Vous et Votre Mac

Vous et Votre Mac

N° 132 • avril 2017 100 % Mac en pratique

- Retrouver les infos de son compte Apple
- Accéder aux fichiers Mac sous iOS
- Bien préparer un disque externe
- Pour un Safari stable et performant !

Chiffrer vos fichiers avant de les poster sur un cloud

FAITES LE PLEIN DE SOLUTIONS !

Sécurisez votre MacBook

Maîtrisez toutes les fenêtres qui envahissent votre écran !

ARCHIVEZ VOS E-MAILS POUR MIEUX LES GÉRER !

FRANCE métropolitaine : 5,90 € • SUISSE : 9,90 FS
DOM - BEL - MUX - PORT CONT : 6,90 € • CANADA 10,99 $
L 11206 - 132 - F : 5,90 € - RD

Automatisation, filtres, préréglages

La boîte à outils pour améliorer vos photos

Pour voyager en sécurité et sérénité protégez vos matériels !

Vous partez prochainement en voyage (d'agrément ou d'affaire) ? Bien sûr, comme tout technophile qui se respecte, vous emportez quelques matériels avec vous ! Probablement un MacBook, peut-être un iPad (Pro), votre iPhone, sûrement. Que se passerait-il si vous égariez ou pire, si on vous volait ses appareils ? Comment assurer la sécurité de vos données personnelles ou professionnelles dans un contexte pas toujours « sécuritaire » que ce soit en France ou à l'étranger ? Quelques précautions s'imposent afin d'assurer la sécurité de vos équipements et de vos données importantes. **DENIS DUBOIS**

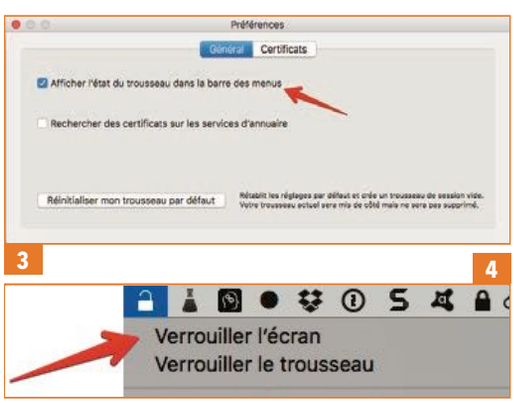
VERROUILLEZ VOS ÉQUIPEMENTS

Exigez un mot de passe à l'ouverture de session de vos iPhone, iPad et MacBook. Activez également un mot de passe au bout de quelques minutes d'inactivité, lors de la mise en veille ou du déclenchement de l'économiseur d'écran de macOS. Ces mesures évitent qu'un individu profite d'un moment de distraction pour accéder, à votre insu, à vos e-mails, à vos contacts ou à vos documents personnels ou professionnels.

Rendez-vous dans les **Préférences Système** de macOS, panneau **Sécurité et confidentialité** > **Général** et cochez **Exiger le mot de passe immédiatement après la suspension d'activité ou au lancement de l'économiseur d'écran** [1]. Ensuite, dans la section **Bureau et économiseur d'écran**, définissez **le temps d'inactivité (en minutes)** après lequel l'écran de veille s'activera [2].

Vous pouvez verrouiller votre Mac directement via la barre des menus. Ouvrez **Trousseau d'accès** (Application/Utilitaires), et dans **Préférences > Général**, cochez **Afficher l'état du trousseau dans la barre des menus** [3] puis sélectionnez le sous-menu **Verrouiller l'écran** [4]. Pour le choix du mot de passe, vous pouvez **faire appel à l'Assistant Mot de passe** d'Apple accessible depuis les comptes utilisateurs et les Trousseaux d'accès.

Une fois rentré de voyage, il est recommandé de changer vos mots de passe... au cas où ils auraient été dévoilés.



