Vous et Votre Mac

Vous et Votre Mac

N° 143 • Avril 2018 100 % Mac en pratique

Instantanés web

3 applications pour réaliser des copies d'écran de pages web dans leur totalité.

Efficacité !

Comment utiliser Calibre pour stocker, organiser et gérer tous ses documents PDF.

Sur les sites web et dans les applications mobiles

Halte aux traqueurs !

Quels sont donc ces mouchards et comment s'en défaire ?

Contre les lenteurs et les bogues...

Le compte Apple

Comprendre la clé d'accès à tout l'univers Apple

Safari

Naviguez avec finesse grâce aux réglages par site

Pourquoi et comment repasser son Mac en HFS+ sans renoncer à High Sierra !

FRANCE métropolitaine : 5,90 € • SUISSE : 9,90 FS
DOM - BEL - MUX - PORT CONT : 6,90 € • CANADA 10,99 $
L 11206 - 143 S - F : 5,90 € - RD

Prendre soin de son Macbook

Tout pour tester et cajoler sa batterie !

- ▶ Des conseils et des astuces pour la faire vivre plus longtemps.
- ▶ Des utilitaires qui vous donneront un petit coup de main.

Sites web, applications mobiles…

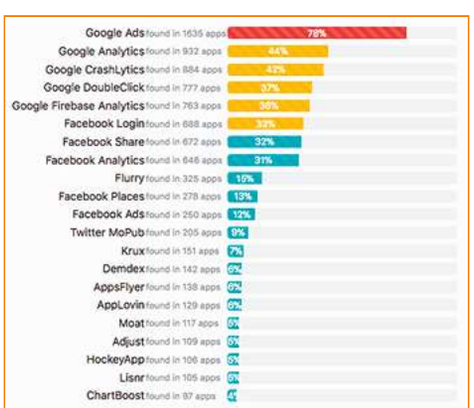
Traquez les mouchards !

Ce n'est une surprise pour personne, les sites web et les applications mobiles contiennent de nombreux mouchards qui récoltent et renvoient discrètement de nombreuses données personnelles à des domaines tiers. En coulisses, un petit nombre d'acteurs inconnus du grand public détiennent des données sur des millions de Français. Quels sont ces mouchards ? Comment les bloquer ? Quels sont les meilleurs outils ? Autant de questions auxquelles je vais tenter d'apporter des réponses. DENIS DUBOIS

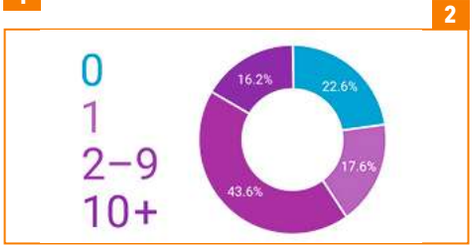
Les mouchards sont de petits bouts de code cachés dans les pages des sites Internet (sous forme de scripts ou d'images) ou dans la plupart des applications mobiles. Mission : collecter et transférer discrètement de nombreuses informations, parfois personnelles, à propos de l'environnement matériel et logiciel sur lequel ils se trouvent, sans que l'utilisateur en ait connaissance.

On peut classer les mouchards **en plusieurs catégories car ils n'ont pas tous la même finalité**.

Il y a ceux qui permettent aux développeurs d'applications ou aux administrateurs de sites d'**obtenir des informations à des fins statistiques, techniques** (Google Crashlytics) ou de **mesurer l'audience** (Google Analytics, Xiti, Weborama). D'autres facilitent **la proposition de publicité** (Google Ads, Facebook Ads). D'autres, enfin, supportent **le profilage et le suivi de l'utilisateur** (les traqueurs) comme DoubleClick (régie publicitaire de Google), les balises internet (comme les balises pixels constitués d'un unique pixel invisible) et les boutons de réseaux sociaux [1].



1



2

LES MOUCHARDS DES SITES INTERNET

Selon une étude récente de Ghostery (*Traquons les traqueurs* • **https://www.ghostery.com/lp/study**), plus de 77 % des pages web contiennent au moins un traqueur. Plus de 16 % des pages en contiennent dix et plus ! [2]

En 2016, des chercheurs de l'Université de Princeton ont livré les premiers résultats d'une étude de grande ampleur sur les traqueurs publicitaires (**http://bit.ly/100D57I**) : sur un million de sites web, ils ont dénombré pas moins de 81 000 traqueurs publicitaires différents !

