100% PRATIQUE

[STOCKAGE] Sécurisez votre Cloud

[CHIFFREMENT] Dossiers & Fichiers

[ESPIONS] Qui vous surveille ?

LES DOSSIERS DU Pirate

3,50 € seulement

Vivez heureux, Vivez cachés

0% PUBLICITÉ

LE GUIDE ANTI-SURVEILLANCE

VIE PRIVÉE
COMMENT ÉCHAPPER À BIG BROTHER

PC & WEB
LES ALTERNATIVES 100 % FIABLES

EN - DE 5 MN CHRONO !

FACEBOOK, GOOGLE, WINDOWS, ETC.
TOUS LES RÉGLAGES & OUTILS INDISPENSABLES

+ DE 80 TUTOS & ASTUCES

LES OUTILS 100% GRATUITS

LES KITS ANTI-SURVEILLANCE

SMARTPHONE
Verrouillez TOUTES vos DATAS et COMMUNICATIONS

SOMMAIRE

EN PARTENARIAT AVEC LES CAHIERS DU HACKER PIRATE [INFORMATIQUE]

NAVIGATEUR, E-MAIL ET RECHERCHE

RÉSEAUX SOCIAUX

CLOUD

EN LOCAL

LES DOSSIERS DU **Pirate**

N°23 - Avril – Juin 2020

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

Directeur de la publication :
David Côme

Eren : Benoît Bailleul

Livaï : Shen Xue

Mikasa & Armin : Stéphanie Compain & Sergueï Afanasiuk

Correctrice :
Marie-Line Bailleul

Imprimé en France par / Printed in France by :
Imprimerie Mordacq
Rue de Constantinople,
ZI du Petit-Neufpré
62120 Aire-sur-la-Lys
France

Distribution : MLP
Dépôt légal : à parution
Commission paritaire : en cours
ISSN : 2267-6295

«Pirate» est édité par SARL ID Presse, RCS : Aix-en-Provence 491 497 665
Parution : 4 numéros par an.

2€95 seulement

LES GUIDES ESSENTIELS À PRIX MINI

NOUVEAU

Chez votre marchand de journaux

NAVIGATEUR, E-MAIL ET RECHERCHE

GOOGLE : LES PARAMÈTRES DE CONFIDENTIALITÉ

Google tous ses services associés sont pratiques et gratuits, mais vous connaissez la contrepartie : des incursions incessantes dans votre vie privée. Nous verrons plus loin quelles sont les alternatives crédibles à Google, Gmail, YouTube ou Maps, mais pour le moment, concentrons-nous sur ce qu'il est possible de paramétrer dans les méandres des paramètres de confidentialité de Google et de son navigateur Chrome...

Il y a cinq ans, Google vous connaissait déjà mieux que votre mère. Pourquoi pas. Mais depuis quelques mois, votre malaise grandit. Il commence même à deviner ce que vous ne savez pas encore de vous-même et vous révèle/suggère/impose régulièrement des désirs, idées et projets jusqu'alors insoupçonnés. Tiens, même de nouveaux amis.
Il semble vous entendre quand vous chuchotez à voix basse et il se comporte de plus en plus comme un majordome (excellent par ailleurs) directif et intrusif.
Raaâh, et cette manie de ne plus vous lâcher d'une semelle ! Il garde un œil par-dessus votre épaule où que vous soyez. Pas un seul endroit où un appareil connecté ne vous suive. Qui est devenu le maître de qui ?

GOOGLE ENCORE CONDAMNÉ… MAIS PAS PRESSÉ

Droit européen, information de l'utilisateur et transparence : Google traîne les pieds… et se fait condamner en France.

Fin janvier, Google a été condamné à une amende record de 50 millions d'euros suite à la mise en cause, en France, de sa politique de gestion des données personnelles. Cette condamnation intervient après des plaintes collectives déposées devant la CNIL par les associations None of Your Business et La Quadrature du Net.

ÉTIQUETAGE, TRIAGE… ET LIBRE-ARBITRE ?

Une cure sans Google s'impose… ne serait-ce que pour retrouver ce qui vous définit : vous, et vous seul. Parce ce que se retrouver dans la case 87b74dd23 de l'algorithme du géant américain, on n'est pas sûr que ce soit très valorisant comme identité. Surtout quand on s'angoisse à l'idée qu'une fois étiquetée, la gare de triage automatisée ne soit jamais très loin…

TRAITEMENTS MASSIFS ET INTRUSIFS

Malgré la mise en place de la RGPD en Europe, censée protéger les citoyens et leur vie privée sur Internet, la CNIL estime que Google a poursuivi une stratégie ne laissant que trop peu de place au consentement de ses utilisateurs quant à l'utilisation de leurs données personnelles. Les internautes français ne seraient ainsi « pas en mesure de comprendre l'ampleur des traitements mis en place par Google. Or, ces traitements sont particulièrement massifs et intrusifs », estime la CNIL, en référence à la galaxie des services proposés par le groupe : Google Search, YouTube, Google Maps, Play Store, Google Photos… Par défaut, Google impose aussi le partage par lot d'un certain nombre de données, données dont les finalités restent obscures et inintelligibles pour le commun des mortels (voir pour tout le monde).
La CNIL demande plus de transparence et de contrôle pour chacun. Les observateurs estiment qu'il s'agit là d'un premier fil tiré par la commission, mais que cette victoire en appelle d'autres…

GOOGLE NOUS OFFRE À TOUS (ET GRATUITEMENT !) UN MAJORDOME D'EXCEPTION POUR NOUS AIDER AU QUOTIDIEN. UNE RELATION MAÎTRE-ESCLAVE TYPIQUE… C'EST À DIRE AMBIGÜE

Suivez vos activités sur Google

Avant de passer aux réglages, voyons tout ce que Google peut savoir sur vos activités en ligne... Attention ça va vous faire un choc !

INFOS [MON ACTIVITÉ]
Où le trouver ? [https://goo.gl/CaJH5K] Difficulté :

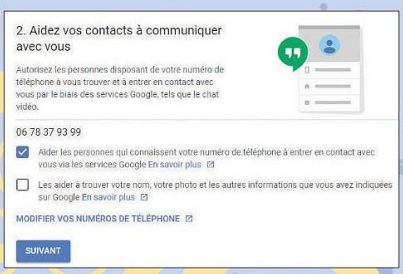
TUTO

01 › TRIER

Suivez notre lien et connectez-vous à votre compte Google. Vous retrouvez tout ce que vous avez fait avec les services de Google, jour après jour. Triez les résultats par groupe (YouTube, images...) ou par élément (pour tout détailler, sans distinction). Optez pour **Vue par groupe** ou **Vue par élément**.

02 › FILTRER LES RÉSULTATS

Pour accéder à l'historique d'un groupe, utilisez les filtres. Cliquez sur le **+** à côté de **Filtrer** par date et produit. Cochez les cases souhaitées puis validez avec la loupe. Pratique si vous avez oublié une recherche que vous avez effectuée.



03 › SUPPRIMER

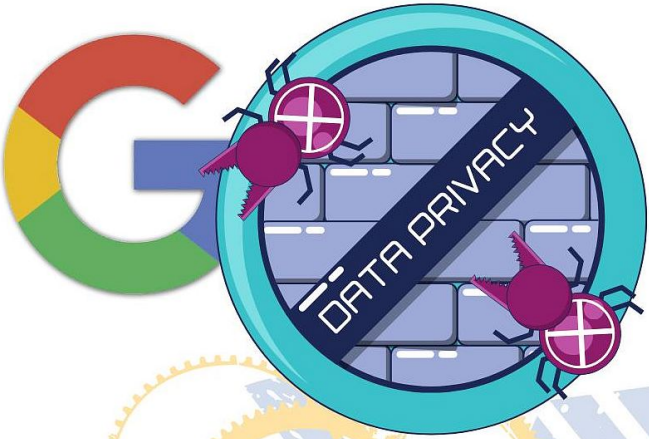
Pour supprimer un élément, cliquez sur les trois traits verticaux puis choisissez **Supprimer**. Pour faire le ménage sur une plage de temps définie, cliquez sur **Supprimer des activités par** et agissez sur les différents champs avant de **Supprimer**.

04 › VÉRIFIER LES HISTORIQUES

En cliquant sur une autre activité Google, vous accédez à d'autres historiques que Google récupère sans forcément vous en demander la permission. Vos trajets, les vidéos regardées sur YouTube, les différents appareils synchronisés avec votre compte. Vous devez accéder à ces historiques pour les effacer.

LIMITEZ LES INTRUSIONS DE GOOGLE DANS VOTRE VIE PRIVÉE

Google c'est bien. Ne le niez pas, leurs nombreux services sont quand même très pratiques. Mais si vous vous souciez aussi de votre vie privée et des données récoltées par leurs soins... Nous allons voir comment concéder le moins d'informations possible au géant américain, tout en continuant à profiter de ses outils.



VOUS ACCORDEZ À GOOGLE UNE LICENCE D'UTILISATION DE TOUTES VOS DONNÉES

- Conditions d'Utilisation Générales de Google -

Vous connaissez la chanson Every Breath You Take de The Police ? Réécoutez là et imaginez que c'est Google qui parle. Vous avez saisi l'idée : à chaque utilisation des services Google, des données plus ou moins personnelles sont enregistrées et envoyées sur leurs serveurs, à des fins commerciales et/ou techniques. Quand on sait que le géant américain est derrière Gmail, YouTube, Drive, Maps, la plupart des publicités ciblées sur Internet, ou encore le navigateur Web Chrome, les occasions de récoltes sont grandes.

QUE PEUT FAIRE GOOGLE AVEC VOS DONNÉES ?

Google avertit les utilisateurs dans ses Conditions Générales d'Utilisation (CGU). Vous savez, ces longues de pages de texte que l'on ne lit jamais même si on coche la case « J'ai lu, et j'accepte les CGU » ? Dans leur dernière version du 14 avril 2014 (à l'heure ou nous écrivons ces lignes), on peut lire : « Lorsque vous importez, soumettez, stockez, envoyez ou recevez des contenus à ou à travers de nos Services, vous accordez à Google (et à toute personne travaillant avec Google) une licence, dans le monde entier, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées (des traductions, des adaptations ou d'autres modifications destinées à améliorer le fonctionnement de vos contenus par le biais de nos Services), de communication, de publication, de représentation publique, d'affichage public ou de distribution publique desdits contenus. Les droits que vous accordez dans le cadre de cette licence sont limités à l'exploitation, la promotion ou à l'amélioration de nos Services, ou au développement de nouveaux Services ».

En clair... Ce n'est pas clair. Ou plutôt volontairement flou. Google peut globalement faire ce qu'il veut de vos données et les litiges se régleront au cas par cas. Pas très rassurant.

JE VEUX QUAND MÊME UTILISER GOOGLE !

Difficile de se passer de son compte Gmail, de Google Maps et de YouTube ! Les alternatives existent, mais elles sont bien souvent moins efficaces que les originaux. Il est heureusement possible de continuer à utiliser Google en limitant au maximum les données qu'il récolte de vous, grâce aux paramètres proposés directement par leurs services. Préparez-vous à dénicher des options parfois bien dissimulées ! Pour commencer, regarder ce que le géant américain sait déjà de vous. Rendez-vous sur www.google.com/dashboard et connectez-vous à votre compte Google. C'est le résumé des données récoltées sur vous jusqu'à présent. Et maintenant que le « Ah oui quand même ! » est passé, voyons comment contrôler tout cela. Oh, une dernière chose : n'oubliez pas de vous déconnecter de votre compte Google quand vous ne vous en servez plus !

ATTENTION AU SMARTPHONE !

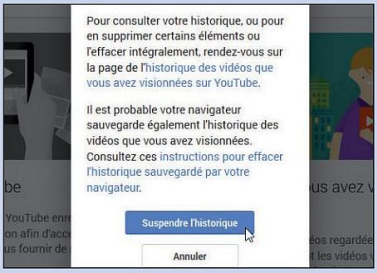
Si vous utilisez aussi les services Google sur votre mobile, il se peut que vous ayez à en régler les paramètres directement dans les applications concernées. Normalement, ce que vous faites sur le PC est appliqué au téléphone, mais n'hésitez pas à vérifier.

CONTRÔLER LES DONNÉES RECUEILLIES PAR GOOGLE

Connectez-vous à votre compte Google, cliquez sur votre portrait puis sur Confidentialité > Consulter les paramètres de compte Google > Historique du compte. Tout part de là sauf indication contraire.

EFFACER ET SUSPENDRE LES HISTORIQUES

Cliquez sur **Gérer l'historique** de chacune des 4 catégories proposées. Effacez tout l'historique puis cliquez sur **Suspendre > Suspendre l'historique**. Google n'enregistrera plus vos recherches, les lieux où vous vous êtes rendu, etc.



ANONYMISER LA RECHERCHE

Une recherche Google est personnalisée, puisqu'elle tient compte des données que la firme possède sur vous. Ce qui explique que parfois, deux personnes n'ont pas les mêmes résultats pour les mêmes mots-clés. Cliquez sur **Modifier les paramètres** en face de **Paramètres de recherche** puis sur **Ne pas utiliser les résultats privés** et **Enregistrer**.

FINI LES PUBS CIBLÉES

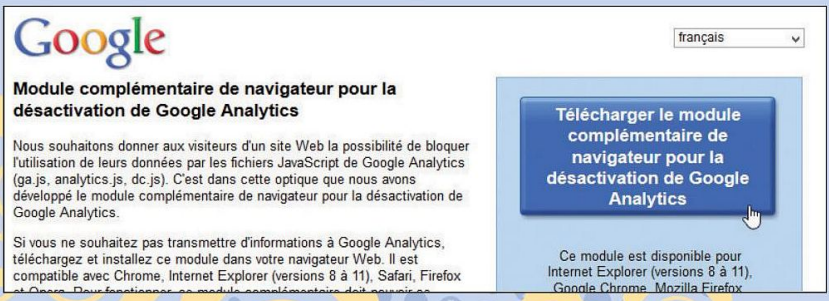
Pour que vos données ne servent plus à afficher des pubs personnalisées, cliquez sur **Modifier les paramètres** en face de **Annonces** puis sur **Désactiver la diffusion d'annonces ciblées par centre d'intérêts sur Google** et **sur le Web**.

LE TRACKER DOUBLECLICK

C'est un cookie publicitaire utilisé par Google. Pour le supprimer définitivement, dans **Modifier les paramètres** (en face de **Annonce**), cliquez en bas de page sur **extension de désactivation DoubleClick** puis sur **Télécharger le plug-in de désactivation du cookie publicitaire**. Suivez la procédure d'installation, fonction de votre navigateur.

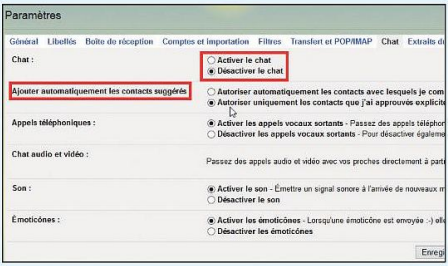
DÉSACTIVER GOOGLE ANALYTICS

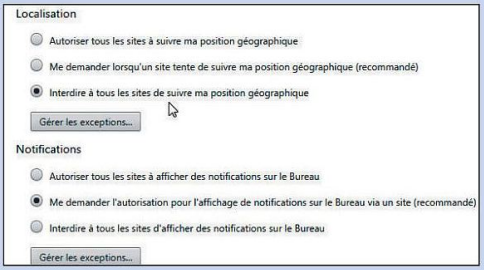
Il s'agit d'un module utilisé par presque 100 % des sites Web et qui enregistre des informations quand vous surfez sur Internet. Allez sur **http://goo.gl/K1u98s** et cliquez sur **Télécharger le module complémentaire de navigateur pour la désactivation de Google Analytics**. Suivez la procédure d'installation, fonction de votre navigateur.



DÉSACTIVER LE CHAT

Par défaut, vos contacts (téléphoniques ou par mail) voient si vous êtes connecté à Gmail. Pour l'empêcher, allez les **Paramètres** de Gmail puis sur **Chat**. Cochez **Désactiver le chat** (radical) ou sur **Autoriser uniquement les contacts que j'ai approuvés à voir si je suis en ligne et à me parler** pour un filtrage ciblé.

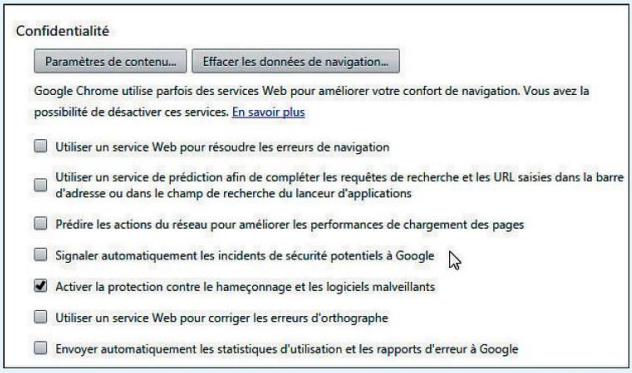




NE PAS ÊTRE LOCALISÉ

Peut-être ne voulez-vous pas que Chrome sache où vous êtes ? Allez dans les **Paramètres du navigateur**, cliquez sur **Afficher les paramètres avancés** puis **Paramètre de contenu**. Sous **Localisation**, cochez **Interdire à tous les sites de suivre ma position géographique**. Validez avec **OK**.

CONTRÔLER CHROME



Pour éviter l'envoi de vos données personnelles à Google, décochez toutes les cases de la partie **Confidentialité** (après avoir affiché les paramètres avancés).

Conserver (quand même) une partie de son historique

Supprimer l'historique est trop radical pour vous et vous appréciez les fonctions comme l'autocomplétion ? Voyons comment effacer les éléments au cas par cas, avec l'option « Gérer l'historique » vue précédemment.

INFOS [MON ACTIVITÉ]
Où le trouver ? [https://goo.gl/CaJH5K] Difficulté :

TUTO

01 › RECHERCHES QUE VOUS AVEZ EFFECTUÉES

Ici s'affiche tout ce que vous avez tapé dans la barre de recherches Google. Notez que vous pouvez filtrer par catégories à gauche, et voir des graphiques sur vos habitudes. Pour effacer tout ou partie de l'historique, cochez les cases de votre choix (où celle à gauche de **Supprimer des éléments** pour tout sélectionner). Cliquez ensuite sur **Supprimer des éléments**.

02 › LIEUX OÙ VOUS VOUS ÊTES RENDU

Moins pratique, vous pouvez soit effacer l'historique de vos positions jour par jour (**Supprimer l'historique de ce jour**), en les sélectionnant dans le calendrier, soit **Supprimer tout l'historique**. Pas beaucoup de latitude donc. Si jamais vous ne trouvez pas certaines positions, cliquez sur **Afficher tous les points**, à gauche de la page.

03 › VOS RECHERCHES YOUTUBE

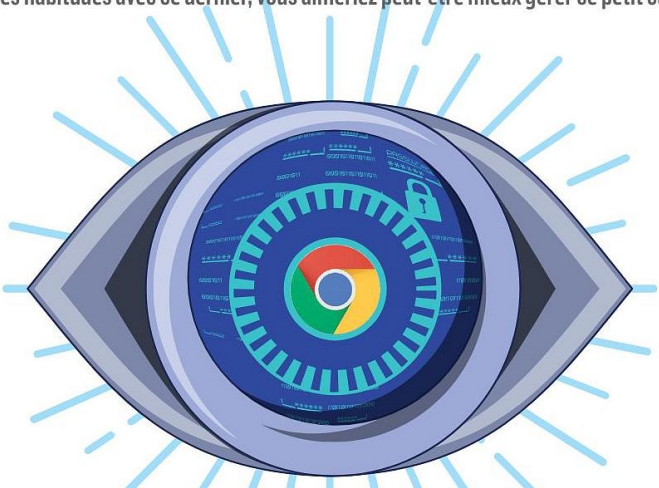
Comme pour les recherches Google, vous pouvez cocher des cases et **Supprimer les entrées**, ou bien **Effacer tout l'historique des recherches**. Cliquez sur **Vidéos que vous avez aimées**, à gauche, pour faire de même avec ces dernières.

04 › VIDÉOS QUE VOUS AVEZ VISIONNÉES SUR YOUTUBE

Même principe, il s'agit là de toutes les vidéos que vous avez regardées sur YouTube (aussi bien sur le service Web que sur l'application mobile d'ailleurs, comme pour les trois étapes précédentes). En plus de **Supprimer** ou d'**Effacer tout l'historique**, vous pouvez en profiter pour **Ajouter à** une playlist quelques-unes des vidéos affichées.

CHROME : UN NAVIGATEUR CURIEUX...

Chrome n'est pas notre navigateur préféré, car il est bien plus intrusif que ses petits camarades. Il est bien sûr mis en avant sur les appareils mobiles et sur PC et si vous avez vos petites habitudes avec ce dernier, vous aimeriez peut-être mieux gérer ce petit curieux...



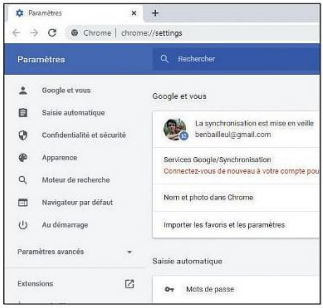
Google Chrome est peut-être un navigateur efficace et personnalisable, mais il est aussi très curieux. C'est d'ailleurs ce que beaucoup d'utilisateurs lui reprochent, Google étant réputé pour récupérer pas mal de données des utilisateurs qui utilisent ses services. Mais saviez-vous qu'il était possible de le configurer pour le rendre un peu moins curieux ? Car oui, dans les réglages du navigateur, il existe plusieurs options qui en font un logiciel bien plus respectueux de la vie privée des utilisateurs. Nous allons justement vous expliquer comment configurer Google Chrome pour mieux protéger votre vie privée.

INFOS [GOOGLE CHROME]
Où le trouver ? [https://tinyurl.com/qltd7th] Difficulté :

TUTO

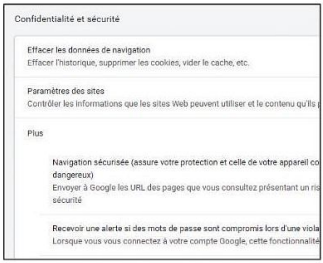
01 › DÉSACTIVER LA SYNCHRONISATION DES DONNÉES

Google Chrome propose une synchronisation de certaines données pour que vous puissiez les retrouver sur d'autres appareils, simplement en vous identifiant avec votre compte Google : historique, identifiants, mots de passe...Pour éviter cela, il vous suffit d'aller faire un tour dans les paramètres du navigateur et de désactiver la partie **Google et vous**. Il faut évidemment être identifié pour que cette option apparaisse dans le menu. Si malgré tout, vous voulez tout de même utiliser le service de synchronisation des données du navigateur, descendez dans le menu suivant et vous verrez une partie appelée **Options de chiffrement**.



02 › DÉSACTIVER LES SERVICES D'AIDE DE GOOGLE

Dans les options, allez dans les paramètres avancés. Vous constaterez que plusieurs options sont activées par défaut pour aider l'utilisateur comme par exemple **Navigation sécurisée (assure votre protection et celle de votre appareil contre les sites dangereux)**. Pour effectuer cela, Google doit récupérer des informations sur votre ordinateur, mais aussi sur les sites que vous visitez. Pour protéger votre vie privée, il est conseillé de décocher cette option au détriment de la sécurité.

