Vous et Votre Mac

Vous et Votre Mac

N° 146 • Juillet-Août 2018 100 % Mac en pratique

Photographie

4 alternatives à Apple Photos pour gérer et retoucher vos images.

S'informer

6 applications Mac pour organiser les flux RSS et lire en différé.

Nouveau !

iOS 12

Performances,
Réalité augmentée,
Bien-être numérique...

Apple dévoile macOS 10.14 Mojave

Un somptueux mode sombre,
Le plein de petits outils sympathiques,
APFS pour tous les disques...

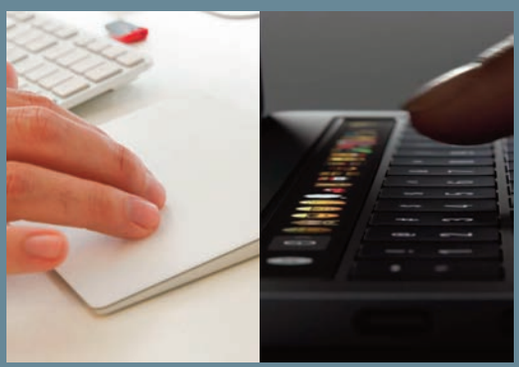
Conseils de sécurité

Comment protéger au mieux votre Box et son réseau Wifi.

Un lecteur PDF

S'en tenir à Aperçu ou lui préférer Adobe Reader ?

FRANCE métropolitaine : 5,90 € • SUISSE : 9,90 FS
DOM - BEL - MUX - PORT CONT : 6,90 € • CANADA 10,99 $
L 11206 - 146 - F: 5,90 € - RD



Trackpad et Touch Bar

Les fonctions à connaître, les bons paramètres à passer, et les petits outils pour exploiter au maximum les interfaces « tactiles » de nos Mac.

Protéger au mieux

Porte ouverte sur l'Internet, votre box mérite que vous preniez un peu de temps pour la configurer. Comme la portée de son réseau Wifi dépasse le cadre de votre domicile, vos voisins ou des inconnus dans la rue, dans un véhicule, à la recherche de réseaux sans fil peu ou pas sécurisés, peuvent intercepter les données transmises, même avec un smartphone. Voire en faire une utilisation malveillante et, en cas de problème, vous êtes seul responsable juridique, si vous ne pouvez prouver que vous aviez pris les mesures nécessaires à votre protection. DENIS DUBOIS

MODIFIEZ L'IDENTIFIANT ET LE MOT DE PASSE D'ACCÈS À L'INTERFACE DE CONFIGURATION

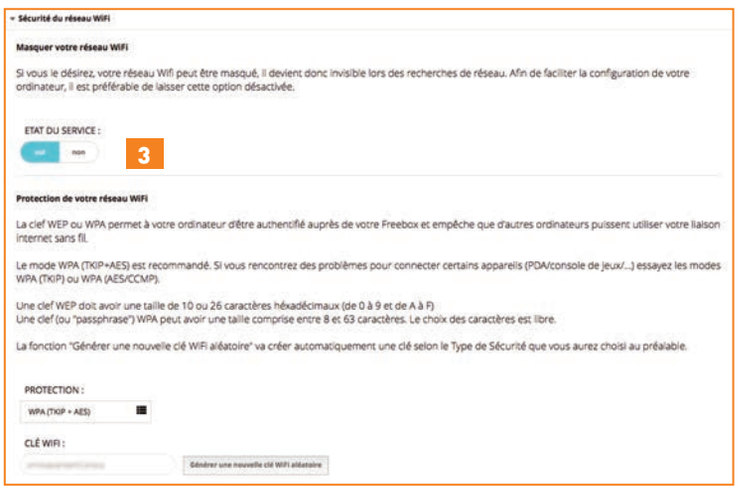
La plupart des box sont configurés avec **un mot de passe par défaut**. C'est le même pour toutes les box d'un même opérateur. Pour éviter qu'un intrus ne puisse accéder à la configuration de votre box, **personnaliser vos identifiants et le mot de passe**. Utilisez un mot de passe suffisamment **long d'au moins 12 caractères** et sans aucun sens logique (éviter les noms, dates de naissance…). En cas d'oubli du mot de passe, les box proposent un lien **[1]** *(ici Livebox et Free)* sur la page d'accueil de l'administration, **pour réinitialiser un mot de passe oublié**. En dernier ressort, elles ont un bouton physique de réinitialisation pour revenir aux paramètres d'usine.

