en bas à droite.

FILMEZ VOS EXPLOITS LUDIQUES

Avec la barre de jeux de Windows 10, enregistrez des captures d'écran ou des vidéos de vos séquences de jeu.

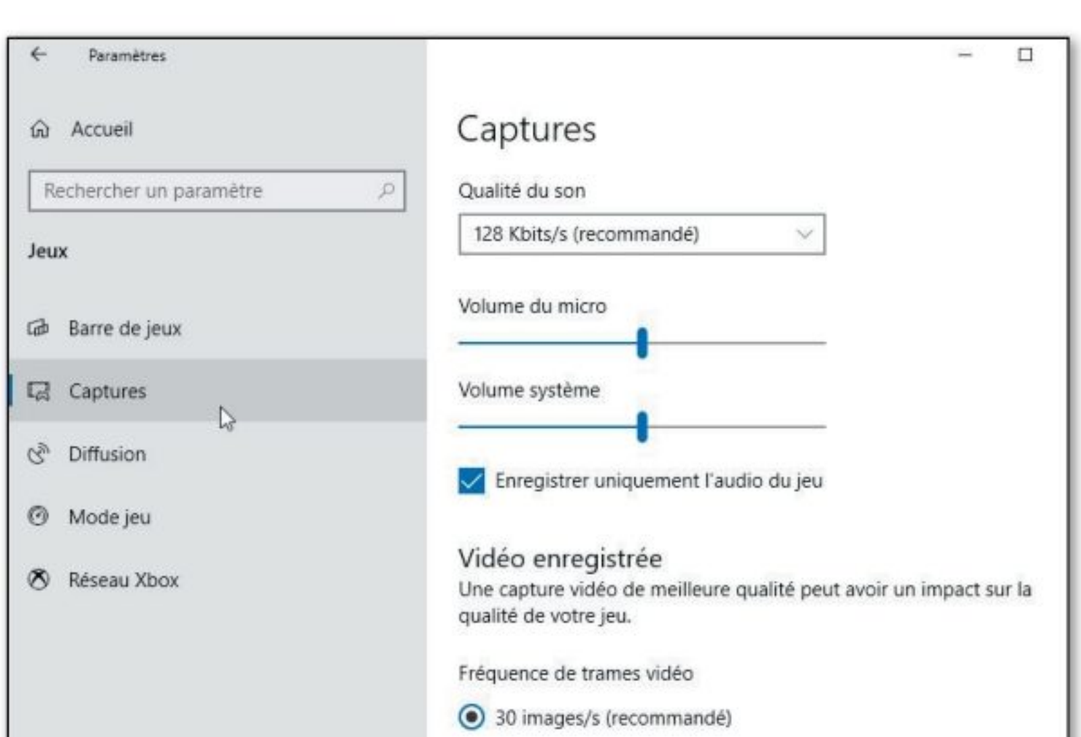
01› ACTIVER LE MODE JEU

Ouvrez les **Paramètres** de Windows et allez à la rubrique **Jeux**. Cliquez d'abord sur l'onglet **Mode jeu** pour passer le curseur **Mode jeu** sur **Activé**. Ceci afin de bénéficier de l'optimisation du PC pour le jeu.



02› ACTIVER LA BARRE DE JEUX

Allez ensuite à la section **Barre de jeux**. Basculez l'indicateur **Enregistrer des clips de jeux, des captures d'écran...** sur **Activé**. À la section **Captures**, vous pouvez régler les paramètres d'enregistrement du son et de l'image.

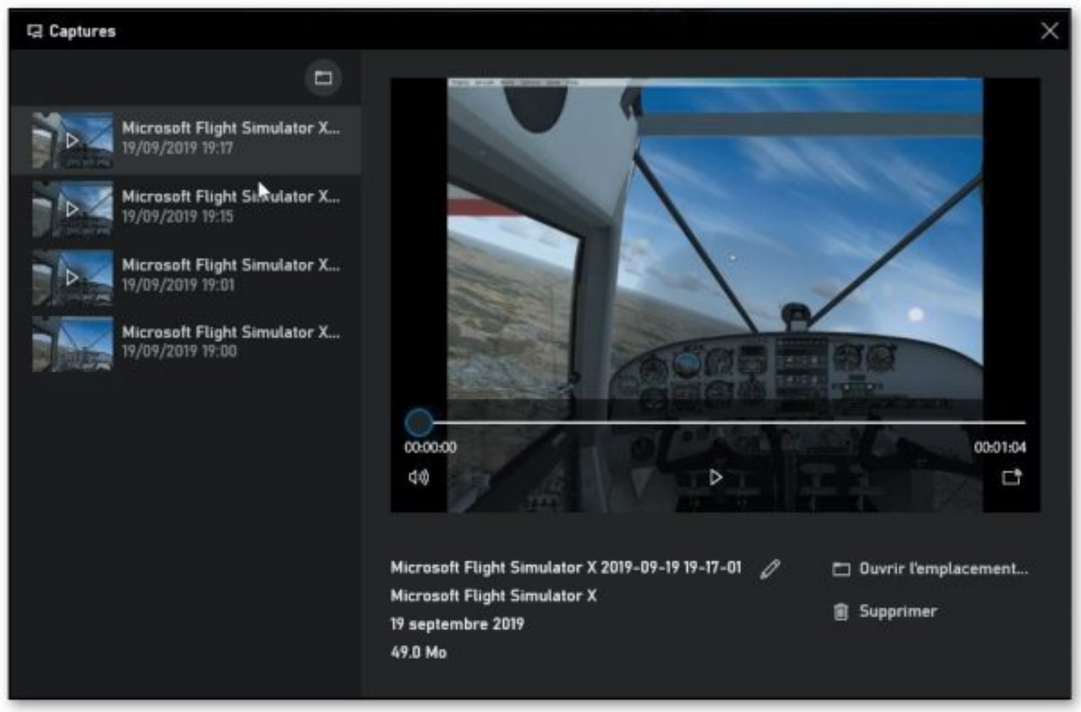


03› ENREGISTRER DES SÉQUENCES

Lancez un jeu vidéo, puis tapez la combinaison **Win + G** pour afficher la barre de jeux et cliquez sur l'appareil photo pour réaliser une capture d'écran, sur le rond pour un enregistrement vidéo. Vous pouvez aussi utiliser les raccourcis clavier.

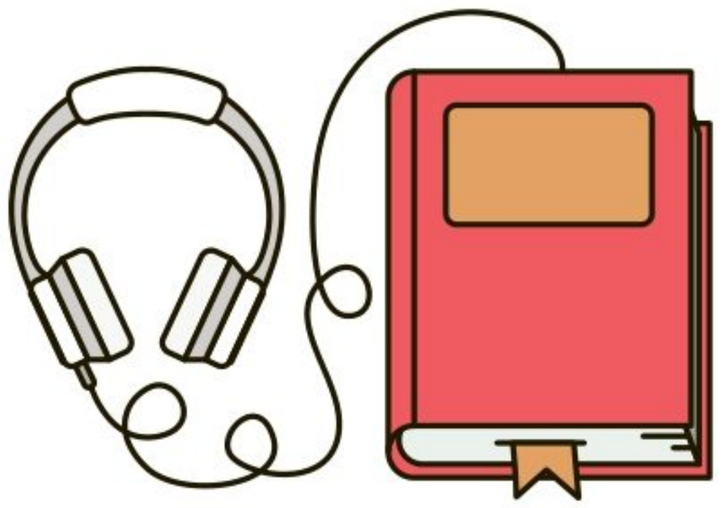
04› VISIONNER LES IMAGES

Cliquez sur lien **Afficher toutes les captures** de la fenêtre **Diffusion et capture** pour retrouver les captures d'écran et vidéos enregistrées. Cliquez sur **Ouvrir l'emplacement** (sous l'image) pour accéder au fichier image ou vidéo correspondant.



INFOS [Astread]
Où le trouver ? [http://astread.com]
Difficulté :

CONVERTISSEZ TEXTES ET E-BOOKS EN LIVRES AUDIO



Astread est un service en ligne gratuit qui convertit vos textes et livres numériques (formats EPUB, PDF, DOC, TXT...) en livres audio, à écouter sur votre autoradio ou votre smartphone.