Google est présent sur plus de 60 % des sites web grâce à ses mouchards Google Analytics et Doubleclick. Suivent ensuite Facebook présent dans 20 % des sites et Twitter dans 10 % des sites. **Les sites qui embarquent le plus de mouchards sont les réseaux sociaux, les sites de rencontre, de banque et les médias** (plus d'une trentaine sur les sites du Figaro, du New York Times et du Huffingtonpost.fr).

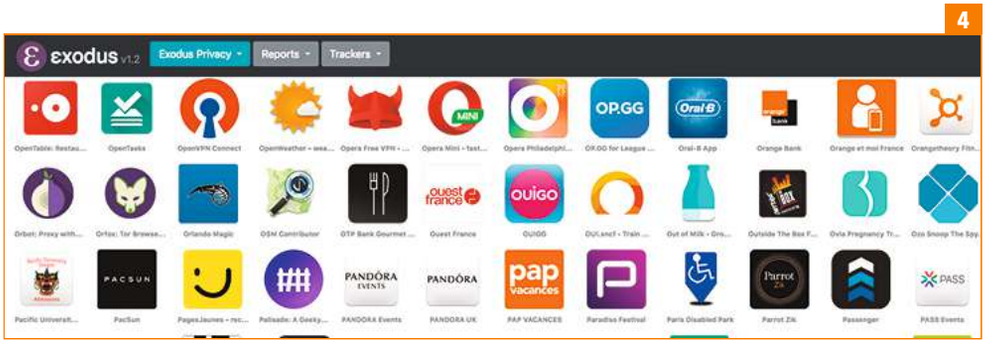
David Legrand du site Next Inpact a développé **l'extension Kimetrack** (**https://github.com/david-legrand/kimetrak**) pour Chrome/UR Browser, Opera et Vivaldi, et bientôt Firefox, qui **permet de visualiser d'un coup d'œil le nombre traqueurs tiers** (contenu provenant de sites ou serveurs autres que celui visité) chargés depuis le site que vous visitez. Un clic sur l'icône de l'extension (dont la couleur de l'étiquette change en fonction du nombre de domaines détectés) affiche la liste [3] des traqueurs et quelques statistiques.

