Vous et Votre Mac

Vous et Votre Mac

N° 136 • Septembre 2017 100 % Mac en pratique

- Développer les RAW gratuitement !
- Les petits secrets de *À propos de ce Mac...*
- Des apps sympas pour prendre des notes.
- 8 outils pour surveiller vos connexions.

Gros plan sur **Calibre**

L'application gratuite incontournable pour gérer tous vos livres numériques.

Les nouvelles fonctions clés d'iOS

4 docks Thunderbolt 3 à l'essai

Les nouveaux MacBook Pro n'ont plus que des prises Thunderbolt 3. Soit vous multipliez les adaptateurs à tout va, soit vous privilégiez la solution plus pratique et pas plus onéreuse du dock !

FRANCE métropolitaine : 5,90 € • SUISSE : 9,90 FS
DOM - BEL - MUX - PORT CONT : 6,90 € • CANADA 10,99 $
L 11206 - 136 H - F : 5,90 € - RD

Envoyer des messages confidentiels en toute simplicité

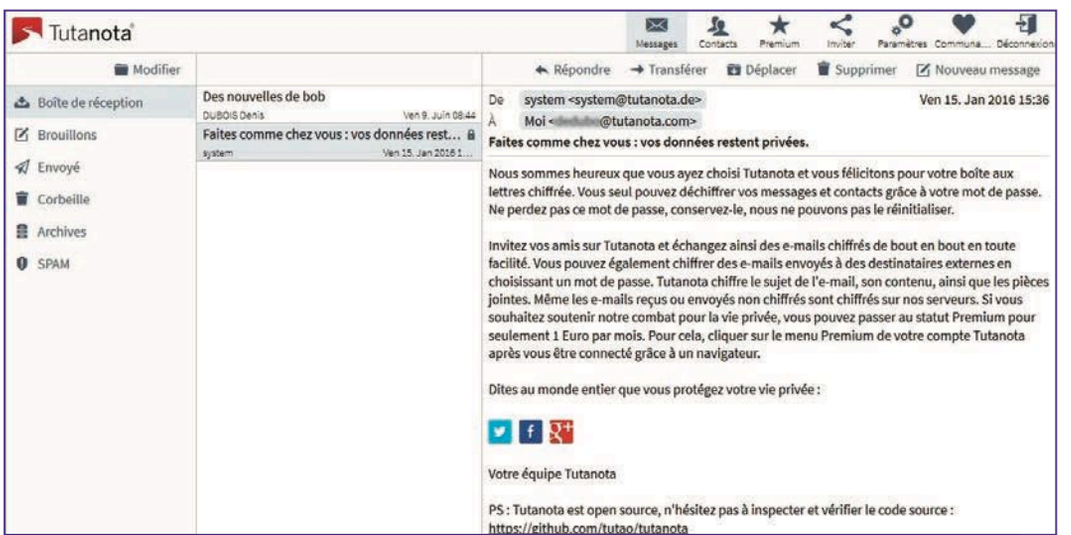
La plupart des solutions de chiffrement d'e-mails nécessitent que chacun de vos contacts adopte le même service, ce qui n'est pas évident à faire. Ce problème ralentit notablement l'adoption de ces solutions pourtant indispensables à la confidentialité des correspondances. Tutanota propose un service de webmail astucieux qui s'affranchit de cette contrainte !

Tutanota

J'AIME
La simplicité d'utilisation ; la transparence du chiffrement (entre deux utilisateurs enregistrés) ; le fait de pouvoir communiquer avec tous ses contacts, de façon confidentielle ou non.

J'AIME MOINS
Quelques métadonnées ne sont pas anonymes ; peu de fonctions avancées dans la version gratuite.

FRANÇAIS
Prix : gratuit • Éditeur : Tutao
https://tutanota.com/fr
App iOS sur l'iOS App Store d'Apple