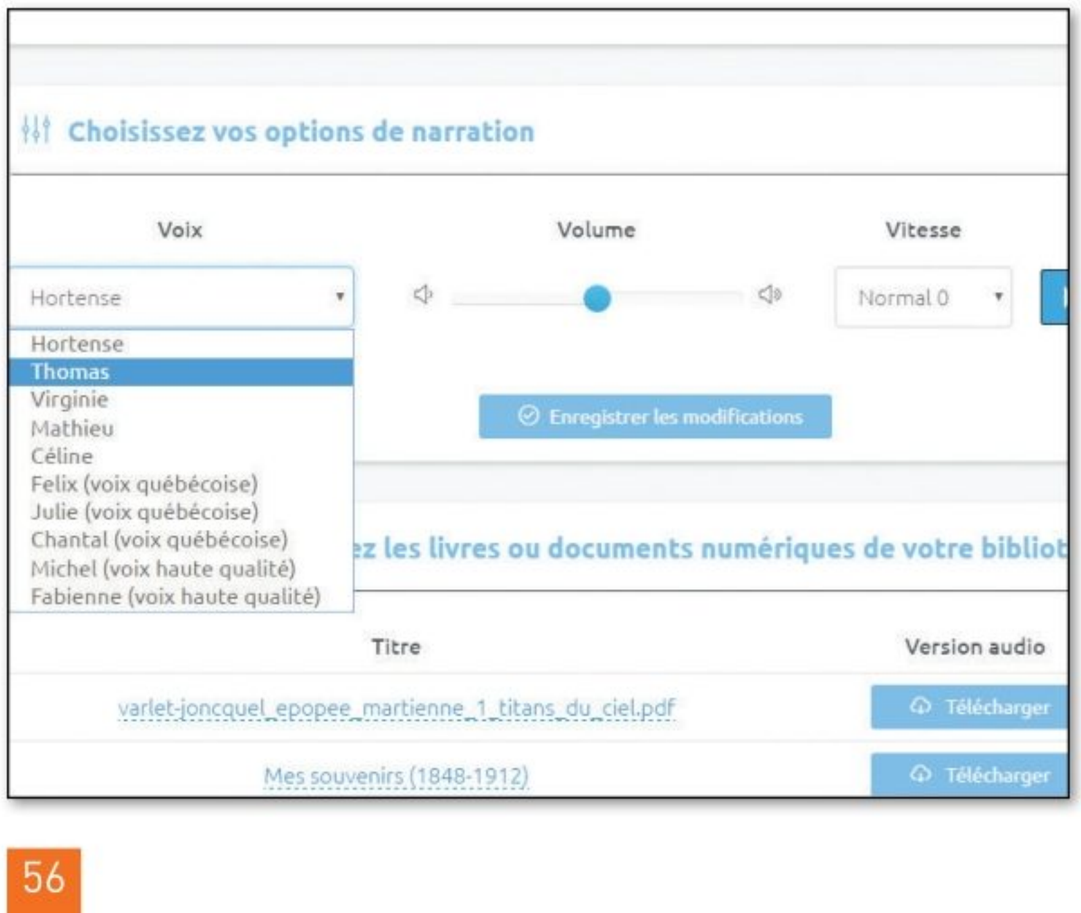
01› IMPORTER LE TEXTE

L'inscription au site s'effectue via une adresse mail. Vous devez cliquer sur le lien de validation que vous recevez.

Une fois connecté au service, cliquez sur **Parcourir** pour téléverser votre texte, via l'explorateur de fichiers qui s'ouvre. Passez ensuite aux réglages en faisant défiler la page jusqu'à **Choisissez vos options de narration.**

02› RÉGLER LE SON

Ici, vous choisissez la **Voix** (féminine ou masculine) qui vous fera la lecture. Définissez un **Volume** puis une **Vitesse**. Avec **Aperçu**, en sélectionnant le bouton lecture, vous contrôlez si les réglages effectués vous conviennent. Lorsque c'est bon, cliquez sur **Enregistrer les modifications**.



03› RÉCUPÉRER SON LIVRE AUDIO

Revenez au premier bloc de la page (**Envoyez vos livres ou documents**...). Cliquez sur **Transférer** puis patientez. Vous recevez un mail provenant d'Astread. Suivez le lien contenu dans le mail, vous êtes renvoyé dans **Ma bibliothèque**. Choisissez **Télécharger** pour votre livre audio. Vous obtenez un dossier compressé. À l'intérieur de ce dernier se trouve votre livre audio au format MP3.

04› ÉCOUTER ET DÉCOUVRIR

Utilisez n'importe quel lecteur multimédia pour écouter vos livres audio. Sachez que vos livres audio sont conservés 48 heures par le service (dans **Ma bibliothèque**) puis ils sont effacés. Via l'onglet **Catalogue**, vous découvrez des ouvrages déjà téléversés sur le service et disponibles en livres audio. Choisissez de les **Ajouter à ma bibliothèque** pour les générer ensuite et les récupérer en MP3.

MESUREZ LA RAPIDITÉ D'AFFICHAGE

PRATIQUE

L'utilitaire gratuit Fraps indique le nombre d'images affichées par seconde dans les jeux en 3D. Bien utile pour vérifier et affiner les réglages graphiques.

INFOS [Fraps]
Où le trouver ? [www.fraps.com]
Difficulté :

01› LANCER FRAPS

Téléchargez et installez Fraps. Tout ce que vous avez à faire pour effectuer une mesure du taux d'affichage, c'est de lancer l'utilitaire avant de lancer le jeu concerné. Décochez la case **Fraps window always on top**, à l'onglet **General**, si l'affichage de la fenêtre au premier plan vous gêne.

02› LANCER LE JEU

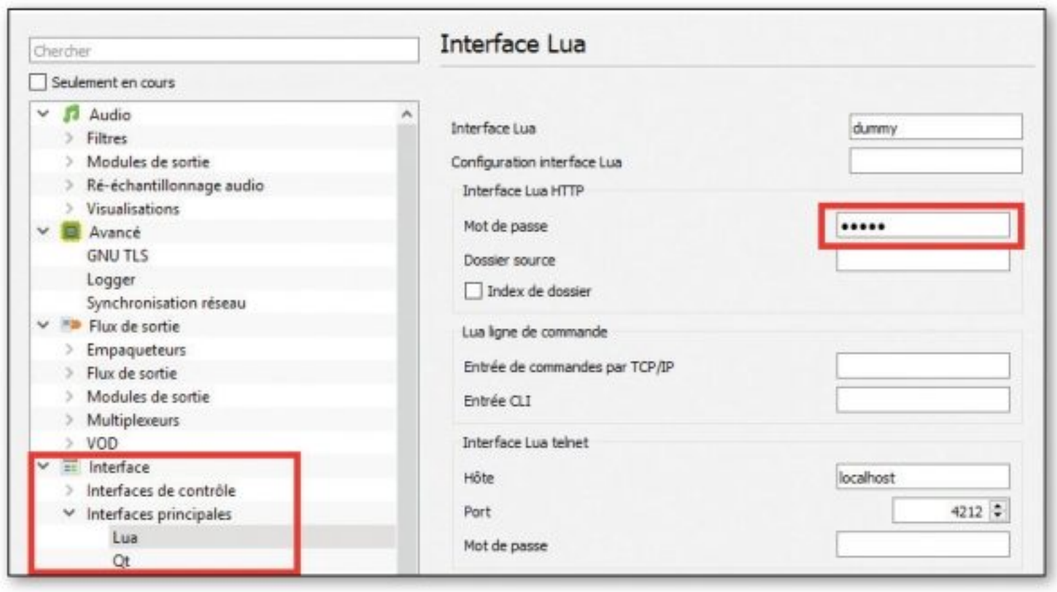
Lancez le jeu pour lequel vous voulez effectuer des mesures (inutile de réduire la fenêtre de Fraps). Le nombre d'images par seconde apparaît dans un coin de l'écran. Il peut varier considérablement suivant les scènes. Faites quelques essais, adaptez les réglages du jeu et de la carte graphique, et refaites une mesure.

TÉLÉCOMMANDEZ VLC DEPUIS SON MOBILE

PRATIQUE

Confortablement installé dans le canapé, vous pouvez contrôler VLC à distance, grâce à une appli installée sur votre smartphone ou votre tablette.

INFOS [Windows]
Difficulté :



01› CONFIGURER VLC

Ouvrez VLC, faites **Outils > Préférences** et cochez **Tous** en bas à gauche. Dans Interfaces principale, cochez Web. Déroulez **Interfaces principales**, allez dans **Lua** et entrez un mot de passe sous **Lua par HTTP**. Notez le numéro du **Port** sous **Lua par telnet**. Validez avec **Enregistrer**, fermez VLC et rouvrez-le. Le pare-feu réagit, **Autorisez l'accès**.