3

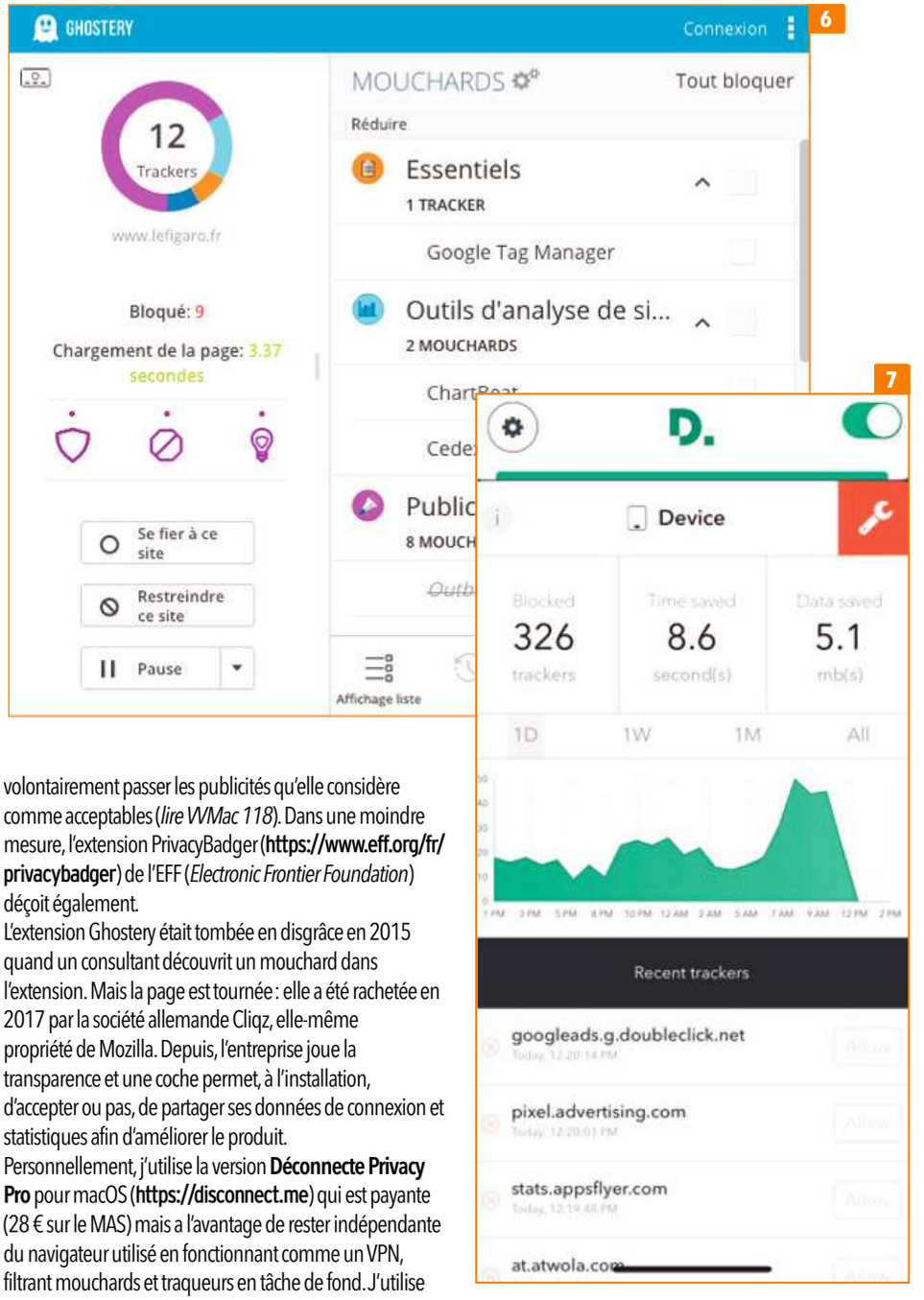
LES MOUCHARDS DES APPLICATIONS MOBILES

En octobre 2014, la rédaction du magazine Que Choisir avait publié une enquête et étudié trente quatre applications sous iOS, Android et Windows Mobile, parmi les plus répandues, afin de déterminer si elles collectaient des données personnelles et de quelle nature. Il s'est avéré que c'était déjà le cas pour la moitié des applications. Depuis, le phénomène n'a fait que s'amplifier.

Très récemment, **les activistes de l'association Exodus Privacy** ont analysé plus de 300 applications Android et publié une base de données [4] contenant actuellement 86 traqueurs, consultable sur leur plateforme libre Exodus (**https://reports.exodus-privacy.eu.org/reports/apps/**).



4



6 7

Il n'y a actuellement pas d'équivalent pour les applications iOS, car cela nécessite des développements au-dessus des moyens de l'association, mais elle prévoit de lancer prochainement un appel à contribution aux internautes. Actuellement, les applications mobiles iOS ou Android contiennent généralement des mouchards, **en fait 2,5 en moyenne**. Mais certaines apps peuvent en héberger une quinzaine (16 pour Le Figaro, 20 pour Allociné). Peu d'applications n'en possèdent aucun ; elles embarquent généralement au moins un composant destiné à mesurer leur audience.

COMMENT BLOQUER LES MOUCHARDS ?

Bloquer les mouchards des pages Internet permet d'avoir une navigation plus rapide et plus fluide, surtout sur les appareils mobiles moins puissants. De plus, certaines apps envoient vos données sans aucun chiffrement, au risque d'être interceptées par des tiers, notamment lors de leur utilisation via les réseaux Wi-Fi.

Le principe est simple : lorsque l'on bloque un mouchard, il ne peut plus communiquer avec son fournisseur tiers, rendant impossible, par ce dernier, la collecte des données personnelles.

Les résultats d'une étude comparative portant sur l'efficacité des différents bloqueurs de mouchards ont été présentés à l'occasion de la conférence *IEEE European Symposium on Security and Privacy* en avril 2017 à Paris (**http://bit.ly/2oCgAbB**) [5]. L'analyse de plus de 123 000 sites web et de 10 000 applications Android tend à démontrer que l'extension **Ghostery** [6] est le meilleur bloqueur de mouchards suivi par **Déconnecte** puis **uBlock**. Des applications bien connues des lecteurs de VVMac ! La surprise vient de la piètre performance de l'extension AdBlock Plus, pourtant la plus utilisée : elle laisse volontairement passer les publicités qu'elle considère comme acceptables (*lire VVMac 118*). Dans une moindre mesure, l'extension PrivacyBadger (**https://www.eff.org/fr/privacybadger**) de l'EFF (*Electronic Frontier Foundation*) déçoit également.

