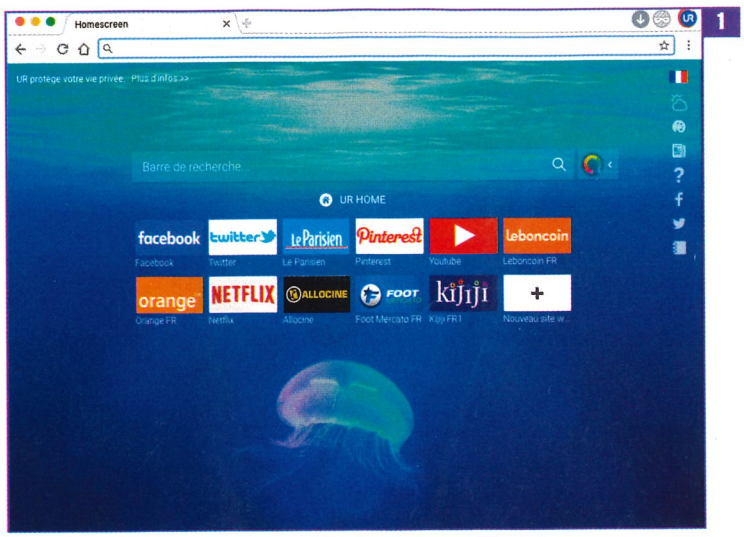
Choisir un navigateur complémentaire pour protéger sa vie privée

Dans le climat de défiance qui règne face à l'Internet, ce peut être une bonne idée que de renforcer sa logithèque d'un logiciel web alternatif dédié à certaines activités sensibles (achats, consultations de santé…). Brave et UR sont deux navigateurs modernes, plus particulièrement orientés vers le respect de la vie privée. Avant de vous décider, je vous propose de comparer leurs fonctions.

Nous sommes de plus en plus inquiets de l'utilisation qui est faite de nos données personnelles. 46 % des Français ont déjà constaté des abus dans leur utilisation (sondage IFOP pour la CNIL de novembre 2018), en grande partie à des fins de prospection commerciale. Or, les navigateurs sont les principaux vecteurs de ces « fuites » effectuées, à notre insu, lors de notre navigation. D'autres études montrent qu'une majorité des utilisateurs ne font pas confiance à leur navigateur Firefox, Chrome ou Safari. Dès lors pourquoi ne pas en changer ou, du moins, associer au navigateur habituel un autre logiciel plus respectueux ?

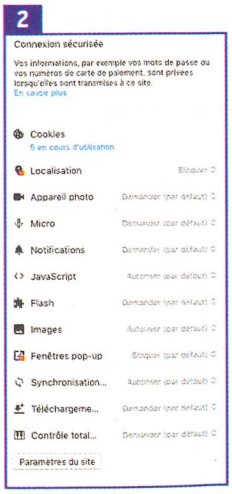


1

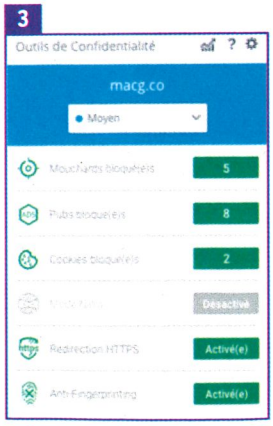
ENCORE UNE INITIATIVE FRANÇAISE !

Développé par une start-up française, AdaptiveBee, UR Browser [1] est encore peu connu. Il a pour ambition de préserver votre identité numérique. Il a été primé par l'Union européenne pour l'efficacité de sa technologie contre l'empreinte digitale (anti-fingerprinting) et pour l'ensemble de ses fonctions de sécurité et de confidentialité. Sécurité et confidentialité… l'une ne va pas sans l'autre. Du côté de la sécurité, on trouve un scanner de malwares intégré pour vérifier vos téléchargements ; le niveau de sécurité de chaque site visité est indiqué par un bouclier de couleur, du vert au rouge pour les sites considérer comme dangereux ; la version sécurisée (HTTPS) des sites web est toujours privilégiée (sans extension dédiée) ; et il utilise un chiffrement renforcé (RSA a 2048 bits) pour les certificats SSL. Un clic à gauche de la barre d'adresses, fait apparaître un menu pop-up [2] afin de contrôler finement l'accès aux informations que le site peut utiliser (localisation, micro, appareil photo, etc.) et le contenu qu'il peut afficher (Notifications JavaScript, Flash…).

Côté confidentialité, il offre des fonctions anti-pistage et anti-profilage regroupées dans la fenêtre Outils de confidentialité [3]. L'anti-pistage est basé sur le blocage des cookies tiers et des mouchards invisibles (tels que les pixels-espions). Un mode navigation privée est bien sûr de la partie, reconnaissable à ses onglets Ninja qui peuvent côtoyer des onglets normaux dans la même fenêtre. UR est basé sur Chromium qui a été « nettoyé » et aucune information n'est envoyée à Google. Qwant est le moteur de recherche par défaut, mais de nombreux moteurs alternatifs sont proposés. Enfin, un bloqueur de publicité est intégré.



