Vous et Votre Mac

Vous et Votre Mac

N° 147 • Septembre 2018 100 % Mac en pratique

Photos
Au retour de vacances, faites le ménage dans la photothèque !

En pratique
Automator expliqué aux débutants.

Apple HomePod
À quoi vous attendre ?

Navigation web
Choisir un autre navigateur que Safari Mobile sur iOS.

iOS
Utiliser l'app Fichiers pour accéder à tous vos documents.

Sur macOS et iOS

8 gestionnaires d'informations personnelles super-sensibles

Comment résoudre le casse-tête des mots de passe !

REDÉCOUVRIR LE DOCK

Pour en tirer un réel bénéfice, il faut en connaître le fonctionnement, éventuellement l'adapter à ses besoins. Et si cela ne suffit pas, il y a des utilitaires qui en démultiplient l'intérêt ou le remplacent, et qui proposent plus de fonctions.

FRANCE métropolitaine: 5,90 € • SUISSE: 9,90 FS
DOM - BEL - MUX - PORT CONT: 6,90 € • CANADA 10,99 $
L 11206 - 147 H - F: 5,90 € - RD

8 gestionnaires de mots de passe et de quelques autres secrets…

La sécurité est-elle suffisamment prise en compte ? Ai-je besoin d'enregistrer mes licences logicielles ou pas ? Gratuité, licence perpétuelle ou abonnement ? Mon navigateur web bénéficie-t-il d'une extension spécifique ? Vais-je pouvoir importer mes identifiants et notes de mon ancien utilitaire ou de mon navigateur ? Bien sûr, l'interface, l'ergonomie et la facilité de prise en main peuvent également avoir leur importance… Choisir un gestionnaire de mots de passe, de données personnelles et de documents sensibles n'est pas évident. Les produits sont nombreux ! Des huit solutions que j'ai testées dans cette sélection, certaines sont parmi les plus populaires, et vous en avez sans doute déjà entendu parler, mais j'ai aussi souhaité vous faire découvrir quelques produits et services nouveaux, comme RememBear et Secrets. DENIS DUBOIS

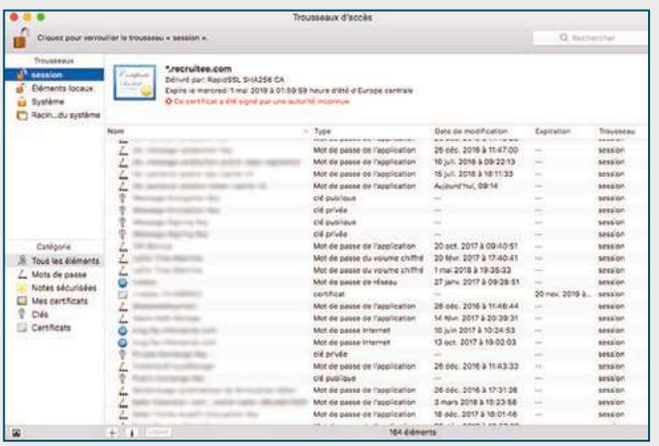
Pour publier sur un forum, faire un achat sur un site marchand, enregistrer une application ou consulter son compte bancaire… il nous faut, à chaque fois, utiliser un identifiant et un mot de passe. D'après les études récentes, nous avons chacun en moyenne plusieurs dizaines de comptes différents sur tous les coins de l'Internet. Difficile de mémoriser toutes ces clés d'accès ! Ceci explique que 52 % des internautes utilisent le même mot de passe pour différents services, bien que ce soit risqué : si ce mot de passe est piraté et revendu, il donne accès à tous vos comptes ! Cela arrive plus souvent que vous ne l'imaginez. Le site *Have I been pwned ?* (Est-ce que je me suis fait avoir ? - **https://haveibeenpwned.com**) vérifie, via une adresse e-mail, si les comptes sur lesquels elle sert d'identifiant ont été compromis lors d'une attaque. Le site recense à ce jour plus de cinq milliards de comptes compromis depuis 2007 sur près de trois cents sites web piratés, de Ashley Madison à Yahoo! en passant par Avast, Dailymotion, Dropbox, LinkedIn et bien d'autres. Aucun site n'est à l'abri. La seule façon de protéger efficacement ses comptes en ligne est d'utiliser un mot de passe unique pour chacun ! La plupart des navigateurs Internet proposent de mémoriser les identifiants à votre place. C'est fort pratique, mais ce n'est pas l'option la plus sûre. Parce que des utilitaires, disponibles sur Internet, se sont spécialisés dans la récupération immédiate de ces mots de passe de navigateurs. Des agences de marketing Internet ont été récemment mises en cause pour avoir utilisé des scripts qui peuvent récupérer vos