L'extension Ghostery était tombée en disgrâce en 2015 quand un consultant découvrit un mouchard dans l'extension. Mais la page est tournée : elle a été rachetée en 2017 par la société allemande Cliqz, elle-même propriété de Mozilla. Depuis, l'entreprise joue la transparence et une coche permet, à l'installation, d'accepter ou pas, de partager ses données de connexion et statistiques afin d'améliorer le produit.

Personnellement, j'utilise la version **Déconnecte Privacy Pro** pour macOS (**https://disconnect.me**) qui est payante (28 € sur le MAS) mais a l'avantage de rester indépendante du navigateur utilisé en fonctionnant comme un VPN, filtrant mouchards et traqueurs en tâche de fond. J'utilise également **le nouveau navigateur Brave** sur mon iMac et sur mon iPhone/iPad (*lire la Prise en main, dans ce numéro de VVMac*) qui intègre tout ce qu'il faut pour visualiser le nombre de mouchards et bloquer les traqueurs sur les pages web. Il est d'ailleurs un des partenaires officiels de Déconnecte.

Sous iOS, **Ghostery** est présent sous la forme d'un navigateur simple et léger. Vous pouvez également installer un navigateur comme **Brave** ou **Firefox Focus** de Mozilla qui bloqueront une grande variété de traqueurs. Sur l'App Store, **Déconnecte** [7] est également disponible, en trois versions (Free pour Safari, Premium et Pro avec VPN) qui offrent une excellente protection contre les traqueurs.

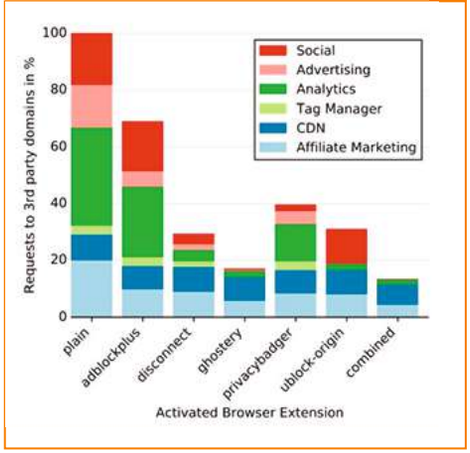
Pour ce qui est des applications mobiles sous iOS, vérifiez que vous avez activé le **Suivi publicitaire limité** dans **Réglages > Confidentialité > Publicité** puis activez l'option **Réinitialiser l'identifiant de publicité de votre iPhone/iPad** ; faites-le régulièrement.

Pensez à arrêter les applications qui tournent en tâche de fond car elles continuent de transmettre des informations vous concernant. Appuyez deux fois sur le bouton d'accueil, situé en bas de l'écran, puis faites glisser vers le haut les applications à quitter.

Soyez vigilant sur les applications qui s'actualisent en arrière-plan. Allez dans **Réglages > Général > Actualisation en arrière-plan** et désactivez toutes celles dont la mise à jour permanente est inutile et qui pourraient en profiter pour vous localiser ou observer votre environnement. Enfin, n'activez que les services de localisation strictement nécessaires dans **Réglages > Confidentialité > Service de localisation**.

Ne vous faites pas d'illusion, les bloqueurs de traqueurs ne peuvent filtrer qu'au mieux 80 % des mouchards présents sur les pages web et beaucoup moins si on prend en compte les nouvelles techniques basées sur l'empreinte digitale numérique (fingerprinting). N'hésitez pas à améliorer ce score en combinant plusieurs outils. Pour les applications mobiles, le taux de filtrage est très faible. N'installez que les applications qui vous sont utiles, n'hésitez pas à supprimer celles qui ne vous servent pas.

5



Un navigateur blindé à découvrir

Dans les précédents numéros de VVMac, nous avons déjà découvert des navigateurs web respectueux de la vie privée comme CLIQZ (VVMac 128) et UR browser (VVMac 135). Brave est un jeune navigateur qui va plus loin que les précédents. Méconnu, il mérite vraiment qu'on lui donne une chance.