2



3

4

UR Browser

J'AIME
Le scanner de malwares intégré ; les outils de confidentialité ; la réduction dynamique de l'empreinte numérique ; un VPN bientôt intégré…

J'AIME MOINS
Rien de particulier à relever.

FRANÇAIS
Prix : Gratuit
Config. : OS X 10.9+
Éditeur : AdaptiveBee
Infos : https://www.ur-browser.com/fr-FR

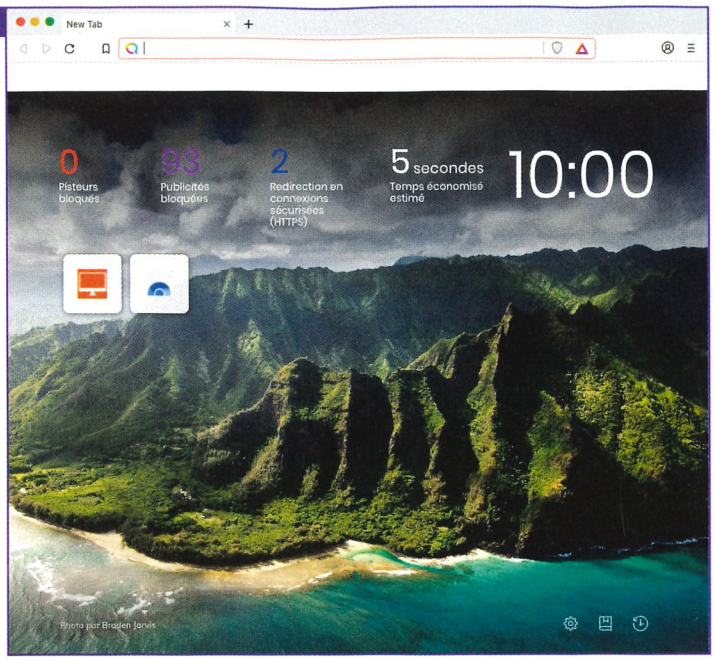
Brave Browser

J'AIME
Le bouclier de protection par site ou global ; l'option de navigation privée via le réseau Tor ; le gestionnaire de mots de passe embarqué ;

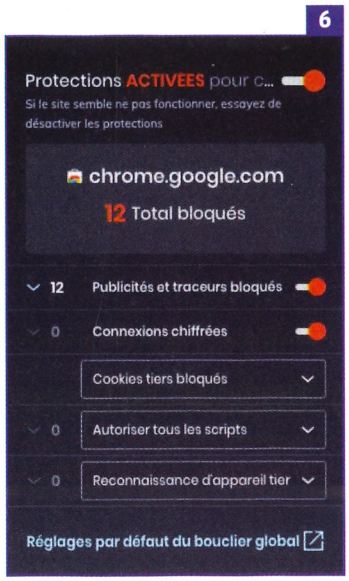
J'AIME MOINS
Le modèle économique de Brave tient encore pour l'instant plus du concept que d'autre chose.

FRANÇAIS
Prix : Gratuit
Config. : OS X 10.9+
Éditeur : Brave
Infos : https://www.brave.com

5



6

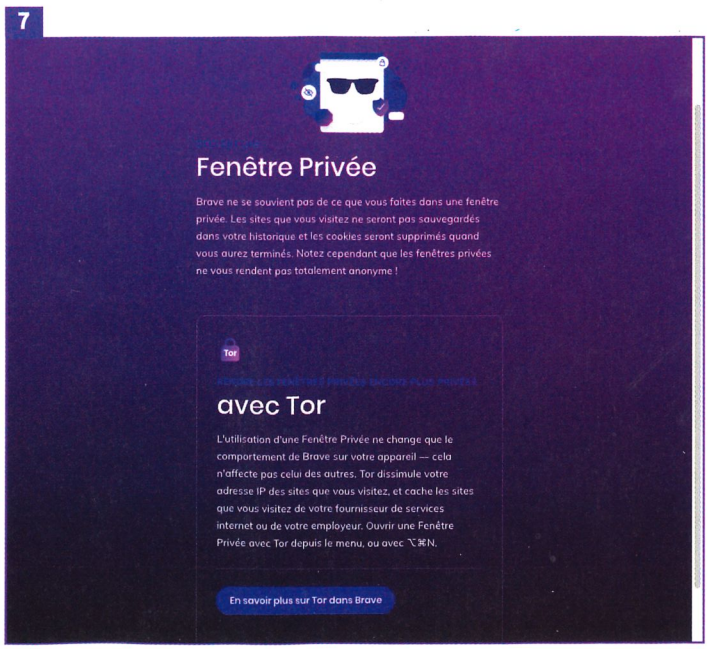


En ce qui concerne les fonctions anti-profilage, l'identification est rendue plus difficile par le blocage des cookies et mouchards.
Le point fort de l'application est sa capacité à réduire l'empreinte numérique en modifiant régulièrement, et de façon aléatoire, les informations matérielles (type d'appareil, OS, adresse IP, etc.) – comme le proposaient déjà certaines extensions tierces.
Chacune de ces fonctions est activée, ou pas, en fonction du niveau de confidentialité (bas, moyen ou haut) définit au premier lancement de l'application [4], mais cela peut être changé d'un clic en fonction du site sur lequel vous naviguez. Comme UR est multi-utilisateur, chacun peut créer son propre profil de configuration.
De nombreuses fonctions et améliorations sont prévues courant 2019, dont l'ajout d'un véritable VPN pour Mac (déjà disponible sous Windows). L'ouverture du code source est également envisagée.