identifiants et mots de passe, et de vous suivre à la trace sur l'ensemble des sites qui utilisent le même script. Cette technique est utilisée pour constituer des profils de navigation pour le ciblage publicitaire.
Les gestionnaires de mots de passe sous forme d'extensions de navigateurs requièrent, eux, une action de l'utilisateur avant de remplir les champsde formulaires, ce qui les met à l'abri de cette technique.
Un gestionnaire de mots de passe mémorise et conserve les identifiants et mots de passe associés dans un coffre-fort numérique chiffré. Sur les huit produits et services ici testés, sept utilisent un chiffrement fort AES-256 bits réputé inviolable ; seul Secrets se base sur une simple clé de 128 bits. Ces coffres-forts sont le plus souvent protégés par un mot de passe « maître » unique, le seul qu'il faut absolument mémoriser et ne jamais noter nulle part. Certaines solutions permettent de récupérer ce mot de passe principal oublié, d'autres non. Secrets propose d'imprimer une clé de récupération. Pour Enpass ou SafeInCloud, dont la base de donnée chiffrée est stockée en local sur l'appareil ou dans un service de cloud, la récupération est impossible.
En plus des identifiants et des mots de passe, des gestionnaires sécurisent

de nombreux autres types de données : vos informations personnelles (nom, adresse, date de naissance, etc.), vos documents officiels (carte d'identité, passeport…), vos cartes de paiement, vos comptes bancaires, vos codes Wi-Fi… Certains proposent des dizaines de catégories ! Grâce à ces informations, le gestionnaire sera à même de remplir automatiquement les champs correspondant au sein des formulaires des pages web, vous permettant un gain de temps appréciable. La plupart enregistrent aussi vos notes confidentielles. Tous proposent un générateur de mot de passe, mais il s'agit le plus souvent d'un système classique (caractères majuscules, minuscules, chiffres et symboles). Suivant les nouvelles préconisations du NIST (National Institute of Standards and Technology), 1Password, RememBear et Enpass vont plus loin et génèrent des phrases de passe constituées d'une suite de mots du dictionnaire (généralement anglais). Certaines applications essayent de se démarquer avec des options originales : mot de passe mémorisable ou prononçable. Dashlane, Enpass, Lastpass proposent d'éviter d'utiliser tout caractère ambigu, c'est-à-dire trop similaire (0 et O, ou 1, l et I [i majuscule])afin d'éviter les erreurs.
De plus en plus de gestionnaires, Dashlane, LastPass, 1Password, Secrets et Enpass, intègrent un véritable système d'audit de sécurité. Cette analyse détaillée des mots de passe met en évidence ceux qui sont faibles, trop anciens, qui sont utilisés plusieurs fois ou qui ont été compromis (en faisant appel à la base dedonnées de haveibeenpwned). C'est, à mon avis, un paramètre important à prendre en compte dans le choix d'une solution. 1Password et Dashlane envoient une notification en cas de fuite de données émanant d'un site sur lequel vous avez un compte.
Des solutions vont plus loin en adoptant la double authentification (2FA) pour l'accès à votre compte, ajoutant une sécurité importante contre le vol de votre mot de passe principal puisque ce système exige une information supplémentaire (code d'authentification à usage unique, clé à insérer dans un port USB ou empreinte digitale). Sur les appareils mobiles, il est courant que les gestionnaires gèrent les systèmes de reconnaissance biométriques d'iOS (Touch ID et Face ID) pour le déverrouillage rapide de leur application mobile.

Faire avec les Trousseaux d'Apple ?

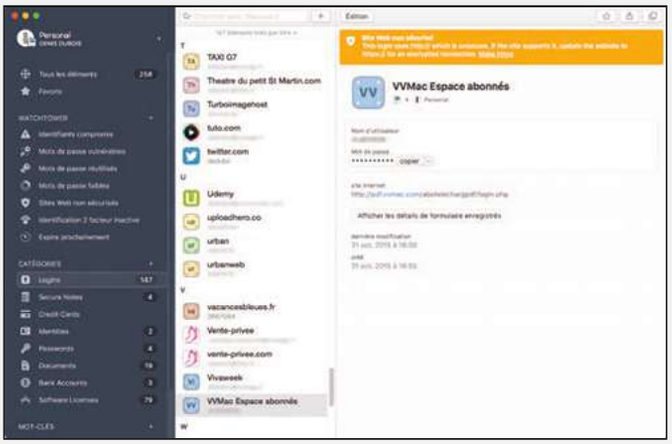
MacOS inclut un gestionnaire de mots de passe, chargé de mémoriser et de remplir automatiquement les informations vous concernant, dans Safari. Trousseaux d'accès (ou Keychain, en anglais) contient bien d'autres informations sensibles : cartes bancaires,réseaux wifi, serveurs FTPS et comptes Internet auxquels vous vous connectez, certificats des sites web et des comptes de messagerie… ou encore des notes sécurisées dans lesquelles on peut enregistrer des informations privées. Cette solution propose aussi un générateur de mots de passe.