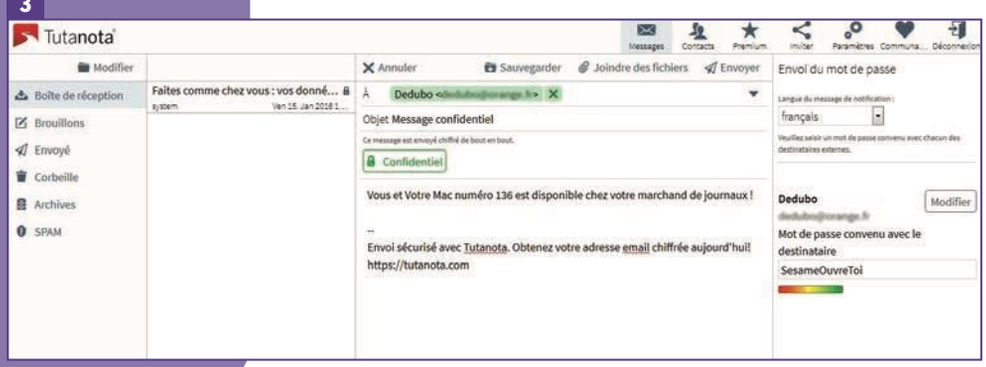


1

Vous pensez, comme la plupart des internautes, que vos e-mails sont protégés, à l'abri des indiscrétions ? Comme une lettre dans son enveloppe ? Si le chiffrement des messages pendant leur acheminement est de plus en plus répandu, afin d'empêcher leur accès non autorisé pendant leur transit, cela ne présage en rien de leur confidentialité ! Car les messages s'apparentent plus à des cartes postales puisqu'ils sont généralement stockés en clair, sous forme lisible, sur les serveurs de votre fournisseur, comme sur chacun des serveurs intermédiaires traversés jusqu'à leur destinataire final. Sur chaque serveur, ils sont à la merci des indiscrétions du fournisseur du service, d'une potentielle intrusion, comme Yahoo Mail en a été victime à plusieurs reprises (http://bit.ly/2tlGK3g), ou des ingérences gouvernementales plus ou moins légales (http://bit.ly/2rvaRUc). Sans parler de leur exploitation à des fins mercantiles, comme avec Gmail dont les robots analysent le contenu des courriels pour cibler vos centres d'intérêt afin d'afficher des bandeaux publicitaires « sur mesure » (http://bit.ly/2rgCktS).

Si vous avez des informations privées, sensibles ou confidentielles à envoyer, il est recommandé d'utiliser une messagerie sécurisée qui rendra vos messages et leurs métadonnées en tout ou partie illisibles, tout en vous assurant un relatif anonymat. Depuis les révélations de Snowden, l'offre explose. Mais attention : toutes les messageries « sécurisées » ne se valent pas. De nombreux critères sont à prendre en compte : facilité d'utilisation, type de chiffrement, accès ou non au code source. Est-ce que l'entreprise conserve ou non les clés de chiffrement, est-ce que la solution prend en compte la protection des métadonnées (sujet du message, date et heure d'envoi, adresses IP, adresses de l'expéditeur et du destinataire) ? L'absence sur le site du service d'une information claire et détaillée sur ces questions est rédhibitoire. La transparence doit être la règle en matière de sécurité !

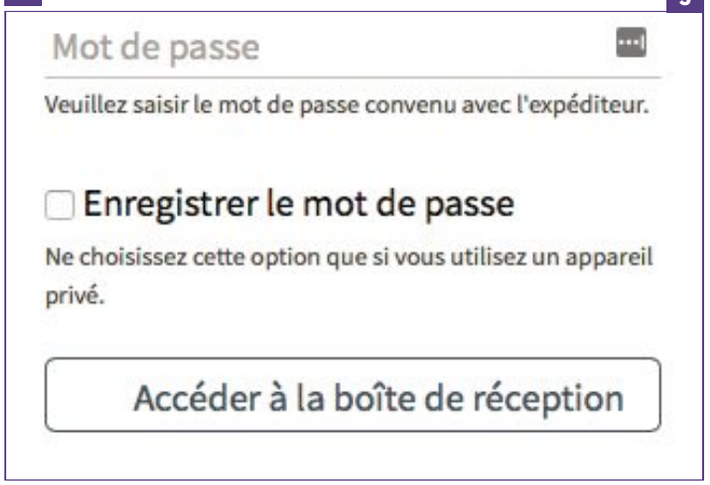
3



ACCÈS PAR LE WEB SUR MAC, PLUS UNE APP SUR IOS

Tutanota est un service de messagerie en ligne (webmail) sécurisé (les messages sont chiffrés), open source avec son code source