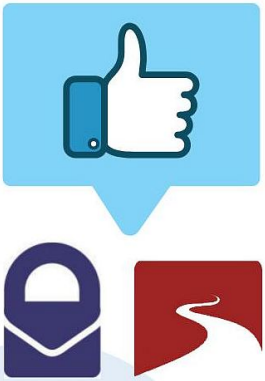


03 › DÉSACTIVER L'ENREGISTREMENT DES DONNÉES RELATIVES À L'ACTIVITÉ

Vous ne le savez peut-être pas, mais Google enregistre des données à propos de vous dès que vous lancez votre navigateur, mais aussi sur mobile lorsque vous utilisez certaines applications tierces : la raison ? Une option appelée **Commandes relatives à l'activité**. Elle permet de retracer toutes vos activités et d'aider Google à vous envoyer les informations dont vous avez besoin à un moment donné, en fonction de votre localisation par exemple. Pour accéder au menu permettant d'activer ou de désactiver cette fonction, il suffit de cliquer sur ce lien : **https://tinyurl.com/ycfpjvvs**.

PROTONMAIL VS TUTANOTA

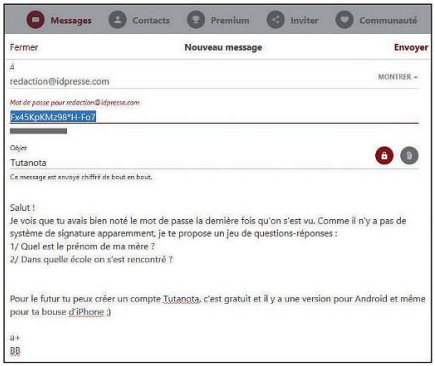
QUI EST LA MEILLEURE MESSAGERIE SÉCURISÉE ?



Vous angoissez quand vous réalisez que Google peut accéder à l'intégralité de vos conversations mails ? Vous avez des sueurs froides quand vous réalisez que la firme de Mountain View sait quasiment tout de vous, et qu'elle peut revendre (elle l'a déjà fait) ses informations au plus offrant ? Commencez à protéger votre vie privée en optant pour une messagerie sécurisée.

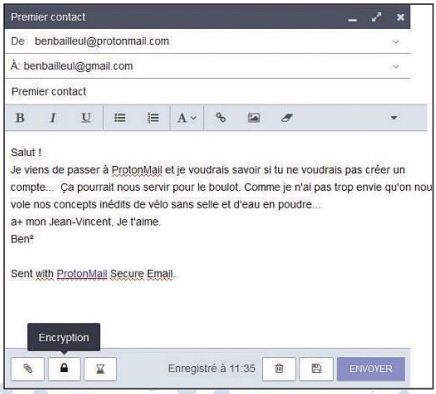
Dites au revoir à Gmail, Hotmail, Yahoo et les autres boites de mail des géants du Net. Dites bonjour plutôt à Protonmail et Tutanota. Ces services de messageries cryptées sont totalement gratuits (des formules payantes existent) et ils luttent tous deux pour protéger les libertés individuelles du web.

ProtonMail est le fruit du travail d'ingénieurs en informatique, d'experts en cryptographie, de développeurs web et mobile, de docteurs en physique, de scientifiques soucieux de la protection de la vie privée. Les trois membres fondateurs sont issus du CERN, la prestigieuse organisation de recherche nucléaire située à Genève. Leur siège se situe d'ailleurs dans la capitale helvétique. Pourquoi la Suisse ? La nation des banques et du fromage offre aujourd'hui l'une des meilleures défenses des données personnelles et de la vie privée au monde, notamment grâce à la Loi fédérale pour la Protection des données (LPD). Pour résumer, ProtonMail propose un système de chiffrement de bout en bout, en local, c'est-à-dire depuis votre navigateur. NSA, hackers, belle-mère, personne ne peut récupérer votre clé privée en ligne, personne ne peut vous espionner.



Tout comme ProtonMail, Tutanota permet d'envoyer des messages chiffrés à des gens qui n'utilisent pas le service. Le système fonctionne avec une interface Web sécurisée très ingénieuse...

Tutanota, c'est l'autre Webmail crypté de référence. Installées en Allemagne à Hanovre, les équipes de Tutanota se voient comme des combattants de la liberté, et œuvrent pour protéger les journalistes, les lanceurs d'alertes, les activistes des droits de l'Homme. En bref, ils n'aiment pas trop la surveillance de masse. Les développeurs de Tutanota ont choisi l'Allemagne pour ses lois strictes et le RGPD, qui garantit là encore l'une des meilleures lois pour protéger votre droit à la vie privée. Tout comme ProtonMail, Tutanota propose lui aussi un chiffrement de bout en bout en local, et prône l'open source. C'est-à-dire que les experts de sécurité peuvent vérifier le code qui protège vos e-mails. De fait, l'application Android n'est pas soumise à Google, et aux fuites et brèches de sécurité potentielles...



L'un et l'autre sont très agréables à l'œil et toutes les fonctionnalités d'un Webmail classique sont de la partie...

PROTONMAIL ET TUTONATA : CE QUE PROPOSENT LES FORMULES GRATUITES

Les deux Webmails ont le mérite de proposer tous deux des formules entièrement gratuites, amplement suffisantes pour une utilisation personnelle. À noter que Tutanota et ProtonMail sont disponibles également en version mobile, sur Android et iOS. Voici un petit tableau récapitulatif de leurs offres respectives :

LES VERSIONS PAYANTES

Quid des versions payantes ? De son côté ProtonMail propose trois formules à 48, 79 et 228€ par an avec plusieurs options et fonctionnalités : entre 1 à 6 utilisateurs autorisés, entre 5 et 20 Go de stockage, de 5 à 50 adresses mail différentes, nom de domaine personnalisé, nombre de messages illimité, et support technique prioritaire. Tutanota ne propose lui que deux offres payantes : premium à 12€ par an et Pro à 60€ par an. Ici aussi, ces versions apportent leur lot d'actions supplémentaires : espace de stockage entre 1 et 10 Go, ajout entre un et deux utilisateurs, domaines personnalisés, possibilité de créer des alias (entre 5 et 20), réglages de la boîte de réception, logo et couleurs interchangeables, et le support par mail est prioritaire.

Comme vous pouvez le voir, les offres ne diffèrent pas énormément et sauront toutes les deux vous satisfaire. À la rédaction, notre cœur balance tout de même pour ProtonMail. Le service suisse inclut en exclusivité un délai d'expiration pour vos mails. Comme pour Snapchat, il est possible de choisir une durée de vie pour vos messages, une très bonne idée. Comme Tutanota, ProtonMail chiffre également vos conversations avec des personnes qui n'utilisent pas le service. Pour ce faire, les deux Webmails utilisent un système d'invitation unique, avec mot de passe. Créez le code d'accès, transmettez-le à votre destinataire et hop, vos mails seront sécurisés. Concernant cette fonctionnalité, ProtonMail possède un léger avantage : la possibilité de créer un indice pour retrouver le mot de passe, en cas d'oubli. Tutanota propose quant à lui une recherche dans les mails chiffrés ce qui s'avère très pratique.

	ProtonMail	Tutanota
Nombre d'utilisateurs	1	1
Capacité de stockage	500 Mo	1 Go
Nombre d'adresses autorisées	1	1
Messages par jour	150	Illimité
Support technique	Limité	Non

Le client desktop de Tutanota

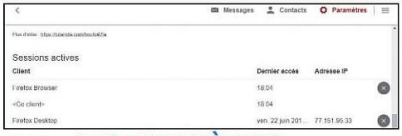
Si vous n'aimez pas trop les interfaces Web, Tutanota propose un logiciel « en dur » pour se connecter à son compte...

INFOS [TUTANOTA]

Où le trouver ? [https://tutanota.com/blog/posts/desktop-clients]

Difficulté : ☠☠☠

TUTO



01 › L'INSTALLATION

Disponible pour les PC sous Windows, Linux, mais aussi sous MacOS, le client est disponible en utilisant notre lien. Si vous avez un compte, vous n'avez qu'à entrer vos identifiants, mais si ce n'est pas le cas vous pouvez vous inscrire depuis le logiciel. Après avoir rentré votre code de vérification, votre navigateur va alors générer votre couple de clés. Tapez une nouvelle fois votre mot de passe pour être dirigé vers l'interface principale.

02 › LES PARAMÈTRES

Comme sur le webmail classique, vous aurez une boîte de réception, d'envoi, un filtre à spam, une liste de contacts et la possibilité d'attacher une pièce jointe. Il est aussi possible depuis **Paramètres** (menu aux trois barres horizontales en haut à droite) de changer de mot de passe, vérifier les heures des précédentes connexions et les tentatives ratées d'accéder à votre boîte (pratique pour savoir si un tiers à tenter de vous pirater).

03 › VOTRE E-MAIL : CHIFFRÉ OU PAS !

En bas à droite, cliquez sur le stylo puis écrivez votre message. De base, il sera chiffré pour les utilisateurs de Tutanota, mais si le service détecte que votre correspondant n'utilise pas Tutanota, il vous demandera alors un mot de passe pour que votre ami puisse lire votre message. Votre correspondant recevra un e-mail avec un lien. Il faudra qu'il clique dessus puis qu'il rentre le mot de passe que vous lui aurez communiqué. Il peut mettre en mémoire ce dernier s'il se connecte d'un ordinateur privé. Il pourra même vous répondre depuis son navigateur. Le même mot de passe sera utilisé pour ce correspondant donc pas besoin d'échanger 50 sésames différents. Mais si vous désirez envoyer un message «normal» c'est aussi possible : il suffit de cliquer sur le cadenas pour supprimer le chiffrement. Notez que les pièces jointes sont aussi chiffrées.

04 › SUR MOBILE AUSSI

Et sur mobile Android ou iOS ? C'est pareil ! Si vous avez beaucoup d'e-mails, la recherche à l'intérieur des messages chiffrés peut prendre un peu plus de temps, mais toutes les fonctionnalités sont là !

TUTANOTA ET PROTONMAIL BLOQUÉ : HALTE À LA SURVEILLANCE !

Tutanota est dorénavant bloqué en Fédération de Russie depuis le 14 février 2020 au soir. Il s'agit d'une volonté délibérée puisque cela fait suite au blocage d'autres services de messagerie chiffrés dans ce pays comme ProtonMail peu de temps auparavant. Ce blocage a été vérifié par l'explorateur OONI, un outil utilisé pour démontrer la censure en ligne. Rappelons que Tutanota propose un canal de communication sécurisé et confidentiel aux citoyens, mais aussi aux journalistes et aux militants. Et bien sûr, les communications chiffrées sont une épine dans le pied des gouvernements autoritaires comme la Russie qui peut alors difficilement surveiller ses citoyens. Notons que Tutanota est aussi bloqué en Égypte depuis octobre 2019. Il par contre possible d'accéder au service en utilisant un VPN ou le navigateur Tor.

ProtonMail en mode « invité »

Si vos amis n'ont pas de compte ProtonMail, il est quand même possible de s'envoyer des e-mails chiffrés...

INFOS [PROTONMAIL]
Où le trouver ? [https://protonmail.com] Difficulté :

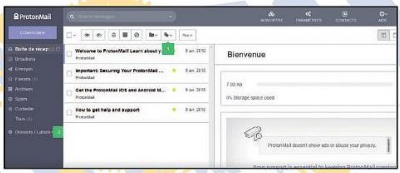
TUTO

01 › L'INSCRIPTION

Sur le site, allez dans **S'inscrire**, optez pour le compte gratuit et choisissez vos identifiants. Il est possible de paramétrer un compte de récupération. Inutile de préciser que ce dernier devra être bien sécurisé avec un mot de passe solide. Libre à vous de télécharger l'appli pour téléphone portable à la fin du processus.

02 › L'INTERFACE

Votre boîte aux lettres devrait comporter 4 e-mails pour vous expliquer le fonctionnement, mais ils sont en anglais. À l'inverse, le tuto dans le bandeau en bas est en français, comme toute l'interface d'ailleurs. Faites **Composer** pour écrire votre premier e-mail.

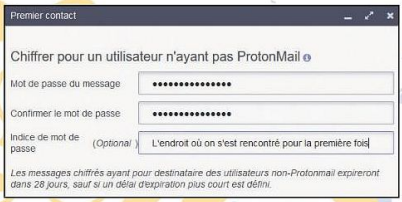


03 › LES 3 BOUTONS

En bas à gauche, vous pourrez trouver des boutons pour ajouter une pièce jointe (qui sera aussi chiffrée) ou mettre un délai d'expiration (en semaines, jours ou heures). Notez que si vous décidez de chiffrer un e-mail pour un utilisateur n'ayant pas ProtonMail, le délai de rétention sera de 28 jours par défaut sauf si vous décidez de mettre un délai plus court.

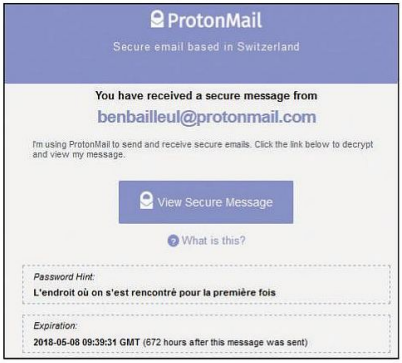
04 › LE MODE « INVITÉ »

Pour un ami qui a un compte ProtonMail, rien ne vous sera demandé, mais si ce dernier ne l'a pas, vous pouvez soit l'envoyer sans chiffrement soit utiliser l'option **Encryption** avec le cadenas. Définissez un mot de passe et éventuellement un indice pour votre ami « *L'endroit où on s'est rencontré pour la première fois* » ou « *Le nom de ton roman préféré* ». Évitez « *La couleur de ta voiture* » ou « *Le nom de ton chien* », trop facile à deviner ou trouver sur le Net (merci Facebook). Vous pouvez aussi ne donner aucun indice et communiquer ce sésame avec une méthode secondaire : de vive voix, depuis Signal ou Telegram.



05 › LA RÉCEPTION

Sur sa boîte non sécurisée, votre ami recevra un e-mail (malheureusement en anglais) pour lui expliquer que vous essayez de le joindre sur un canal sécurisé. Il lui suffira de cliquer sur le lien **View Secure Message** et de rentrer le mot de passe qu'il aura deviné grâce à l'indice. Il peut y répondre et échanger librement ou s'inscrire et lui aussi opter pour ProtonMail.



06 › SUR MOBILE

Sur smartphone c'est la même chose. L'appli est très bien conçue, mais si votre correspondant n'a pas ProtonMail, il sera dirigé vers son navigateur pour répondre… comme sur PC. En ayant testé les deux solutions (ProtonMail et Tutanota), nous ne saurons en conseiller une plus que l'autre. Pour être franc, c'est le nombre d'amis qui ont opté pour l'un ou l'autre service qui fera pencher la balance.

L'INFORMATIQUE FACILE
POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

MARRE DE GOOGLE ?

CHANGEZ !

Vous étiez un utilisateur des produits Google mais plus ça va et plus vous désirez vous en éloigner. Malgré les réglages censés préserver votre vie privée, vous ne souhaitez plus utiliser la Galaxie Google ? Dans les pages suivantes nous allons nous intéresser aux alternatives crédibles : moteur de recherche, navigateur, mais aussi toute la gamme de services annexes de Google.

QWANT, UNE VRAIE ALTERNATIVE À GOOGLE...

Il ne se passe pas une semaine sans qu'une start-up ne se lance dans un combat perdu d'avance contre des géants du Web. Le français Qwant ne cherche pas à contrer Google, mais à proposer une alternative au moteur de recherche numéro 1. Pour cela, il mise sur une interface innovante et met l'accent sur le respect de la vie privée...

Qwant ne se place pas comme un concurrent de Google, mais plutôt comme une alternative. Les incursions du moteur dans votre ordinateur se limitent à un cookie de session permettant de retrouver vos préférences de navigation lors de la prochaine connexion. Qwant ne mémorise pas vos recherches, ne fouille pas votre historique et ne vous propose pas des liens sponsorisés ou des liens commerciaux à chaque recherche. Le moteur vit grâce aux produits que vous achetez par son biais, mais il ne vous bombardera pas de liens pourris à chaque utilisation. Contrairement à Google, si Qwant pense que les résultats sont peu pertinents, il ne les affichera pas. Vous mettez souvent le nez dans la page n°2 de Google vous ? Nous non plus... Qu'il s'agisse de requêtes simples (PSG), maladroites (*«Comment ouvrir un script sous Linux»*) ou avec des inclusions/exclusions (*+foire +Rouen -vin*), le moteur répond sans problème et pendant notre phase de test nous n'avons jamais été tentés de revenir vers Google...

FAITES VOUS AUSSI L'ESSAI DE QWANT SUR LE LONG TERME. VOUS OUBLIEREZ GOOGLE TRÈS RAPIDEMENT...

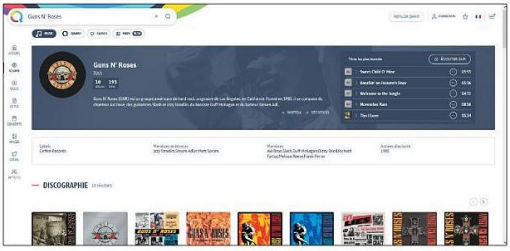
L'interface de Qwant

INFOS [QWANT]
Où le trouver ? [www.qwant.com] Difficulté :

TUTO

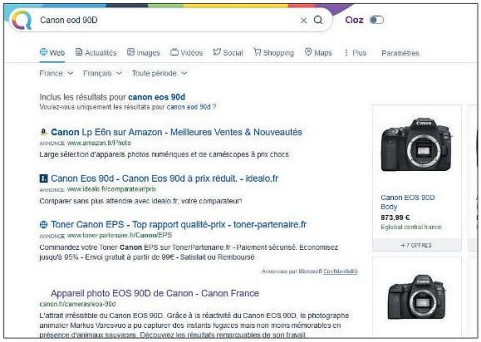
01 › COMME GOOGLE MAIS MOINS CURIEUX...

Rien de sorcier concernant la recherche. Il est intéressant de noter qu'en fonction de ce que vous cherchez, Qwant va afficher des informations différentes. Pour un groupe de musique, vous verrez leur discographie, la possibilité d'écouter des chansons, les différents événements (concert, etc.), des images ou leur réseau sociaux.



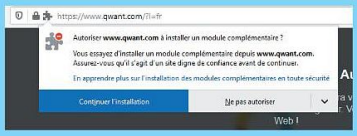
02 › DES ANNONCES COMMERCIALES QUI PAYENT LES FACTURES

Au lieu de vendre vos données ou de vous en servir contre vous, Qwant va vous proposer des annonces commerciales lorsque c'est le bienvenu. En cherchant le nom d'un appareil photo, vous trouverez donc les informations utiles (Wikipedia, vidéos, actus,), mais aussi des magasins en ligne qui vendent le produit. Qwant prendra une commission au passage. Il est même possible d'ajouter des annonces commerciales avec le programme Qoz (le bouton en haut), ce dernier va verser de l'argent à l'association de votre choix.



QWANT, SUR TOUS VOS APPAREILS !

Il est possible d'opter pour Qwant sur mobile (Android/iOS) mais aussi d'en faire facilement son moteur de recherche par défaut. Pour cela, il faut aller tout en bas et cliquer sur Faire de Qwant mon moteur par défaut. Selon votre navigateur, vous devrez alors suivre les instructions pour que l'extension s'installe...
Il est bien sûr possible de se créer un compte pour synchroniser vos activités...



DUCK DUCK GO : CONTRE LES RECHERCHES CIBLÉES

Saviez-vous qu'en utilisant le même mot clé sur Google, un de vos amis ne trouvera pas les mêmes résultats que vous ? La faute à Google qui traque vos recherches pour vous ranger dans des «cases» : homme, femme, UMP, coco, fan de sport ou de poker, etc. ne vous faites plus ficher et utilisez Duck Duck Go !

Duck Duck Go est un moteur de recherche basé en Pennsylvanie et qui a pour philosophie de préserver la vie privée et de ne stocker aucune information personnelle concernant les utilisateurs. Pas de cookies intrusifs, d'adresse IP ou autres informations concernant la localisation, le navigateur et la configuration de l'Internaute. Pour démontrer la nécessité d'un tel service,

l'équipe de Duck Duck Go a mené une sorte d'expérience sur Google et ses résultats en fonction de différents critères. Sans être connecté à leur compte Google (qui s'active automatiquement lorsqu'on se connecte à Gmail ou à un autre service Google), plus de 130 internautes américains ont réalisé les mêmes recherches sur certains mots clés.

LA RECHERCHE CIBLÉE, MÊME SI VOUS NE VOULEZ PAS

La conclusion de ces recherches montre que les utilisateurs n'ont jamais les mêmes résultats. Certains vont avoir des publicités ciblées en fonction de leur emplacement géographique ou de leurs précédentes recherches. Prenons l'exemple de deux internautes qui auraient tapé «gun control» («contrôle des armes», un sujet brûlant concernant le second amendement des USA) sur Google. Le premier ayant fait des recherches sur le site de la NRA (la National Rifle Association, le lobby en faveur de la détention d'arme à feu) n'aura pas les mêmes résultats que l'autre, qui n'a pas d'avis sur la question ou surfera sur des sites anti second amendement. Même en désactivant l'historique de navigation (voir notre tutoriel) ou avec la navigation privée, Google tiendra compte tout de même de votre localisation. Bien sûr, il n'est pas question de pointer Google du doigt puisque les résultats pourront être les mêmes avec Yahoo!, Bing ou n'importe quel autre moteur de recherches. C'est, en fait, la fin des résultats standards et l'avènement des résultats ciblés pour tout le monde.

MARTINE A DE L'HERPÈS

Et cela pose plusieurs problèmes. Prenons un exemple qui figure sur le site Duck Duck Go. Imaginons une femme qui tape «herpès» dans Google et clique sur un des liens. Sa recherche sera envoyée avec son IP et d'autres informations de localisation à différents sites : autres moteurs et pourvoyeur de publicité ciblée. Martine Dubois (alias 168.152.41.25) voit donc ses prochaines recherches sur Google et d'autres moteurs se transformer en un cruel rappel de son petit problème de santé. Imaginez qu'elle fasse une recherche de chez elle avec une amie ou sa famille. La personne verra des publicités pour des crèmes, des pilules et autres remèdes avec des noms qui en diront long sur Martine. Les informations sur Martine peuvent aussi être vendues à des tiers. Aux USA, on pourra, par exemple, vous refuser une assurance santé si l'on sait que vous avez des problèmes de ce type. Plus fort, certains sites de réservation d'hôtel proposent des prix supérieurs aux utilisateurs de Mac, réputés plus riches que les utilisateurs de PC... L'autre problème réside dans la création d'une «bulle» autour de l'internaute. À force d'avoir des résultats qui abondent dans votre sens sur des sujets de société ou de politique, vous ne risquez pas d'être confronté à d'autres avis, d'autres personnes, d'autres idées.

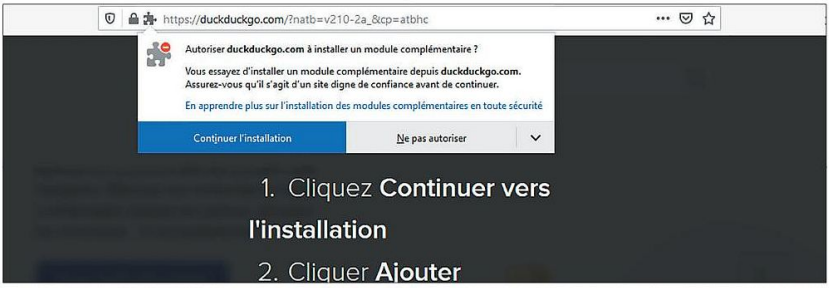
DUCK DUCK GO EST UNE BONNE ALTERNATIVE À GOOGLE, MAIS AUSSI À QWANT...

Faites l'essai !