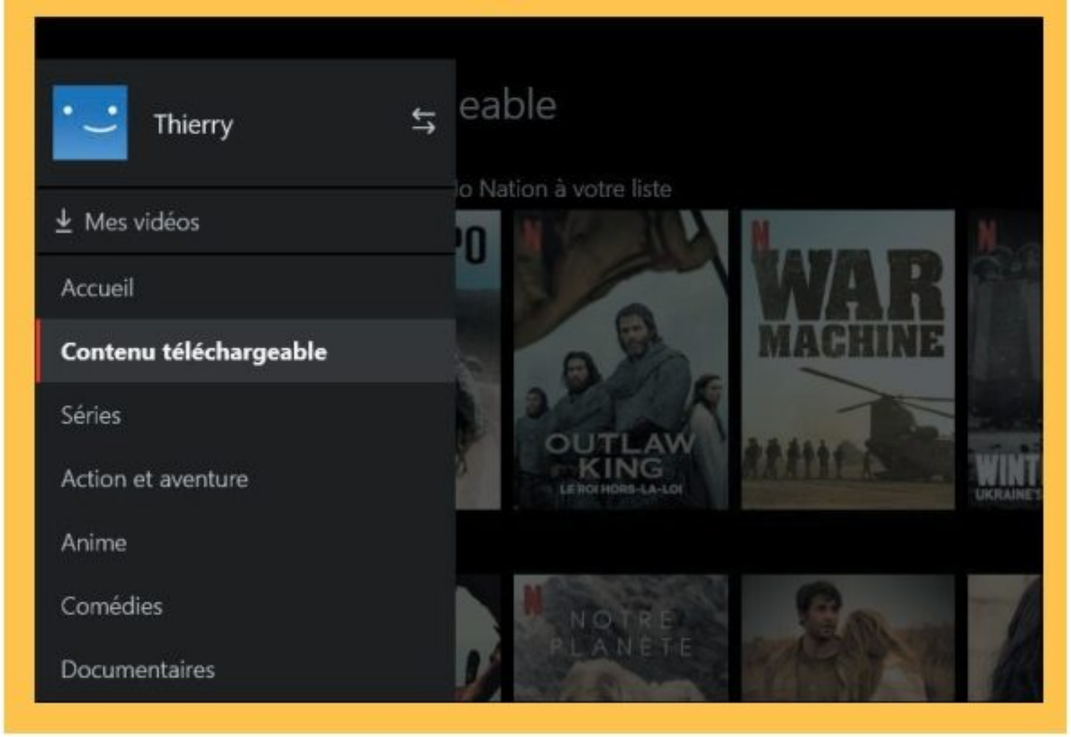
02› LANCER L'APPLI

Installez VLC Mobile Remote sur votre mobile, connectez ce dernier en Wi-Fi sur le même réseau que le PC et lancez l'appli. Entrez l'adresse IP du PC, le mot de passe du port défini à l'étape 1, et validez avec **Save**. Touchez le nom de votre ordinateur et lancez le film depuis le mobile.

Télécharger des films

> avec Netflix

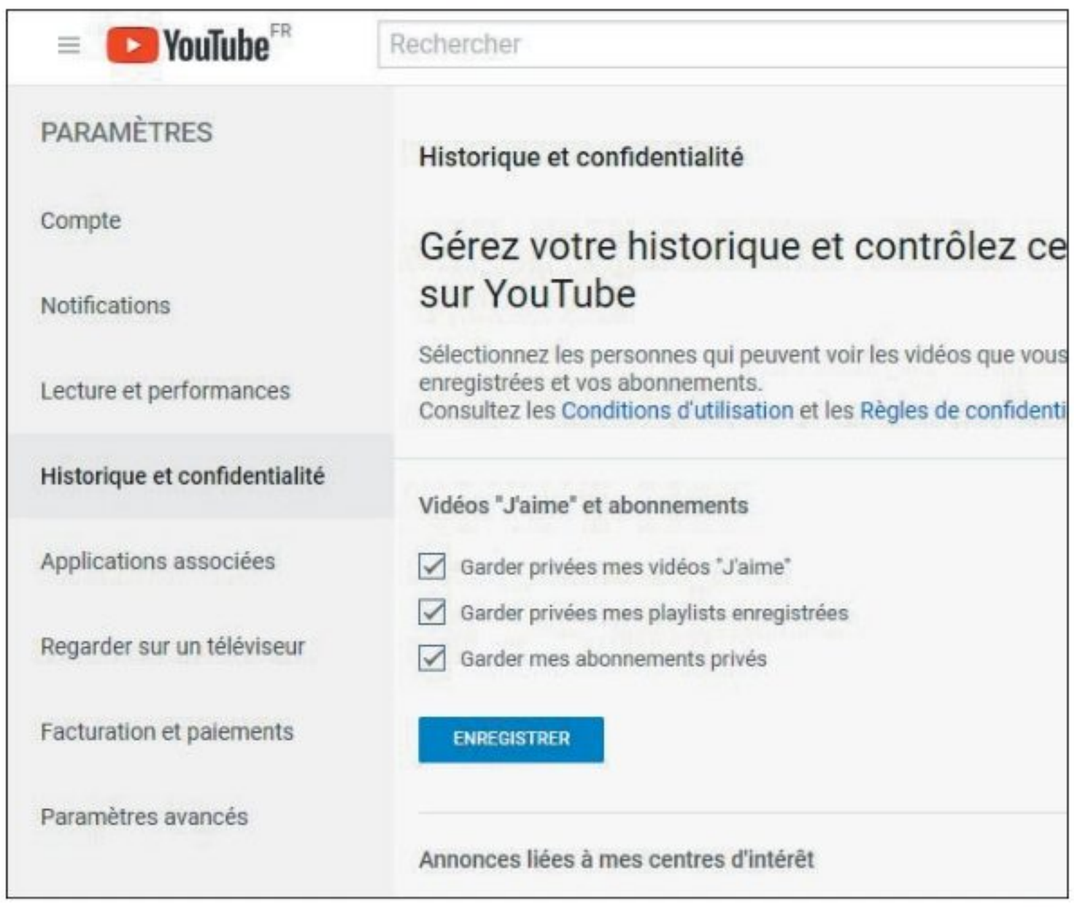
L'application mobile Netflix, sur Android ou iPhone, permet de télécharger des films et des séries pour les regarder hors connexion, en train ou en avion par exemple. Si votre PC tourne sous Windows 8 ou 10, vous pouvez installer l'appli Netflix disponible dans le Microsoft Store pour profiter de cette fonctionnalité, absente du service Web. Un bouton **Télécharger** apparaît sur la fiche des films ou épisodes téléchargeables. Tous ne le sont pas : pour afficher uniquement les titres téléchargeables, cliquez sur le menu, en haut à gauche, puis sur **Contenu téléchargeable**.



Masquer ses abonnements

> avec YouTube

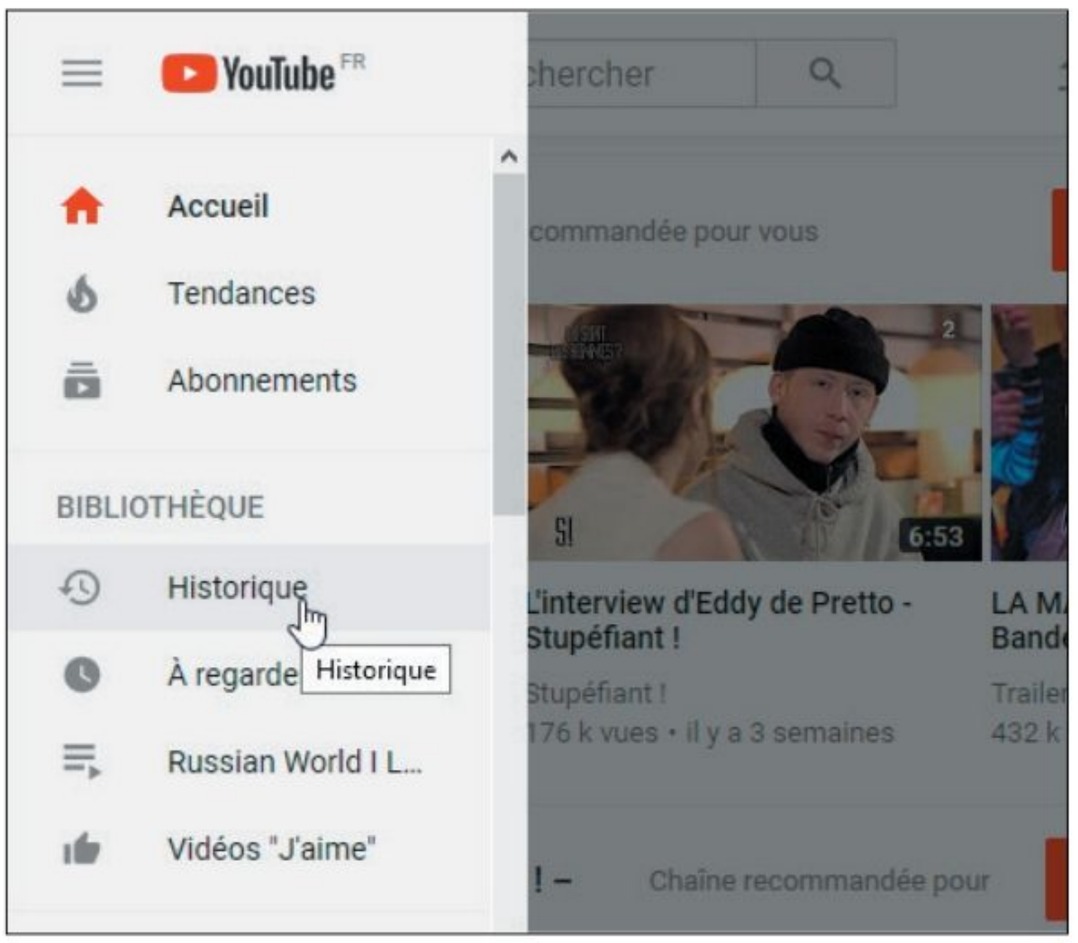
Vos abonnements à des chaînes YouTube sont a priori visibles par tous les autres internautes. Si vous souhaitez les garder privés, connectez-vous à votre compte, rendez-vous dans les **Paramètres** YouTube (cliquez sur votre avatar puis sur la roue crantée). Dans **Confidentialité**, cochez la case **Garder mes abonnements privés**. Validez avec **Enregistrer**.