4



5

disponible sur Github (**https://github.com/tutao/tutanota**) et libre (licence GPLv3). Il a été développé par trois anciens étudiants allemands, devenus experts en chiffrement, engagés et militants pour la vie privée et contre la surveillance de masse. Le nom vient de la combinaison de deux mots latins, «tuta» (sécurisé) et «nota» (message ou note). C'est un webmail gratuit **[1]** (une version payante est aussi proposée). Sur Mac comme sur tout ordinateur, on y accédera via un navigateur web. Il y a en revanche des applications pour iOS **[2]** et pour Android. Tutanota effectue un chiffrement de bout en bout, c'est-à-dire que les messages sont chiffrés et déchiffrés en local dans le navigateur de l'expéditeur (ou dans l'app mobile) puis acheminés (via des «tuyaux» chiffrés SSL et DANE) vers les serveurs de Tutanota, situés en Allemagne, sous l'aile protectrice des strictes lois allemandes pour la vie privée. Tutanota n'utilise pas PGP, contrairement à GMX Caramail (VVMac 128), mais des algorithmes éprouvés comme RSA (2048 bits) et AES (128 bits) pour chiffrer automatiquement l'objet, le contenu du message ainsi que les pièces jointes (dans la limite de 25 Mo par message). La liste de vos contacts est également chiffrée. Les adresses IP des e-mails envoyés et reçus sont retirées, mais quelques métadonnées subsistent en clair et restent donc accessibles.

UN CHIFFREMENT DE BOUT EN BOUT

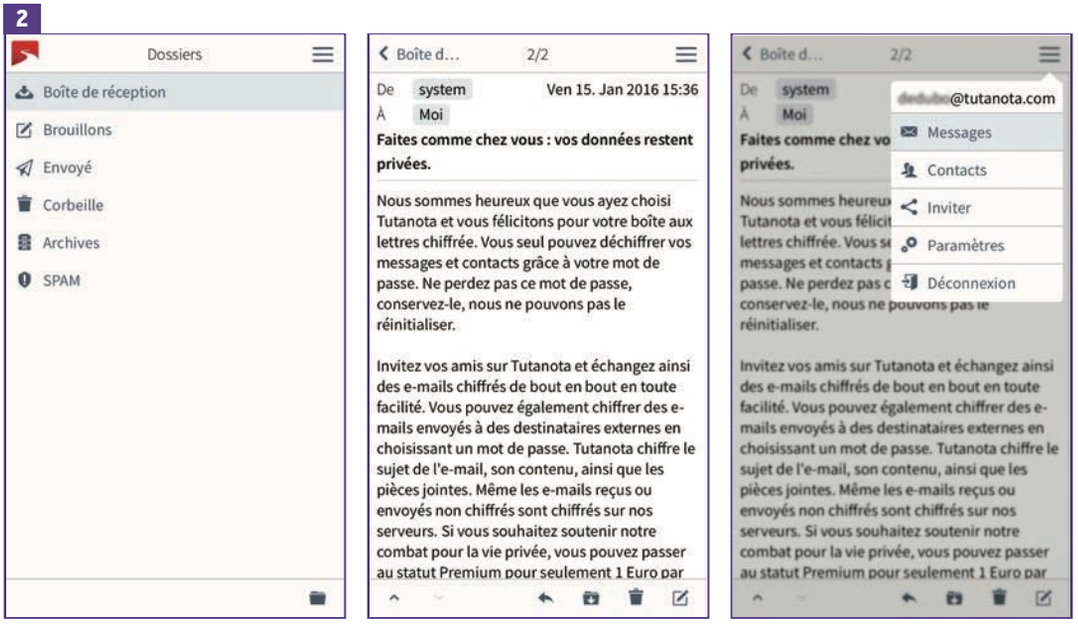
Tutanota présente quelques points originaux qui le distinguent de ses concurrents. Généralement, le point faible de ces services en ligne est la procédure d'inscription. Chez Tutanota, elle est anonyme ; aucune donnée personnelle n'est requise. Les fonctions payantes (optionnelles et plutôt destinées aux professionnels) peuvent même être réglées en Bitcoin (ce n'est pas anonyme, mais ça offre de fortes garanties de discrétion). Le processus de chiffrement est totalement transparent entre deux utilisateurs de Tutanota. Mais lorsque votre correspondant n'a pas de compte ? Tutanota est tout de même capable de lui expédier votre message. En ce la, il est différent de nombreux services similaires qui imposent à vos destinataires d'ouvrir un compte sur le même service pour pouvoir échanger des messages chiffrés – ce qui peut s'avérer fastidieux, surtout si vous avez de nombreux contacts !

