Vous et Votre Mac

Vous et Votre Mac

N°117 • Décembre 2015 100 % Mac en pratique

Choisir un stockage distant

La taille et le prix ne sont pas les seuls critères à prendre en compte !

Voyages, voyages…

Apple Plans et Google Maps, deux solutions plus complémentaires que concurrentes

Sécurité et confidentialité

Des pistes et des solutions pour masquer fichiers et dossiers sur votre Mac

Compacte, légère, performante, cette tablette supporte toutes les nouvelles fonctions d'iOS 9

Une tablette formidable !

L'iPad mini 4

Photographie numérique

Les premières extensions de retouche et d'effets pour Photos Mac sont disponibles

Apple HomeKit veut automatiser votre confort et votre sécurité

Comment, demain, la domotique *made in* Apple peut-elle révolutionner votre maison ?

France métropolitaine : 5,90 €
DOM/BEL/LUX : 6,90 € • Suisse : 9,90 FS • Canada 10,99
L 11206 - 117 - F : 5,90 € - RD

Camoufler ses fichiers sensibles !

Dans son numéro 115, VVMac vous a présenté des outils de chiffrement de fichiers. Ces méthodes se destinent plus particulièrement à l'échange, souvent par e-mail. Dans cet article, je vous propose de nous intéresser aux outils et techniques qui garantissent une confidentialité en local, sur votre Mac. ■ Denis Dubois

Il est parfois nécessaire, dans notre milieu professionnel ou même personnel, de dissimuler des informations, des documents, qu'ils soient privés ou confidentiels. Des données financières, médicales, administratives ou simplement personnelles qu'il vaut mieux soustraire à la curiosité de nos proches, de nos enfants, des collègues de travail, voire de concurrents.

Cacher manuellement des fichiers

L'astuce la plus simple pour dissimuler un fichier ou un dossier privé est de faire précéder son nom d'un point (.). Le Finder refusant cette manipulation, il faut ruser.

Le plus direct est le Terminal (**Applications/Utilitaires**) avec la commande :

mv monfichier .monfichier [entrée]

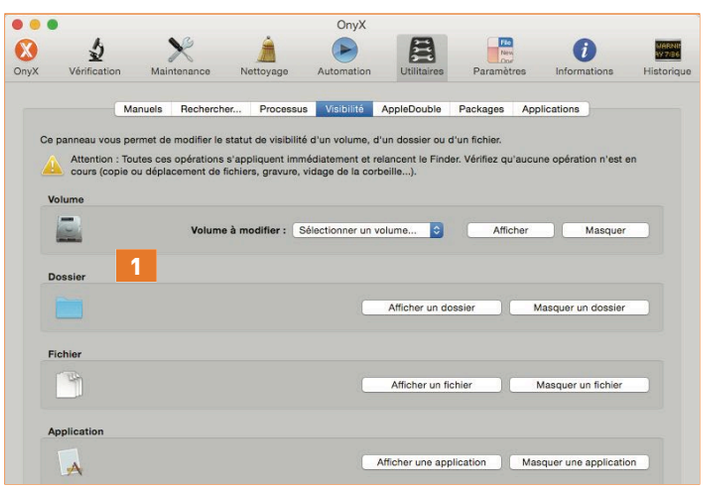
mv .monfichier monfichier [entrée] restaure la visibilité.

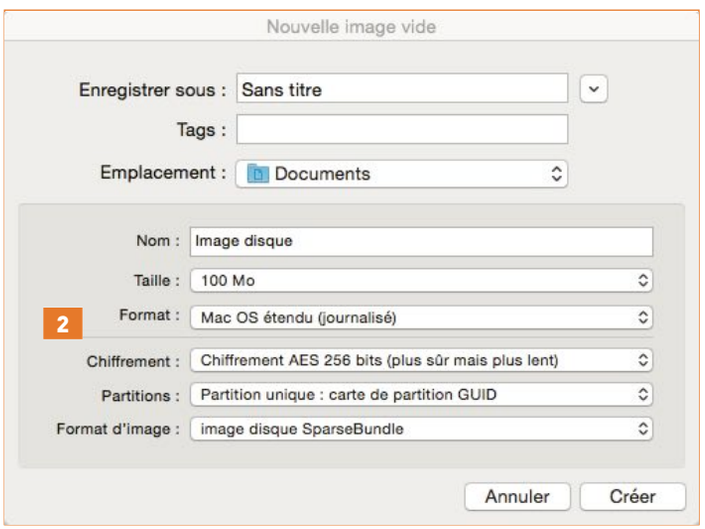
*Remplacez **monfichier** par le nom du fichier concerné par l'opération.*