Contrôler l'historique

> avec YouTube

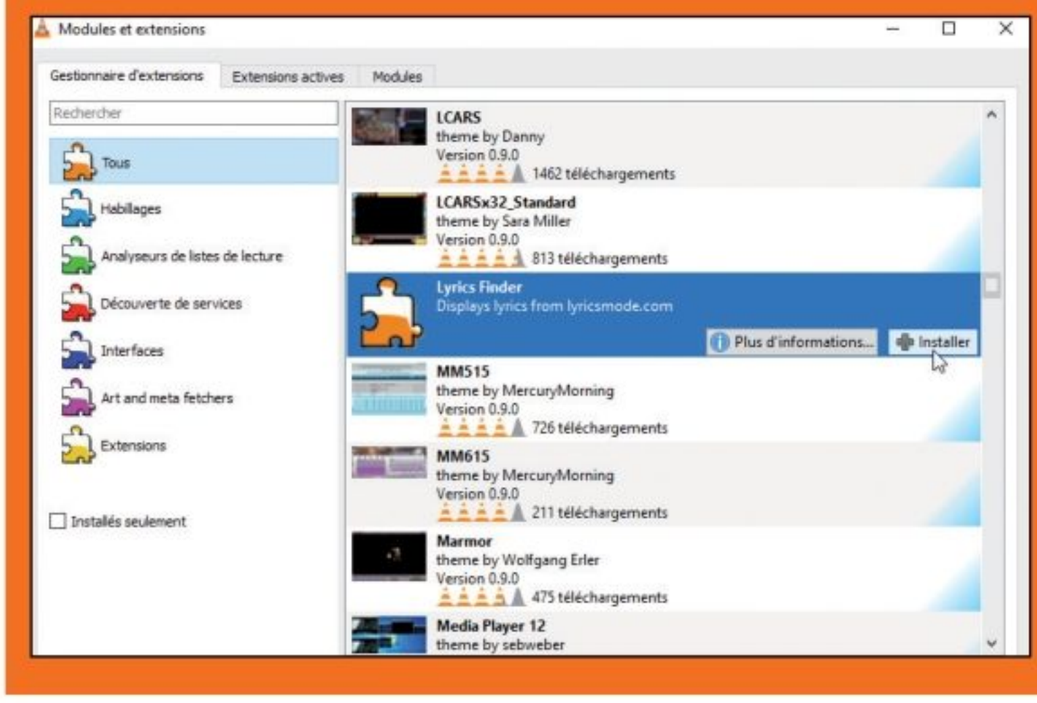
Vous ne voulez pas que quiconque ayant accès à votre compte Google puisse voir les vidéos YouTube que vous avez préalablement consultées ? Dans ce cas, pensez à supprimer ou désactiver votre historique ! Pour ce faire, connectez-vous à votre compte, cliquez sur **Historique** dans la barre latérale de menus, choisissez l'historique que vous voulez : des **vidéos regardées** ou des **recherches**, ou cliquez sur **Effacer tout l'historique** et/ou **Désactiver l'historique**.



Installer des extensions

> avec VLC

VLC peut être amélioré avec l'installation d'extensions permettant d'écouter la radio, de regarder la TV, ou encore de changer son apparence. Cliquez sur le menu **Outils**, puis sur **Extensions et greffons**. Cliquez sur **Trouver plus d'extensions en ligne**. Lorsque vous en trouvez une qui vous intéresse, cliquez dessus, puis cliquez sur **Installer**. Cliquez sur **Plus d'informations** pour en savoir plus sur le fonctionnement de l'extension.



Comme dans une série américaine, le papier peut revenir pendant plusieurs saisons.

La force de tous les papiers, c'est de pouvoir être recyclés au moins cinq fois en papier. Cela dépend de chacun de nous.
www.recyclons-les-papiers.fr

Tous les papiers ont droit à plusieurs vies.
Trions mieux, pour recycler plus !

2 NOUVEAUX MINI PC BLUFFANTS

LE MONDE DES MINI PCS EST UN UNIVERS PARALLÈLE POUR GEEKS ET PROFESSIONNELS : ILS FONT TOUT COMME LES GRANDS MAIS À MOINDRE PUISSANCE ET SOUVENT POUR DES USAGES BIEN DÉFINIS (SON, ROBOTIQUE, DOMOTIQUE, BIDOUILLAGES DIVERS ET VARIÉS). TOUJOURS PLUS PETITS, TOUJOURS PLUS PUISSANTS : ATTENTION, CETTE RENTRÉE MARQUE UNE RUPTURE ! L'EXEMPLE AVEC DEUX MINI PCS AUX DEUX EXTRÊMES DU SPECTRE.

BEELINK GT-R, IL VEUT DÉTRÔNER VOTRE PC FAMILIAL

Cette nouveauté Beelink est un monstre dans sa catégorie. Déjà, le prix (env. 550 €) se rapproche du prix d'une tour PC. Mais, surtout, ses composants internes en font une Rolls de performances qui concurrence directement celles d'un PC familial justement. Le tout dans des dimensions bien moindres : 16.8 cm de large pour 12 cm de profondeur et 3.9 cm d'épaisseur pour seulement 753 gr. Certains n'hésitent plus à dire que ce standard risque rapidement de s'imposer sur le marché grand public.

DU HAUT DE GAMME À TOUS LES ÉTAGES

Ce Beelink GT-R est seulement le deuxième mini PC à intégrer la nouvelle puce Ryzen 5 R3550H. Après le Minisforum Deskmini DMAF5, Beelink utilise ce nouveau processeur AMD qui impressionne : quatre cœurs et huit threads cadencés de 2.1 à 3.7 GHz et associé à un Radeon Vega 8. Une petite puce survoltée qui permettra de faire de la retouche photo, du montage vidéo HD et même de jouer à des jeux récents pas trop gourmands. Enfin, tout ce que fait un PC familial quoi...

CONFIGURATION :

- Rysen 5 R3550H (quatre cœurs et huit threads cadencés de 2.1 à 3.7 GHz)
- Carte graphique AMD Radeon Vega 8
- Mémoire 16 Go RAM
- Disque dur HDD 1 To + SSD 512 Go
- Connectique : 6 x USB3.0 + 2 x HDMI + 1 x DP + 1 x Type-C
- Lecteur de cartes MicroSD
- WiFi 6, Bluetooth 5.1,Ethernet (x2)
- Système d'exploitation non fourni (Linux ou Windows)

Dans cette version du GT-R, vous ajoutez 1 To de stockage HDD + 512 Go en SSD, 16 Go de DDR (!), du Wi-Fi 6 : n'en jetez plus, vous avez trouvé votre PC pour la rentrée. Allez, petit cadeau : deux microphones intégrés sont aussi de la partie, dont un compatible pour interagir avec Cortana et d'autres assistants IA... Bluffant, on vous dit.