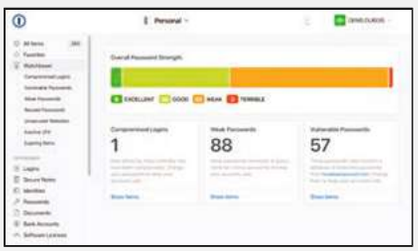


Trousseaux d'accès (au pluriel, car on peut gérer plusieurs bases de données) est une application uniquement disponible sur macOS, à dénicher dans le sous-dossier Applications/Utilitaires. Elle n'a pas d'équivalent sur iOS. En revanche, la base de données, synchronisée par iCloud, rend toutes ces informations accessibles sur les Mac d'un même compte Apple, et pour les identifiants/mots de passe et les certificats sur tous vos matériels iOS dans Safari mobile et Mail.
Toutes ces informations sont protégées par un chiffrement AES 256 bits, de bout en bout, sous la condition que l'identification à deux facteurs de l'identifiant du compte Apple soit activée sur tous les matériels.
Alors, pourquoi ne pas se contenter de Trousseaux, pourquoi utiliser un gestionnaire externe, le plus souvent payant ?
L'application Trousseaux d'accès reste austère et minimaliste. Elle offre un éventail de fonctions restreint par rapport à ses concurrents commerciaux. Elle est tellement peu agréable à utiliser qu'Apple a proposé un accès aux identifiants et aux mots de passe web directement dans Safari (Préférences > mots de passe). Les Trousseaux iCloud ne possèdent pas d'interface en ligne sur le portail icloud.com, pas d'application mobile autonome, et aucune portabilité vers Android ou Windows. Sur les appareils iOS, seul Safari Mobile y accède.
Reste que cela pourrait bien changer avec macOS Mojave et iOS 12 ! En effet, le service de Trousseaux sur iCloud est en passe de devenir un gestionnaire à part entière avec une véritable interface de gestion, accessible via iCloud, et un système d'analyse destiné à avertir l'utilisateur de la récurrence de certains mots de passe. Enfin, le Trousseau iCloud pourrait s'ouvrir aux applications tierces qui utiliseront la nouvelle API Password Manager.

1Password

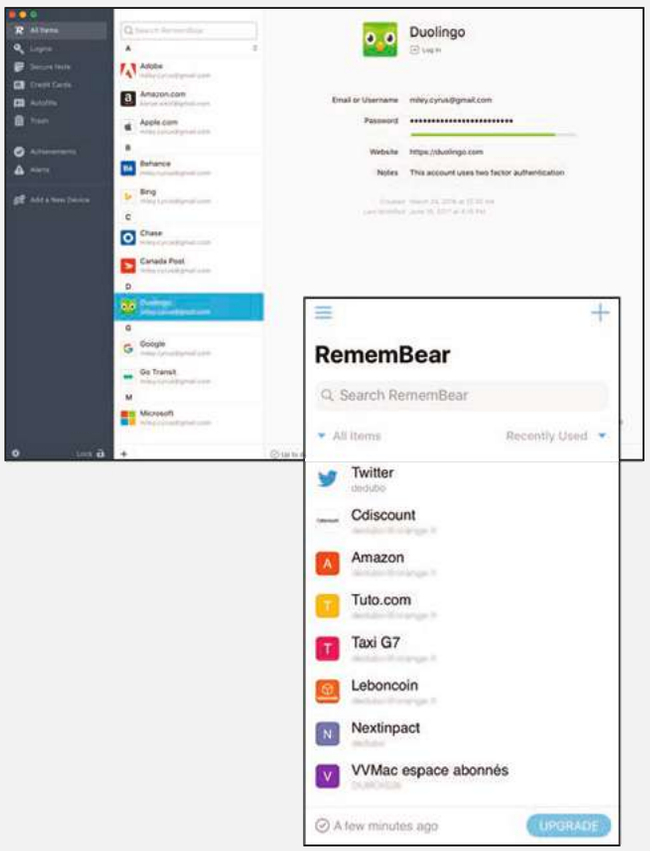
*macOS 10.12+ et iOS 11.0 • **Éditeur** : Agilebits • **Distribution** : Mac App Store ou 1Password.com • **Prix** : abonnement à 4,50 €/mois ou 41 €/an sur la Mac App Store (avec 1 Go) ou encore licence perpétuelle à 69 € (MàJ 53 €) directement depuis l'app.*





Agréable et fonctionnel, doté d'une bonne ergonomie, 1Password propose un panneau latéral sombre rétractable et la possibilité d'afficher des icônes élaborées pour les sites et les licences d'applications. La fenêtre d'identification est détachable et superposable pour copier plus facilement les informations dans une application et le nouveau module 1Password mini en barre des menus détecte et propo se les identifiants d'un site ou d'une application. 1Password prend en charge de nombreux types d'éléments : notes sécurisées, comptes bancaires et cartes de crédits, identité, documents, licences logicielles… chacun avec un formulaire spécifique (non francisé et un peu austère). Une extension pour Safari est intégrée à l'app (et se met à jour avec elle) et d'autres sont proposées pour Chrome, Firefox et Opéra. Une application mobile pour iOS et Android donne accès à la base des données. Pour les abonnés au service, la synchronisation des données entre appareils est gérée de façon transparente. Les autres passent par iCloud, Dropbox ou quelques autres clouds. Sur iOS, on peut utiliser le navigateur intégré (1Browser) ou l'extension pour Safari Mobile. 1Password est compatible avec Touch ID et Fac e ID et offre même une mini app sur l'Apple Watch. Quand on est abonné, on accède à ses mots de passe et à ses notes sécurisées sur n'importe quel appareil, via une interface web. Comme Dashlane et LastPass, 1Password dispose d'un système d'audit intégré, Watchtower (Tour de guet), qui contrôle le niveau de sécurité des éléments stockés dans les coffres-forts. Il alerte lorsque des identifiants ont été compromis ou sont vulnérables, prévient des mots de passe faibles ou réutilisés et propose d'activer l'identification à 2 facteurs sur les sites qui en dispose.