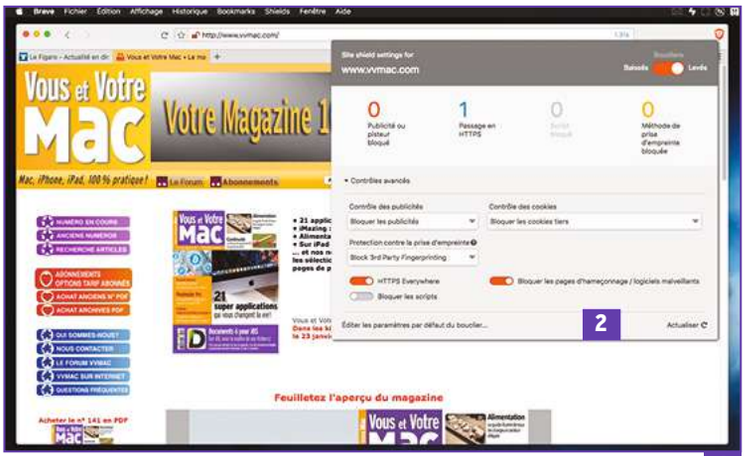
Brave

J'AIME
La richesse des options de sécurité et de confidentialité intégrées ; le volet des Boucliers ; les nombreuses plateformes supportées.

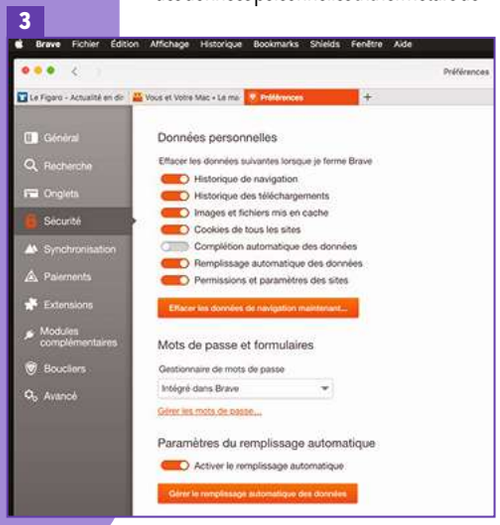
J'AIME MOINS
L'interface n'est que partiellement traduite ; quelques options de protection ne sont pas validées par défaut ; le choix de Google comme moteur de recherche par défaut.

FRANÇAIS
Versions : 0.20.30 (OS X 10.9+) et 1.5.2 (iOS 9+)
Prix : gratuit (sur toutes les plateformes)
Éditeur : Brave Software
https://github.com/brave

Afin de supprimer la publicité, ou d'améliorer la sécurité ou la confidentialité lors de nos visites sur le web, nous installons de nombreuses extensions dans nos navigateurs. Pourquoi ne pas utiliser un navigateur qui a tout ça en standard ? Développé par Brendan Eich, cofondateur de Mozilla Firefox et créateur du JavaScript, Brave promet « le respect de la vie privée et la protection contre les logiciels malveillants ». Brave n'est pas un navigateur comme un autre, et il ne déçoit pas !
Brave est open source, gratuit et en français sur macOS [1] et les autres plateformes de bureau et mobile. Ses fonctions de protection de la vie privée intégrées sont si complètes qu'il rend inutiles les extensions qui encombrent nos navigateurs, sources de vulnérabilités. Brave est un navigateur web qui intègre nativement un bloqueur de publicités (AdBlock), fluidifie la navigation en réduisant le temps de chargement des pages, bloque les pisteurs publicitaires (trackers), force la connexion en HTTPS (HTTPS Everywhere) pour la sécurité, intègre une protection contre la prise d'empreintes digitales numériques (Fingerprinting) et assure le blocage des scripts ! Ces fonctions sont configurables individuellement à travers le volet Bouclier (Shield) [2]. La suppression des données personnelles à la fermeture de l'application peut être définie finement [3].