UN NAVIGATEUR « BOÎTE À OUTILS »

Brave [5] est un navigateur Internet open source (son code de programmation est ouvert) basé lui aussi sur Chromium. Il a été créé en 2016 par Brendan Heich, cofondateur du navigateur Mozilla Firefox et inventeur du langage JavaScript, et il est disponible sur de nombreuses plateformes, Mac, Linux, Windows, iOS et Android.
Brave se veut être à l'avant-garde d'une approche renouvelée du web, axée sur la confidentialité, sans renoncer à la performance.
La confidentialité de Brave repose sur un bouclier de protection, disponible à tout moment dans la barre d'outils. Il est chargé de protéger contre les publicités intrusives et les traceurs indésirables (cookies, scripts, prise d'empreinte numérique de l'appareil…) cachés dans les pages visitées. On peut personnaliser les paramètres du bouclier de protection (shield) pour chaque site [6] ou de façon globale.
Alors qu'un navigateur ordinaire utilise (en l'absence d'extension spécifique comme HTTPS Everywhere), une connexion non sécurisée, Brave force automatiquement la connexion vers la version sécurisée et chiffrée (HTTPS) des sites web visités. Le moteur de recherche proposé par défaut est Qwant, un excellent choix conforme à la philosophie de ce navigateur.
Toute fenêtre de navigation privée [7] rend le navigateur oublieux de toutes vos activités dès sa fermeture – mais ça ne vous rendra pas anonyme pour autant. En revanche, opter pour la Fenêtre Privée avec Tor garantit en plus l'anonymat puisque la connexion passe alors par une chaîne de trois ordinateurs sur le réseau Tor (lire VVMac 149) – c'est inévitable, la vitesse de connexion est le plus souvent nettement ralentie.
Brave permet de désactiver les boutons de réseaux sociaux, qui sont des traqueurs, et la possibilité de connexion avec leurs identifiants sur les sites tiers (Google Twitter, Facebook et LinkedIn).
En termes de sécurité, Brave intègre un gestionnaire de mots de passe avec remplissage automatique des champs d'édition. Par défaut, il désactive les extensions qui représentent un risque pour la sécurité. Moins banal, il offre des options de gestion des adresses IP WebRTC. Et alors ? WebRTC est une fonction JavaScript qui permet des communications audio (VoIP) et vidéos, en temps réel, directement dans le navigateur. Cette fonction de pair à pair (P2P) expose votre adresse IP à votre correspondant.

7



Différentes politiques proposées permettent de ne pas exposer son adresse IP locale.
Cette option avancée ne concernera que les utilisateurs experts.
Enfin, il est possible d'effacer ses données de navigation (historique, cookies, cache, etc.) de façon globale ou sur une période donnée.
Brave repose sur son modèle économique plutôt particulier. En activant le programme des Récompenses Brave [8], les publicités envahissantes et ciblées présentes sur les pages web sont remplacées par… des publicités plus « propres », respectueuses de la vie privée, mises en place par l'éditeur de Brave. À cette occasion, Brave accélère le chargement des pages (40 % plus rapide que Chrome sur les ordinateurs et 4 fois plus rapide sur les mobiles). Le temps ainsi gagné s'affiche fièrement sur la page d'accueil du navigateur, à côté du nombre de publicités et de pisteurs bloqués. En acceptant de visualiser des publicités sur des sites choisis au préalable, vous pouvez être « rémunérés » en fonction des revenus publicitaires générés et, pour l'heure, affecter les gains aux sites que vous désirez soutenir. Toutefois ce modèle économique est loin d'être en place et n'a évidemment pas fait ses preuves.

8

Alors, que choisir de Brave ou d'UR ? Le fait est qu'ils ont un moteur commun, Chromium, et un même objectif, le respect de votre vie privée. Reste qu'ils déploient deux approches différentes. L'un supprime les empreintes numériques lorsque l'autre les remplace par de fausses informations ; l'un propose un VPN lorsque l'autre préconise Tor. L'un supprime les publicités lorsque l'autre perpétue un modèle basé sur la publicité en les substituant aux siennes, « respectueuses de la vie privée ».
Si sur mobile seul Brave est disponible, sur macOS, ils sont tous les deux proposés et comme ils sont gratuits, le plus simple est de les télécharger et de les essayer (ils reprennent tous les deux au moins vos favoris Safari, Chrome ou Firefox). **DENIS DUBOIS**