Pour créer un dossier caché, tapez la commande **mkdir .mondossier** [entrée]

*Remplacez **mondossier** par le nom du dossier concerné par l'opération.*

Alternativement, choisissez l'un des nombreux utilitaires qui permettent de modifier le statut de visibilité d'un fichier ou d'un dossier. **Onyx** 1, la boîte à outils gratuite, sait le faire.



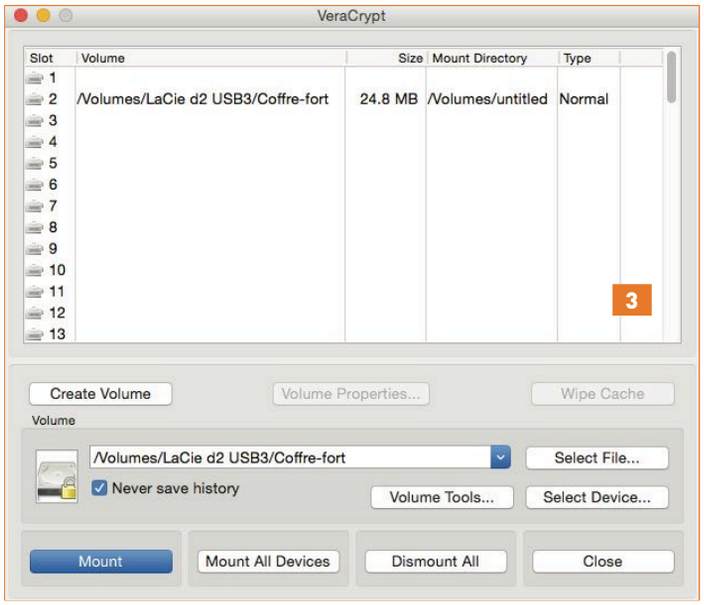


Dans le même ordre d'idée, on peut également, toujours à l'aide du Terminal, modifier l'attribut de visibilité d'un fichier ou d'un dossier, avec la commande **chflags** (une fonction du système de fichiers du Mac). Voici comment cacher un dossier placé dans votre répertoire utilisateur (home) :

chflags hidden ~/secrets/ et inversement **chflags nohidden ~/secrets/**

Une recherche Spotlight pourrait cependant vous trahir !

Afin d'empêcher l'indexation des contenus cachés, une option consiste à créer un dossier dans **/Bibliothèque** (à la racine du disque) qui contiendra vos documents confidentiels – en effet, le contenu de ce répertoire n'est pas indexé. Cependant, cette astuce ne résiste pas à ces nombreux utilitaires qui, à l'instar de TinkerTool, proposent d'afficher l'intégralité des fichiers cachés d'un volume, dévoilant ainsi le subterfuge !



Cacher dans une image

La **stéganographie** est une technique ancienne qui permet de camoufler des données (un texte, une image, un fichier .pdf ou zip, etc.) **dans une image** (ou une vidéo ou un fichier son), sans que celle-ci n'en soit visuellement altérée (en tout cas pas significativement). Cette image peut ensuite être envoyée par e-mail ou postée sur un site Web (comme image ou comme élément graphique constitutif de la page). Le destinataire de l'image n'a plus qu'à extraire le message – qui peut même être parfois protégé par un mot de passe!

Cette technique souffre de quelques limitations.
Le message (ou le fichier à dissimuler) **ne doit pas être trop volumineux** afin de ne pas trop altérer l'image originelle. L'image est intrinsèquement modifiée (même si cette modification n'est pas visible) et donc son empreinte numérique (appelé *hash*) également. Aussi, **il faut s'assurer d'utiliser une image originale**, si possible une création, afin **d'empêcher tout point de comparaison entre l'image codée et son originale**. Cela peut éveiller les soupçons. **Outguess 1.1.0** (rbcafe.com) est un programme open source et gratuit, très simple d'utilisation, pour cacher un fichier dans une image au format JPEG et la révéler au moyen d'un mot de passe. Dans le même registre, **iSteg 1.6.2** de Hanynet (**hanynet.com**) est simplement basé sur les sources de Outguess.