1Password est un excellent gestionnaire, très complet, bien sécurisé et intégré à macOS. La toute dernière mise à jour apporte le balisage Markdown dans les notes sécurisées. Mais on comprend mal pourquoi de nombreux éléments de l'interfac e ne sont pas francisés.



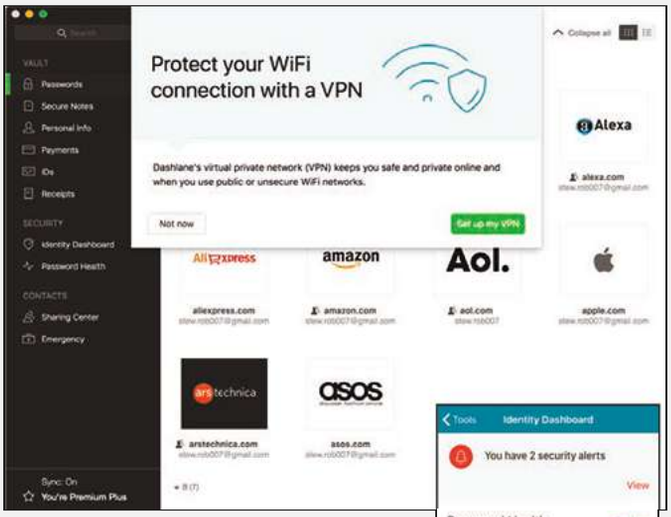
RememBear

*macOS 10.11+ et iOS 9.0+ • **Éditeur** : TunnelBear • **Distribution** : www.remembear.com • **Prix** : gratuit (pour 1 appareil), abonnement Premium (36 $/an – env. 33 €).*

RememBear est un nouveau venu. Doté d'une interface, malheureusement non francisée, mais plaisante et graphique, avec quelques animations sympathiques, il stocke les identifiants/mots de passe et les informations de cartes de paiement… et c'est tout. Pas de notes sécurisées ni d'autres catégories d'éléments. Il s'interface via des extensions à Safari, Chrome et Firefox afin de remplir automatiquement les champs des identifiants des sites web visités. L'extension affiche un champ de recherche et un générateur de mots de passe de nouvelle génération cap able, outre des mots de passe constitués par une suite de caractères, de créer des « phrases » complètes. RememBear importe les données du Trousseau iCloud (la solution d'Apple), de 1Password et de LastPass, ainsi que les identifiants sauvegardés par les navigateurs Chrome et Firefox.

Des versions mobiles sont disponibles pour iOS et Android. L'application iOS gère la reconnaissance sécurisée Touch ID e t dispose de son propre navigateur, Bear-owser, ainsi que d'une extension pour Safari Mobile. RememBear est une application à la sécurité sans concession (son éditeur propose aussi le VPN TunnelBear) : le chiffrement est robuste, la synchronisation des données ne peut s'effectuer qu'avec des matériels dûment autorisés. Même s'il possédait votre mot de passe maître, un hacker ne pourrait pas accéder à votre compte RememBear. Enfin, la sécurité du code source est régulièrement vérifiée par une autorité indépendante, affirme l'éditeur.

RememBear est un bon gestionnaire, efficace et agréable à l'utilisation. On peut regretter qu'il ne soit pas prévu d'option, comme dans Dashlane, qui supprime le logo dans les champs des formulaires d'identification – ça s'avère agaçant à la longue (et gênant pour les c aptures d'écran). Dommage aussi qu'il ne propose pas d'outil d'audit de sécurité intégré. Si vous souhaitez l'adopter, il en faudra en passer obligatoirement par un abonnement.