Où le trouver ? **fr.geekbuying.com**
Prix : **env. 550 €**

LA BÊTE EST ÉVOLUTIVE, DISPOSE D'UNE FINITION ALUMINIUM DU PLUS BEL EFFET (ET TRÈS UTILE POUR LA DISSIPATION DE CHALEUR)... AINSI QUE D'UN LECTEUR D'EMPREINTE POUR SÉCURISER (ET CHIFFRER!) LE TOUT.

» XCY M1T, ÉPURE ET RIGUEUR DANS LA POCHE

Le XCY M1T est un minuscule PC équipé d'un Celeron N4100 : rendez vous compte, il ne mesure que 6.2 cm de côté sur 4.2 cm d'épaisseur. Épuré, son design ne laisse rien au superflu et cette sobriété efficace en impose. Sa puce Celeron Gemini Lake N4100 est connue pour sa bonne facture et ses qualités de dissipation thermique dans un environnement aussi contraint. Le circuit graphique UHD 600 saura prendre en charge la gestion de contenus Ultra HD et suivra la cadence pour tous vos usages bureautiques et Internet habituels. Côté connectique, pas de choix au rabais : de l'HDMI 2.0 et deux prises USB 3.0.

De la même manière, le stockage (SSD 128 Go) et la mémoire vive (8 Go) en font un mini PC tout terrain, optimisé et sans fausse note. Le ventilateur est peut-être un point discutable, encore que nécessaire, puisqu'il implique un usage non silencieux de la bestiole.

CONFIGURATION :

- Celeron Gemini Lake N4100 (4 cœurs et 4 threads cadencés de 1.1 à 2.4 Ghz avec 4 Mo de mémoire cache)
- Circuit graphique Intel UHD 600
- Mémoire 8 Go RAM
- Disque dur SSD 128 Go
- Connectique : 2 x USB3.0 + 1 x HDMI2.0 + 1 x USB-C (alimentation),
- Lecteur de cartes MicroSD
- WiFi, Bluetooth 4, pas de connectique Ethernet
- Système d'exploitation non fourni (Linux ou Windows)

Où le trouver ? **Aliexpress.com** Prix : **env. 150 €**

» FLIPPER LE HACKER !

FLIPPER ZERO ET FLIPPER ONE SONT DES TROUSSES À OUTILS PORTABLE POUR LES PENTESTERS ET LES GEEKS DANS LE CORPS D'UN TAMAGOCHI ! PROPOSÉ SUR KICKSTARTER, LE PROJET EST DEVENU LE TUBE DE L'ÉTÉ.

Élevez et faites progresser votre dauphin en lui fournissant ce qu'il adore le plus : apprendre de nouveaux hacks et bidouillages. Il adore pirater des éléments numériques tels que les protocoles radio, des systèmes de contrôle d'accès, du hardware connecté, etc. Flipper est entièrement open source et personnalisable afin que vous puissiez apprendre et développer vos talents de hacker éthique en même temps que lui. Différentes missions vous permettent, au minimum de le transformer en télécommande universelle, voire en clé de sécurité (lire page suivante !) ou de pentester les réseaux du quartier. Selon sa version (Zero ou One), Flipper le Hacker embarque des composants et antennes RFID, WiFi, Bluetooth, NFC, Infra-rouge, pins GPIO, etc.

Où le trouver ? **flipperzero.one** Prix : **à partir de 130 €**

CLÉS D'AUTHENTIFICATION : SÉCURISEZ VOS TERMINAUX COMME UN PRO

Double-authentification : une petite clé USB ou NFC pour les protéger tous.

Vous utilisez différents mots de passe pour vos différents comptes et services en ligne. Vous les changez même régulièrement. Mais vous avez toujours la crainte que vos identifiants vous soient un jour dérobés, par phishing (cela arrive même aux meilleurs), inadvertance ou piratage. De nombreux services en ligne proposent déjà la « double authentification » qui exige par exemple que vous receviez un SMS en plus de votre login et mot de passe habituels pour vous connecter.
Mais de plus en plus de professionnels se tournent vers la double authentification matérielle : pour vous identifier, vous aurez besoin d'une clé physique personnelle (clé USB, lightning ou NFC) que vous connecterez à votre PC ou smartphone par exemple. Sans cette clé, personne ne peut accéder à vos comptes, même avec les bons identifiants !

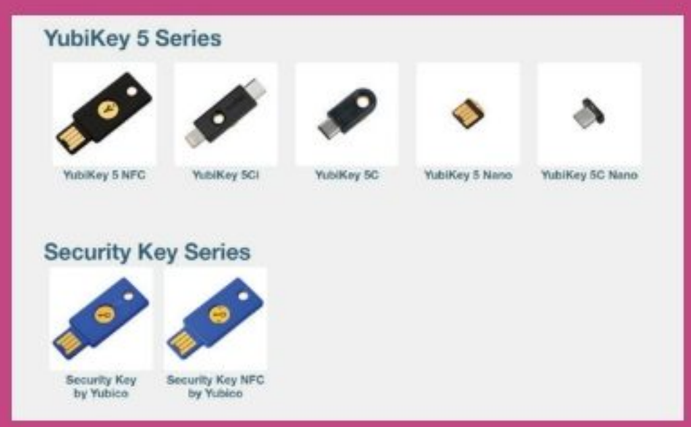
Comment ça marche?

Ces clés ne fonctionnent pas avec tous les comptes en ligne mais uniquement avec ceux qui intègrent certains standards de sécurité compatibles. Mais ne vous inquiétez pas, tous les plus grands et les plus populaires y sont passés depuis longtemps et travaillent en étroite collaboration avec les éditeurs certifiés de clés d'authentification pour rendre l'expérience utilisateur la plus fluide possible. Tous les services Google, Facebook, Windows, Dropbox, etc. sont ainsi compatibles parmi des centaines d'autres (y compris des gestionnaires de Bitcoins !).
Prenons l'exemple des clés Yubico dont nous vous expliquons le fonctionnement en pratique page suivante. L'entreprise combine dans ses clés plusieurs composants d'authentification de haut niveau comme OTP, FIDO2, FIDO U2F, PIV, OATH & OpenPGP. Selon les services utilisés, un ou plusieurs de ces protocoles seront mis à contribution. L'avantage ? Pas besoin de configurer ces technologies de sécurisation très pointues une à une. Enfin si, tout de même, puisque vous devrez autoriser dans les paramètres de chaque application et service l'utilisation d'une clé de sécurité. Vous pouvez ainsi limiter l'usage de votre clé à vos comptes Google, à votre service de cloud préféré, à votre

compte Microsoft... ou le généraliser à tous vos comptes. Une fois activée, l'expérience est transparente pour l'utilisateur car la clé communique avec vos services en ligne de façon automatisée, chiffrée et totalement sécurisée de bout en bout grâce à la compatibilité de ces standards. Hier réservé aux administrateurs réseaux et sécurité, ce type d'outil professionnel est désormais accessible au grand public pour quelques dizaines d'euros.

YUBICO : LE PIONNIER

Yubico est la marque de clés authentification la plus connue, elle a notamment participé à la création de plusieurs standards désormais utilisés par la concurrence. Ses clés fonctionnent avec Microsoft Windows, MacOS, iOS, Android et Linux, ainsi que sur les principaux navigateurs.



Prix de la la YubiKey 5C présentée ci-contre : **60 €**
Où le trouver ? **www.yubico.com**

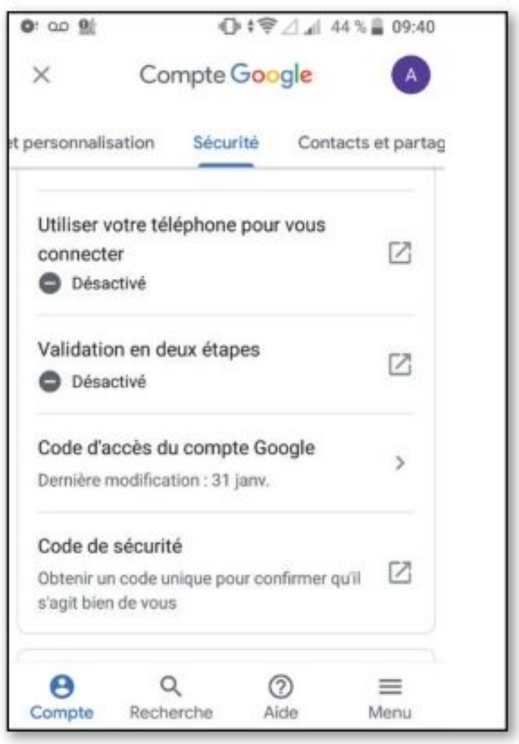
GOOGLE PROPOSE LUI AUSSI SES PROPRES CLÉS D'AUTHENTIFICATION AVEC SA GAMME TITAN. POUR LES POSSESSEURS DE SMARTPHONES GOOGLE PIXEL 3 ET 4, LA PROCÉDURE EST ENCORE SIMPLIFIÉE AVEC L'INTÉGRATION D'UNE PUCE DE SÉCURITÉ COMPATIBLE TITAN M.