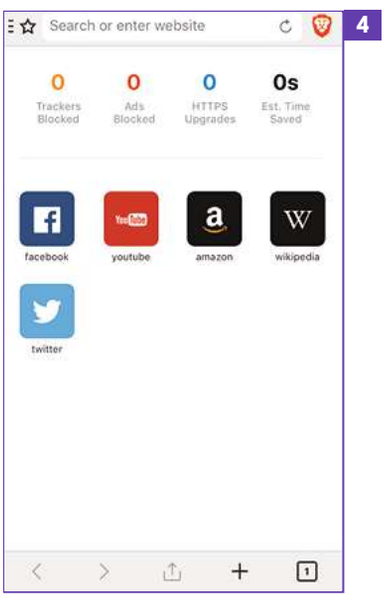


1



3

Sous iOS [4], l'éditeur annonce une vitesse de chargement des pages de 2 à 4 fois plus rapide avec une économie importante de la batterie.



4

ON PEUT MÊME GAGNER DE L'ARGENT AVEC BRAVE !

Brave se distingue aussi par sa gestion des publicités. Il ne se contente pas de bloquer les bannières comme d'autres le font (mais il propose également cette option). Par défaut, il remplace les publicités intrusives ou dotées de pisteurs, par ses propres annonces, plus respectueuses. En échange, Brave s'engage à reverser aux éditeurs des sites une partie des recettes publicitaires. Mais ce n'est pas tout : les utilisateurs du navigateur en percevront également une partie (de l'ordre de 15 %) en bitcoin qu'ils pourront (ou non) attribuer, sous forme de don anonyme, aux sites qu'ils souhaitent soutenir. C'est le service optionnel Brave Payments, qui est actuellement en phase bêta. Cette politique a valu à Brave une levée de boucliers de l'association des médias américains qui représente quelque 1 200 journaux parmi les plus prestigieux. Une pétition est signée contre l'éditeur Brave Software pour dénoncer un détournement des publicités à son propre bénéfice. Hors ce problème, Brave est indéniablement une bonne application à considérer si vous êtes soucieux de votre vie privée. Mais il requiert un paramétrage minutieux au premier lancement, car curieusement les options de protection ne sont pas toutes validées par défaut. Ainsi l'option Ne pas me pister (DNT) n'est-elle pas activée sur macOS.
Et Google est le moteur de recherche par défaut, même si de nombreux autres sont proposés comme Qwant, StartPage ou DuckDuckGo. **DENIS DUBOIS**

Une messagerie en direct sécurisée sur Mac, iOS et les autres…

Depuis les révélations de Snowden sur la surveillance de masse, de nombreuses messageries qui protègent les communications ont vu le jour. Signal d'Open Whisper Systems se distingue pour sa simplicité d'utilisation et par la qualité de sa protection. Son éditeur jouit d'une excellente réputation auprès des défenseurs de la vie privée.