RETROUVER VOS APPAREILS PERDUS OU VOLÉS

Avant de partir, pensez à activer la fonction **Localiser mon iPhone, iPad, iPod Touch** dans **Réglages > iCloud d'iOS** ou **Localiser mon Mac** sur **icloud.com** ou via les **Préférences Système > iCloud** [5]. Cette fonction vous permet de localiser votre matériel sur une carte en cas de perte ou de vol, d'envoyer un message, de le verrouiller ou encore d'effacer les données à distance.

Le Mac n'intégrant pas de GPS, sa localisation sur une carte peut ne pas être aussi précise car elle est basée sur les réseaux Wifi situés à proximité de l'appareil. **Localiser mon Mac** permet également d'émettre un message sonore,afin de le retrouver en cas de perte (dans une gare ou un aéroport par exemple).

CHIFFREZ VOS DONNÉES

En cas de perte ou de vol de votre Mac, le mot de passe de session, même fort, ne pourra empêcher une personne très motivée et bien informée de pénétrer dans votre

appareil. **Seul le recours au chiffrement est à même de vous assurer le niveau de confidentialité qui garantit la sécurité de vos données**.
Depuis OS X 10.3, Apple propose une solution très bien intégrée au système : FileVault. Mais ce n'est que depuis OS X 10.7, avec la version 2 de FileVault, que cette solution s'est avérée véritablement aboutie en permettant de chiffrer l'intégralité du disque de démarrage (chiffrement XTS AES 128 bits) et non plus seulement les dossiers utilisateurs. Seule la clé de chiffrement (256 bits) associée au compte utilisateur permet de déverrouiller les données. Notez que cela n'empêche pas d'utiliser le service **Localiser mon Mac**. FileVault sait aussi chiffrer **les disques externes**. Il suffit de les monter sur le Bureau, de les sélectionner et de **demander à les chiffrer dans le menu contextuel**. Il existe d'autres solutions open source pour vos disques et vos périphériques de stockage amovibles (clés USB, cartes mémoire, etc.) en créant des conteneurs chiffrés protégés par un mot de passe, comme VeraCrypt de IDRIX (gratuit • http://veracrypt.codeplex.com) ou CypherShed (gratuit • https://www.ciphershed.org).

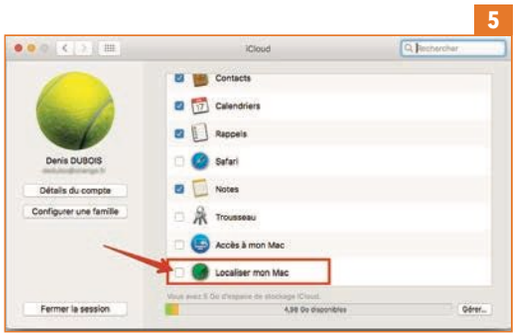
RIEN D'IMPORTANT OU DE CONFIDENTIEL DANS UN CLOUD !

Méfiez-vous des clouds, même si cette solution est tentante tant elle s'avère pratique. **N'y placez pas vos papiers officiels ou documents confidentiels !**
Aucun cloud n'est à l'abri d'un accès frauduleux et les données sont parfois stockées en clair sur les serveurs, lesquels sont à la merci de la curiosité des exploitants du service ou d'un accès non autorisé.
Si vous souhaitez malgré tout, utiliser ce type de stockage, privilégiez les services chiffrés de bout en bout comme SpiderOak One (https://spideroak.com). **Vous pouvez aussi simplement chiffrer préalablement à leur envoi les fichiers et dossiers**. Le plus simple sur Mac est d'utiliser Encrypto (gratuit• MAS).
iCloud (donc iCloud Drive) chiffre les données en transit et stockées sur le serveur avec un chiffrement AES de 128 bits (256 bits pour le trousseau iCloud).