INFOS [DUCK DUCK GO]
Où le trouver ? [http://duckduckgo.com] Difficulté :
TUTO

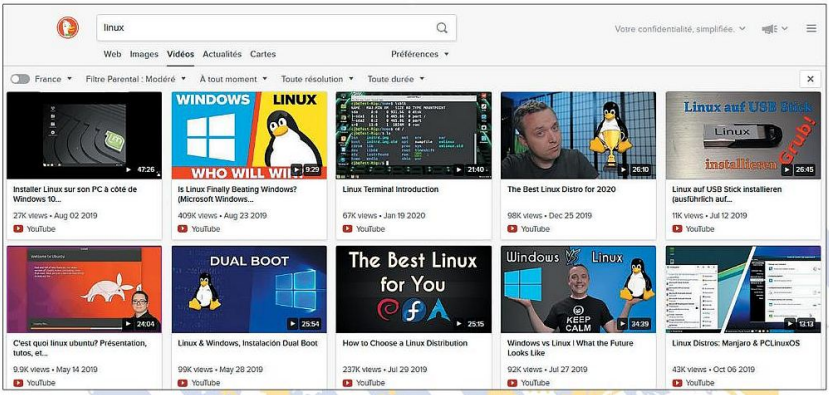
01› AJOUTER DUCK DUCK GO À VOTRE NAVIGATEUR

Pour être sûr de toujours faire vos recherches avec Duck Duck Go, vous pouvez installer le plugin pour Firefox ou pour Chrome. Vous aurez alors la possibilité de faire vos recherches directement depuis votre logiciel proféré.



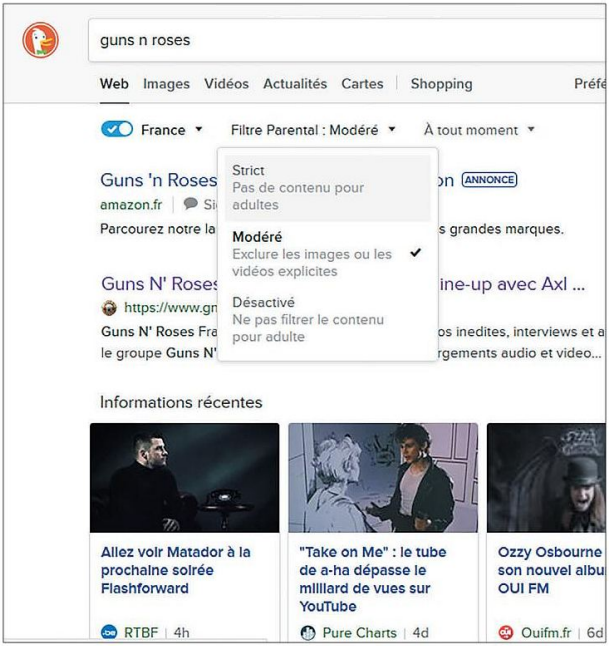
02› ACTUALITÉS, IMAGES, VIDÉO, ETC.

Comme Google, Duck Duck Go propose différents champs de recherche. Il suffit de chercher dans les différents onglets. Dans les préférences, vous pourrez paramétrer le moteur à votre convenance. Tout est en français.



03 › LE FILTRE PARENTAL

Duck Duck Go propose aussi un filtre parental réglable directement sur la page de recherche. Dans les Préférences, on trouvera aussi une partie confidentialité. On pourra aussi synchroniser ses données dans un cloud protégé par mot de passe.



SEARX, LE MÉTAMOTEUR OPEN SOURCE

Searx est un métamoteur de recherche open source qui rassemble les résultats d'autres moteurs de recherche tout en respectant la confidentialité des utilisateurs. Searx est personnalisable en indiquant les sources de recherche que vous préférez et vous pourrez affiner les résultats via différentes catégories. La force de SearX, c'est la possibilité d'affiner les résultats par catégorie, date et langue de recherche ainsi que via les « Préférences » qui vous permettent de choisir les sources de recherche à privilégier ou à bannir.

Lien : **searx.me**

TROIS NAVIGATEURS QUI RESPECTENT VOTRE VIE PRIVÉE

En 2019, le navigateur le plus utilisé est Chrome : C'est aussi le champion toute catégorie puisqu'en cumulant les versions PC, Android et iPhone, le navigateur de Google équipe 60 % des internautes dans le monde. Sur mobile comme sur ordinateur, les outsiders se partagent les miettes, mais vous n'êtes pas obligé de faire comme tout le monde et opter pour un navigateur qui respecte votre vie privée...

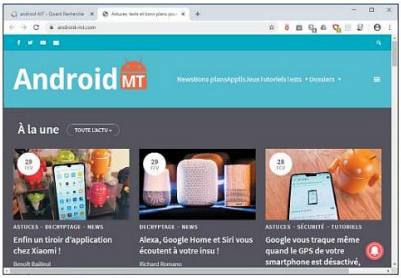
CHROMIUM, LE MÉCONNU

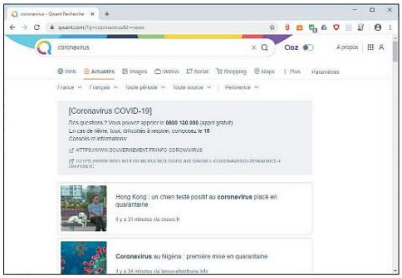
Chromium est un navigateur open source qui a été initié par Google. Pourtant, il est préféré par les utilisateurs pour son côté « pur » : pas de fonctionnalités de pistage ajouté dans ce logiciel. Google Chrome n'est qu'un Chromium à qui on a ajouté quelques options supplémentaires : intégration de Flash Player, d'un lecteur PDF, d'un système pour prévisualiser les impressions, un module de mise à jour automatique et d'autres choses très superflues. Si vous aimez Chrome, mais que vous n'en pouvez plus des incursions de Google, Chromium est fait pour vous. Ce navigateur libre qui sert de base à plusieurs autres navigateurs, dont certains open sources comme Iridium13 ou d'autres propriétaires comme Vivaldi Browser et même le Edge de Microsoft ! Cerise sur la gâteau, les extensions de Chrome fonctionnent aussi avec Chromium la plupart du temps. Attention, il ne faut pas confondre Chromium avec Chromium OS qui est quant à lui un système d'exploitation complet et cousin de Chrome OS...

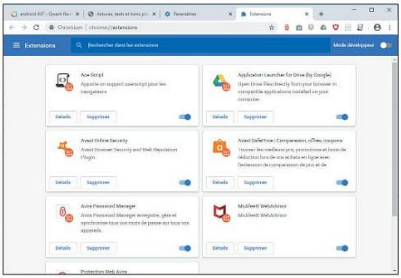
INFOS [CHROMIUM]

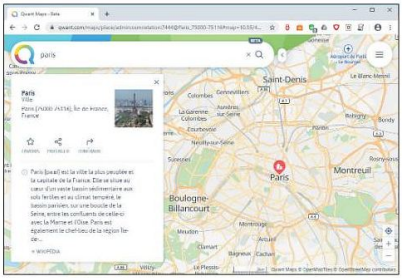
Où le trouver ? [www.chromium.org] Difficulté :

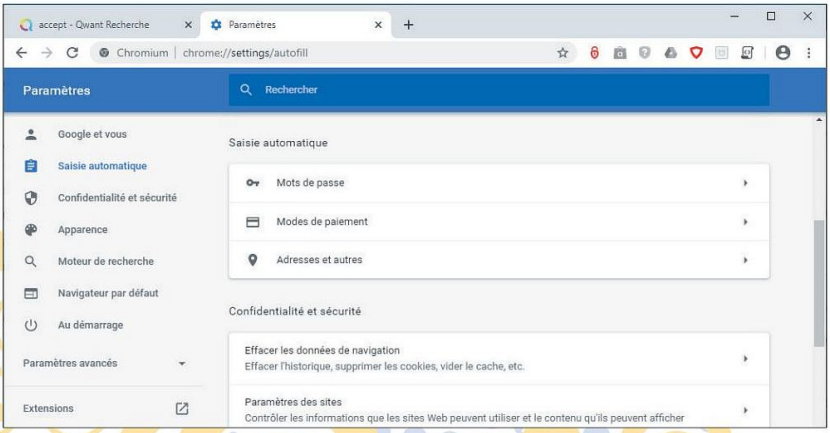
TUTO











PASSEZ À FIREFOX !

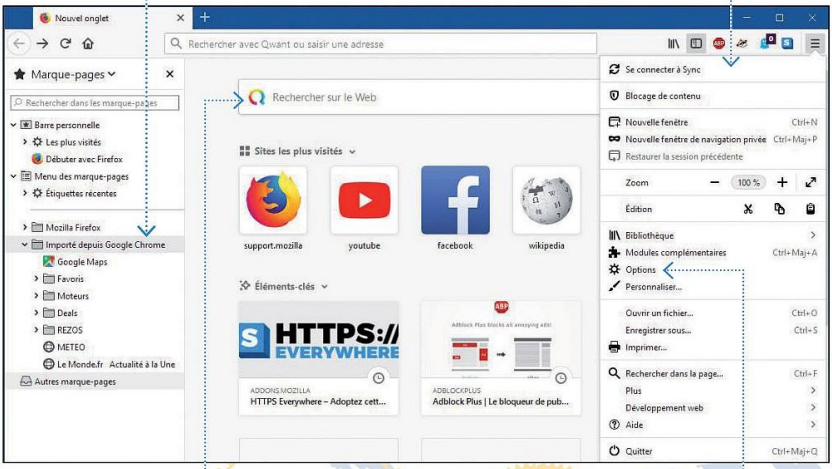
Google ne cesse d'être critiqué pour son manque de respect de la vie privée, mais une majorité d'internautes continue d'utiliser son navigateur, Chrome, pour accéder à Internet. Il existe pourtant un logiciel aussi performant et beaucoup plus discret : Firefox. Voici comment l'installer et le sécuriser au maximum.

Transition

Pour une transition en douceur, importez vos favoris et mots de passe depuis votre ancien navigateur.

Extensions

Installez des modules complémentaires pour blinder Firefox contre la publicité ou les traqueurs.



Moteur de recherche

Adoptez un moteur par défaut respectueux de votre vie privée, et basculez à volonté d'un moteur à l'autre.

Options

Réglez Firefox pour une discrétion maximale, contre les sites qui pillent vos données ou les amis indiscrets.

Bien démarrer avec Firefox

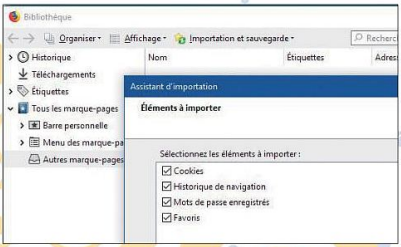
INFOS [FIREFOX]
Où le trouver ? [https://www.mozilla.org/fr/firefox] Difficulté :
TUTO

01› TÉLÉCHARGER ET INSTALLER

Allez sur le site de Mozilla, cliquez sur **Télécharger Firefox** pour récupérer le module d'installation du logiciel, puis lancez ce dernier. L'installation effectuée, Firefox est lancé. Dans la fenêtre qui s'affiche alors, cliquez sur **Faire de Firefox mon navigateur par défaut** si vous êtes décidé à franchir le pas, sur **Plus tard** si vous voulez essayer d'abord.

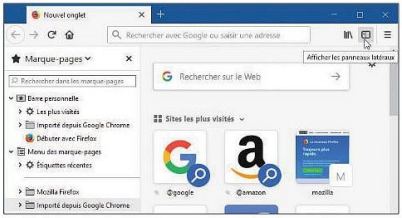
02› RÉCUPÉRER SES DONNÉES

Pour récupérer vos favoris, mots de passe et historique de navigation, tapez le raccourci clavier **Ctrl + Maj + B**. Dans la fenêtre qui s'ouvre alors, faites **Importation et sauvegarde > Importer des données d'un autre navigateur**. Sélectionnez votre précédent navigateur (fermez-le s'il est ouvert), et cliquez sur **Suivant**, à deux reprises, puis sur **Terminer**.



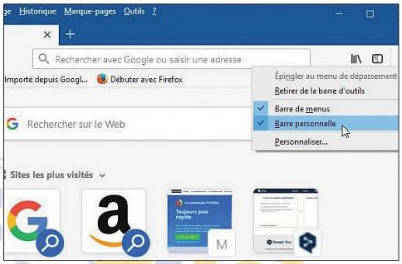
03› ACCÉDER AUX MARQUE-PAGES

Sous Firefox, les favoris s'appellent marque-pages. Pour y accéder, cliquez sur l'icône **Afficher les panneaux latéraux**, en haut à droite (ou tapez le raccourci **Ctrl + B**). Vous retrouvez les favoris récupérés à l'étape précédente dans un dossier nommé **Importé depuis...**, sous **Barre personnelle** et/ou **Menu des marque-pages**.



04› EXPLORER L'INTERFACE

Faites un clic droit sur une zone vierge de la barre d'outils. **Barre personnelle** affiche une barre de marque-pages immédiatement accessibles, sous la barre d'outils. **Personnaliser** sert à personnaliser cette dernière. **Barre de menus** affiche une série de menus en haut de la fenêtre, alternative au menu principal situé en haut à droite (les 3 traits).



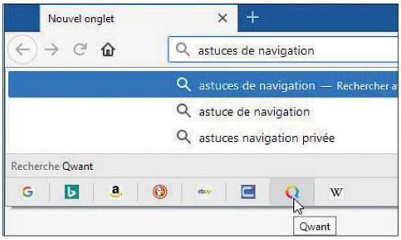
Adopter un moteur de recherche respectueux de la vie privée

INFOS [FIREFOX]
Où le trouver ? [https://www.mozilla.org/fr/firefox] Difficulté :

TUTO

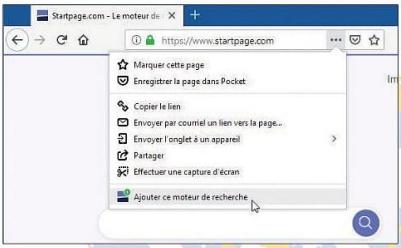
01 › BASCULER D'UN MOTEUR À L'AUTRE

Tapez les termes de votre recherche dans la barre d'adresse de Firefox. Si vous validez, c'est le moteur de recherche par défaut, qui sera utilisé (au départ, Google). Mais vous pouvez en choisir un autre, comme Qwant ou DuckDuckGo, en cliquant sur l'icône correspondante, sous la liste de suggestions.



02 › AJOUTER UN MOTEUR

Vous pouvez enrichir la liste de moteurs proposés par Firefox. Pour cela allez sur la page du moteur que vous souhaitez incorporer, **www.startpage.com** dans notre exemple. Puis cliquez sur les 3 points, à droite dans la barre d'adresses et choisissez **Ajouter ce moteur de recherche**.

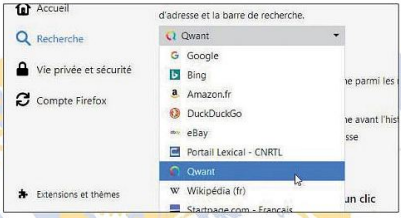


03 › PASSER PAR LES OPTIONS

Autre solution pour ajouter un moteur, allez dans les **Options** de Firefox (via le menu principal, en haut à droite), à la rubrique **Recherche**. Allez en bas de la page, et cliquez sur le lien **Découvrir d'autres moteurs de recherche**. Des centaines d'outils de recherche, généralistes ou spécialisés, vous sont alors proposés.

04 › CHANGER LE MOTEUR PAR DÉFAUT

Pour changer le moteur de recherche par défaut, c'est encore dans la rubrique **Recherche** des **Options** que cela se passe. Faites votre choix dans la liste déroulante de la section **Moteur de recherche par défaut**. Nous vous conseillons d'en choisir un autre que Google – que vous pourrez toujours consulter ponctuellement (étape 1).



Naviguer en mode privé

INFOS [FIREFOX]
Où le trouver ? [https://www.mozilla.org/fr/firefox] Difficulté :

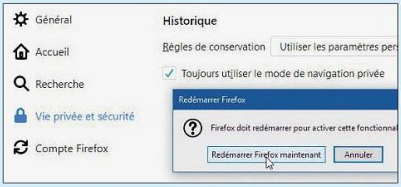
TUTO

01 PASSER EN NAVIGATION PRIVÉE

Si vous avez épinglé l'icône de Firefox, dans le menu Démarrer ou dans la barre des tâches, vous pouvez démarrer directement en mode navigation privée, via un clic droit sur l'icône puis **Nouvelle fenêtre privée**. Si Firefox est déjà ouvert, passez par le menu (en haut à droite) pour choisir **Nouvelle fenêtre de navigation privée**.

02 ACTIVER LE MODE PRIVÉ PAR DÉFAUT

Dans le menu de Firefox choisissez **Options**, puis affichez la rubrique **Vie privée et sécurité** (à gauche). Faites défiler la page jusqu'à la section **Historique**, choisissez **Utiliser les paramètres personnalisés** dans la liste déroulante, et cochez **Toujours utiliser le mode de navigation privée**. Cliquez sur **Redémarrer Firefox** : désormais, le navigateur fonctionne en mode privé.



Effacer automatiquement ses traces

INFOS [FIREFOX]
Où le trouver ? [https://www.mozilla.org/fr/firefox] Difficulté :

TUTO

01 EFFACER L'HISTORIQUE

Dans **Options > Vie privée et sécurité > Historique**, choisissez les paramètres personnalisés, comme à l'étape 2 ci-dessus, mais ne cochez pas le mode de navigation privée. Cochez en revanche **Vider l'historique lors de la fermeture**. Vous conserverez l'historique en cours de session, ainsi que la possibilité d'enregistrer des mots de passe.

02 EFFACER LES COOKIES

Toujours dans la rubrique **Vie privée et sécurité**, à la section **Cookies et données de sites**, cochez **Supprimer les cookies et les données des sites à la fermeture de Firefox**. Avec ces réglages, l'historique de navigation et les cookies déposés par les sites sur votre ordinateur sont effacés lorsque vous quitter Firefox.

5 compléments pour blinder Firefox

Bloquer la pub → Avec Adblock Plus

Outre son caractère agaçant, la publicité est une source avérée d'indiscrétion : la régie publicitaire qui vous envoie une bannière de pub a évidemment connaissance de votre adresse IP (l'identifiant de votre PC sur Internet), et du site que vous êtes en train de visiter. La parade, c'est un bloqueur de publicité. Le plus utilisé aujourd'hui est Adblock Plus, qui remplit parfaitement sa fonction.

Lien : **https://adblockplus.org**

Arrêter les traqueurs → Avec Ghostery

Sur le Web, vous êtes pisté par des petits programmes, les traqueurs, qui enregistrent les pages que vous visitez, les données ainsi collectées servant à alimenter votre profil de consommateur à des fins publicitaires. Ghostery bloque ces indiscrets. Notez que Firefox dispose en standard de fonctions de lutte contre les traqueurs (astuce « Renforcer la protection contre le pistage », pages suivantes). Rien ne vous empêche de les activer, Ghostery intervenant alors en complément.

Lien : **www.ghostery.com/fr**

Sécuriser les connexions → Avec HTTPS Everywhere

De nombreux sites Web offrent au choix une connexion standard (préfixe « http » dans la barre d'adresses), où les données sont transmises en clair, ou une connexion sécurisée (préfixe « https »), où les données sont chiffrées de façon à être illisibles si elles sont interceptées par un tiers. L'extension HTTPS Everywhere active automatiquement le chiffrement lorsqu'il est disponible.

Lien : **www.eff.org/fr/https-everywhere**

Stopper les espions → Avec Privacy Badger

Proposée par la célèbre Electronic Frontier Foundation (également éditrice de HTTPS Everywhere), l'extension anti-espions Privacy Badger viendra utilement renforcer la protection apportée par Ghostery et la fonction anti-traqueur de Firefox. Pourquoi plusieurs modules différents pour la même tâche ? Parce qu'en matière de lutte contre les malwares et l'espionnage, aucune protection n'est efficace à 100%. Multiplier les barrières est une bonne précaution.

Lien : **www.eff.org**

Piéger les keyloggers → Avec KeyScrambler

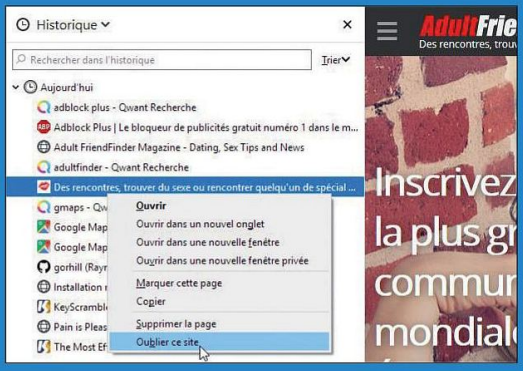
Les keyloggers sont des programmes espions qui enregistrent toutes les frappes effectuées au clavier. Et que tape-t-on dans un navigateur ? Mots de passe, coordonnées bancaires, adresse mail... Ces malwares sont normalement arrêtés par votre antivirus, mais deux précautions valent mieux qu'une : KeyScrambler chiffre ce que vous tapez pour tout rendre inexploitable en cas d'espionnage.

www.qfxsoftware.com

7 astuces indispensables pour rendre Firefox plus discret et plus sûr

Nettoyer l'historique

Vous désirez non pas supprimer totalement l'historique (astuce « Effacer toutes ses traces »), mais en effacer seulement certains sites ? Ouvrez le panneau latéral de Firefox, via l'icône en haut à droite ou le raccourci **Ctrl+B**, et sélectionnez **Historique** dans la liste déroulante, en haut. Parcourez la liste, ou tapez le nom du site dans le champ de recherche. Puis faites un clic droit sur une ligne à effacer et **Supprimer la page** pour effacer seulement cette ligne, ou **Oublier le site** pour effacer toutes les occurrences du site.



Gérer les permissions

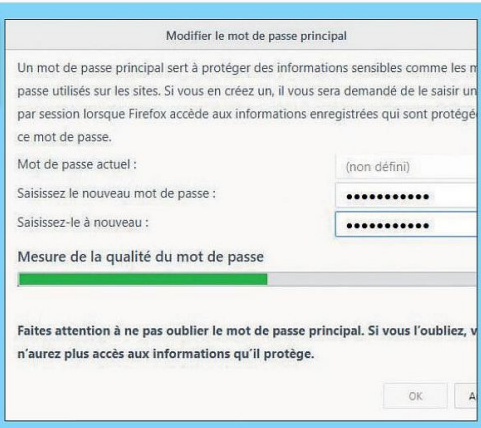
Les sites Web que vous visitez peuvent avoir accès à votre position, activer votre webcam ou exploiter votre microphone. Autant de sources d'indiscrétion ! Pour accorder des permissions au cas par cas ou bloquer systématiquement l'accès à ces éléments, cliquez sur le « **i** » à gauche de la barre d'adresse, puis sur la roue dentée de la section **Permissions**, en bas. Cliquez sur le bouton **Paramètres** associé à chaque ressource pour gérer leur exploitation.

Vérifier les options de sécurité

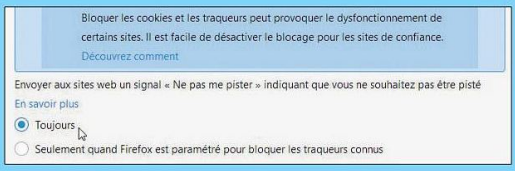
Firefox intègre des protections contre les sites ou logiciels malveillants, ainsi que les téléchargements jugés dangereux. Activées par défaut, ces protections peuvent être levées ponctuellement, dans les options du logiciel, rubrique **Vie privée et sécurité**, section **Sécurité**, si par exemple vous êtes certains qu'un site bloqué est inoffensif. À vos risques et périls. En temps normal, veillez à ce que toutes les cases restent cochées.