PRISE EN MAIN DE LA YUBIKEY 5C

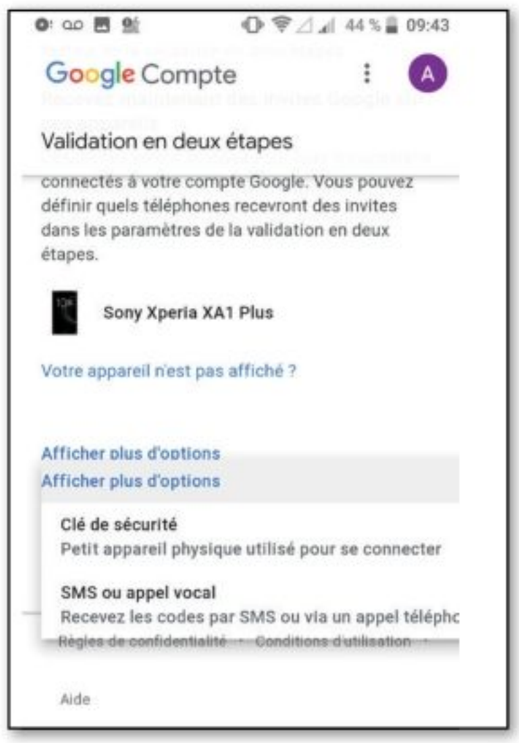
Nous vous présentons ici une prise en main de la clé d'authentification YubiKey 5C de Yubico. Le mode de fonctionnement détaillé ci-après est assez similaire chez les autres fabricants. La YubiKey 5C dispose d'une connectique USB de type C, dédiée aux PC et terminaux mobiles compatibles.

#1 Vous devez configurer le ou les services que vous souhaitez sécuriser un à un. Ici, nous vous montrons comment faire avec votre compte Google. Chaque service compatible avec la YubiKey propose la **Double authentification** avec une **clé d'authentification** à activer depuis les paramètres.

#2 Ici, nous allons sécuriser notre compte Google sur notre smartphone. Allez dans votre appli **Google** puis **Gérer votre compte Google**. Dans l'onglet **Sécurité**, activez (si ce n'était déjà fait) la **Validation en deux étapes**.



#3 Par défaut, Google vous propose une validation en deux étapes via SMS. Mais ici, nous allons dans **Afficher plus d'options**. C'est là qu'apparaît la fonctionnalité **Clé de sécurité** que vous sélectionnez. Notez que votre smartphone Android est toujours associé par défaut à votre compte Google : même sans clé, vous aurez accès à votre compte sur ce smartphone uniquement. Tous les autres terminaux devront utiliser en plus la double authentification avec votre YubiKey.



#4 Vous pouvez demander à Google que votre smartphone principal exige une authentification uniquement avec la clé YubiKey. Mais cela est dangereux : si vous perdez votre clé, vous devez prévoir une autre solution de récupération ! Google est ici le service le plus intrusif et maître puisqu'il est intimement lié à votre écosystème Android.

#5 Revenons à nos moutons. Vous allez maintenant appairer votre clé à votre smartphone et compte Google. Ici, nous choisissons **Utiliser la clé de sécurité avec USB**. Google vous invite à connecter maintenant votre clé. Sur ce modèle de clé YubiKey 5C, une fois branchée sur votre smartphone, vous devez appuyer avec vos doigts sur les deux reliefs métalliques présents sur chaque côté de la clé pour valider l'activation finale.

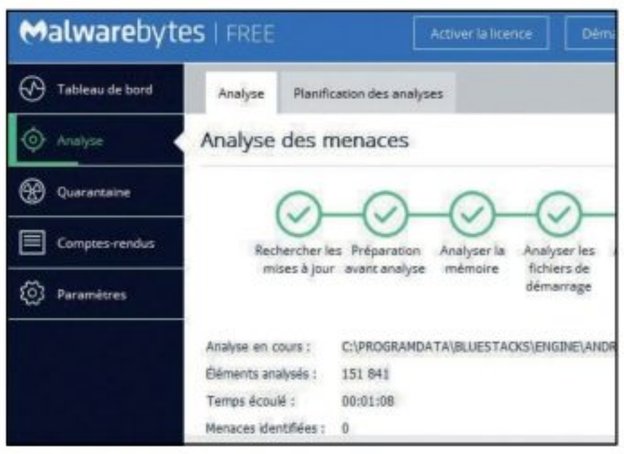
#6 Vous l'aurez compris, hormis sur votre smartphone, toute personne voulant se connecter dorénavant sur vos comptes Google devra utiliser la YubiKey comme deuxième méthode d'authentification après avoir entré vos logins et mots de passe !

SÉLECTION

TOP 15 Logiciels & services GRATUITS

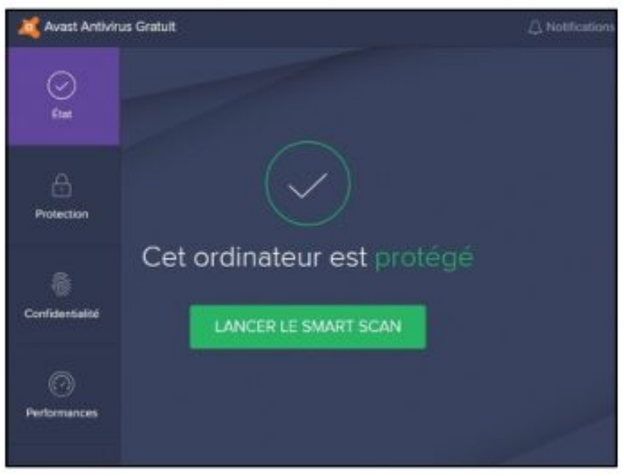
TOP5 ANTIMALWARES

MALWAREBYTES > Le dénicheur



Certains malwares, vers ou virus particulièrement retors réapparaissent après un redémarrage de Windows. Il peut s'agir d'une infection du registre ou d'un fichier système. Malwarebytes propose une désinfection en profondeur et permet même d'avoir accès aux fichiers verrouillés par Windows. Vous pouvez aussi procéder à une désinfection en mode sans échec pour que Windows ne charge pas ce maudit virus par erreur lors de son démarrage.

Lien : www.malwarebytes.com



AVAST > L'essentiel et la puissance

C'est l'antivirus gratuit le plus populaire. Il installe une protection permanente de l'ordinateur contre les logiciels malveillants et empêche les mauvais plaisantins d'installer des extensions indésirables sur votre navigateur ou de pirater vos historiques. Sa version gratuite possède aussi un anti ransomware, un gestionnaire de mots de passe et un outil de mise à jour de vos logiciels préférés. Sûr et pratique.

Lien : www.avast.com

KASPERSKY VIRUSDESK > En cas de doute

Kaspersky, célèbre éditeur d'antivirus, propose un service Web qui vous permet de vérifier qu'un fichier ou un lien Internet est sans risque pour votre PC. Pour les fichiers, le logiciel antivirus maison est exploité. Pour les sites Internet, VirusDesk utilise la base de données de réputation KasperskySecurity Network. Une aide précieuse en complément de votre antivirus pour obtenir un scan le plus large possible.

Lien : virusdesk.kaspersky.fr

RANSOMWARE FILE DECRYPTOR > Récupérez vos données

Victime d'un ransomware, vous vous retrouvez avec des fichiers chiffrés auxquels vous ne pouvez plus accéder ? Ransomware FileDecryptor, proposé par Trend Micro, peut vous aider à décrypter vos données. Il faut d'abord indiquer le nom du ransomware (une grosse vingtaine est prise en compte), mais vous pouvez transmettre un exemple de fichier crypté pour l'identifier. Résultat non garanti, mais à essayer.

Lien : success.trendmicro.com

IOBIT MALWARE FIGHTER > Pour les exotiques

Moins facile d'accès et cherchant ses cibles dans les tréfonds de votre PC, IObit Malware Fighter traque ce qu'un autre antimalware n'aurait pas détecté. La bonne réputation de l'équipe de dévelopement et les améliorations régulières de son ergonomie le rendent de plus en plus recommandable aux novices, même si quelques notions de registre sont bien venues pour ne pas se retrouver à bloquer des composants essentiels de votre système par inadvertance.