Dashlane

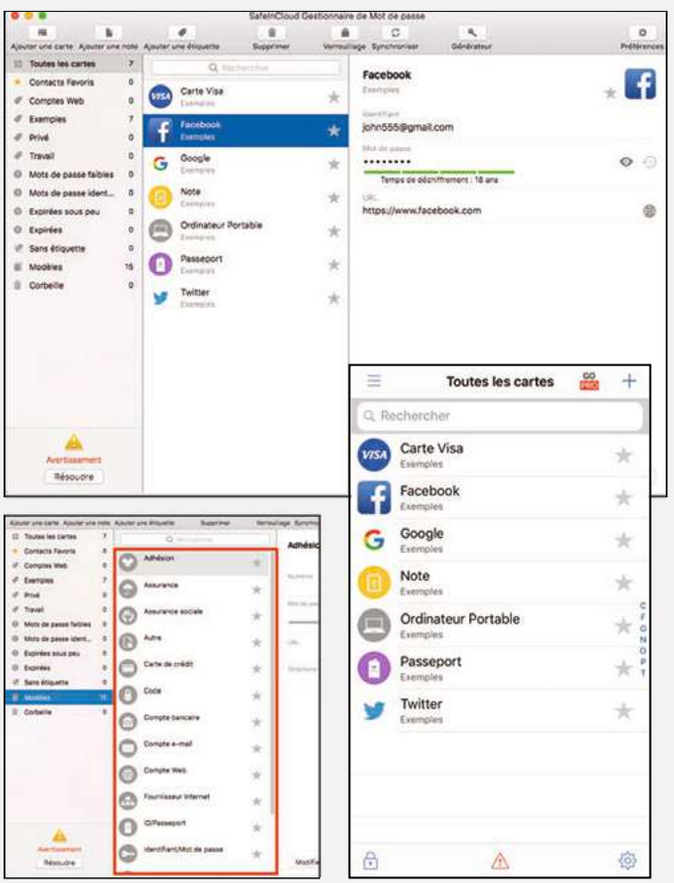
*macOS 10.11.5+ et iOS 11.0 • **Éditeur** : Dashlane • **Distribution** : Mac App Store ou www.dashlane.com/fr • **Prix** : gratuit (1 seul appareil) ou licence Premium (abonnement de 40 €/an sur le site ou 44 €/an via les achats intégrés de la Mac App Store).*

Ce logiciel, dont la version 6 est sortie au cœur de l'été, est doté d'une interface sophistiquée (pas encore francisée), dans laquelle les sites apparaissent sous forme de briques graphiques. Un panneau latéral, non rétractable, présente les différents types d'éléments gérés : données personnelles (adresse, mail, téléphone), moyens de paiement (carte bancaire, compte PayPal, compte bancaire), pièces d'identité (CNI, passeport, permis de conduire, etc.) et reçus. Les licences logicielles ne sont pas prises en charge. L'application est disponible sur toutes les plateformes, bureau et mobiles. La synchronisation implique un compte Premium. L'app mobile, qui gère Touch ID, est d'une grande simplicité d'utilisation, avec la même sobriété dans l'interface. Un navigateur « maison » est propos é ainsi qu'une extension pour Safari Mobile. Dashlane sait importer les mots de passe de Safari, de Chrome et de Firefox, pour lesquels il a aussi des extensions dédiées. Il offre une interface web pour ses clients Premium, avec accès aux mots de passe, aux notes sécurisées et aux informations de cartes bancaires. Le nouveau Centre de contrôle (Dashboard) intégré s'assure du niveau de sécurité des m ots de passe stockés, indique les mots de passe faibles ou réutilisés, trop anciens ou compromis et classe les sites et identifiants en fonction de leur niveau de sécurité… Il affiche un score de sécurité assorti de conseils pour l'améliorer. La fonction Password Changer remplace en un clic vos anciens mots de passe trop faibles ou compromis par de nouveaux plus forts. Un système d'alerte en temps réel sur vos appareils se déclenche si un compte est compromis. En plus de la synchro, un compte Premium gère la double authentification avec les apps compatibles 2FA ou les clés USB compatibles FIDO U2F, fournit un VPN et un espace de stockage de 1 Go pour les mots de passe (illimité) et les fichiers sensibles. Esthétique, sobre et fonctionnel, ce logiciel français se place d'emblée parmi les meill eurs. L'absence d'une licence perpétuelle est regrettable, mais Dashlane propose des abonnements à tarifs dégressifs si on prend plusieurs années.

SafeInCloud

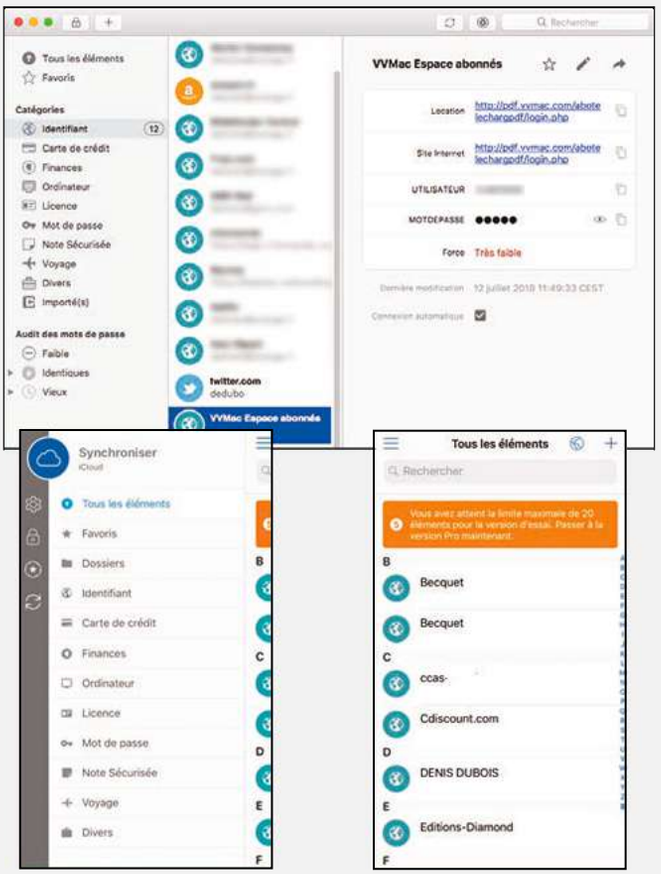
*OS X 10.10+ et iOS 9.0+ • **Éditeur** : Andrey Shcherbakov • **Distribution** : (Mac App Store et safe-in-cloud.com/) • **Prix** : Gratuit et Version Pro (7 €)*