Protéger ses mots de passe

Les mots de passe que vous enregistrez dans votre navigateur sont accessibles à tous ceux qui ont accès à votre ordinateur, collègues ou membres de votre famille. Pour protéger vos sésames, allez dans les **Options** de Firefox, à la rubrique **Vie privée et sécurité**. Descendez jusqu'à la section **Identifiants et mots de passe**, et cochez **Utiliser un mot de passe principal**. Ce mot de passe vous sera demandé avant toute utilisation des identifiants enregistrés (une seule fois par session).



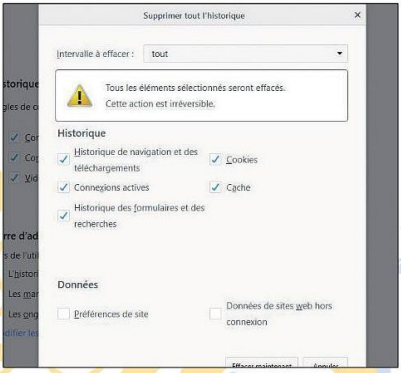
Demander aux sites de ne pas vous pister



Mesure moins radicale que le blocage des traqueurs (astuce « Renforcer la protection contre le pistage » ou extensions Ghostery et Privacy badger, page 28), vous pouvez simplement demander aux sites que vous visitez de ne pas vous pister. Pour cela, à la rubrique **Vie privée et sécurité** des options de Firefox, section **Blocage de contenu**, choisissez **Toujours** au paragraphe **Envoyer aux sites web un signal « Ne pas me pister »**. Mais ils ne sont pas obligés d'obtempérer…

Effacer toutes ses traces

Si vous mettez en place les options de confidentialité évoquées page 27, votre ordinateur conservera peu ou pas de traces de vos navigations. Pour effacer celles qui restent (ou qui ont pu être enregistrées avant), allez dans les **Options** de Firefox, rubrique **Vie privée et sécurité**, section **Historique**. Cliquez sur le bouton **Effacer l'historique**, sélectionnez **Tout** dans la liste Intervalle à effacer, cochez **toutes les cases de la partie Historique**, et faites **Effacer maintenant**.



Renforcer la protection contre les traqueurs

Par défaut, Firefox bloque les traqueurs uniquement en navigation privée. Pour les bloquer aussi en mode de navigation standard, choisissez **Blocage de contenu** dans le menu de Firefox, et cochez l'option **Strict**. Certains traqueurs passent tout de même, pour assurer le bon fonctionnement de certains sites. Pour un blocage plus sévère, cochez **Personnalisé**, cliquez sur **Changer de liste de blocage** et choisissez **Protection stricte**.

ESSAYEZ UN NAVIGATEUR RAPIDE ET DISCRET

Brave est un navigateur Web qui érige en principe de base la protection de la vie privée. Autre atout de taille : il est presque deux fois plus rapide que Chrome ! Essayez-le.

Développé à partir de Chromium, la base open source de Chrome, Brave mise sur la protection des données et de la vie privée de ses utilisateurs pour trouver son public. Pour cela, différents moyens sont utilisés : le blocage des pisteurs des sites Web visités, le blocage des publicités, l'accès automatique aux pages sécurisées lorsqu'il y en a (un préfixe https s'affiche devant l'adresse, au lieu de http), etc. Il est possible de personnaliser les paramètres, pour adapter ces blocages en fonction des sites que vous consultez.

NE PLUS SUBIR LA PUB

Les développeurs de Brave estiment que votre temps et votre attention ont de la valeur. Ils ont mis en place un système de récompense : vous pouvez gagner des BAT (Basic Attention Token) en acceptant de regarder de la pub, et les utiliser ensuite pour soutenir des projets de votre choix. Vous n'êtes ainsi plus passif devant la publicité, mais acteur de ce mode économique. Vous pouvez cependant désactiver cette option si elle ne vous intéresse pas.

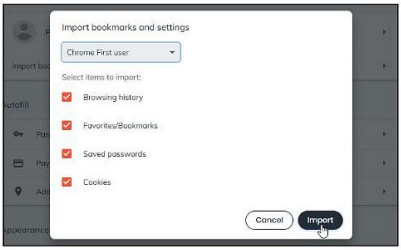
RAPIDE ET RESPECTUEUX DE LA VIE PRIVÉE, BRAVE MÉRITERAIT PLUS DE RECONNAISSANCE...

Naviguer avec Brave

INFOS [BRAVE]
Où le trouver ? [https://brave.com] Difficulté :
TUTO

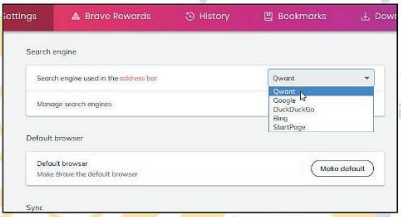
01 › IMPORTER FAVORIS ET PARAMÈTRES

Après avoir téléchargé et installé Brave, le navigateur s'ouvre automatiquement, et vous propose un tutoriel. Cliquez sur **Let's go** pour commencer. Pour importer vos favoris et vos paramètres, cliquez sur **Import**, choisissez votre navigateur précédent dans la liste déroulante, cochez les éléments à importer, puis cliquez sur **Import**. Fermez l'onglet **Settings** pour revenir au tutoriel.



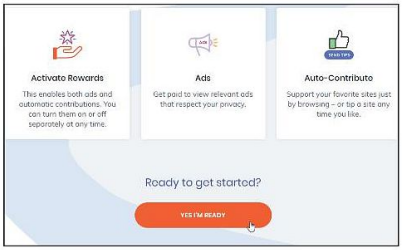
02 › RÉGLER LE NAVIGATEUR

L'étape suivante vous permet de choisir votre moteur de recherche par défaut, à sélectionner dans la liste déroulante. Vous pouvez également choisir d'utiliser Brave comme navigateur par défaut, en cliquant sur **Make default**. Fermez l'onglet **Settings** pour l'étape suivante : le choix du thème couleur (**Choose your theme**, sélectionnez votre préférence dans la liste déroulante).



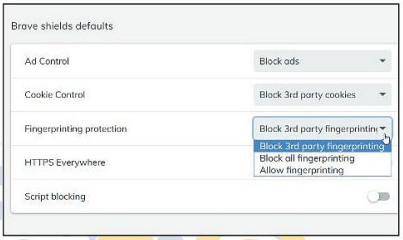
03 › ACTIVER LES RÉCOMPENSES

Un message vous informe que les blocages (**Shields**) sont paramétrables, cliquez sur **Next**. L'étape suivante concerne les récompenses. Pour en savoir plus, cliquez sur **Enable Rewards**. La page qui s'affiche explique le fonctionnement de ce système de récompenses. Pour l'activer, cliquez sur **YES I'M READY**. Pour le laisser inactif, fermez l'onglet **Rewards**, et dans le tutoriel cliquez sur **Done**.



04 › GÉRER LES BLOCAGES

Le tutoriel ne permet pas de modifier directement les blocages. Pour cela, retournez dans **Settings**. Dans la partie **Brave shields defaults**, vous pouvez choisir de débloquer certains éléments (les publicités, les cookies...), en cliquant sur la petite flèche à droite de chaque élément pour afficher la liste déroulante.



NOTRE COMPILATION DE SERVICES COMPLÉMENTAIRES

Google ne propose pas qu'un moteur de recherche et un navigateur. On compte pas mal de services annexes. Pour éviter de revenir vers Google à la moindre occasion, voici notre sélection...

2 DRIVES ALTERNATIFS

1# SYNC

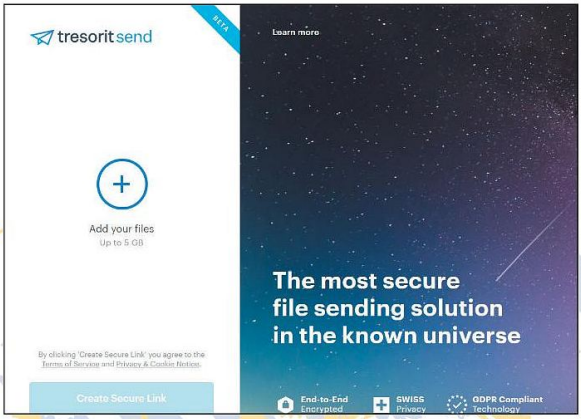
Encrypté de bout en bout, 5 Gb dans sa version gratuite. Partage et accès même sans compte Sync pour les invités : c'est simple et complet !

Lien : **www.sync.com**

2# TRESORIT

Tout pareil que Sync avec ses 5 Gb offerts et son encryption. Mais, par contre, pas de gestion collaborative, le service est principalement destiné à l'échange sécurisé de gros fichiers.

Lien : **send.tresorit.com**

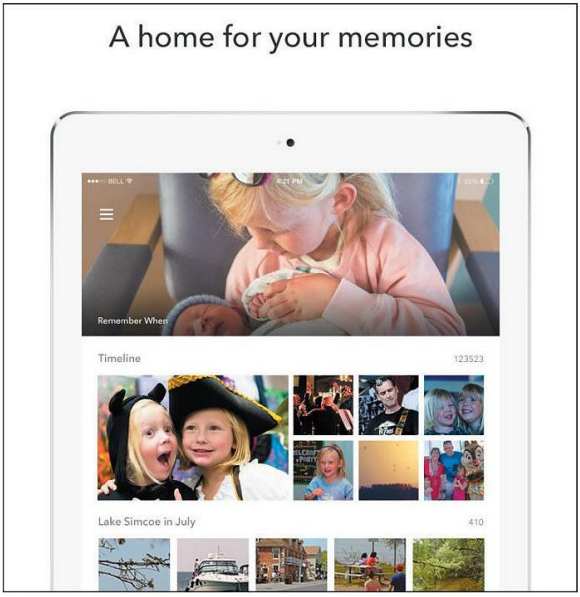


2 GOOGLE PHOTOS ALTERNATIFS

1# SHOEBOX

Même dans version gratuite, Shoebox vous offre un stockage illimité pour vos photos... et le tout sécurisé par une bonne dose d'encryption. Accédez à vos clichés sur tous les supports puisque Shoebox est compatible Windows, Mac, iOS etAndroid.

Lien : **shoeboxapp.com**



2# PIWIGO

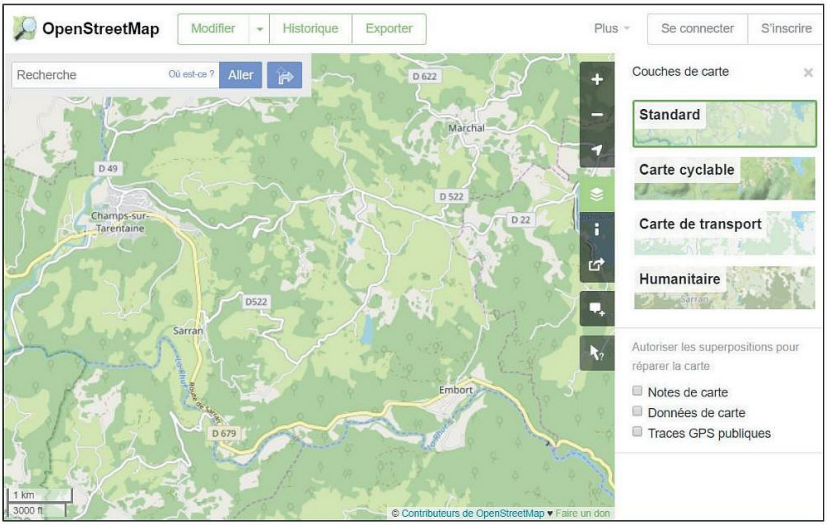
Sans pub et open source, Piwigo présente l'avantage de proposer une version en français. Cet excellent gestionnaire de photothèque ne gère par contre pas le stockage (il vous faut un hébergement ailleurs) dans sa version gratuite pour particuliers.

Lien : **fr.piwigo.com**

2 MAPS ALTERNATIVES

1# OPENSTREETMAP

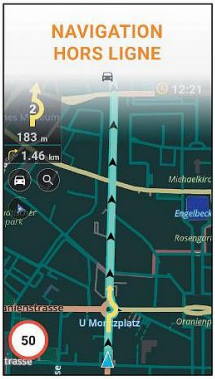
OpenStreetMap est un service de cartographie gratuit et open source, ce qui signifie que de nombreux développeurs se le sont approprié pour proposer leur propre outil personnalisé, pour plusieurs plateformes (PC, Mac, Android, iOS notamment) et en ajoutant des fonctionnalités bienvenues. La base OpenStreetMap a cependant été conçue pour un environnement Windows/PC. Mais vous trouverez des variantes mobile comme l'application OsmAnd (Android et iOS).

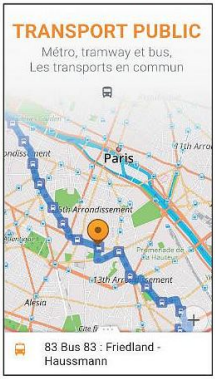


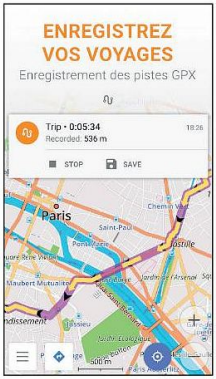
PAS DE COMPTE, PAS DE PUB

Le gros plus de OpenStreetMap et de ses déclinaisons, contrairement à Google Maps, c'est de pouvoir utiliser le services sans compte associé, c'est à dire en évitant le tracking centralisé même si la localisation GPS est bien sûr un impondérable la plupart du temps. La désactivation du GPS est cependant très simple et vos informations de localisations peuvent être maintenues complètement privées.

Lien : **www.openstreetmap.org**



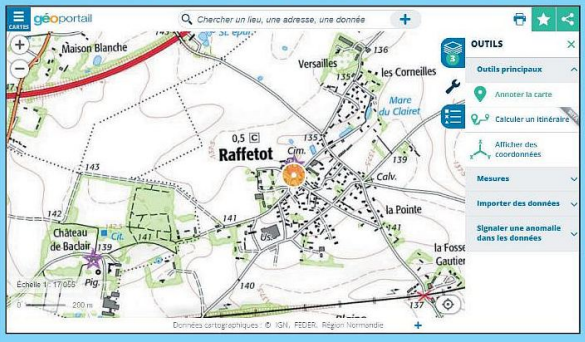




OpenStreetMap est une base libre et opensource dont de nombreux développeurs se sont emparés pour proposer des services de cartographie multiplateforme, incluant bien sûr iOS et Android

2# GÉOPORTAIL

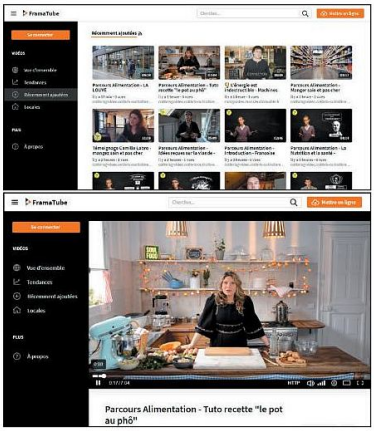
Alors les petits gars, cela vous ébouriffe le poil que nous vous proposions un service gouvernemental parmi notre sélection. Passez un peu d'huile de coco sur votre pelage velu et tout se passera bien. Géoportail est un excellent service qui exploite les données cartographiques publiques (IGN et BRGM) sur le territoire français. Pas de connexion obligatoire, pas de conservation de vos données privées, pas de publicité et une précision meilleure que Google Maps pour la France rurale. Le service public, ça a du bon, préservons-le et soutenons-le. Des applications mobiles (iOS et Android) complètent la version desktop. Cartographies 2D et 3D, cadastres, chemins de traverse, topographie, lieux-dits improbables, itinéraires bien sûr : l'essentiel et même plus est sur Géoportail. Le seul bémol, vous l'aurez sans doute compris, c'est que vous êtes limités au territoire français pour accéder à l'ensemble de ces fonctions.



Lien : **www.geoportail.gouv.fr**

2 ALTERNATIVES À YOUTUBE

1# FRAMATUBE



Framatube, plateforme développée par Framasoft, héberge des milliers de vidéos et refuse tout tracking de ses utilisateurs. Ici, pas d'hébergement centralisé, ce sont les utilisateurs qui forment un réseau de type P2P pour mutualiser bande passante et espace de stockage grâce à leur propre PC ou serveur. Une économie de coût qui permet de se passer de publicité (mais pas de dons) et qui rompt avec la culture centralisée et propriétaire de YouTube. L'interface est une réussite et votre vie privée est garantie par Framasoft, l'un des piliers les plus anciens du logiciel libre en France. Même l'outil de mise en ligne obéit à cette logique et Framatube ne restreint pas le type de contenus publiés (contrairement à YouTube encore) tant que la loi est respectée.

Lien : **framatube.org**

2# HOOKTUBE

On ne va pas se mentir, l'hégémonie de YouTube signifie aussi que, côté contenus, il est impossible de trouver plus fourni et diversifié (même si certaines vidéos sont bannies selon le type de contenu ou la zone géographique de consultation). Difficile de s'en passer donc. Plutôt que de créer une concurrence illusoire, HookTube a eu une idée simple et géniale : pouvoir consulter n'importe quelle vidéo de YouTube… mais en bloquant toutes les pubs, requêtes de tracking et enregistrements de données de la plateforme américaine ! Pour ce faire, il vous suffit de remplacer la racine YouTube de n'importe quel lien par « hooktube.com ». Exemple :

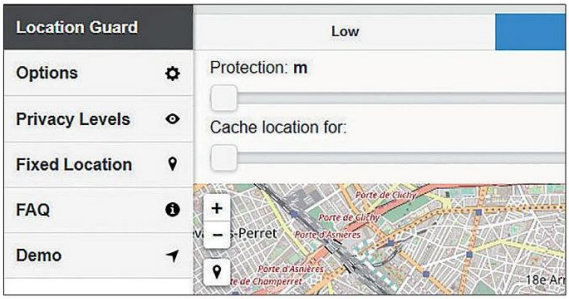
« https://youtube.com/watch?v=S6bOkFLrsAc »
devient « https://hooktube.com/watch?v=S6bOkFLrsAc ».
Aussi simple que cela.

Lien : **hooktube.com**

Empêcher la localisation

→ Avec Location Guard

Même si vous n'utilisez pas de VPN ou de solution d'anonymat, vous n'avez pas forcément envie que les sites sur lesquels vous vous connectez sachent où vous vous trouvez. L'extension Location Guard évite d'avoir à refuser manuellement le partage de sa localisation. Vous pouvez paramétrer pour chaque site un refus permanent, l'envoi d'une localisation aléatoire, voire fantaisiste.



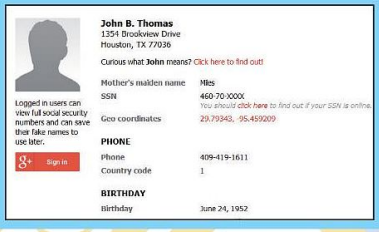
Lien : **https://goo.gl/PHSVLf** (Firefox); **https://goo.gl/TvGwdU** (Chrome)

Fakenamegenerator

→ Avec Fakenamegenerator

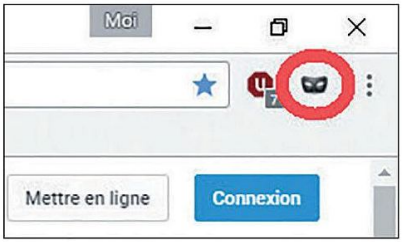
Quand vous remplissez un formulaire obligatoire sur un site qui n'a pas besoin de connaître votre nom, prénom, adresse ou autre, vous pouvez bien sûr rentrer n'importe quoi. Mais parfois, il faut une adresse valide dans tel ou tel pays. Fakenamegenerator se charge de créer de toutes pièces une identité fictive et très complète.

Lien : **www.fakenamegenerator.com**



Basculer Chrome en navigation privée

→ Avec Go Incognito

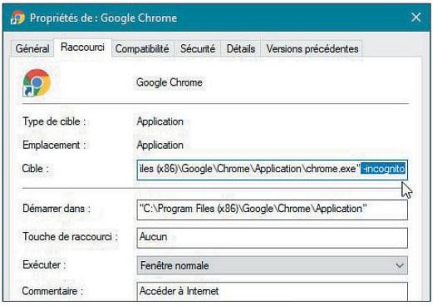


Disponible sur Chrome, l'extension Go Incognito est parfaite pour faire passer un onglet en navigation privée, même si vous l'avez ouvert en mode normal. Appuyez simplement sur l'icône de l'extension, à droite de la barre d'adresse. Cela ferme l'onglet initial, l'efface de l'historique, et le rouvre dans une fenêtre de navigation privée. Simple et efficace.

Lien : **https://goo.gl/eSAEvc**

Démarrer en navigation privée → Avec Chrome

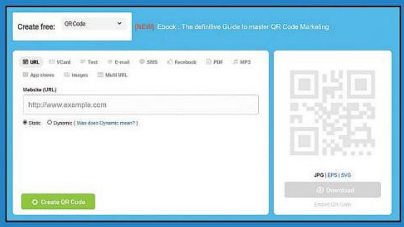
Vous souhaitez ouvrir systématiquement Chrome en mode navigation privée ? Faites un clic droit sur son icône, dans le menu Démarrer et choisissez **Plus > Ouvrir l'emplacement du fichier**. Puis clic droit sur le raccourci Chrome et **Propriétés**. Dans le champ **Cible**, ajoutez un espace à la fin de la ligne et tapez **-incognito**. Faites **OK** (et confirmez). Lancez Chrome via le menu Démarrer : il démarre en mode navigation privée. Attention, si vous avez placé un raccourci dans la barre des tâches, il faut le supprimer et le récréer pour qu'il soit également concerné.



Créer des QR Codes en ligne → Avec Barcode Generator

Placé sur une affiche, une carte de visite, ou même un site Web, un QR Code peut avantageusement remplacer un lien Web, particulièrement lorsqu'il s'agit d'un renvoi vers une page précise (vidéo, CV en ligne...). Barcode Generator peut transformer n'importe quel lien en QR Code, en quelques clics. Le service comporte d'autres options, comme l'envoi d'un SMS ou d'un mail préenregistré à chaque scan du code.

Lien : **www.barcode-generator.org**

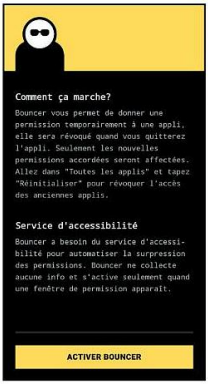


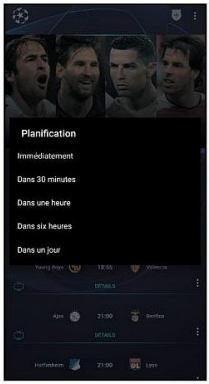
Un moteur de recherche pour enfants → Avec Qwant Junior

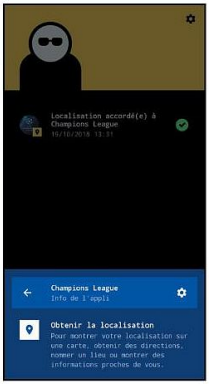
Les logiciels de contrôle parental, ce n'est pas votre truc, et la surveillance à outrance de l'historique Web de vos bambins non plus. Les Français de Qwant ont pensé à vous avec une version « junior » de leur moteur de recherche. Il exclut bien sûr tout contenu pour adultes, ainsi que l'accès aux sites marchands, et propose autant que possible des liens approuvés par le Ministère de l'Éducation nationale pour leur vertu éducative.