Lien : iobit.com/fr/malware-fighter.php

TOP5 GESTIONNAIRES DE MOTS DE PASSE

LASTPASS > Le + populaire

LastPass retient l'ensemble des mots de passe qui vous sont utiles au quotidien pour les sites que vous avez l'habitude d'utiliser. Il propose également un outil permettant de remplir automatiquement les formulaires avec vos données personnelles (nom, prénom, adresse...).

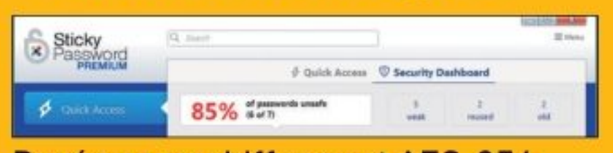
Lien : www.lastpass.com/fr

KEEPASS > L'usine blindée

Mais qu'est-ce qu'il est moche ! Oui, mais ce qui compte c'est la sécurité intérieure ! Avec sa certification délivrée par l'Autorité Nationale de Sécurité Informatique, Keepass est même recommandé par l'état français. Et si on vous dit qu'il est entièrement gratuit...

Lien : keepass.fr

STICKY PASSWORD > Biométrie intégrée



Basé sur un chiffrement AES-256, nous avons surtout remarqué la prise en charge par Sticky Passworfd de la biométrie. Cela signifie que si vous verrouillez votre smartphone par empreinte digitale, StickyPassword suivra le mouvement ! La version gratuite est complète, hormis une offre Cloud réservée aux membres Premium.

Lien : www.stickypassword.com

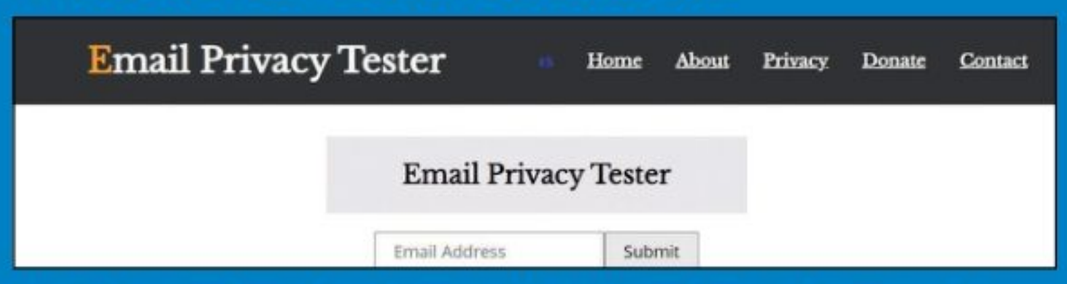
TOP5 MAILS SÉCURISÉS

MAILFENCE > Petit mais costaud

La messagerie est exempte de publicité et l'éditeur s'engage à n'envoyer aucun spams ni sollicitations, à ne jamais commercialiser sa base d'utilisateurs ni de partager leurs données avec des tiers et précise que son certificat SSL/TLS ne comporte aucune autorité de certification américaine. Créée et hébergée en Belgique, la version gratuite de Mailfence propose 500 Mb de stockage.

Lien : mailfence.com

EMAIL PRIVACY TESTER > Testez votre confidentialité



Ici, l'idée n'est pas de changer de boite mail mais d'apprendre à rendre votre messagerie préférée (Gmail au hasard) plus respectueuse de votre vie privée Pour tester la discrétion de votre compte mail, le service en ligne Email Privacy Tester vous permet de savoir quelles informations sont transmises lorsque vous échangez par mail. À vous ensuite de colmater les fuites, il faut s'y connaître un peu.

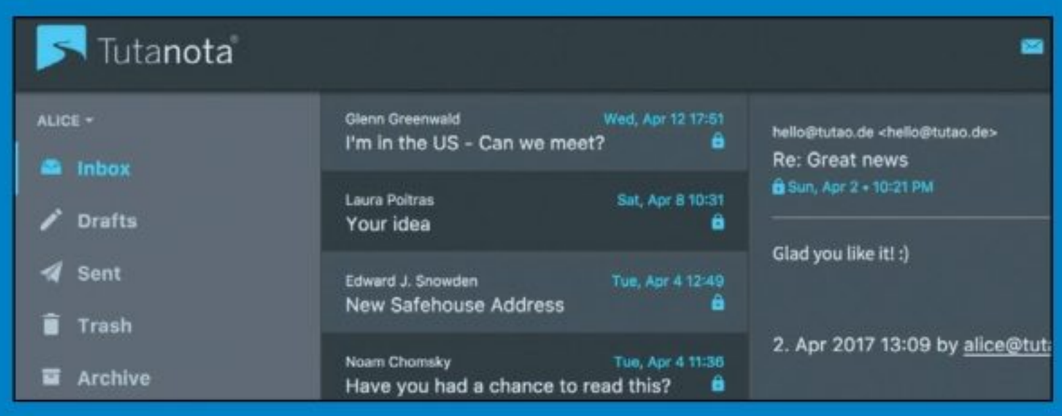
Lien : www.emailprivacytester.com

YOPMAIL > Email jetable !

Parfois, la façon la plus simple de sécuriser sa boîte mail, c'est de ne jamais l'utiliser pour vous inscrire à des services non indispensables ou écrire à des contacts douteux. Avec Yopmail, bénéficiez d'un mail jetable sans divulguer votre véritable adresse. Vous choisissez librement votre adresse (que d'autres peuvent utiliser aussi !).

Lien : www.yopmail.com

TUTANOTA > La référence



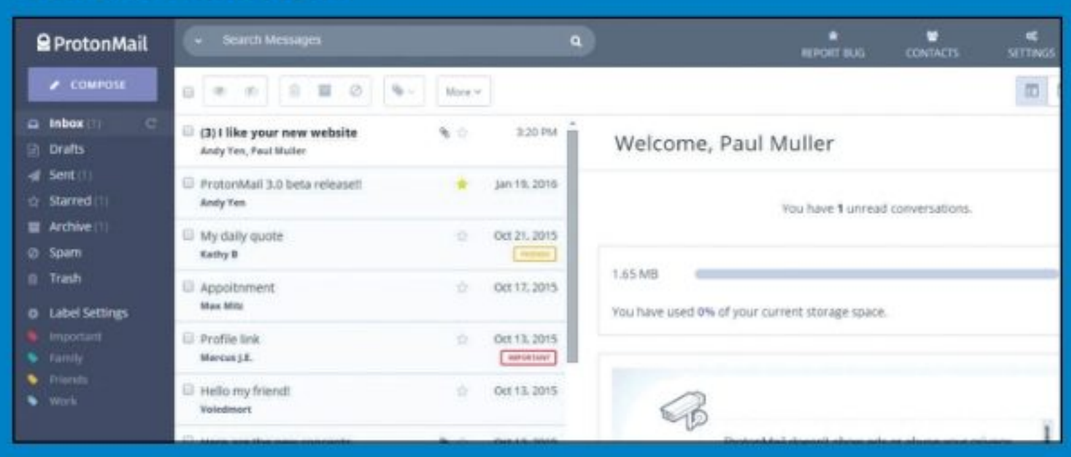
Le mot Tutanota est dérivé du Latin et contient les mots «tuta» (sécurisé) et «nota» (message, note). Voici pour l'étymologie de cette messagerie gratuite et open source développée à Hanovre, en Allemagne. Tutanota est gratuite dans sa version « 1 Go de stockage » pour les particuliers. Avec le chiffrement de bout-en-bout et l'A2F, personne (y compris Tutanota) ne peut déchiffrer ou lire vos données. Des versions mobiles Android et iOS sont bien sûr disponibles.

Lien : tutanota.com

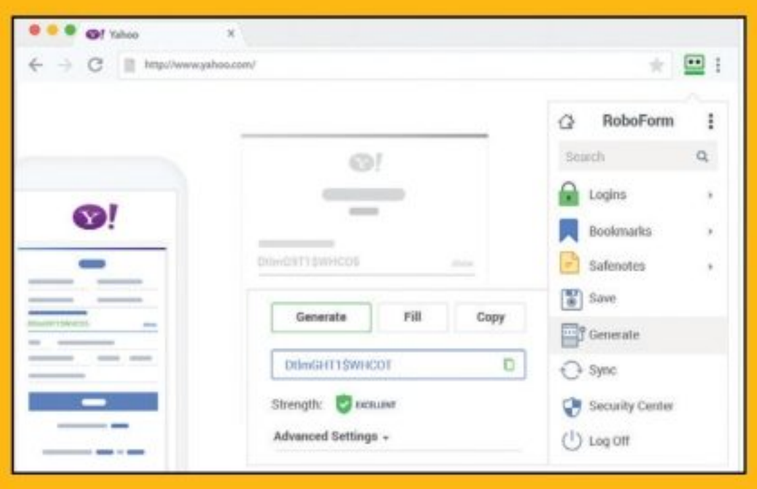
PROTONMAIL > Le plus abouti

Développé par des chercheurs du CERN et du MIT, ProtonMail propose un chiffrement de vos échanges mails de bout-en-bout, sans que personne ne puisse y jeter un œil indiscret. Depuis 2017, ProtonMail dispose de sa version 100 % francophone et de 5 Gb de stockage gratuits. S'ajoutent à cela une ergonomie et des fonctionnalités proches de Gmail, une sécurisation de votre liste de contacts et un data center réputé inviolable sous les montagnes suisses : what else ?