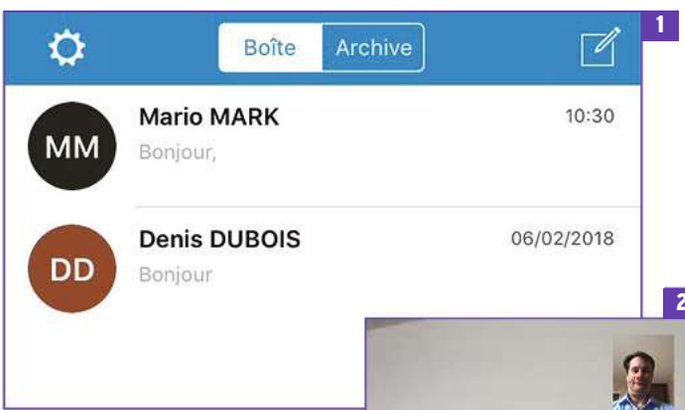
Signal

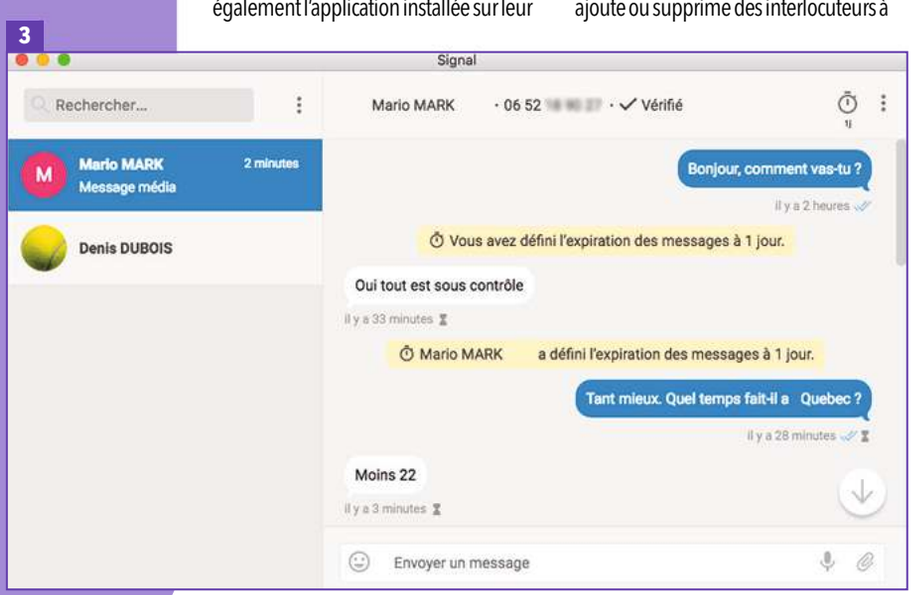
J'AIME
La simplicité d'utilisation ; le haut degré de confidentialité

J'AIME MOINS
Quelques métadonnées sont susceptibles d'être récupérées par Google ou Apple.

FRANÇAIS
Prix : gratuit sur toutes les plateformes supportées
Éditeur : Open Whisper Systems
iOS App Store, Mac App Store
https://signal.org

Signal est une messagerie gratuite et open source, qui fut d'abord disponible sur les smartphones iOS [1] et les terminaux multifonctions sous Android. Elle permet de communiquer avec des contacts sous forme de messages du même genre que les SMS et MMS, mais aussi en audio et en vidéo [2].
Sa particularité est de chiffrer de bout en bout toutes les communications et d'intégrer des mécanismes de vérification de la sécurité afin d'assurer de manière optimale la parfaite confidentialité des conversations. Signal fait partie des quelques outils recommandés par Edward Snowden.
Non, ne croyez pas que seuls les gens du microcosme politique et médiatique, des stars ou des militaires, par exemple, sont concernés. Vous pouvez fort bien être visé parce que, pour telle ou telle raison, vous avez été repéré sur un réseau social !
Pour pouvoir communiquer avec des destinataires, ces derniers doivent avoir également l'application installée sur leur appareil mobile. Signal affiche la liste de ses utilisateurs reconnus parmi vos contacts. Dans le cas contraire, il se propose de leur envoyer un SMS pour les inviter à installer l'app. On peut lancer une discussion chiffrée à plusieurs personnes en créant des groupes. Il suffit de donner un nom au groupe (par exemple, amis ou famille) puis d'ajouter le numéro de téléphone des personnes. De même, on ajoute ou supprime des interlocuteurs à tout moment.
Plus récemment, Signal a été développée aussi pour les ordinateurs de bureau [3]. Signal Desktop est disponible sur macOS, Windows et Linux. Le pas à pas, sur la page en regard, montre la procédure de synchronisation entre Signal iOS et Signal Desktop afin de générer les clés de chiffrement et de récupérer, sur un ordinateur, la liste des contacts, des groupes et des conversations associées.





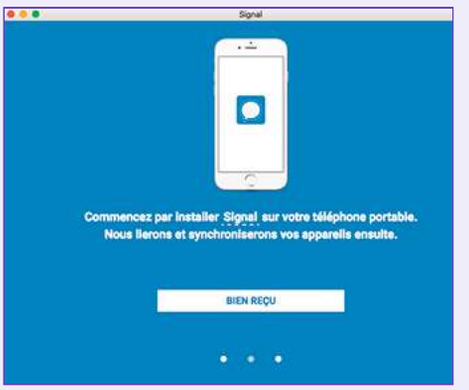
VÉRIFICATION DES CONTACTS

Une fois que l'on est en communication avec un destinataire, il est recommandé

Prise en main : synchronisation de Signal iOS avec Signal macOS

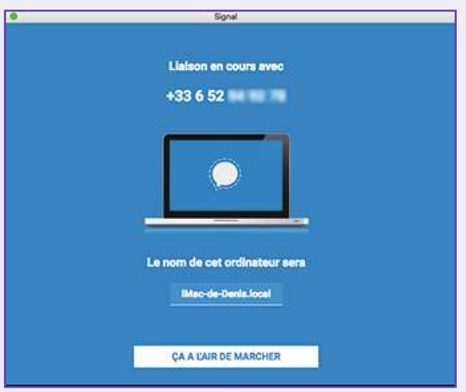
Commencez par installer l'application Signal – Private Messenger sur votre smartphone, depuis l'iOS App Store ou le Google Play Store.