Lien : **www.qwantjunior.com**

Gérez vos permissions → avec Bouncer





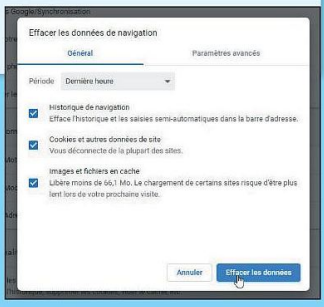


Vous le savez, Android est issu d'un noyau Unix. Il reprend donc son modèle de sécurité basé sur un système de permissions. Une application a un accès exclusif à ses propres fichiers et aucune autre application n'est capable de venir fouiller dans ses affaires…sauf si vous lui donnez la permission. Lorsque vous installez une application, celle-ci vous demande d'avoir accès à vos contacts, vos appels, votre appareil photo, etc. C'est parfois justifié, mais parfois non. Si vous refusez la permission, l'appli risque de ne pas s'installer… à moins de lui forcer la main. C'est ce que propose l'application Bouncer (c'est un «videur» de boîte de nuit dans la langue de Kim K). Cette dernière va donner des permissions temporairement. Vous pouvez les révoquer au bout de 30 minutes, une heure, un jour. Lorsque vous installez Bouncer, l'appli vous proposera de réinitialiser toutes les permissions pour redémarrer sur des bases saines, mais si vous décidez de ne pas le faire, vous aurez une notification à chaque installation d'une nouvelle appli. L'intérêt est bien sûr d'utiliser une fonctionnalité (par exemple la géolocalisation) sur une appli sans pour autant la laisser faire ce qu'elle veut tout le temps. Bouncer est disponible sur le Google Play Store et coûte la somme folle de 89 centimes. Le prix de la tranquillité !

Lien : **https://frama.link/2h4qNvz7**

Effacer rapidement ses traces

→ avec Chrome



L'historique et les cookies permettent de savoir quels sites vous avez visités, voire même de se connecter à vos comptes sans vérification d'identité (voir « Penser à se déconnecter »). Vous pouvez effacer tout cela dans les **Paramètres** de Chrome (via les 3 petits points en haut à droite), dans **Confidentialité et sécurité > Effacer les données de navigation**). Il y a aussi un raccourci clavier bien pratique : tapez la combinaison de touches **Ctrl + Maj + Suppr**.

Anonyme sur Google

→ AVEC SEARCHONYMOUS

Si vous en avez marre que Google vous propose des résultats ou des publicités en fonction de vos recherches antérieures vous pouvez vous déconnecter de votre compte et passer en mode anonyme. Le problème c'est que lorsque vous avez besoin de vous connecter à YouTube ou à Gmail, vous êtes de nouveau «traçable». L'extension Firefox Searchonymous vous donne le beurre et l'argent du beurre. Tout en restant connecté aux services de la galaxie Google, vous aurez à disposition un moteur de recherche totalement anonyme, sans cookie !

Lien : **http://goo.gl/He3cd9**

Vérifier les identifiants enregistrés

→ AVEC CHROME

Les identifiants de connexion enregistrés dans Chrome permettent d'accéder librement aux comptes concernés depuis votre machine. Vérifiez les comptes concernés dans les **Paramètres** de Chrome (via les 3 petits points en haut à droite), section **Saisie automatique > Mots de passe**. Cliquez sur l'œil pour dévoiler un mot de passe (si votre session Windows est protégée par un mot de passe, ce dernier vous est demandé). Cliquez sur les 3 points en bout de ligne pour supprimer un mot de passe.

Vous déconnecter de plusieurs services automatiquement → AVEC SUPER LOGOUT

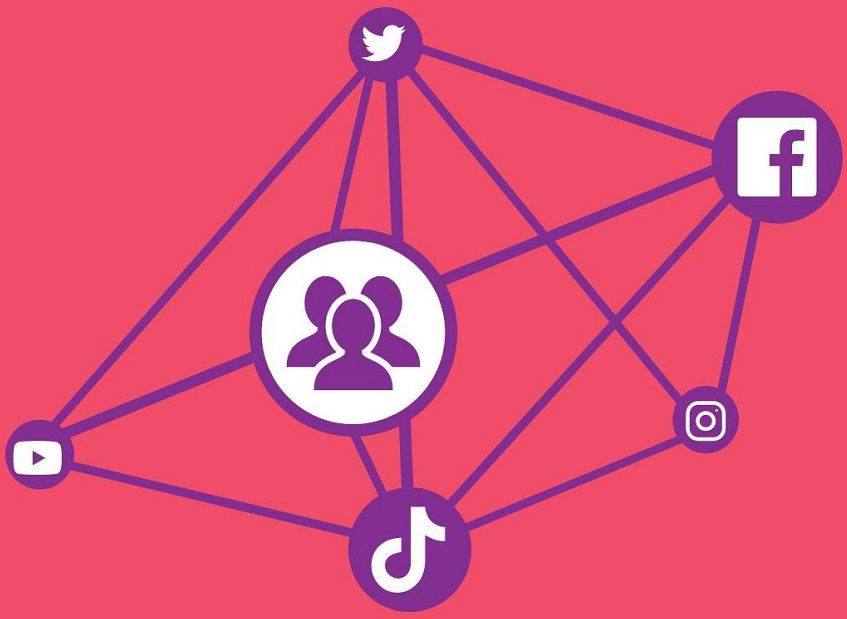
Vous avez ouvert vos comptes Google, YouTube, eBay, Netflix, Wikipedia, AOL... dans différents onglets de votre navigateur et, en partant dans la précipitation, vous avez oublié de vous déconnecter. Une omission dangereuse sur un ordinateur partagé... Pour ne plus prendre de risques, suivez notre lien pour arriver sur Super Logout. Dès que le site s'affiche dans votre navigateur, les déconnexions commencent. Patientez jusqu'à ce que les **OK** verts apparaissent à la droite des services, signe que la déconnexion a été réalisée.

Lien : **http://superlogout.com**

SUPER LOGOUT

- **AOL**: OK
- **Amazon**: OK
- **Blogger**: OK
- **Delicious**: OK
- **DeviantART**: OK
- **DreamHost**: OK
- **Dropbox**: OK
- **eBay**: OK
- **Gandi**: OK
- **GitHub**: OK
- **GMail**: OK
- **Google**: OK
- **Hulu**: OK
- **Instapaper**: OK
- **Linode**: OK
- **LiveJournal**: OK
- **MySpace**: OK
- **NetFlix**: OK
- **New York Times**: OK

RÉSEAUX SOCIAUX



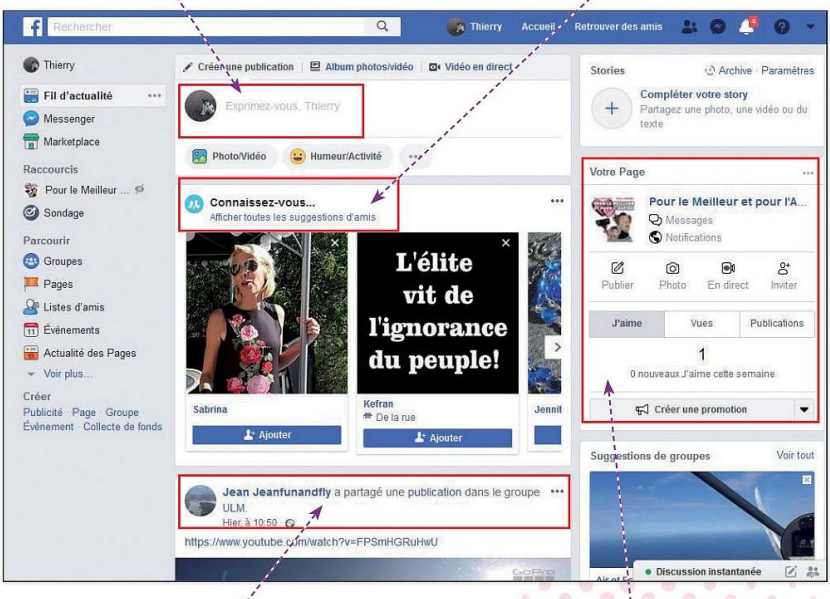
FACEBOOK : MIEUX GÉRER SES DONNÉES

Qu'il s'agisse d'entretenir des relations personnelles, de promouvoir une activité professionnelle, ou d'échanger autour d'un centre d'intérêt, Facebook est devenu pratiquement incontournable. Pour éviter de voir des informations sensibles être visibles par tout le monde, il existe quand même des petites choses à savoir.

Connaissez-vous toutes les facettes de Facebook ? Le plus grand des réseaux sociaux n'est pas seulement une immense collection de « journaux » de particuliers sur lesquels chacun raconte ses petits bonheurs ou malheurs du quotidien pour les partager avec famille et amis. Il y a aussi des « groupes » constitués autour de hobbies, de passion ou de thèmes d'intérêt communs, qui permettent discussions et échanges d'informations. Il y a encore les « pages » des personnalités, des partis politiques, des entreprises, des associations ou des commerces, qui véhiculent idées, publicités, informations... Dans les pages qui suivent, vous trouverez des conseils importants concernant

Publiez infos, humeurs, événements pour les partager avec tous vos contacts.

Famille, amis, collègues : développez votre réseau en ajoutant des personnes à votre liste d'amis Facebook.



Votre fil d'actualité affiche les publications de vos contacts et des groupes auxquels vous participez.

Créez des pages Facebook pour promouvoir une passion, une activité ou un projet.

la diffusion de vos données et informations. Car Facebook n'a pas que des aspects positifs. C'est une formidable machine à collecter et à enregistrer les informations, avec tous les dangers que cela comporte pour la vie privée. Certains ont ainsi payé cher une imprudence, un dérapage, un coup de mauvaise humeur... Nous n'avons pas vocation à vous rabâcher une énième fois toutes les précautions à prendre lorsqu'on donne des informations personnelles ou que l'on s'exprime sur un espace public comme Facebook. En revanche, nous nous attarderons sur les outils et fonctions à votre disposition pour mettre en œuvre concrètement ces précautions.
Un aspect à ne surtout pas négliger !

Contrôlez les informations affichées

Cliquez sur votre nom, en haut de la page, pour afficher votre profil Facebook. Complétez-le, et veillez à bien choisir qui peut voir vos informations et vos activités.

INFOS [FACEBOOK]
Où le trouver ? [www.facebook.com] Difficulté :

TUTO

01 › ILLUSTRER LE PROFIL

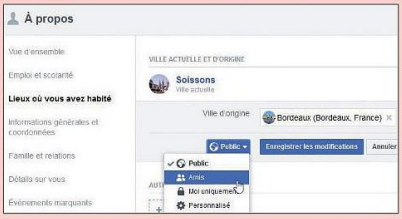
Pour ajouter ou modifier une photo de profil (en haut à gauche) ou une image de couverture (en bandeau, en haut), pointez le cadre correspondant et cliquez sur le bouton qui apparaît alors. Si vous désirez supprimer la photo de profil, sélectionnez l'onglet **Photos**, pointez l'image en question et cliquez sur le petit crayon qui apparaît en haut à droite.

02 › COMPLÉTER LES INFORMATIONS

À gauche de votre profil, et dans l'onglet **À propos**, peuvent figurer diverses informations vous concernant : scolarité, emploi, goûts et affinités, etc. Pour renseigner ces informations, sélectionnez cet onglet et remplissez à votre gré les rubriques **À propos**, et **Sport**, **Musique**, **Films**, etc.

03 › DÉCIDER QUI VOIT QUOI

Une étape à ne pas négliger ! Vous pouvez décider, pour chaque information complétée à l'étape précédente, qui y aura accès : tout le monde (**Public**), vos amis, personne (**Moi uniquement**), ou seulement certaines personnes (**Personnalisé**). Utilisez pour cela la liste déroulante proposée en bas à gauche des champs de saisie.



04 › RÉGLER LA CONFIDENTIALITÉ

Cliquez sur la petite flèche vers le bas, en haut à droite de l'écran, choisissez **Paramètres**, et sélectionnez la section **Confidentialité**, à gauche. Les choix que vous effectuez ici sont importants, inspectez toutes les rubriques, et décidez à chaque fois qui peut accéder aux éléments correspondants : tout le monde, vos amis, les amis de vos amis...

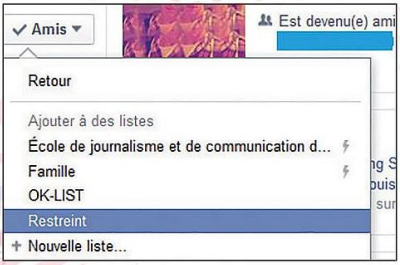
10 ASTUCES INDISPENSABLES POUR MIEUX GÉRER FACEBOOK

→ Vérifier ce que voient les autres

Pour voir ce que voient les internautes qui visitent votre profil Facebook, affichez ce dernier (cliquez sur votre nom, en haut), puis cliquez sur le bouton **Voir en tant que**, dans le bandeau de haut de page. Vous pouvez vérifier ce que voit un ami en choisissant **Aperçu du profil en tant que personne particulière**, en haut de l'écran. Cliquez sur la croix, en haut à gauche, pour sortir de ce mode.

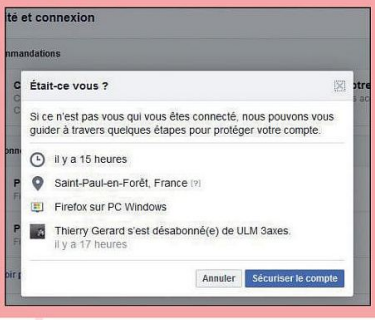
→ Restreindre des amis

Restreindre ses amis est un bon moyen d'éviter les mauvaises surprises sur Facebook. Une façon d'éviter par exemple que vos collègues ou parents voient toutes vos publications. Pour ce faire, cliquez sur l'onglet Amis depuis votre page puis, pour chaque ami à restreindre, passez le curseur sur **Amis**, cliquez **Ajoutez à une autre liste** et cochez **Restreint**.



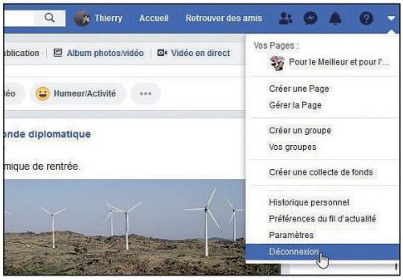
→ Repérer une connexion frauduleuse

Rendez-vous dans **Paramètres**, puis **Sécurité et connexion** et vérifiez à la rubrique **Vos connexions** que les différentes connexions à votre compte sont bien les vôtres. Si un appareil ou un lieu vous semblent suspects, cliquez sur les 3 petits points et sélectionnez **Ce n'est pas vous ?** puis **Sécuriser le compte** et suivez les instructions.



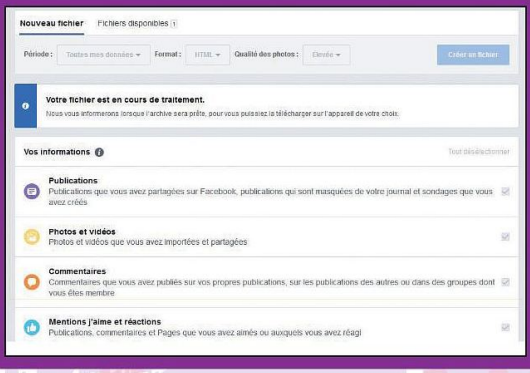
→ Penser à se déconnecter

Si vous vous connectez à Facebook chez un ami, sur un ordinateur public, ou même sur votre propre ordinateur si d'autres personnes y ont accès, pensez à vous déconnecter : déroulez le menu Facebook (la petite flèche vers le bas, en haut à droite), et sélectionnez **Déconnexion**. Refermer le navigateur ne suffit pas, suivant le paramétrage de ce dernier, en le relançant et en allant sur la page d'accueil de Facebook, on peut très bien se retrouver connecté au dernier compte utilisé.



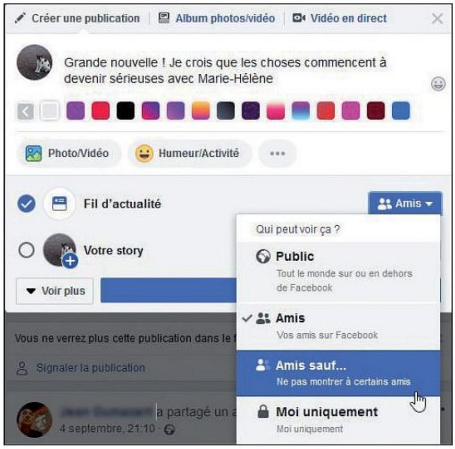
→ Télécharger toutes ses données

Il est possible de télécharger une copie de toutes vos publications, photos, vidéos, messages, etc. Pour cela, cliquez sur la flèche en haut à droite et allez dans **Paramètres**. À la rubrique **Vos informations Facebook**, cliquez sur **Télécharger vos informations**. Sélectionnez une période, cochez les types d'information désirés, et cliquez sur **Créer un fichier**. Une fois le fichier prêt, vous pouvez le télécharger à l'onglet **Fichiers disponibles**.



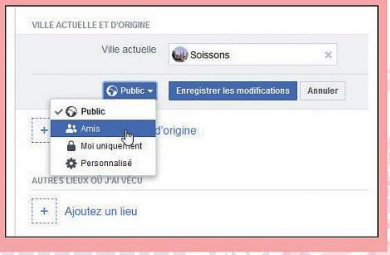
→ Publier avec précaution

Lorsque vous créez une publication sur Facebook, n'omettez jamais de vérifier son audience, en bas à droite de la fenêtre de saisie : **Public**, réservée aux **Amis**, ou à certains **Amis spécifiques**. La valeur par défaut est déterminée dans vos paramètres de confidentialité. Affichez votre journal (cliquez sur votre nom, en haut de l'écran) pour voir vos publications. Pour revenir sur l'une d'elles, cliquez sur les 3 petits points en haut à droite et **Modifier**... Vous pouvez corriger le texte, supprimer une image, ou changer l'audience.



→ Se faire plus discret

A priori, toutes les informations saisies dans votre profil Facebook sont publiques : n'importe qui peut les voir. Pour en limiter la visibilité, allez sur votre profil (cliquez sur votre nom, en haut), onglet **À propos**. Cliquez sur l'information concernée, puis sur **Modifier**. Utilisez la liste déroulante pour basculer de **Public** à **Amis** ou **Personnalisé** (seulement à certaines personnes désignées), puis faites **Enregistrer les modifications**.

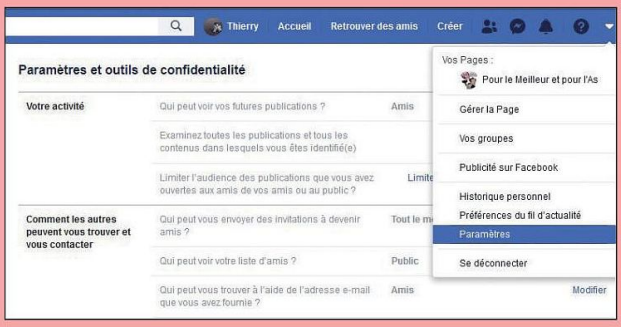


→ Désactiver ou supprimer son compte

Vous voulez disparaître de Facebook pendantquelque temps ? Ou carrément quitter définitivement le réseau ? Allez dans les **Paramètres**, à la section**Vos informations Facebook**, et sélectionnez **Supprimer votre compte et vos informations**. **Désactiver le compte** rend votre profil inaccessible, mais vos infos sont conservées et vous pouvez réactiver quand vous voulez. **Supprimer le compte** efface tout définitivement.

→ Décider qui voit quoi

Si vous ne l'avez jamais fait (ou il y a longtemps), vérifiez impérativement les paramètres de confidentialité de Facebook. Affichez les **Paramètres** via la petite flèche en haut à droite, et allez à la rubrique **Confidentialité**, à gauche. Inspectez chaque section soigneusement pour décider qui peut accéder aux éléments correspondants, vos publications anciennes et futures ou votre liste d'amis par exemple.



→ Disparaître des moteurs de recherche

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...**.

Le nouveau site des utilisateurs ANDROID

- Des dizaines de tutoriels et dossiers pratiques
- Mobiles & Tablettes : des tests complets !
- Sélection des meilleures applis + des vidéos et du fun !

Android MT

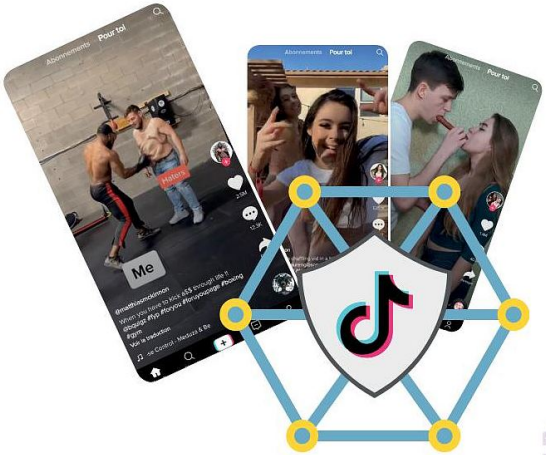
Solutions & Astuces

www.android-mt.com

NOUVEAU SITE !

3 ASTUCES POUR PROTÉGER SA VIE PRIVÉE

L'application TikTok est un réseau social qui a la cote chez les jeunes. Or ces derniers ne sont pas toujours très regardants quant à la protection de leur vie privée. Que vous ayez un compte TikTok ou qu'il s'agisse de celui de vos enfants, voici quelques astuces pour éviter de trop se dévoiler ou de se protéger du cyberharcèlement…



Si vous ne connaissez pas ce réseau social venu de Chine, vos enfants le connaissent sans doute. Cette appli qui permet aux utilisateurs de partager de courtes vidéos humoristiques ou à caractère artistique (danse, chant, etc.), a été très décriée lors de sa sortie pour certains débordements et un certain laxisme au niveau de la modération. Comme il n'est pas nécessaire d'avoir un compte pour regarder des vidéos, les pervers en tout genre utilisent aussi l'appli pour entrer en contact avec de jeunes gens, pas toujours très concernés par la protection de leur vie privée. On compte aussi pas mal de cas de cyberharcèlement. Désireux de se montrer concerné, TikTok s'est doté d'une équipe de modérateurs français et d'une charte de bonne conduite appelée « consignes communautaires ». C'est un pas dans le bon sens, mais vous pouvez prendre les choses en main de votre côté et en parler avec les ados de votre entourage puisque sur TikTok on trouve des paramètres et des fonctionnalités pour se protéger des trolls et des personnes malveillantes…

INFOS [TIKTOK]
Où le trouver ? [https://www.tiktok.com/fr/] Difficulté :

TUTO

01 › PASSER EN COMPTE EN « PRIVÉ »

En créant un compte TikTok, vos vidéos sont visibles par tout le monde. Il s'agit d'un compte public «par défaut». C'est d'autant plus grave que n'importe quelle personne qui installe TikTok peut voir ce que vous faites ou ce que font vos enfants puisqu'il n'est pas nécessaire de créer un compte pour accéder aux différents contenus. Allez sur votre profil, puis dans le menu avec les trois petits points horizontaux. Sélectionnez **Confidentialité et sécurité** et passez en mode privé.

02 › SIGNALER UN COMPTE, UN COMMENTAIRE OU UNE VIDÉO

Même si TikTok a fait des progrès en ce qui concerne la modération, il existe toujours des abus. C'est bien normal, il n'y a qu'à voir la quantité de choses horribles postées sur Twitter ou Facebook pour se rendre compte qu'il est bien difficile de faire le ménage sur les plates-formes populaires. Pour signaler un commentaire haineux, raciste ou dérangeant, restez appuyé sur ce dernier jusqu'à ce que **Signaler** apparaissent et sélectionnez la raison de votre signalement. Pour signaler un utilisateur ou une vidéo en particulier, cela fonctionne de la même manière.