Cette solution multiplateforme, également disponible pour l'Apple Watch, sauvegarde identifiants, mots de passe et autres informations privées dans une base de données chiffrée, en local ou synchronisée avec Google Drive, DropBox, OneDrive, ou avec un serveur WebDav (pour la synchronisation vers un NAS personnel).
Une quinzaine de modèles de cartes pour stocker toutes vos informations personnelles est disponible . Identifiants et mots de passe, cartes bancaires, comptes bancaires, assurances, passeports et permis de conduire, licences de logiciels sont de la partie. Chaque carte peut être associée à un ou plusieurs mots-clés (Privé, Travail, etc.). L'application propose également un outil de prise de notes sécurisées, auxquelles on peut même joindre des images et des fichiers.
La version de bureau, gratuite, sait importer les identifiants de 1Password, Dashlane, LastPass, Enpass… et exporter la base de données vers un fichier au format TXT, XML ou CSV. Des extensions pour Safari, Firefox, Chrome, Opera ou Yandex sont fournies. SafeInCloud existe aussi pour iOS ou Android, et contient un navigateur web intégré. Mais pas d'extension pour Safari Mobile !
En termes de sécurité, les données sont chiffrées AE S-256 bits en local ou avant d'être envoyés dans un nuage. SafeInCloud avertit lorsqu'il détecte des mots de passe faibles ou un même mot de passe utilisé sur différents comptes. Une option, présente tant sous iOS que sous macOS, permet de supprimer définitivement des données après un certain nombre de tentatives d'accès en échec.
SageInCloud est un gestionnaire peu connu mais bien noté sur les stor es. Il s'adresse surtout aux utilisateurs novices qui cherchent une solution économique. Avec une interface francisée et claire, il est accessible au plus grand nombre. Toutefois, malgré le chiffrement, la sécurité n'est pas le point fort de l'application. On aurait apprécié une analyse approfondie des mots de passe pour mettre en avant les mots de passes vulnérables, compromis ou anciens…



Enpass

*macOS 10.8+ et iOS 9.0+ • **Éditeur**: Sinew Software Systems • **Distribution**: Mac App Store et sur le site www.enpass.io • **Prix**: Gratuit ou Pro (11 €)*



L'installation à partir du Mac App Store est très rapide. Attention, en cas d'oublie, aucune récupération du mot de passe maître n'est possible. On se rend compte immédiatement que l'interface, entièrement francisée, s'inspire beaucoup de celle de 1Password. En plus des mots de passe, Enpass stocke de très nombreux éléments, en catégories : cartes de crédit, passeports, comptes bancaires, notes sécuri sées… C'est un des plus complets en la matière.

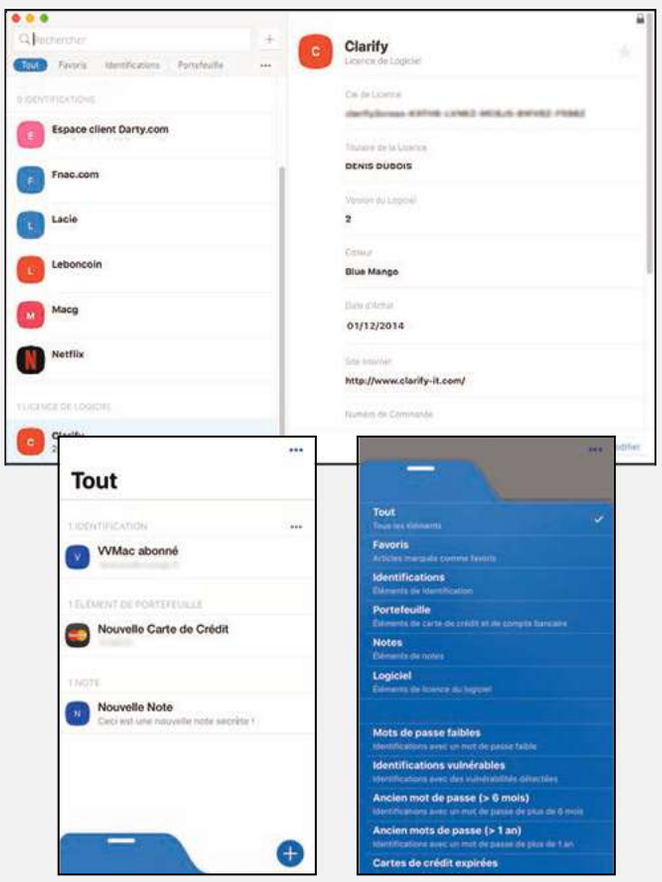
Des extensions permettent de remplir automatiquement les champs des formulaires d'identification dans Safari, Google Chrome, Firefox et Opera. Il sait également importer depuis LastPass, Dashlane, 1Password et SafeInCloud, ou depuis un format générique CSV (mais il ne peut pas récupérer les mots de passe stockés dans un navigateur).