Si votre message n'est pas confidentiel, il sera envoyé en clair via le classique protocole SMTP (Simple Mail Transfer Protocol), mais il sera toujours présent so us forme chiffrée sur les serveurs de Tutanota pour consultation (à l'abri des indiscrétions du service et des intrusions). En revanche, dans le cas d'un message confidentiel **[3]**, le destinataire reçoit un e-mail **[4]** contenant un lien pointant vers le site de Tutanota. Il sera ensuite invité à saisir le mot de passe **[5]** que vous aurez pris soin de lui communiquer préalablement via un canal sécurisé (de la m ain à la main, par SMS via l'app Signal…). Bien sûr, ce mot de passe d'authentification n'est pas diffusé en clair, seule son empreinte (hashage Bcrypt) non réversible est envoyée aux serveurs de Tutanota (et on ne peut pas reconstruire un mot de passe à partir d'elle). L'application iOS est, pour sa part, semblable au webmail où seules les options essentielles sont présentes (en tout cas pour la version g ratuite). La simplicité et l'efficacité l'emportent sur la richesse fonctionnelle, on ne s'en plaindra pas. Dans le futur, Tutanota compte proposer d'autres outils orientés vie privée chargés de se substituer à ceux de Google – un agenda, une application de prise de notes, un service de stockage. Le service envisage également la possibilité de cacher les métadonnées des messages confidentiels comme la date, l'expéditeur et le destinataire du message chiffré.

Si techniquement, Tutanota s'avère moins sécurisé que des solutions comme ProtonMail ou GMX Caramail, il est en revanche plus simple d'emploi, à la portée de tout un chacun. Tutanota peut donc être parfaitement utilisé en remplacement de votre client de messagerie habituel pour envoyer des messages «en clair». Il n'oblige pas vos interlocuteurs à adhé rer à cette solution pour pouvoir déchiffrer vos messages «confidentiels», mais la sécurité repose alors sur le choix du canal d'échange du mot de passe. Sa simplicité et surtout sa gratuité (et l'absence notable de publicité) sont des atouts indéniables.

DENIS DUBOIS (@DEDUBO)

2



Logitech Brio

J'AIME
La qualité de l'image ; la prise en charge du HDR ; l'application localisée et très simple.

J'AIME MOINS
Le prix élevé ; le manque d'applications pouvant déjà tirer pleinement partie de l'Ultra-HD 4K.

Prix : 239 €
Fabricant : Logitech
http://www.logitech.fr/fr-fr/product/brio
Téléchargement des pilotes :
http://bit.ly/2thWUKz

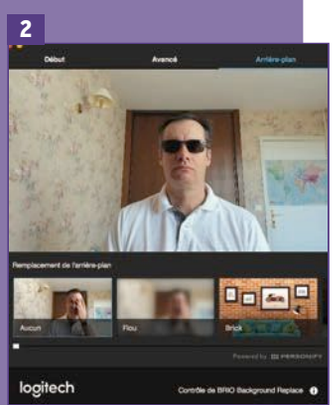
Une visio « pro » en Ultra-HD 4K

Logitech dévoile sa webcam Brio 4K qui se positionne d'emblée sur le marché professionnel de la visioconférence avec des caractéristiques et un prix en conséquence. Mais, si vous êtes un particulier adepte du streaming ou simplement exigeant, alors pourquoi ne pas casser la tirelire ?

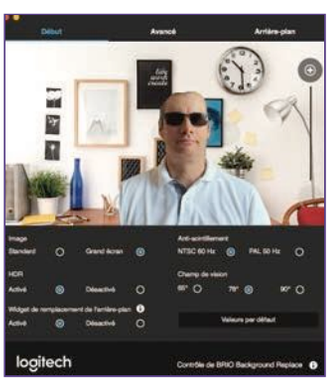
La caméra livrée se trouve placée et parfaitement protégée dans une petite boîte cartonnée de forme cubique, accompagnée d'un étui de transport et d'un cache de confidentialité en plastique (un peu toc). Ce dernier s'appose devant l'objectif pour bloquer toute indiscrétion. Un câble USB de bonne longueur est fourni ; il peut être branché sur un port USB 2.0 ou USB 3.0, même USB C. Pratique, un pas de vis standard permet de monter la webcam sur un trépied photo, à la place du clip de fixation fourni, ce que j'ai fait pour ma part puisque je n'ai pas suffisamment de place au-dessus de l'iMac à cause d'une étagère. Globalement, la qualité de fabrication se veut rassurante, solide.