03 › FILTRER LES COMMENTAIRES

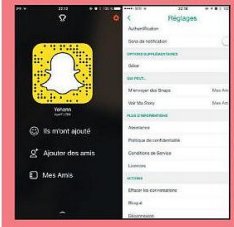
Toujours dans la partie **Confidentialité et sécurité** des paramètres de votre profil, vous pourrez choisir qui a le droit de faire quoi (commenter, réagir, Duo, messages privés, etc.) On peut régler toutes ces actions : tout le monde, seulement mes amis, seulement moi, etc.) Vous évitez alors les spams, les commentaires désobligeants, etc. On peut même ajouter des mots clés pour bloquer des commentaires.

Chiffrer vos conversations sauvegardées sur Google Drive → avec WhatsApp

WhatsApp va bientôt se doter d'un niveau de sécurité supplémentaire. Il pourrait désormais être possible de chiffrer nos conversations sauvegardées sur le Cloud de Google Drive. Quand vient l'heure de changer de smartphone, WhatsApp n'est pas l'application de messagerie instantanée la plus intuitive, non. L'utilisateur doit procéder à de nombreux backups, sauvegarder l'intégralité de ses conversations, les transférer sur Google Drive puis sur le nouveau téléphone avant de réinitialiser son ancien appareil, sous peine de perdre les messages les plus récents. Une procédure qui se révèle être un beau parcours du combattant. Et d'un point de vue sécurité, ces backups sont un véritable cauchemar. En effet, vos messages ont beau être chiffrés sur Whatsapp, ils ne le sont plus une fois sauvegardés sur le Cloud sur Google Drive. Or, WhatsApp serait en passe de changer ça et travaillerait actuellement sur une protection supplémentaire pour les sauvegardes sur le Cloud : une couche de chiffrement disponible dans les paramètres de WhatsApp, dans l'onglet Chat puis Sauvegarde du chat. Une nouvelle entrée de sauvegarde protégée par mot de passe s'affichera à cet endroit, sous les paramètres de Google Drive. Surveillez la prochaine mise à jour !

Quelques précautions → avec Snapchat

Snapchat n'est pas sans risque. Pour éviter les surprises, il faudra passer par les réglages...



Commençons par masquer votre numéro de téléphone pour éviter d'être enregistré par des utilisateurs que vous ne connaissez pas ou que vous ne souhaitez pas connaître. Allez dans les **Paramètres généraux** puis décochez la case **Autoriser mes amis à me retrouver**. Au même endroit vous trouverez **Qui peut m'envoyer des Snaps** puis **Mes amis**. Vous réduirez les risques de vous faire importuner. Dernière précaution : utilisez un pseudo. Celui-ci protège votre identité ou vous permet d'être introuvable à partir de votre nom / prénom !

Lien : **www.snapchat.com**

Une alternative libre à Twitter → avec Mastodon

Mastodon est un logiciel accessible par un navigateur et des applications iOS ou Android qui vise, par ses fonctions de base, le même public que Twitter. L'interface est très similaire, on suit des comptes, des comptes nous suivent, on a une timeline, des mentions, des hashtags, on peut mettre un message dans nos favoris et/ou le partager tel quel à nos abonnés. Même les comptes protégés et les DMs sont là. La différence de taille réside dans le caractère libre et décentralisé. Attention, Mastodon est un logiciel.

Au contraire de Twitter qui est un service. Personne ne peut installer le site Twitter sur son ordinateur et permettre à des gens de s'inscrire et d'échanger ailleurs que sur twitter.com. Par contre toutes celles qui ont les connaissances nécessaires peuvent télécharger Mastodon, l'installer quelque part et le rendre accessible à d'autres. C'est là que se trouve toute la beauté du truc : les personnes inscrites sur n'importe laquelle de ces instances peuvent discuter avec les personnes inscrites sur les deux autres de manière transparente. Et tout le monde est libre d'en créer de nouvelles et de les connecter ou non avec les autres.

Lien : **https://mastodon.social**

Quelques précautions → avec Twitter

Twitter est considéré comme un réseau social peu intrusif : il n'y a pas grand-chose à configurer pour assurer sa confidentialité. Cependant, comme tout réseau social, il reste vulnérable vis-à-vis du partage à outrance ou de la fuite de données... Tout comme Facebook et Google, Twitter profite également des revenus de la publicité, ainsi il s'intéresse de près aux centres d'intérêts de ses utilisateurs, quand ils sont sur Twitter ou quand ils ne le sont pas. Allez dans **Paramètres et Confidentialité** depuis Plus en bas à gauche (sur ordinateur) ou depuis l'icône de votre profil en haut à gauche. Dans **Confidentialité et sécurité** vous pourrez protéger vos tweets, paramétrer vos messages privés, votre localisation, le rapprochement avec Périscope, mais aussi la Confidentialité des tweets. Par défaut, **Protéger mes Tweets** est désactivé, et n'importe qui sur Twitter, ou quiconque cherchant sur Google, peut voir vos Tweets. Si vous cochez cette case, afin de protéger vos tweets, cela verrouille votre visibilité, mais de manière plutôt radicale. Si vous choisissez de garder vos tweets accessibles au public, soyez alors très prudent à propos de ce que vous écrivez. Tout le monde pourra le voir, et cela signifie donc que vous ne devrez pas écrire quoi que ce soit qui doit rester dans la sphère privée. L'option **Permettre de me trouver grâce à mon adresse email** est par défaut activée, et permet aux gens, qui ne connaissent pas le "handle" de votre compte Twitter, mais connaissent par contre votre adresse email, de vous trouver. De même, l'option **Personnaliser les publicités en fonction des informations partagées par les partenaires annonceurs** est activée par défaut. Désactivez-la en décochant la case.

Lien : **https://twitter.com**

Rester invisible → avec WhatsApp

La messagerie utilisée par un milliard et demi d'individus a une grosse faille : elle fonctionne comme l'application SMS : pas possible de voir un statut de connexion comme ses petits camarades. Pas de Absent, Ne pas déranger ou de mode Invisible comme sur Skype par exemple. C'est assez embêtant, car on sait tous que c'est très tentant de regarder son smartphone à la moindre notification. Pourquoi ne pas commencer par afficher un statut qui incitera vos contacts à ne pas vous spammer de messages ? Allez dans le menu avec les trois petits points en haut à droite puis **Paramètres**. Sélectionnez votre avatar puis **Actu**. Ici vous pourrez mettre un statut comme **Occupé(e)**, **Au cinéma**, **Ne peux pas parler**, etc. Vous pouvez aussi mettre ce que vous voulez avec des émoticônes. Les messages précédemment écrits seront sauvegardés. Il faudra juste penser à remettre un statut disponible, car ce message apparaîtra juste à côté de votre nom sur les appareils de vos contacts. Pour éviter d'être importuné, l'autre solution consiste à interagir uniquement avec vos contacts. Retournez dans le menu avec les trois petits points en haut à droite puis **Paramètres**>**Mon Compte**>**Confidentialité**. Ici vous pouvez faire en sorte que seuls vos contacts voient la dernière fois où vous avez ouvert WhatsApp (**Vu à**), votre avatar (**Photo du profil**) et votre **Statut**. Cela permet de « faire le mort » pour tout ou une partie des personnes susceptibles de vous contacter. Notez que ces réglages seront aussi appliqués dans l'autre sens. Si vous décidez que personne ne doit voir votre photo, vous ne verrez pas celle des autres.

Lien : **www.whatsapp.com**

Le chat a neuf vies. Le papier en a cinq. (Pour le papier, c'est prouvé.)

Tous les papiers ont droit à plusieurs vies.


journaux · magazines


publicités · prospectus


enveloppes · papiers


catalogues · annuaires


courriers · lettres


livres · cahiers

recyclons-les-papiers.fr | ecofolio

CLOUD

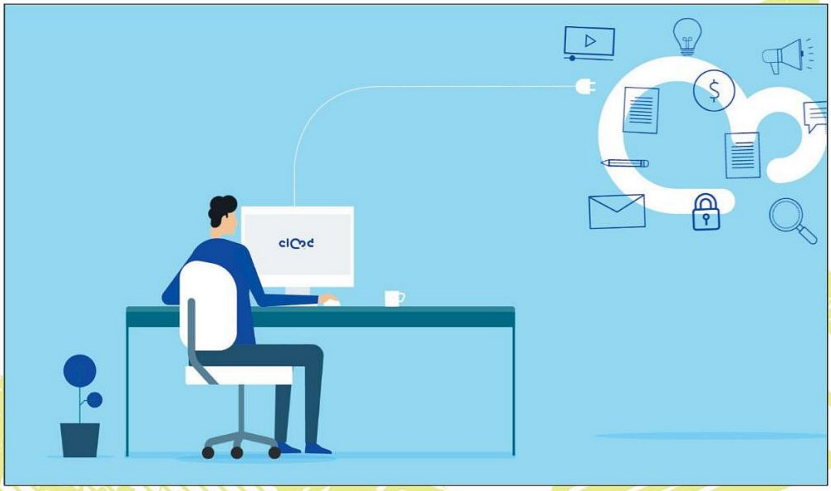
CLOOD : UN CLOUD CHIFFRÉ POUR LES PROS !

Il y a peu de solutions qui permettent aux professionnels de stocker de manière chiffrée leurs documents. Les services gratuits sont rarement adaptés aux besoins des entreprises tandis que les solutions pros sont parfois trop complexes à appréhender. Il est de surcroît dangereux de compter uniquement sur une solution en local à cause des ransomwares et autres saletés. Pour ces TPE/PME, Clood propose une solution sur-mesure à un prix abordable.

Les infections et les ransomwares sont devenus la bête noire des entreprises. En faisant confiance à une sauvegarde en local sur un petit serveur ou sur un simple disque dur, les TPE/PME se mettent en danger, car le chiffrement ne met pas à l'abri d'un chiffrement malicieux supplémentaire. Et c'est sans compter les vols de matériel ou les erreurs de manipulation. Rien ne vous empêche d'utiliser une solution locale, mais le cloud a plusieurs avantages. Le seul hic c'est que le chiffrement est souvent absent et qu'on ne sait jamais vraiment où sont les données...

POURQUOI CELUI-LÀ ET PAS UN AUTRE ?

Clood est un service pensé pour les petites et moyennes entreprises et les micro-entrepreneurs pour stocker des documents importants : fiches de paye, comptabilité, feuille de présence, contrats, etc. Clood est aussi localisé en France et géorépliqué dans notre beau pays : cela veut dire que vos données sont stockées dans plusieurs endroits à la fois, mais toujours sur le territoire national. Cela garantit l'intégrité de vos données même en cas d'attaque de sauterelles, d'épidémie de gale afghane, de tremblement de terre ou de panne d'un des serveurs. Vos données sont aussi à l'abri de nos belles lois européennes comme la GPRD. Un ransomware a sévi dans les ordinateurs de votre entreprise ? Pas de problème puisque Clood est loin (genre en Auvergne ou à Vesoul) et même en cas de «boulette», il gère très bien le «versioning» (gestion de versions). Une attaque des «Chinois du FBI» ? Avec du RSA 2048 bits, le club des ninjas du 13ème arrondissement pourra s'amuser quelques siècles sur votre clé solide comme un pilier All Blacks sous MDMA.



Clood stocke et chiffre vos documents dans plusieurs serveurs en France...

Chiffrez vos fichiers stockés

INFOS [CLOOD]
Où le trouver ? [https://clood.co] Difficulté :

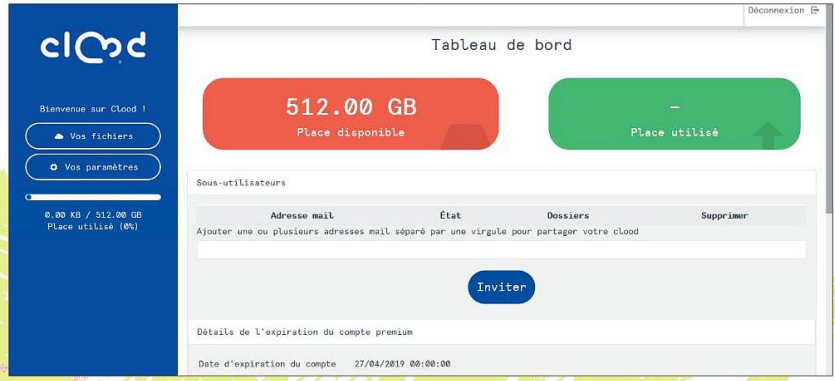
TUTO

01 L'INSCRIPTION

Pour utiliser Clood, il suffit de s'inscrire comme avec n'importe quel service en ligne. Vous pouvez aussi demander un essai si vous venez de notre part...

02 L'INTERFACE

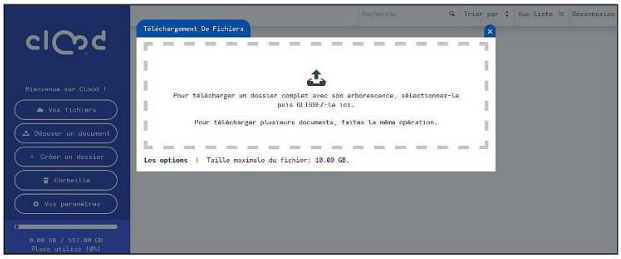
Le tableau de bord est très simple : combien il vous reste d'espace, liste de vos fichiers, etc. Invitez vos collaborateurs à travailler sur vos fichiers... Le chiffrement est géré par le site : vous n'avez rien à faire.

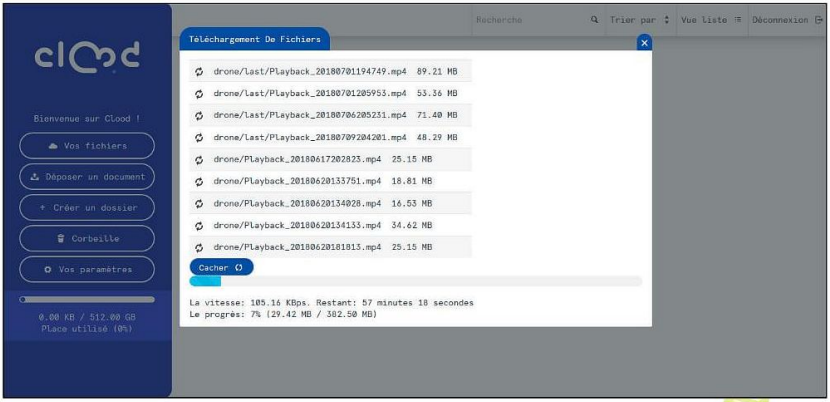


03 › L'UPLOAD

Et sur mobile

Android ou iOS ? C'est pareil ! Si vous avez beaucoup d'e-mails, la recherche à l'intérieur des messages chiffrés peut prendre un peu plus de temps, mais toutes les fonctionnalités sont là !





MAIS COMBIEN ÇA COÛTE ?

Clood propose 3 formules : une à 9,90€/mois sans engagement avec 20 Go de stockage, une seconde option à 49€/mois (100 Go, 10 utilisateurs avec engagement de 36 mois) et une dernière à 99€/mois pour 500 Go. Il est aussi possible de demander une offre sur-mesure et d'accéder à un compte de démo pour tester le service, mais il faut demander gentiment !

Interview de Esteban Mauvais,

CTO et co-fondateur de Clood

Esteban Mauvais, qui écrit parfois des articles dans nos pages quand il ne fait pas de jardinage avec son Raspberry Pi ou qu'il ne trolle pas son monde sur LinkedIn, est le CTO et co-fondateur de Clood. Il répond à nos questions...

COMBIEN DE PERSONNES TRAVAILLENT CHEZ CLOOD ET COMMENT EST PARTIE CETTE AVENTURE ?

Actuellement nous sommes 5 personnes à travailler chez Clood. Christophe (CEO et cofondateur) s'occupe de la stratégie et du business development. Kevin s'occupe de faire coller la stratégie de développement aux ressources disponibles. Florian et moi-même sommes en charge de l'ensemble des développements produit. Notre objectif est de le faire évoluer au fil du temps pour coller à 100% avec nos valeurs : transparence, sécurité, assistance ! Nous travaillons avec une agence de communication pour le marketing, mais nous attendons une sixième personne qui viendra prendre le relais sur ces sujets.

Il y a 1 an, nous lancions Monkey Co avec Florian et étions à la rechercher de projets innovants, et à forte capacité de croissance. Notre objectif était de devenir CTO externalisé afin de voir évoluer un projet dans le temps. Nous avons reçu plusieurs centaines de propositions en quelques jours ! Parmi les propositions, celle de Christophe et Kevin avec l'ambition de développer un cloud français, simple et intuitif, avec une nouvelle technologie de chiffrement et de stockage de données qui permettait d'assurer un niveau de protection inédit des documents des entreprises. Le projet nous a de suite plu, car il venait répondre à une véritable problématique actuelle, et le sérieux de l'équipe nous a convaincus. Après quelques réunions téléphoniques et un après-midi de brainstorming dans un bar, la collaboration commençait !

À QUI EST DESTINÉ CLOOD ?

Il faut savoir déjà que Clood émerge d'un constat : la sécurisation de la donnée dans les TPE/PME est très souvent reléguée au second plan. Pourquoi ? Parce que la digitalisation des données s'est faite brutalement.
Avec Clood nous avons souhaité offrir une solution à la portée de tous, initiés ou pas. Nous mettons à disposition de nos utilisateurs un moyen sécurisé de stocker leurs documents professionnels. Le tout sur une interface épurée et intuitive. Nous avons vu beaucoup trop d'usines à gaz lors de notre étude de l'offre existante.
En bref, notre promesse est simple : Tu es une startup, un indépendant, une TPE, une PME ? Tu n'as pas envie que tes données finissent n'importe où ? Tu as envie d'avoir de la visibilité

sur ce que deviennent tes données une fois dématérialisées ? Viens chez Clood ! On te promet de la transparence (tout est stocké sur des serveurs dans nos belles campagnes françaises), de la réactivité (t'as un problème ? Tape notre 05 et une personne de notre équipe te répond directement), et de la sécurité (nous sommes certains de la fiabilité de notre produit, vous pouvez y aller !). Clood est en plus spécialement conçu pour le partage et la collaboration. Un onboarding en 4 clics et une gestion des partages hyper intuitive.

ON ENTEND PARLER DE CLOUD DEPUIS DES ANNÉES, POURTANT LES PETITES ENTREPRISES ONT DU MAL À S'Y METTRE, COMMENT VOUS EXPLIQUEZ CELA ?

Je pense qu'il y a plusieurs raisons à cela. D'abord cela est probablement dû à la mauvaise réputation des clouds existants en matière de sécurité de la donnée et de leurs politiques de confidentialité. Qui n'a pas entendu parler du « Patriot Act » qui permet au gouvernement US de lire tous les documents des entreprises ? Quand on sait que la plupart des acteurs du cloud sont américains, on comprend que les entreprises n'aient pas vraiment envie de leur confier leurs documents... C'est pour ça que Clood est français, c'est pour ça que Clood stocke les documents des entreprises sur des serveurs français, et c'est pour ça que Clood respecte les lois françaises, dont le fameux RGPD. Les clouds sont aussi trop techniques. Les chefs d'entreprise dont ce n'est pas le métier et n'ayant pas de spécialiste informatique au sein de leurs équipes ne s'intéresseront pas d'eux-mêmes au cloud. C'est pour ça que Clood est là !

SI LE CLIENT DISPARAÎT DANS LA NATURE, VOUS LUI DONNEZ COMBIEN DE TEMPS AVANT DE SUPPRIMER LES DONNÉES ?

Les tarifs de Clood sont mensuels, sans engagement, sans limites d'utilisateurs. Les clients peuvent stopper à tout moment sans justificatif. Tant que le règlement est effectué, nous conservons les données. Dans le cas contraire, en cas de cessation de paiement, nous prévenons par mail et téléphone l'entreprise afin de leur permettre d'extraire leurs données. Dans notre politique d'utilisation, il est stipulé que les données sont conservées 6 mois après cessation de paiement. Au-delà de ce délai, nous nous donnons le droit de les supprimer.

COMMENT FONCTIONNE LE CHIFFREMENT ET POURQUOI NE PAS AVOIR OPTÉ POUR UN CHIFFREMENT DE BOUT EN BOUT ?

Nous avons choisi de lancer Clood avec les fondamentaux d'un cloud : stockage et partage collaboratif, pour une question de temps. Le chiffrement de bout en bout n'est pas encore présent pour des raisons techniques comme la prévisualisation des documents, le partage du cloud et surtout pour ne pas perdre les données en cas de perte de mot de passe. Une alternative arrive avec un chiffrement de bout en bout sur des clés dossiers.

L'APPLI MOBILE, C'EST PRÉVU ?

Très clairement oui, cependant une application bureau (Windows, Mac et Linux) sera présentée en priorité.

C'EST QUOI LA PROCHAINE ÉTAPE CHEZ CLOOD ?

La prochaine étape, ou plutôt les prochaines étapes, car chez Clood on a plein d'idées ! D'un point de vue technique : développer la sauvegarde par version, le chiffrement de bout en bout, la synchronisation et un gestionnaire de mots de passe...
D'un point de vue stratégique : consolider notre présence sur le marché français en faisant grandir le nombre d'entreprises clientes de Clood. Nous avons pour ambition de devenir le partenaire privilégié des TPE/PME françaises !

pCLOUD : LE CLOUD CHIFFRÉ POUR MONSIEUR TOUT LE MONDE

Si vous cherchez un cloud chiffré qui propose une interface simple avec des prix abordables, pCloud est peut-être la solution qu'il vous faut. Si vous n'avez pas envie de tout chiffrer vous-même et que vous êtes prêt à payer pour votre tranquillité, pCloud se pose comme un service de choix.

pCloud est un service de stockage de type « cloud » qui propose un chiffrement de vos données. Avant de parler de la protection des fichiers, voyons les fonctionnalités annexes de ce service : personnalisation des liens de téléchargement, multi-plates-formes (Windows + MacOS/iOS, Linux et Android) et mémorisation des versions de fichiers (pour éviter les problèmes liés aux manipulations). L'offre Business est dédiée aux entreprises, à partir de 5 utilisateurs. La création d'un utilisateur est très facile : ajouter des utilisateurs au compte.

L'administration du compte business est très simple depuis l'interface Web ou le client. On peut créer des équipes, par exemple : production, comptabilité, marketing, accueil, etc. Puis vous définissez les utilisateurs de chaque équipe. Les consommateurs de vidéos et de musiques pourront profiter de leur contenu directement en streaming.

UN CHIFFREMENT SOLIDE

La sécurité est au cœur de pCloud. L'authentification au service repose sur un mécanisme à deux facteurs. Et durant les transferts de fichiers, tout est chiffré, en utilisant TLS & SSL, pour éviter toute fuite de données.

Les clés privées de chiffrement utilisent le standard 4096-bit RSA et les clés fichiers et dossiers sont chiffrés en AES 256 bits. Autre fonction qui plaira aux pros : la possibilité de personnaliser les liens de téléchargement en ajoutant un titre, votre logo, votre photo et une description.