Lien : protonmail.com



ROBOFORM > Les robots sont éternels



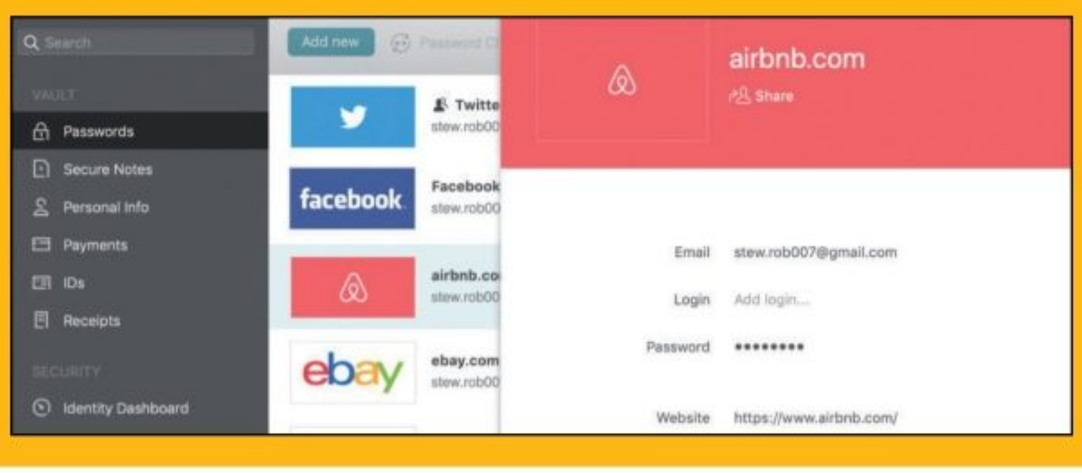
Le plus populaire des gestionnaires dans les années 2000... et toujours l'une des valeurs sûres. Bravo, une telle longévité mérite le respect et est surtout le garant d'une assurance tous risques. Sa version gratuite enregistre, remplit les formulaires, vérifie et génère de nouveaux mots de passe. Simple et efficace.

Lien : www.roboform.com

DASHLANE > La tentation PC

Le très bon et très complet Dashlane (gestionnaire, formulaires, moyens de paiement, notifications, ...) propose ses services gratuitement sur 1 seul poste... ce qui vous poussera peut-être à la version Premium pour vos autres terminaux.

Lien : www.dashlane.com



Casser les codes et décrypter l'info

JE M'ABONNE à PIRATE INFORMATIQUE

LIVRAISON SOUS PLI DISCRET

OFFRE ABONNEMENT

1 AN POUR 17 € (au lieu de ~~19,60 €~~)

2 ANS POUR 29,40 € (au lieu de ~~39,20 €~~)

- LIVRÉ CHEZ VOUS !
- PRATIQUE & ÉCONOMIQUE !

LES GUIDES du HACKER et du PIRATE

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

RÉDUCTION DE -25%

À DÉCOUPER (OU À PHOTOCOPIER), À COMPLÉTER ET À RENVOYER SOUS ENVELOPPE AFFRANCHIE À :
ID PRESSE - IMPASSE DE L'ESPÉRON - VILLA MIRAMAR - 13960 SAUSSET LES PINS

☐ **Abonnement à Pirate Informatique pour 4 numéros, je joins mon règlement de 17,00 €**

☐ **Abonnement à Pirate Informatique pour 8 numéros, je joins mon règlement de 29,40 €**

☐ OUI, JE M'ABONNE :

Nom .....

Prénom .....

Adresse .....

.....

Code Postal .....

Ville .....

E-Mail .....

Signature obligatoire :

☐ Je joins mon règlement par chèque à l'ordre de ID PRESSE (France uniquement)

Offre valable en France métropolitaine uniquement.

POUR NOUS CONTACTER :
abonnement@idpresse.com

Offre valable jusqu'au 31 décembre 2020. Les délais d'acheminement de La Poste varient selon les régions et pays. Conformément à la loi Informatique et Libertés du 6/1/1978, vous disposez d'un droit d'accès et de rectification quant aux informations vous concernant, que vous pouvez exercer librement auprès de ID PRESSE – IMPASSE DE L'ESPÉRON - VILLA MIRAMAR - 13960 SAUSSET LES PINS

LES AVANTAGES :

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

LE MAILING-LIST OFFICIELLE de

Pirate Informatique et des *Dossiers du Pirate*

INSCRIVEZ-VOUS GRATUITEMENT !

De nombreux lecteurs nous demandent chaque jour s'il est possible de s'abonner. La réponse est non et ce n'est malheureusement pas de notre faute. En effet, nos magazines respectent la loi, traitent d'informations liées au monde du hacking au sens premier, celui qui est synonyme d'innovation, de créativité et de liberté. Depuis les débuts de l'ère informatique, les hackers sont en première ligne pour faire avancer notre réflexion, nos standards et nos usages quotidiens.

Mais cela n'a pas empêché notre administration de référence, la «Commission paritaire des publications et agences de presse» (CPPAP) de refuser nos demandes d'inscription sur ses registres. En bref, l'administration considère que ce que nous écrivons n'intéresse personne et ne traite pas de sujets méritant débat et pédagogie auprès du grand public. Entre autres conséquences pour la vie de nos magazines : pas d'abonnements possibles, car nous ne pouvons pas bénéficier des tarifs presse de la Poste. Sans ce tarif spécial, nous serions obligés de faire payer les abonnés plus cher ! Le monde à l'envers...

La seule solution que nous avons trouvée est de proposer à nos lecteurs de s'abonner à une mailing-list pour les prévenir de la sortie de nos publications. Il s'agit juste d'un e-mail envoyé à tous ceux intéressés par nos magazines et qui ne veulent le rater sous aucun prétexte.

Pour en profiter, il suffit de s'abonner directement sur ce site

http://eepurl.com/FlOOD

(le L de «FlOOD» est en minuscule)

ou de scanner ce QR Code avec votre smartphone...

NOUVEAU !

La rédaction se dote d'un compte Twitter !

twitter.com/ben_IDPresse

Vous trouverez des news inédites, des liens exclusifs vers des articles au format PDF et nous vous tiendrons aussi au courant de la sortie des publications. Rejoignez-nous !

TROIS BONNES RAISONS DE S'INSCRIRE :

1. Soyez averti de la sortie de *Pirate Informatique* et des *Dossiers du Pirate* en kiosques. Ne ratez plus un numéro !
2. Vous ne recevrez qu'un seul e-mail par mois pour vous prévenir des dates de parutions et de l'avancement du magazine.
3. Votre adresse e-mail reste confidentielle et vous pouvez vous désabonner très facilement. Notre crédibilité est en jeu.

Votre marchand de journaux n'a pas *Pirate Informatique* ou *Les Dossiers du Pirate* ?

Si votre marchand de journaux n'a pas le magazine en kiosque, il suffit de lui demander (gentiment) de vous commander l'exemplaire auprès de son dépositaire. Pour cela, munissez-vous du numéro de codification L12730 pour *Pirate Informatique* ou L14376 pour *Les Dossiers du Pirate*.

Conformément à la loi «informatique et libertés» du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent.

WI-FI

ESPIONS WINDOWS 10

ANTIVIRUS

SCAN

CLOUD PRIVÉ

RECONNAISSANCE FACIALE

SMARTPHONE

MOTS DE PASSE

SURVEILLER GMAIL

HACKINTOSH

PIRATE

INFORMATIQUE

IDPRESSE

L 12730 - 46 - F: 4,90 € - RD

BEL/LUX : 6 € - DOM : 6,10 € - CH : 8,50 ChF - PORT.CONT. : 6 € - CAN : 7,99 $ cad – POL/S : 750 CFP – NCAL/S : 950 CFP - MAR : 50 mad - TUN : 9,8 tnd