Utiliser les images disques

Vous connaissez probablement les images disque car la plupart des applications OS X s'installent via une image disque (.dmg). C'est un disque virtuel qui « monte » sur le bureau lorsqu'on double clic sur son icône. L'image disque est une « enveloppe », dans laquelle on peut glisser divers éléments (documents, images, dossiers, etc.) et elle peut être compressée, chiffrée, protégée par un mot de passe, voire morcelée en plusieurs segments pour être envoyée en pièces jointes d'un e-mail (moins utile si vous utilisez Apple Mail Drop ou un système similaire). Il existe différents formats d'image disque DMG **qui peuvent être créés simplement et gratuitement avec Utilitaire de disque** 2 (Applications/Utilitaires). Utilitaire de disque utilise Filevault pour le chiffrement.
On peut aussi recourir à une application payante comme **DropDMG**. Elle est payante mais regroupe des possibilités avancées dans la création des différents formats, la gestion et la conversion d'images disques, tout en restant très simple à utiliser (25 € • Mac App Store • http://c-command.com).

Des coffres-forts chiffrés

Les conteneurs chiffrés, très simples à utiliser, sont comme des coffres-forts numériques. Ils permettent de créer des disques virtuels chiffrés d'une taille définie ou peuvent chiffrer la totalité d'une partition, d'un volume ou d'un support de stockage (clé USB, carte mémoire ou disque dur externe). Une fois monté sur le Bureau, un conteneur chiffré se présente comme un volume de stockage physique, qui après saisie d'une phrase de passe ou par le biais d'un fichier de déverrouillage ; le chiffrement/déchiffrement des fichiers s'effectue à la volée, en toute transparence. Ce système offre une sécurité accrue en termes d'algorithmes de chiffrement et permet de créer des volumes cachés à l'intérieur du volume principal, dont l'existence ne peut être dévoilée même sous la contrainte.
Le plus connu de ces outils est sans conteste l'application open source et gratuite **TrueCrypt 7.1a** – *la version 7.2 est à éviter* – (https://truecrypt.ch). TrueCrypt a suscité une vive polémique quand en mai 2014, ses auteurs ont subitement annoncé son abandon sous des prétextes qui ont paru suspects à la communauté. Reste que TrueCrypt a été audité fin 2013 et il a reçu une certification de l'ANSSI (l'Agence Nationale de la Sécurité des Systèmes d'Information). C'est donc toujours une valeur sûre – malgré la découverte récente de quelques vulnérabilités mineures. Amazon chiffre les données de ses utilisateurs à l'aide de TrueCrypt.

Petit problème : depuis Yosemite, l'outil ne s'installe plus automatiquement ; un message d'erreur s'affiche recommandant d'utiliser OS X 10.4 ou supérieur ! Il faut donc l'installer manuellement. La manière la plus simple de le faire consiste à faire un clic droit sur l'archive .mpkg et à demander **Afficher le contenu du paquet**, puis à installer individuellement chacun des packages .pkg présents. Au final, l'application fonctionne parfaitement.
La communauté du libre a déjà pris la relève et conçoit sur la base de TrueCrypt, une application open source multiplateforme nommée CipherShed. Elle reprend l'interface de l'original. Comme **VeraCrypt** 3, un clone open source de TrueCrypt, développé par la société de sécurité informatique IDRIX, qui reprend aussi le « design » de l'original, avec la particularité d'être dorénavant compatible avec les conteneurs TrueCrypt.

Les solutions commerciales

Il existe aussi des solutions payantes telles **Secret Folder** d'Apimac (25 € • Mac App Store) ou **Hide Folders for Mac** d'Altomac 4 (www.altomac.com/hide_folders). Ce dernier est gratuit dans sa version de base ; la version Pro ajoute l'indispensable protection d'un mot de passe pour rendre visible les documents. Ces solutions se chargent **de camoufler/dévoiler vos documents à la demande** avec un confort d'utilisation et des interfaces propres aux applications modernes et grand public. Mais elles utilisent souvent les mêmes classiques techniques jouant sur les attributs de visibilité des fichiers. D'ailleurs, on peut dans le Terminal, révéler le contenu des fichiers cachés par Secret Folder via la commande **chflags nohidden** suivi du nom du fichier (avec son extension) ou du dossier ! À ce niveau, Hide Folders est plus sécurisé.