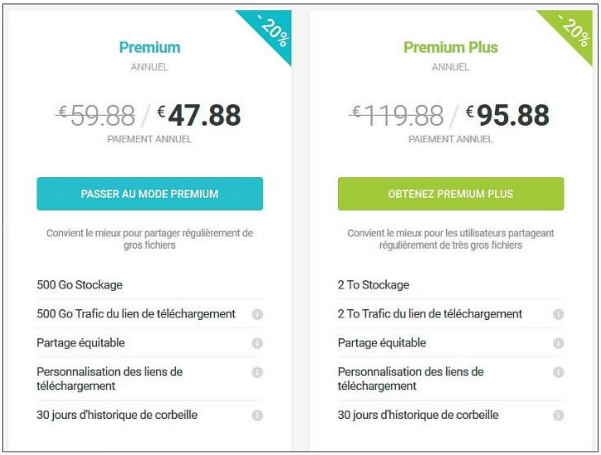
SI VOUS N'AVEZ PAS ENVIE D'HÉBERGER VOTRE PROPRE CLOUD CHIFFRÉ À LA MAISON, PCLOUD EST UNE BONNE SOLUTION DE REMPLACEMENT...

LE SAVIEZ-VOUS ?

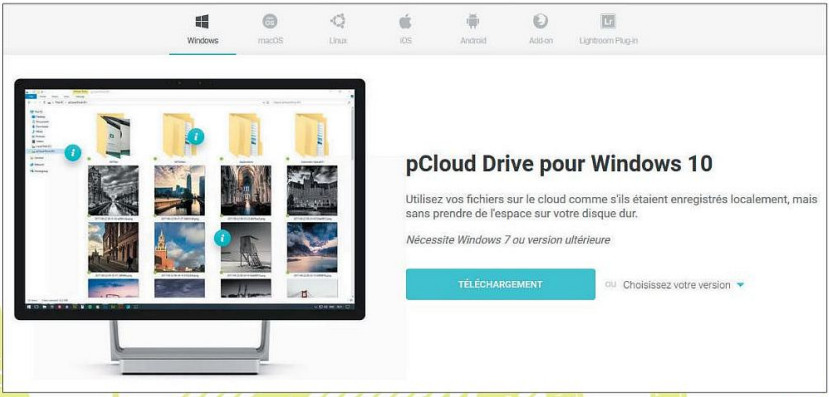
Drive, le clood de Google n'est absolument pas chiffré. Pire, en tapant une requête sur le moteur de recherche, on peut très bien trouver des documents en clair. Si vous avez un Google Drive avec des fichiers sensibles, il est temps de les bouger ou de les chiffrer. En tapant par exemple **«*.avi site:drive.google.com»** on ira chercher des fichiers vidéo au format AVI dans les comptes Google Drive de Monsieur et Madame tout le monde. Chose amusante, on peut même tenter de voir un film entier. En tapant **«Le Parrain site:drive.google.com»** nous avons trouvé le film de Coppola et lancé la lecture depuis le navigateur! À l'aise. En fouillant un peu on peut trouver des photos personnelles, des documents bancaires (RIB), médicaux et encore pleins de fichiers qui n'ont pas vocation à se retrouver au vu et au su de tous. Dans les pages suivantes, nous verrons avec BoxCryptor et Cryptomator comment ajouter une couche de chiffrement à Google Drive...

INFOS [PCLOUD]
Où le trouver ? [www.pcloud.com/fr] Difficulté :

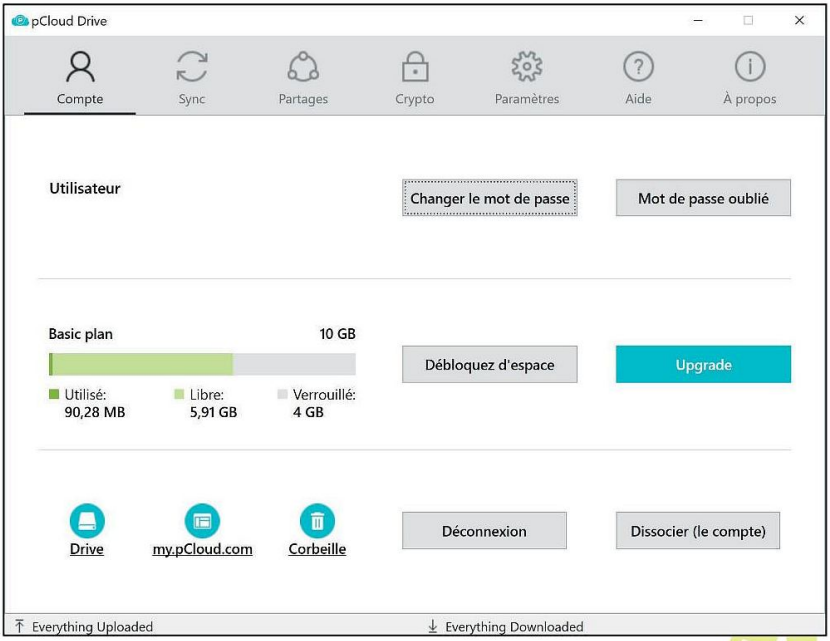
TUTO

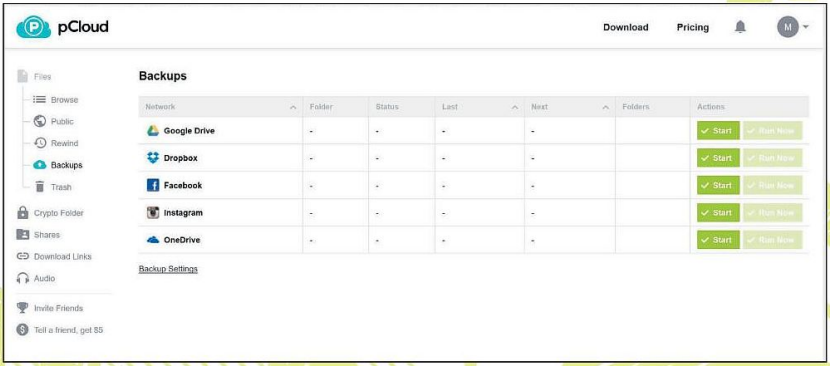


Le service propose une version gratuite avec 10 Go de données. Il existe un abonnement « à vie » qui coûte 175 € pour 500 Go et 350 € pour 2 To. Après vous pouvez aussi payer par an : respectivement 47,88 € et 95,88 €. Pour les familles et les entreprises, il y a aussi des offres...



Vous avez accès à votre cloud depuis tous les appareils que vous désirez. Vous pouvez aussi faciliter vos transferts avec les plugins sous Chrome, Firefox et Opera. Vous êtes photographe et utilisateur de Adobe Lightroom ? Il existe même un plugin pour partager vos clichés édités sur votre compte pCloud directement depuis Lightroom..





Les 10 Go de stockage gratuits ne donnent pas le droit à toutes les options, mais vous pourrez quand même synchroniser pCloud avec vos autres « cloud », disposer de lien de téléchargement et bien sûr tout est chiffré !

ONIONSHARE : UN PARTAGE CHIFFRÉ ET CONFIDENTIEL

OnionShare n'est pas un vraiment un cloud. En s'appuyant sur le réseau Tor, il permet de partager des fichiers de manière complètement sécurisée et sans avoir une grosse infrastructure derrière...

OnionShare va créer un serveur temporaire sur votre ordinateur. Il va générer une URL en .onion uniquement accessible via Tor. La sécurité est de mise puisqu'en plus de cette URL, le logiciel va aussi lui adjoindre une clé unique qui servira à authentifier votre correspondant. Il faudra juste que votre machine reste allumée le temps du transfert. Il est même possible de fermer le serveur lorsque les fichiers seront transférés. Cerise sur le gâteau, votre correspondant n'aura même pas à installer OnionShare pour réceptionner les fichiers puisqu'une simple connexion à Tor depuis son navigateur suffit pour accéder à l'URL de votre service caché.

DEUX SOLUTIONS ALTERNATIVES POUR UN CLOUD CHIFFRÉ

SPIDEROAK ONEBACKUP & CRYPTSYNC

SpiderOak a fait le buzz lorsque Edward Snowden l'a mentionné dans une interview. Le service coûte 14 dollars pour 2 To Go de stockage, mais il y en a pour tous les budgets. Bien sûr, il existe des versions pour Windows, mobiles, MacOS et Linux. Sachez enfin que le chiffrement est un mélange entre RSA 2048 bits et AES 256 bits et tout se fait en local. Impossible pour un pirate de récupérer la clé donc...

De son côté, CryptSync est compatible avec tous les services de type Dropbox (avec un répertoire en local sur votre PC), ce programme va chiffrer tout ce que vous lui présenterez pour le placer directement dans votre espace de stockage. Une bonne alternative gratuite pour utiliser un cloud déjà existant et automatiser les tâches.

Lien : **https://spideroak.com**;

Lien : **https://sourceforge.net/projects/cryptsync-sk**

Première utilisation de OnionShare

INFOS [ONIONSHARE]
Où le trouver ? [https://onionshare.org] Difficulté :

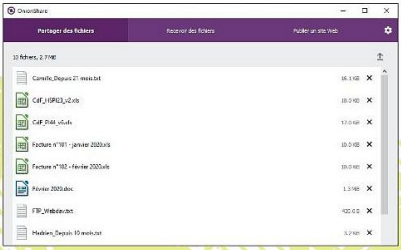
TUTO

01 › PRÉ-REQUIS

Pour envoyer des fichiers avec OnionShare, il faudra que vous ayez Tor installé sur votre PC. Pour la réception, vos correspondants n'auront pas besoin de OnionShare, mais Tor reste obligatoire. Téléchargez la dernière version du Tor Browser et paramétrez-la en suivant les recommandations de l'assistant de connexion.

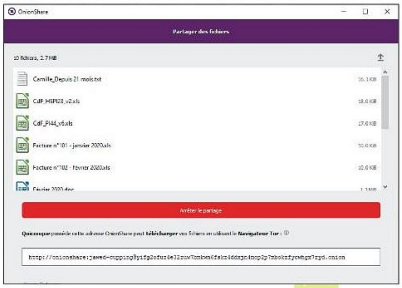
02 › L'INTERFACE

Il faudra ensuite installer OnionShare. Une fenêtre devrait s'afficher avec un espace pour glisser-déposer des fichiers, des boutons pour ajouter des éléments et une case à cocher si vous voulez arrêter le serveur automatiquement. Cette dernière est utile si vous souhaitez arrêter le partage lorsque votre correspondant aura récupéré les fichiers.



03 › VOTRE SERVEUR «MAISON»

Mettez autant de fichiers et dossiers que vous voulez et cliquez sur **Démarrer le serveur**. Attention, il faudra que Tor soit connecté à Internet pour que la magie opère. OnionShare va alors simplement générer un lien qui dirigera sur un service caché (hidden service), une page Internet accessible uniquement aux utilisateurs de Tor. À tous les utilisateurs? Non! Seulement à celui de votre choix.



04 › LA RÉCEPTION

Envoyez ce lien à votre ami par un moyen sécurisé si le contenu est sensible. Armé de Tor, votre petit camarade n'aura qu'à cliquer pour récupérer les fichiers/dossiers regroupés en un seul ZIP. Une fois que le transfert sera terminé, le serveur qui aura été créé sur votre machine va automatiquement s'arrêter si vous avez cliqué sur la case idoine.

NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC

+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3,50 €

Chez votre marchand de journaux

CRYPTEZ TOUT CE QUE VOUS METTEZ SUR VOTRE CLOUD !

Vous n'avez pas envie de changer vos habitudes et d'opter pour un cloud chiffré à la base, pourquoi ne pas continuer à utiliser Dropbox, OneDrive ou Google Drive en y ajoutant votre grain de sel? Cryptomator permet simplement de chiffrer vos fichiers avant de les envoyer n'importe où...

Depuis les révélations d'Edward Snowden sur les petites habitudes de la NSA, on sait bien qu'il est impossible de faire confiance aux services qui stockent vos fichiers. Pour être sûr à 100 % que vos fichiers sont entre de bonnes mains, il suffit de les chiffrer ! BoxCryptor, une application permettant de chiffrer en AES256 vos documents et de les envoyer sur le service de stockage de votre choix.

DES FICHIERS PERSONNELS À L'ABRI

Si vous avez un PC, un Mac, un appareil Android ou iOS, il existe forcément une version pour vous à télécharger sur le site. Une fois sur votre cloud, même si un petit curieux met son nez dans votre compte il ne pourra savoir de quoi il retourne. Alors bien sûr, BoxCryptor n'a pas que des avantages puisque le service est payant si vous utilisez plus de deux appareils ou si vous utilisez plus d'un hébergeur, mais la version gratuite permet quand même de se faire un avis avant de passer à la caisse (36 €/an avec des tarifs dégressifs).

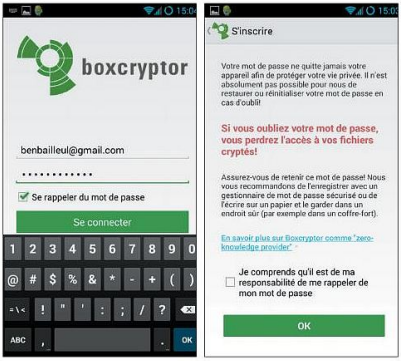
BoxCryptor est très simple à prendre en main et toutes les fonctionnalités de base sont gratuites

Premiers pas avec BoxCryptor

INFOS [BOXCRYPTOR]
Où le trouver ? [www.boxcryptor.com] Difficulté :
TUTO

01› INSTALLATION

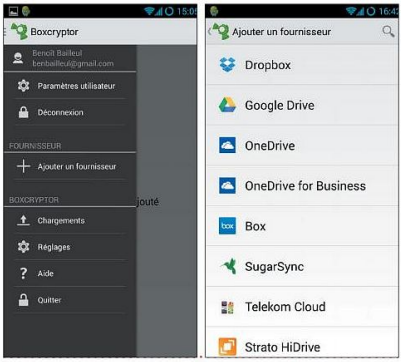
Passez la présentation en faisant défiler vers la droite et ouvrez-vous un compte en appuyant sur **S'inscrire**. Renseignez les champs et confirmez que vous comprenez les



risques du chiffrement en cochant la case (si vos perdez votre mot de passe, BoxCryptor ne pourra pas vous le rendre). Confirmez l'utilisation de BoxCryptor depuis votre boîte aux lettres.

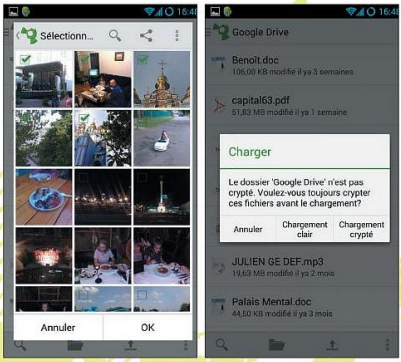
02› LE FOURNISSEUR

Depuis le panneau latéral (un appui sur le logo **BoxCryptor**), faites **Ajouter un fournisseur**. Dans notre cas nous avons choisi Google Drive mais vous en trouverez une vingtaine d'autres. Vous verrez alors les dossiers/fichiers déjà présents sur votre cloud. Attention ces derniers ne seront pas chiffrés automatiquement. N'oubliez pas de valider cette nouvelle activité sur votre compte mail (par exemple Google vous demandera si vous êtes bien à l'origine de cette connexion).



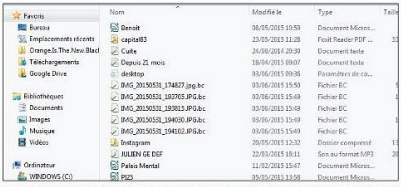
03› UPLOAD DES FICHIERS

En bas de l'interface, vous trouverez un petit bouton pour uploader. Choisissez de quel type de fichier il s'agit et sélectionnez-les dans la liste. Choisissez le **Chargement crypté** et vos fichiers (ici des photos) iront dans votre compte Google Drive. Attention, ils ne seront pas protégés en écriture (un pirate pourra les effacer).



04› ATTENTION À LA SÉCURITÉ !

Notez que dans la version gratuite, les noms des fichiers ne sont pas chiffrés : nos photos apparaîtront donc en tant que **XXXXX.JPG. bc**. Bien sûr vous pourrez les renommer pour brouiller les pistes. Sans votre mot de passe, un pirate qui aura accès à votre compte Google ne pourra pas les afficher. Par contre sur votre appareil, les photos ne seront pas chiffrées à leur emplacement d'origine, il convient donc de bien protéger l'accès à votre téléphone en cas de vol (ou de les effacer au fur et à mesure avec une appli spécialisée).

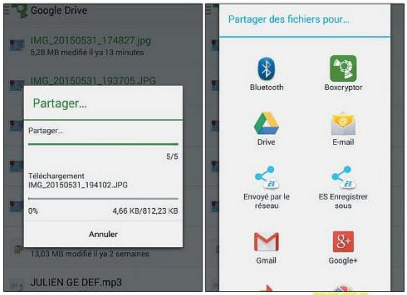


05› SUR D'AUTRES APPAREILS

Pour plus de clarté entre les documents chiffrés et ceux qui ne le sont pas, vous avez la possibilité de créer un **Dossier crypté**. Pour accéder à ces fichiers/dossiers cryptés depuis un autre appareil, il suffit d'installer BoxCryptor sur votre PC, Mac ou un autre appareil compatible muni de vos identifiants.

06› LE PARTAGE

Pour partager vos photos avec d'autres personnes, il suffit de les sélectionner dans l'interface et de sélectionner l'icône partage (les trois petits points reliés par deux traits). BoxCryptor ira déchiffrer les fichiers à la volée et vous proposer une liste d'applis installées : Gmail, Whatsapp, Bluetooth, Facebook, etc. Vos amis recevront les fichiers «en clair».



LES SERVICES DE CLOUD COMPATIBLES

BoxCryptor est compatible avec une trentaine d'hébergeurs dont certains sont presque inconnus. Vous trouverez la liste à cette adresse : **www.boxcryptor.com/fr/provider**. Ci-dessous les clouds les plus utilisés en France... Vous disposez d'un NAS à la maison ? BoxCryptor le prendra aussi en charge !

Dropbox : **www.dropbox.com/fr**

Google Drive : **https://drive.google.com**

Microsoft OneDrive : **https://onedrive.live.com**

SugarSync : **www.sugarsync.com**

Box.net : **www.box.ne**

CRYPTOMATOR : CHIFFREZ DANS LE CLOUD OU SUR VOTRE PC

Cryptomator est un logiciel très utile : il va vous permettre de chiffrer vos fichiers pour les protéger. C'est facile et cela fonctionne en local sur votre ordinateur et dans votre cloud préféré...

Protéger ses données personnelles est devenu un enjeu majeur ces dernières années : impossible de les utiliser contre vous ou de vous voler puisqu'elles seront inutilisables en l'état. Avec Cryptomator, vous pouvez décider de chiffrer des dossiers locaux ou chiffrer les dossiers qui sont connectés à votre cloud, ainsi toutes les données hébergées ' dans les nuages ' seront elles aussi inaccessibles. Cryptomator est un logiciel open source et qui permet de chiffrer en AES tous les fichiers que vous voulez mettre sur Dropbox, Google Drive ou autre. Il suffit de spécifiez le dossier qui vous intéresse (votre répertoire Dropbox par exemple), mettre un mot de passe bien solide et de créer un disque virtuel chiffré sur votre cloud, qui sera monté sur votre ordinateur. Le logiciel est gratuit (vous donnez ce que vous voulez) et il est disponible sous Windows, MacOS, Linux, Android et iOS.

Open source, multi-plate-forme et gratuit, Cryptomator n'a que des avantages...

Chiffrez vos fichiers stockés

INFOS [CRYPTOMATOR]
Où le trouver ? [https://cryptomator.org] Difficulté :

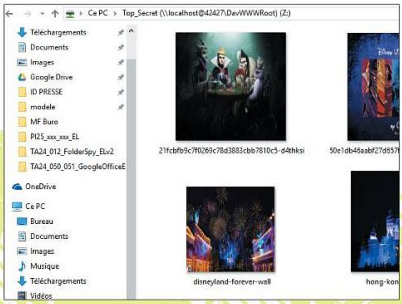
TUTO

01 › CRÉER L'ESPACE

Lancez le logiciel et cliquez sur le **+ créer un nouveau coffre** en bas à gauche. Sélectionnez le dossier de votre service de Cloud, Google Drive dans notre exemple, choisissez un nom pour votre coffre-fort et faites **Enregistrer**. Définissez un mot de passe sécurisé pour ne pas compromettre vos données puis cliquez sur **Créer le coffre.**

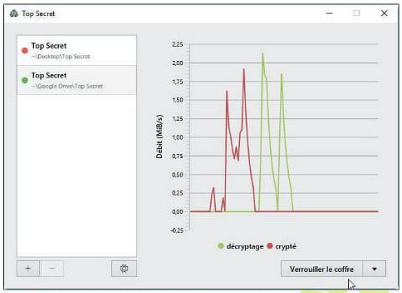
02 › Y STOCKER SES FICHIERS

Votre coffre est verrouillé d'office. Entrez le mot de passe précédemment renseigné et cliquez sur **Déverrouiller le coffre**. Cryptomator ouvre automatiquement le dossier virtuel dans lequel vous pouvez placer tous vos fichiers.



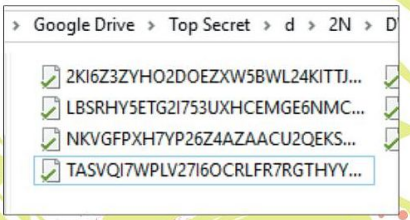
03 › VERROUILLER L'ESPACE

Le logiciel affiche également un graphique de débit de cryptage et décryptage. Pour surveiller qu'il fait bien son travail. Une fois que vos fichiers sont bien dans votre coffre, cliquez **sur Verrouiller le coffre**. Vous pouvez voir dans le poste de travail que le lecteur virtuel a disparu.



04 › VÉRIFIER LA SÉCURITÉ

Le coffre verrouillé, personne ne peut y accéder. Allez dans le dossier de votre Cloud sur votre PC, il y a bien votre dossier, mais les fichiers sont illisibles. Idem sur le site du Cloud, si quelqu'un télécharge les fichiers, il ne pourra pas les lire. Vos fichiers sont définitivement à l'abri tant que le coffre est verrouillé. Si vous oubliez le mot de passe, vos fichiers sont définitivement perdus.



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.

EN LOCAL

WINDOWS 10, CE PETIT CURIEUX...

Le M de GAFAM correspond à Microsoft. La société créée par Bill Gates, même si elle a raté le tournant « mobile », est encore un géant de l'informatique. Copiant sur ses concurrents Google et Apple, la firme de Redmond a intégré pas mal de mouchards dans son Windows 10. Il s'agit officiellement d'améliorer « l'expérience utilisateur »... Bien sûr !

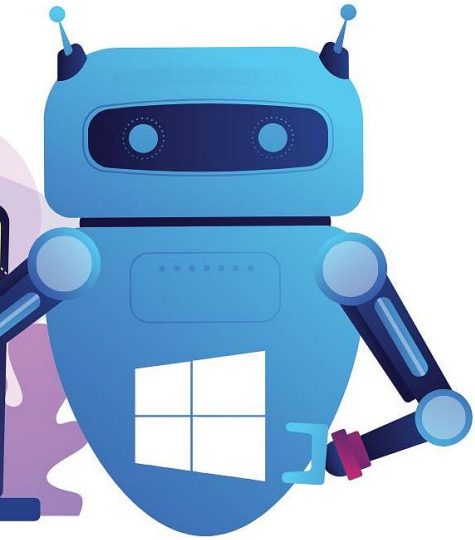
Dans son OS Windows 10, la société américaine se permet par défaut de scruter ce que nous tapons sur notre clavier, d'écouter les requêtes que nous faisons à Cortana, de potentiellement s'emparer du contrôle de la webcam, de nous localiser ou de lire nos SMS ! C'est terrible, mais c'est exactement ce que font Google et Apple sur leurs systèmes et services respectifs. Bien sûr, ce n'est pas une raison pour accepter sans broncher cette politique de l'espionnage...