CHOISIR DES POINTS D'ACCÈS WIFI SÉCURISÉS

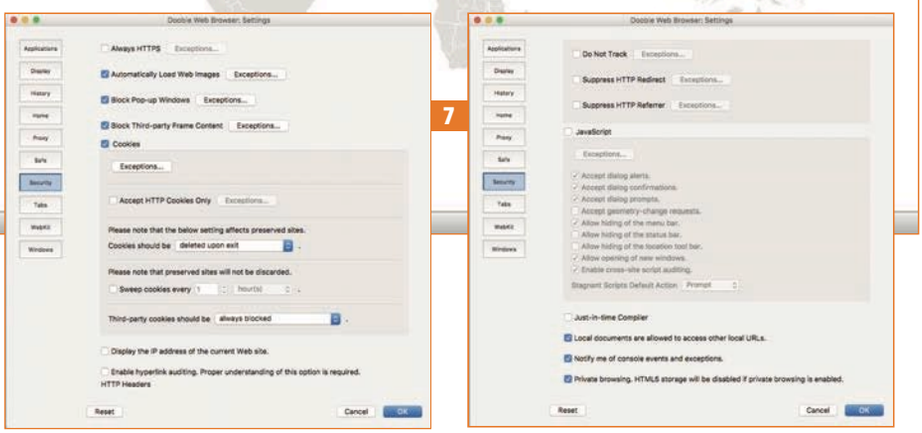
Les points d'accès Wifi gratuits ou publics (cafés, aéroports, hôtels, salons et centres commerciaux) n'offrent aucune garantie de confidentialité. Il est très risqué de consulter son webmail, son compte en banque ou de faire des achats en ligne à partir d'une telle connexion.
Rien n'assure que vous êtes connecté au réseau légitime. Certains hotspots usurpent les noms « officiels »

5



6

7



pour que vos appareils s'y connectent afin d'intercepter vos données, notamment vos mots de passe et numéros de cartes bancaires.
Pour vos achats et transactions, vous pouvez passer par des navigateurs web sécurisés que l'on trouve dans les suites de sécurité de certains éditeurs d'antivirus. **Comme alternative, je vous propose le navigateur Dooble Web Browser [6]** (gratuit et open source • http://dooble.sourceforge.net) dont les options de sécurité sont particulièrement fournies **[7]** mais que vous devrez configurer manuellement (si ce n'est qu'il n'est pas en français, ça ne présente aucune difficulté : il suffit de cocher des cases).
En dernier recours vous pouvez acheter **une carte SIM locale** et effectuer vos connexions via la 3G/4G.
Privilégiez toujours le mode https pour vous connecter de manière sécurisée aux sites web, il vous suffit de taper **https://** à la place de **http://**. Vous pouvez ajouter le plugin de l'Electronic Frontier Foundation, **HTTPS Everywhere** (pour Firefox, Chrome et Opéra • https://www.eff.org/https-everywhere) qui automatisera la procédure.

OFFREZ-VOUS LA SÉCURITÉ D'UN VPN

Pour sécuriser au mieux vos connexions Wifi, rien ne vaut **l'utilisation d'une connexion VPN** (réseau privé virtuel) pour accéder à vos services depuis l'étranger, au travers d'une connexion chiffrée et anonyme (votre adresse IP est remplacée par une adresse virtuelle). Cette solution est la plus efficace mais aussi la plus onéreuse car un abonnement est généralement requis.
Vous pouvez toutefois installer Opéra VPN qui est gratuit et illimité sur macOS (http://www.opera.com/fr, au moins la version 43) **[8]** – ainsi que, sur vos appareils iOS où il fera office de VPN pour toutes les applications.
Si vous avez des données confidentielles, envisagez l'achat **d'un filtre de confidentialité** pour protéger les informations affichées à l'écran de vos appareils des regards indiscrets notamment dans les lieux publics ou à l'hôtel. Il en existe également pour iPhone et iPad.
Investissez dans un chargeur de batterie (la marque Aukey est spécialisée dans ce type de produits). Un chargeur de haute capacité assurera plusieurs charges à vos appareils.
Enfin, gardez une sauvegarde en lieu sûr (à la maison, dans la famille…) est une règle essentielle. En cas de perte ou de vol, vous aurez l'assurance de pouvoir récupérer vos données à votre retour de voyage.

8