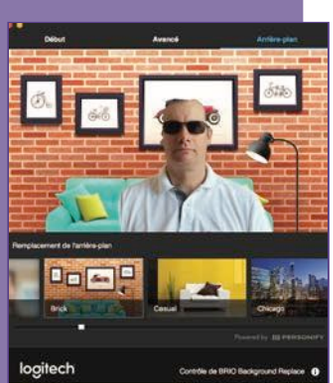
DEUX APPLICATIONS UTILES

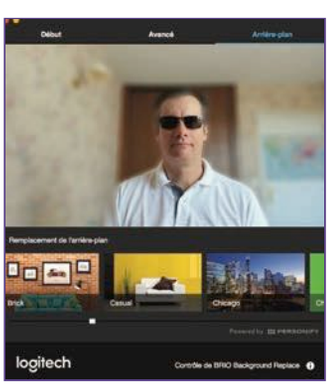
L'application Paramètre de la caméra ou Camera Settings [1] est d'usage optionnel mais, à mon avis, indispensable ! Il convient de la télécharger sur le site de Logitech.



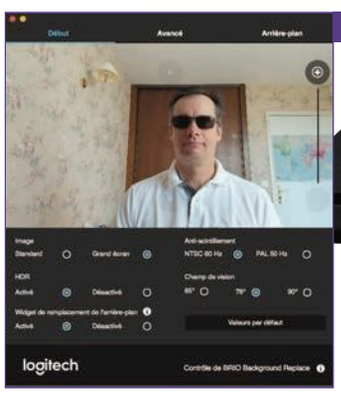
2





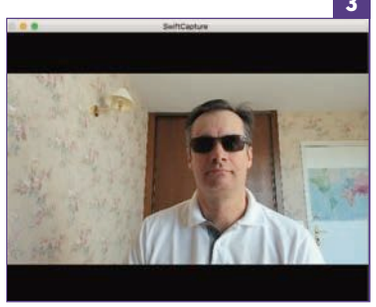


Comme elle est localisée, le paramétrage de la caméra est vraiment simple et fonctionnel – ce qui n'est pas si courant pour un produit professionnel. Ce pilote offre une option pour élargir au besoin le champ de vision de la caméra jusqu'à 90°. Un autre pilote, optionnel aussi, servira à remplacer ou à flouter l'arrière-plan de l'image pendant une diffusion en direct. Le principe est intéressant mais, à mon avis, le résultat reste encore à améliorer [2].



1

qui coûte 36 €), recommandée par Logitech. Elle permet d'enregistrer et de décoder les vidéos directement en 4K. Dommage qu'Apple ne fournisse pas encore de codec 4K pour QuickTime Player.



3

L'ULTRA-HD, C'EST EXIGEANT

Au niveau des caractéristiques, c'est de l'Ultra HD 4K en 4096 x 2160 pixels à 30 i/s, un zoom numérique 5x, un autofocus pour la mise au point automatique, 2 microphones omnidirectionnels pour un son amélioré et un capteur infrarouge. L'algorithme maison RightLight 3 supporte le HDR (High Dynamic Range) pour un meilleur rendu de l'image dans les hautes et basses lumières.
Cependant, pour tirer profit de toutes les capacités de la « bête », il faut disposer de toute la chaîne de diffusion : un Mac récent avec ports USB 3.0 (pour transmettre jusqu'à 5 Go de données par seconde), une application lecteur/encodeur vidéo avec les codecs 4K, et un moniteur tout aussi compatible 4K.
Pour la capture des vidéos en Ultra-HD 4K sur votre Mac à partir de cette Brio, il vous faudra acquérir l'application SwiftCapture [3] de Ben Software (https://www.bensoftware.com

Une fois la vidéo 4K enregistrée, vous visualisez le résultat dans votre lecteur multimédia habituel. VLC Media Player (de videolan.org) ou QuickTime Player feront très bien l'affaire.
Encore peu d'applications de conversation vidéo sont compatibles avec l'Ultra-HD.
On peut néanmoins utiliser la Brio avec Skype et FaceTime à une résolution moindre et sans aucun problème jusqu'en HD 1080.
Reste qu'à cette heure, la plupart des utilisateurs exigeants, même pros, se satisferont très bien encore quelque temps de la Logitech C930e, moins onéreuse (149 € - et moi ns chère encore sur Internet) : sa résolution atteint tout de même un respectable Full HD 1080 à 30 i/s, avec un zoom x4 légèrement moins puissant et pas de prise en charge du HDR (RightLight 2).

DENIS DUBOIS (TWITTER @DEDUBO)