DES ESPIONS DOCILES...

Car Microsoft a eu la bonne idée de presque tout mettre dans le même menu et même de nous expliquer exactement à chaque fois ce que Windows espionne. Lorsque Windows 10 vous dit qu'il veut « *apprendre à reconnaître votre voix* » et « *collecter [...] l'historique des frappes* » pour proposer de meilleures suggestions il faut lire « *enregistrer tout ce que vous racontez et ce que vous écrivez pour mieux vous vendre des trucs par la suite* ». Il faut savoir lire entre les lignes donc... Pour aller plus loin dans cette lutte contre la surveillance de Microsoft, nous allons vous présenter différents logiciels permettant d'automatiser les réglages pour un peu plus de confidentialité.

INSTALLATION

Mais avant cela, rappelons qu'il est assez facile de refuser ces incursions dans notre vie privée, et ce, dès l'installation de Windows 10. Même si vous êtes pressés d'utiliser votre nouvel OS, lisez bien les messages avant de cliquer sur **Suivant**. De même, soyez



prudent lors des mises à jour. Lorsque vous accédez à l'écran **Démarrer rapidement**, cliquez sur **Paramètres de personnalisation**. C'est ici que vous déciderez transmettre des informations à Microsoft sur votre géolocalisation, sur votre calendrier, etc. Il vous sera aussi possible de refuser ou non l'accès des applications et des "partenaires" de Microsoft à votre **Identifiant de publicité**, ainsi qu'aux informations sur votre géolocalisation. Vous pourrez en outre choisir de ne pas envoyer aux serveurs de Microsoft vos **Données de navigation**. Enfin, et même si cela deviendra bientôt obligatoire, vous n'êtes pas obligé de créer un compte Microsoft. Bien sûr on vous incitera à le faire, mais vous pouvez très bien opter pour un compte local...comme au bon vieux temps d'XP. Faites **Ignorer cette étape**.

DÉSACTIVEZ LES APPLICATIONS DU WINDOWS STORE

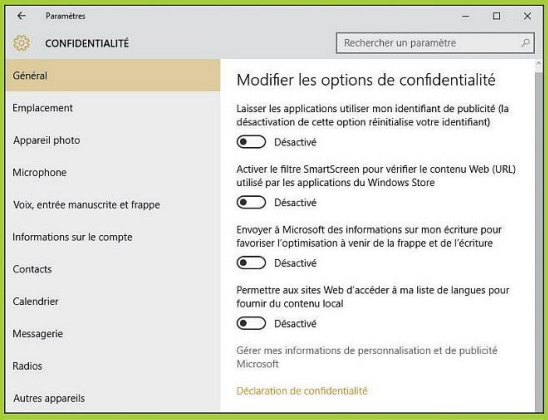
Depuis Windows 8, Microsoft essaie de réunir les utilisateurs mobiles et PC en créant une interface commune et des applications (les fameuses tuiles Metro ou ModernUI). Même si Windows 10 revient un peu en arrière en proposant de base un bureau « standard », ces applications sont toujours de la partie. Sur Windows 10, ces applis préinstallées sont au nombre de 23 sur votre système : Photos, Xbox, Store, Money, Maps, etc. Si vous utilisez Windows 10 sur un PC et que vous ne comptez pas acheter d'appareil mobile avec l'OS de Microsoft, ces applications sont complètement superflues puisque vous avez déjà vos programmes « desktop » préférés. Le logiciel 10Appsmanager va enterrer ces « tuiles » pour ne plus jamais les voir dans votre menu démarrer ou ailleurs.

Lien : **http://goo.gl/YMUr5y**

MICROSOFT N'ÉTAIT PAS CONNU POUR ESPIONNER SES UTILISATEURS, MAIS COMME ON NE DIT RIEN À GOOGLE ET AUX AUTRES, ILS NE SE GÊNENT PLUS...

DÉSACTIVER LES MOUCHARDS DE MICROSOFT « À LA MAIN »

Dans notre dernier numéro, nous avons vu où se trouvaient les paramètres de confidentialité,mais nous allons revenir brièvement dessus avant d'aller encore plus loin. Allez dans **Paramètres** depuis le menu **Démarrer** puis **Confidentialité**. Dans **Général** désactivez l'envoi d'information sur vos frappes. Dans **Emplacement**, il est possible de désactiver l'envoi de votre position ou de choisir quelles applis pourraient y avoir accès. Dans **Appareil photo**, désactivez l'accès à votre webcam et faites de même pour votre microphone dans l'onglet **suivant**. Dans **Voix**, entrée manuscrite et frappe, cliquez sur **Arrêter de me connaître** pour rendre Cortana sourde et aveugle. Enfin, si vous n'avez pas d'antivirus tiers, Windows Defender sera alors activé par défaut (ce que nous déconseillons fortement). Ce logiciel enverra aussi des informations chez Microsoft si vous ne l'empêchez pas ! Allez dans **Paramètres > Mise à jour et sécurité > Windows Defender** et désactivez **Envoi d'un échantillon** et **Protection dans le cloud**.



Microsoft a échoué avec son OS mobile, mais il a bien vu comment Android a gagné la guerre... Les données personnelles ont de la valeur et si vous dites « Ok Microsoft, espionne-moi », ils ne se feront pas prier.

Allons encore plus loin...

Phrozen.io ne propose plus ce logiciel sur son site officiel, mais il fonctionne toujours (suivez notre lien) ! Windows Privacy Tweaker lave plus blanc que blanc et vous permet de faire le ménage depuis une seule et même interface...

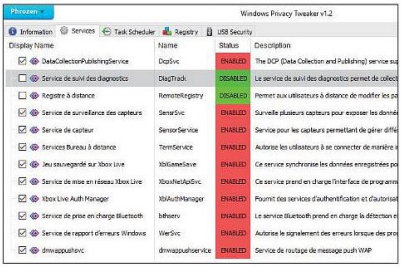
INFOS **[WINDOWS PRIVACY TWEAKER]**
Où le trouver ? [https://tinyurl.com/wmz2bbu] Difficulté : TUTO

01 › LE CODE COULEUR

L'utilisation de Windows Privacy Tweaker n'a vraiment rien de sorcier. Lorsque l'icône est verte, c'est que vous ne risquez pas de voir compromettre vos habitudes, vos données ou que les interactions entre votre PC et les serveurs de Microsoft sont désactivées. Même en ayant fait le ménage dans **Paramètres > Confidentialité** (comme expliqué dans le précédent pas-à-pas), vous verrez que la plupart des paramètres sont dans le rouge...

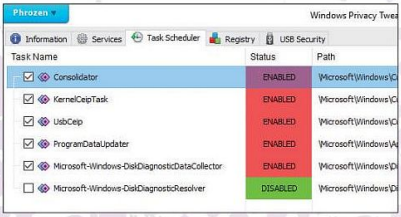
02 › LES SERVICES WINDOWS

Dans l'onglet **Services**, vous pouvez par exemple désactiver le **DcpSvc** qui permet à certaines applis d'uploader des données dans un cloud propriétaire. Pour chaque ligne, vous trouverez une description en français. Pas la peine de désactiver les fonctions jeu Xbox si vous possédez cette console et que vous souhaitez synchroniser les informations du Live avec votre PC. À l'inverse, avez-vous vraiment besoin du **Service de bureau à Distance**, du **SensorService** ou du **Registre à distance** ?



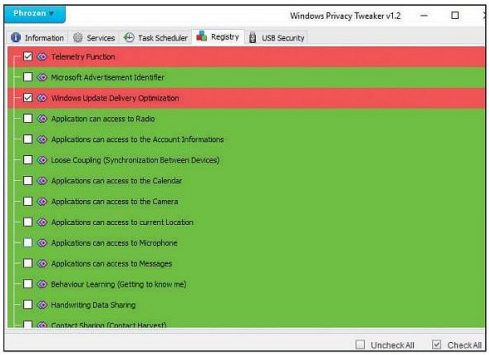
03 › LE PLANIFICATEUR DE TÂCHES

Dans **Task Scheduler**, il s'agit autant de fuites de données que d'opérations réalisées sur votre système à votre insu: diagnostic de vos disques durs, vérification des mises à jour de certains programmes, statistiques liées à vos périphériques USB, etc. Consolidator est aussi un mouchard qui envoie des données sur vos petites habitudes. Vous pouvez tout remettre en **DISABLED** et revenir en arrière si vous connaissez des problèmes avec certaines fonctions.



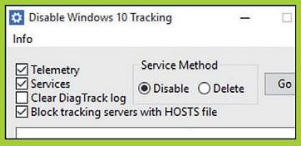
04 › LA BASE DE REGISTRE

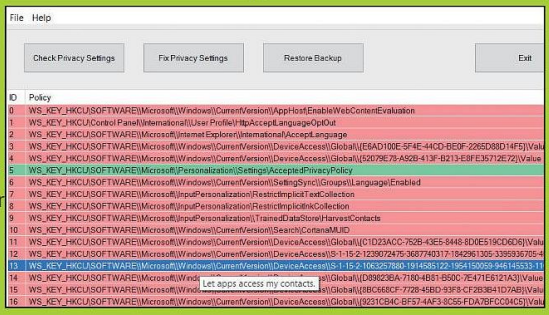
Ce qui se trouve dans **Registry** est plus complexe, mais si vous avez suivi notre précédent pas-à-pas, la plupart des lignes devraient être vertes (accès au Calendrier, au micro, géolocalisation, etc.) Décochez **Telemetry Function** et **Windows Update Delivery Optimization**. En bas, supprimez ce dont vous n'avez pas besoin : **Bing, Smartscreen, Microsoft Feedback**, etc. Dans le doute, virez tout ! Le dernier onglet permet de mettre les clés USB en lecture seule, mais ce n'est vraiment pas nécessaire.



DEUX SOLUTIONS ALTERNATIVES

Disable Win Tracking propose peu ou prou la même chose que Windows Privacy Tweaker. Lancez ce logiciel en mode administrateur, cochez toutes les cases et laissez l'option Disable. Une fois terminé, faites Get privacy et laissez les différentes fenêtres s'ouvrir et se fermer. À la fin du processus, une fenêtre vous fera un compte-rendu détaillé de ce qui a été fait (suppression de la télémétrie, de la traque d'IP, etc.). Redémarrez le système pour que les modifications soient prises en compte. Pour revenir en arrière, il faudra tout cocher et faire Revert. Fix Windows 10 Privacy est l'autre solution que nous vous proposons. Plutôt que de devoir fouiller dans la base de registre, ce logiciel vous propose une compilation des réglages pour empêcher Windows d'être trop curieux. Toutes les clés traitées par le soft sont clairement identifiées, et l'opération est complètement réversible à tout moment. En outre, FW10P est entièrement gratuit et open source.





Lien : **https://goo.gl/oVBdwZ**
Lien : **https://modzero.github.io/fix-windows-privacy/**

TRUPAX : LE CHIFFREMENT SUR MESURE

TruPax fonctionne différemment des autres logiciels de chiffrement : au lieu de créer un espace défini où vous mettriez vos fichiers sensibles, TruPax ajuste la taille du conteneur au fichier que vous voulez chiffrer. La sécurité sans prise de tête !

Le très bon logiciel VeraCrypt ne permettant pas de faire des conteneurs sur mesure, nous vous présentons ici TruPax. Alors pourquoi utiliser ce logiciel ? Avec VeraCrypt par exemple (voir les microfiches pages suivantes), l'espace chiffré que vous avez créé est fixe. S'il devient trop réduit, il faudra tout refaire. Pas très pratique pour envoyer des fichiers chiffrés sur le cloud ou à un ami. TruPax propose de chiffrer un fichier ou un dossier à la demande. Chaque élément sera considéré comme un conteneur à part entière. Plus besoin de créer des volumes chiffrés trop grands de peur de manquer de place un jour. Pas de problème d'interopérabilité puisque les conteneurs sont formatés en UDF, un système de fichier qui peut être exporté sur plusieurs OS. Bien sûr, les sources sont disponibles et il est possible d'utiliser TruPax dans vos propres applications.

PLUS BESOIN DE PARAMÉTRER UN VOLUME CHIFFRÉ EN AMONT !

Chiffrez vos fichiers sensibles

INFOS [TRUPAX]
Où le trouver ? [https://coderslagoon.com] Difficulté :

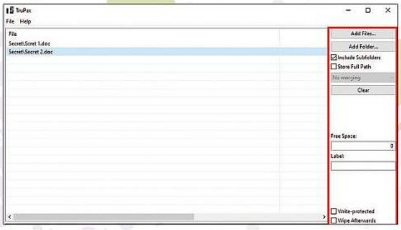
TUTO

01 › CRÉER LE DOSSIER

Téléchargez TruPax, décompressez le dossier, et lancez **install**. Double-cliquez sur le raccourci créé sur le bureau et choisissez la langue anglaise (**English**). Faites un glisser-déposer des éléments à chiffrer dans la fenêtre principale ou cliquez sur **Add Files** (fichiers) ou **Add Folder** (dossier). Intégrez les sous-répertoires en cochant **Include Subfolders**.

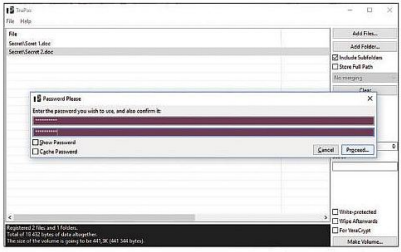
02 › CONSULTER LES OPTIONS

No Merging signifie que les éléments ne seront pas combinés lors du chiffrement (dans le cas où les noms des dossiers seraient les mêmes par exemple). **Free Space** permet de garder un peu de place pour ajouter des fichiers ou pour des mises à jour. Cochez **Wipe Afterwards** pour effacer les éléments qui auront été chiffrés dans leur répertoire d'origine.



03 › CHIFFRER

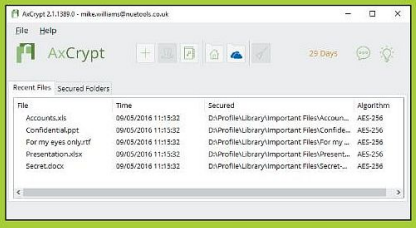
Lorsque tout est près, cliquez sur **Make Volume**. Choisissez un dossier, tapez un nom pour le conteneur crypté et faites **Enregistrer**. Spécifiez un mot de passe et validez avec **Proceed**. Cocher **Cache Password** l'enregistre sur le PC pour ne pas avoir à le retaper (attention que personne d'autre n'y accède) et surtout gardez le mot de passe en cas de panne.



04 › DÉCHIFFRER

Vous obtenez un fichier en **.tc**. Pour le décrypter, cliquez sur **Clear** dans TruPax et glissez-déposez le fichier **.tc** dans la fenêtre. **Extract** extrait le tout, tandis que **Invalidate** détruit la clé, ce qui empêche quiconque (même vous) d'accéder au contenu. Utile en cas d'oubli du mot de passe. Faites **Extract**, spécifiez l'emplacement, tapez votre mot de passe et validez avec **Proceed**.

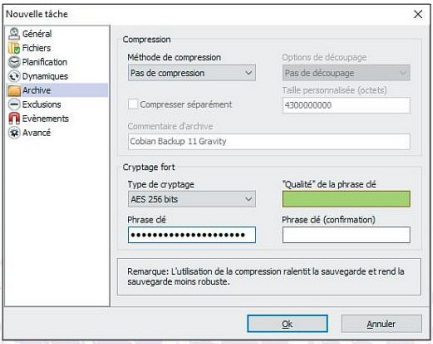
Un chiffrement simple → avec AxCrypt



AxCrypt est un logiciel de chiffrement qui va au plus simple. L'interface graphique est réduite à sa plus simple expression et la plupart des fonctionnalités sont accessibles via le menu contextuel du clic droit. Il suffit de pointer un dossier ou un fichier puis de faire un clic droit pour voir apparaître : **Crypter**, **Crypter et créer un exécutable** et **Brouiller et supprimer**. La deuxième option permet d'envoyer un document à une personne qui ne possède pas le logiciel tandis que la troisième va effacer toute trace du fichier/dossier cible en réécrivant des données aléatoires à son emplacement d'origine. Notez que l'algorithme d'AxCrypt est de l'AES 128 d'où la nécessité de se choisir un mot de passe correct pour éviter le «Brute Force». Cet algo est suffisamment costaud pour protéger vos données en local, mais est un peu léger si vous voulez chiffrer des documents professionnels en ligne par exemple. Pourquoi ne pas utiliser AxCrypt en seconde passe alors ?

Lien : **www.axcrypt.net**

Sauvegarde chiffrée → avec Cobian Backup



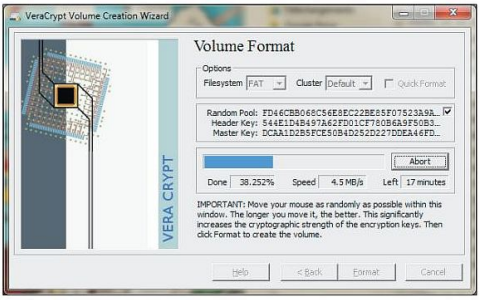
Vous sauvegardez vos données en cas de crash ? Très bien ! Le problème c'est que vos données ne sont pas à l'abri en cas de vol. La solution ? Chiffrer vos backups ! Cobian Backup propose à peu près les mêmes options que la plupart des logiciels de sauvegarde tout en restant plus facile d'accès, mais surtout en ajoutant une couche de chiffrement pour éviter que vos données ne tombent entre de mauvaises mains. Gratuit et régulièrement mis à jour, ce dernier permet de faire des sauvegardes standards ou incrémentielles qui peuvent être compressées pour gagner de la place et surtout programmées pour ne pas avoir à y penser lorsqu'il est déjà trop tard ! Cobian Backup gère parfaitement la technologie Volume Shadow Copy de Windows et permet de sauvegarder vers un disque externe, un serveur FTP ou un volume disponible sur votre réseau local. Compatible avec toutes les versions de Windows depuis XP, ce programme malin prend en charge le chiffrement AES 256 bits.

Lien : **www.cobiansoft.com**

Chiffrer un disque ou une clé USB

→ avec VeraCrypt

Chiffrer les données d'un disque dur vous permet de vous assurer de la confidentialité de ces données, même dans le cas où un attaquant a un accès physique au disque dur, par exemple dans le cas d'un vol d'ordinateur portable. Pour cela, vous pouvez utiliser VeraCrypt, un logiciel open source et gratuit de chiffrement de données. VeraCrypt permet de chiffrer et déchiffrer les données à la volée, c'est-à-dire de manière transparente pour l'utilisateur et le système. Il est possible de créer un volume chiffré sur un disque dur, une partition ou une clé USB.



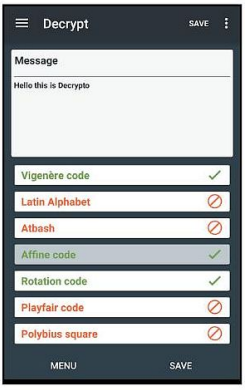
Lien : **www.veracrypt.fr**

Protégez vos mots de passe → avec Clood MdP

Vous le savez, choisir le même mot de passe partout est aussi dangereux que d'utiliser des mots de passe de SEGPA (toto123, azerty ou PSGmonAmour). Pourtant, faites-vous vraiment l'effort de choisir des mots de passe comme A5)D69J;&lKi89 pour chacun de vos sites et services ? Si la réponse est non, Clood MdP est la solution que vous attendiez. En effet, Clood MdP permet de générer et gérer vos mots de passe depuis une seule interface. Inscrivez-vous gratuitement et choisissez une clé de dérivation de 8 caractères qui va être utilisée pour ajouter un peu d'aléatoire lors de la génération de vos mots de passe (cette suite est la seule chose à mémoriser). Libre à vous ensuite de choisir si vous voulez que vos mots de passe soient générés avec des minuscules, des majuscules, des chiffres et des caractères spéciaux (oui, ceux-là, vous les voulez !). Sélectionnez ensuite la longueur, tout en sachant que 12 est le minimum de nos jours. Ce mot de passe sera enregistré dans l'appli et sera accessible via copier-coller. Il suffit de coller directement un mot de passe dans le champ adéquat. L'authentification à l'appli est sécurisée (mot de passe plus un deuxième facteur via un code SMS) et elle ne stocke rien dans sa base de données. Bien sûr la synchronisation est de mise entre vos différents appareils (ordinateur, mobile, tablette, etc.)

Lien : **https://tinyurl.com/wq3bfkj**

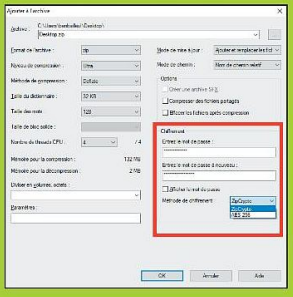
Un coffre fort sur Android → avec Decrypto



Decrypto est une application fournissant une série d'outils de cryptage et de décryptage de textes. Plus de 25 techniques traditionnelles de cryptage sont implémentées, comme le code César, le code ASCII ou encore le code de Vigenère. Une explication ainsi qu'un historique sont fournis avec chaque type de chiffrement, permettant de mieux comprendre ceux-ci. Si vous possédez un message crypté, mais que vous ne connaissez pas le type de code, l'application peut tenter de déchiffrer le message pour vous ! En effet, un outil permet de tester les différents types de codes et d'afficher les résultats possibles sur base d'un dictionnaire. Un outil d'analyse fréquentielle de textes cryptés est également disponible. Vous pourrez en quelques clics savoir exactement le nombre d'occurrences de chaque lettre présente dans votre texte. Encore mieux, l'application peut effectuer une analyse fréquentielle et remplacer chaque lettre du message crypté par la lettre décryptée la plus probable ! Vous pouvez également enregistrer vos messages cryptés afin de les consulter plus tard, ou encore les partager avec vos amis !

Lien : **https://tinyurl.com/yxy88of5**

Protégez une archive par mot de passe → avec 7-Zip



Pour interdire l'ouverture d'une archive, nous allons utiliser le logiciel gratuit 7-Zip. Il permet de créer des fichiers ZIP, TAR, WIM, etc. Il dispose en plus de son propre format très performant, le 7Z. Téléchargez ce logiciel en fonction de votre système d'exploitation (32 ou 64 bits). Si vous ne le savez pas, faites un clic droit dans **Ordinateur** ou **Ce PC** (menu démarrer) et cliquez sur **Propriétés**. Après avoir choisi un dossier, un fichier ou un groupe de fichiers, faites un clic droit puis dans le menu contextuel, sélectionnez **7-Zip** > **Ajouter à l'archive...** Vous pourrez ici choisir le format, le niveau de compression et d'autres données techniques qu'il vaut mieux laisser par défaut. Dans la partie **Chiffrement**, entrez votre mot de passe (sans caractères accentués). Notez que selon le format d'archives choisi vous pouvez changer la méthode. Restez sur l'**AES-256** plus sûr que **ZipCrypto**.

Lien : **www.7-zip.org**

CHEZ VOTRE
MARCHAND DE JOURNAUX

LES PIRATES CRYPTENT, NOS LECTEURS DÉCRYPTENT !

WI-FI,
ANONYME,
MOBILES,
HACKING,
ENCODAGE,
ANTIVOL,
CRYPTAGE,
MOTS DE PASSE,
SURVEILLANCE

NOUVELLE FORMULE
68 PAGES !

VIE PRIVÉE
SURVEILLANCE
BIG DATA

NE SOYEZ PLUS UNE VICTIME

BEL/LUX/PORT CONT. : 4,60 € - CH : 6 FS – DOM/S : 4,70 € - POL/S : 660 XPF - N CAL/S : 620 XPF - MAROC : 43 DH

L 14376 - 23 - F: 3,50 € - RD

IDPRESSE