Téléchargez la version Desktop à l'adresse suivante : **https://signal.org/download**
Lancez l'application puis sélectionnez **Configurer comme nouvelle installation**.

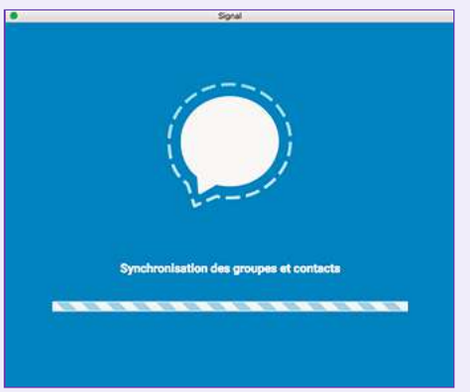


Confirmez, en cliquant le bouton **Bien reçu** que vous avez préalablement procédé à l'installation de Signal sur votre téléphone mobile.

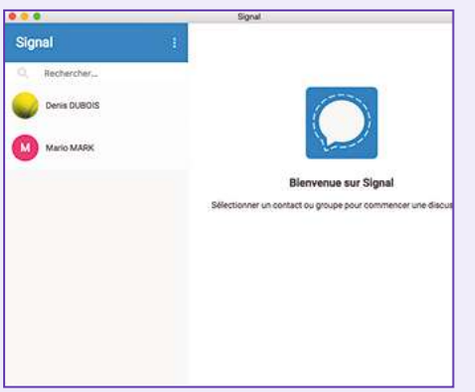
Lancez Signal sur votre appareil mobile. Rendez-vous dans **Réglages > Appareils liés > Connectez un nouvel appareil** et scannez **le code QR** qui s'affiche à l'écran de votre Mac.



Le numéro de téléphone s'affiche, ainsi que **le nom de l'ordinateur** associé au téléphone.



Signal va ensuite générer automatiquement **les clés de chiffrement** puis va importer la liste des contacts, des groupes et des conversations associées à partir de votre téléphone.



On peut dès lors chercher le nom d'un contact ou entrer un numéro de téléphone de l'un d'entre eux pour commencer à converser.

4

d'afficher le numéro de sécurité afin de comparer la clé de chiffrement de la communication de bout en bout. Il s'agit de s'assurer qu'elle n'a pas été compromise par un tiers (attaque de l'homme du milieu) qui pourrait « écouter » la conversation. Sous iOS, on touche le nom du contact puis dans *Informations du contact*, on touche *Afficher le numéro de sécurité*. S'affichent *un code QR* [4] et *une série de chiffres* unique pour chaque contact. Comparez ces chiffres avec ceux de votre interlocuteur : ils doivent être strictement identiques. Pour ce faire, vous pouvez les envoyer à votre interlocuteur par SMS/MMS ou e-mail – via le bouton Partage d'iOS (le carré d'où part une flèche tirée vers le haut). Si celui-ci est à vos côtés, sélectionnez Scan code afin de scanner le code QR qui s'affiche sur son écran.
Dans l'application Desktop, on clique sur *les trois points verticaux*, à droite du nom du contact, dans le menu qui s'affiche et on sélectionne *Afficher le Numéro de Sécurité*. Une fois la vérification effectuée, on clique *Marquer comme vérifié*. Une coche apparaît dorénavant sous le nom du contact avec le statut *Vérifié* et une notification est envoyée si la clé du correspondant change.

MESSAGES ÉPHÉMÈRES

Sacrifiant à la mode des messages qui s'autodétruisent – popularisés par Snapchat –, Signal permet d'envoyer des messages qui disparaissent de votre appareil et de celui de votre contact, après un délai déterminé.
Activer la fonction Messages éphémère dans la page Informations du contact d'iOS ou par le menu de l'application de bureau. Déterminez le délai (de 5 secondes à une semaine) après lequel les messages envoyés et reçus disparaîtront une fois lus. **DENIS DUBOIS**