Les données sont stock ées, chiffrées, en local sur votre appareil ou dans les nuages iCloud, Dropbox, Google Drive, OneDrive et Box. Donc, il n'existe pas d'interface web d'accès aux données.

Enpass est proposé aussi pour iOS (et l'Apple Watch) et Android, mais la synchronisation en ligne est limitée. Au-delà de 20 mots de passe, il faut un compte Pro vendu en licence perpétuelle à un coût très raisonnable. Enpass gère Tou ch ID et possède son propre navigateur pour lequel on peut choisir son moteur de recherche parmi sept dont Qwant. On peut aussi modifier l'agent utilisateur pour le faire passer pour Safari, Chrome ou Firefox auprès des serveurs web.

La fonction Audit de mots de passe est intégrée, mais pas la double authentification.

Enpass est très similaire à SafeInCloud dans ses fonctions comme dans son modèle éco nomique. Au final, c'est une bonne surprise. Le niveau de sécurité est correct, mais légèrement en dessous des ténors du marché. C'est une solution à prendre en compte si vous recherchez un gestionnaire complet, néanmoins économique et sans abonnement.



Secrets

*macOS 10.11+ et iOS 9.0+ • **Éditeur**: Outer Corner • **Distribution**: Mac App Store et https://outercorner.com/secrets-mac • **Prix**: Gratuit (10 éléments) / Premium 22 € macOS et 11 € iOS (Secrets Touch)*

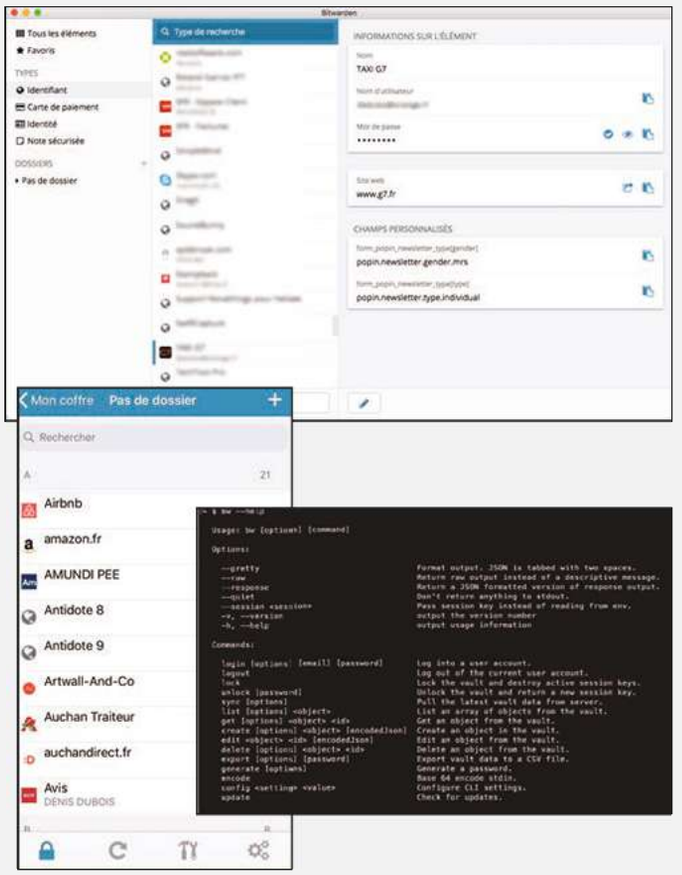
L'installation est simplifiée au maximum grâce à un assistant. On découvre un gestionnaire simple, mais complet. Secrets stocke les éléments d'identification de connexion aux services web, les informations de cartes et de comptes bancaires, les notes sécurisées et même les licences des logiciels. Il ne propose à cette heure qu'une extension pour Safari et Safari mobile, mise en place automatiquement lor s de l'installation, et il n'a pas de navigateur intégré.

Il sait importer depuis 1Password ou LastPass, ou via le format de fichier générique CSV. Par contre, il n'est pas proposé de récupérer les identifiants stockés dans les navigateurs.

Une application mobile, à l'interface minimaliste, Secrets Touch, est disponible dans l'iOS App Store. La synchronisation des données s'effectue par iCloud. Pour se connecter à l'application, la reconnaissance biométrique Touch ID et Face ID est prise en charge.

Concernant la sécurité, là aussi c'est le service minimum. Les données sont stockées au format OpenPGP avec un chiffrement AES-128bits et RSA, là où ses concurrents utilisent tous une dé de chiffrement de 256 bits. Contacté, l'éditeur affirme ne pas vouloir pénaliser les performances des anciens app areils iOS. Toutefois, des filtres intéressants sont proposés afin d'identifier les mots de passe faibles, anciens ou vulnérables, de rechercher les comptes et mots de passe piratés ainsi que les cartes de crédit expirées. Il est également possible de créer ses propres filtres.

Secrets sait générer un mot de passe unique, associé à un QR code, pour les services qui supportent la double authentificati on (Google, Facebook, etc.). Reste que Secrets est un produit (trop ?) jeune. Son utilisation n'est pas aussi intuitive que celle de bon nombre d'autres gestionnaires concurrents, même en passant par l'extension Safari. Il s'adresse donc aux utilisateurs de Safari dont c'est le tout premier gestionnaire, qui veulent une solution simple à un prix raisonnable, sans abonnement.



Bitwarden

*macOS 10.9+ et iOS 9.0 • **Éditeur**: 8bit Solutions • **Distribution**: Mac App Store ou bitwarden.com • **Prix**: Licence personnelle Gratuite ou Premium (10 $/an)*

Voici une application native multiplateforme, open source et francisée, à l'interface sobre et assez classique, qui prend en charge quatre types d'éléments : identifiants de sites/mots de passe, informations de cartes de paiement, informations d'identité (numéros de passeport, de permis, de sécurité sociale), et notes sécurisées. La version gratuite permet de stocker un nombre illimité d'éléme nts. Elle offre le plus grand nombre d'extensions, avec le support de navigateurs « très sécurisés » comme Vivaldi, Brave et Tor Browser. Depuis l'extension, comme depuis l'application native, un bouton permet de vérifier si un mot de passe a été exposé ou non à une fuite de sécurité connue. Des apps mobiles sont disponibles pour iOS et Android, avec un classique générateur de mots de passe et le déver rouillage Touch ID. La version gratuite permet même la synchronisation sur un nombre illimité d'appareils ! Une fois l'extension activée, on utilise Bitwarden dans Safari Mobile pour le remplissage automatique (il n'y a pas de navigateur intégré). Bitwarden importe les données depuis une impressionnante brochette de gestionnaires et des navigateurs web. Son coffre web est accessible depuis n'importe qu el navigateur, même dans la version gratuite. Le support de base de l'authentification à double facteur (2FA) renforce la sécurité de la connexion.

La version Premium autorise des méthodes avancées d'authentification et offre un espace de 1 Go pour stocker des fichiers sensibles.

Une des particularités de Bitwarden, est la possibilité d'accéder à votre coffre par le Terminal et d'éditer et exécuter des scripts pour gérer les éléments et toutes les fonctions. Enfin, pour davantage de confidentialité, rien ne vous empêche d'héberger vous-même une instance de Bitwarden.

Bitwarden est un produit unique dans le monde des gestionnaires parce qu'il est open source et parce que sa version gratuite est parfaitement fonctionnelle (stockage d'un nombre illimité d'éléments, synchronisation sans limite, accès web !). Un très bon choix.

LastPass

*macOS 10.11+ et iOS 10.0 • **Éditeur**: LogMeIn • **Distribution**: Mac App Store et www.lastpass.com/fr • **Prix**: Gratuit, Premium (27 €/an) ou Famille (4 $/mois)*

C'est un gestionnaire très populaire, disponible sur de nombreuses plateformes qui a pour particularité une gestion entièrement en ligne des mots de passe ; ils sont stockés sur le web et les applications ne sont qu'une interface. L'application permet l'enregistrement des identifiants des sites Internet et des notes sécurisées pouvant contenir des informations de comptes bancaires ou de cartes de paiement, des mots de passe Wi-Fi et même des licences logicielles… Formulaires permet de préremplir des formulaires de sites web avec les informations courantes (adresse, contacts, infos bancaires, cartes de paiement…). LastPa ss dispose d'extensions pour Safari, Firefox, Chrome et Opera dont il importe les mots de passe qui y sont enregistrés. Les principaux gestionnaires concurrents sont supportés à l'import également (ainsi que le fichier générique CSV). Les applications mobiles pour iOS (et Apple Watch et reconnaissance biométriques) et Android ont leur propre navigateur intégré, en plus des extensions pour Safari mobi le et Chrome. On note la possibilité de partager des mots de passe et notes de manière sécurisée avec d'autres utilisateurs et de spécifier un ou plusieurs contacts de confiance qui auront un accès au coffre en cas d'urgence. Question sécurité, l'algorithme AES-256 est mis à contribution pour chiffrer et déchiffrer les données en local sur l'appareil, ainsi que TLS, qui offre une protection contre *le s attaques par intermédiaire* lors de la synchronisation des données. La fonction Challenge de sécurité analyse les mots de passe (force, doublons, compromission…) et gratifie d'un score de sécurité. L'authentification à deux facteurs est disponible pour sécuriser l'accès au coffre – même en version gratuite. L'option Premium propose comme Bitwarden des solutions d'authentification avancées (clés USB FI DO U2F et YubiKey dotés d'un lecteur d'empreintes digitales) ainsi que 1 Go d'espace de stockage. C'est donc un produit relativement classique, complet et bien sécurisé, avec des fonctions intéressantes, mais il est, pour moi, pénalisé par une interface spartiate, partiellement traduite tant sur macOS que sous iOS, et qui souffre d'une ergonomie rudimentaire.