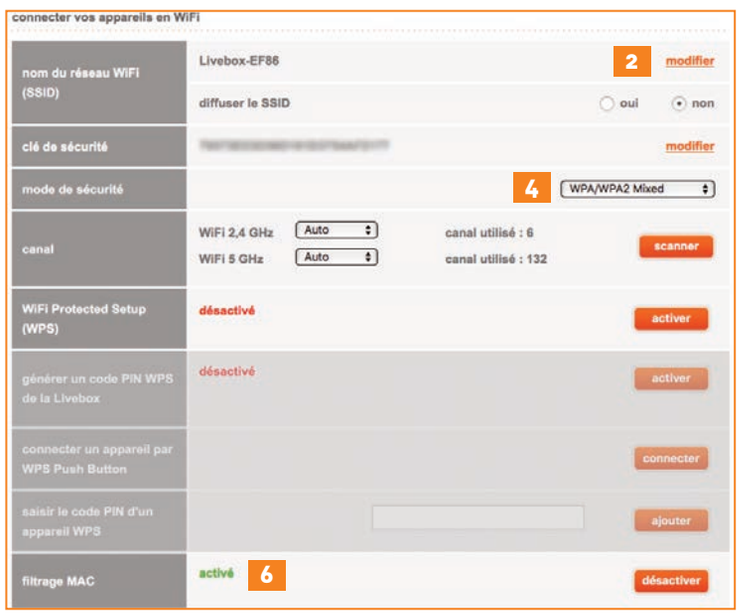
CHANGEZ ET MASQUEZ LE NOM DE VOTRE RÉSEAU WIFI

Le nom de votre réseau, le SSID (Service Set Identifier), permet aux points d'accès et aux appareils d'identifier votre réseau sans fil, et donc de s'y connecter. Il permet aussi aux utilisateurs d'identifier votre réseau Wifi dans la liste des réseaux présents dans leur environnement. Si votre box est fourni avec un SSID par défaut, **changez son nom [2] pour le rendre unique parmi ceux que vous détectez tout autour de vous**. Sinon, vous pourriez rencontrer des difficultés de connexion. Le SSID étant sensible à la casse, vous pouvez utiliser des minuscules, des majuscules et même des chiffres. Ensuite, **je vous conseille de masquer le nom de votre réseau [3]**. Inutile de diffuser son nouveau SSID. Concrètement, personne ne verra votre réseau dans la liste des points d'accès disponibles. Pour ce faire, allez dans la section des paramètres Wifi de la console d'administration de votre box.

- ▶ **Freebox** : Dans **Sécurité du réseau Wifi** > **Masquez votre réseau Wifi** > **Oui**
- ▶ **Livebox** : Onglet **Mon Wifi** > **Wifi avancé** > **Diffusez le SSID**, cochez **Non**
- ▶ **SFR** : Onglet **Configuration** > **Diffusion du SSID**, cochez **Désactivé**.

Notez toutefois que cela ne renforce pas démesurément la sécurité car, entre des mains compétentes, il existe d'autres moyens pour détecter le SSID.



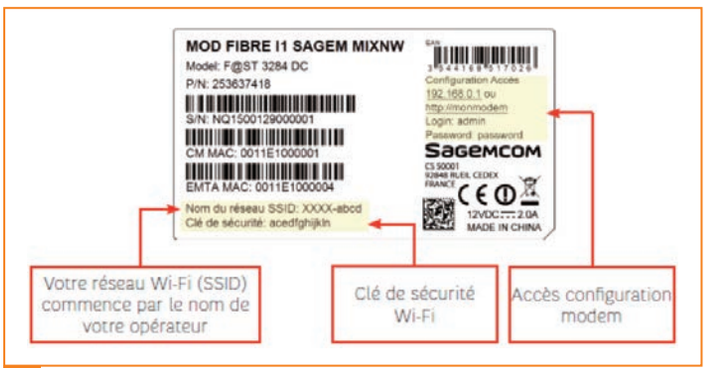


ADOPTEZ UN PROTOCOLE DE CHIFFREMENT SOLIDE

En l'absence de chiffrement, n'importe qui peut lire les données qui transitent sur le réseau à l'aide d'un « renifleur » comme WireShark ; il intercepte le trafic réseau et affiche le contenu des paquets en transit.

Les box proposent **différents niveaux de chiffrement** via les protocoles **WEP**, **WPA** et **WPA2**. Le premier est à éviter : il est obsolète et sa clé de chiffrement est reconstituée

votre box Internet et son Wifi



5

en quelques minutes avec un logiciel spécialisé. WPA (Wifi Protected Access) est mieux sécurisé, il utilise le chiffrement TKIP et une clé pré-partagée, appelée PSK, qui empêche un attaquant de reconstituer la clé de chiffrement en analysant les données. **WPA2, lui, s'appuie sur le chiffrement AES (parfois nommé CCMP) ; c'est actuellement le meilleur choix en termes de sécurité et il est, de plus, le seul protocole à tirer pleinement parti des performances du Wifi 802.11n**.
Certaines box, comme la Livebox, proposent **un mode WPA/WPA2 mixed [4]** qui sélectionne automatiquement le meilleur mode en fonction de votre appareil.
Il permet de concilier des matériels anciens, compatibles avec WPA-TKIP et des matériels récents qui utilisent le chiffrement WPA2 AES.
Pensez à sélectionner **le même protocole sur tous vos matériels**, mobiles ou portables, lorsque vous vous connectez à votre réseau Wifi.

RENOUVELEZ LA CLÉ DE SÉCURITÉ WIFI

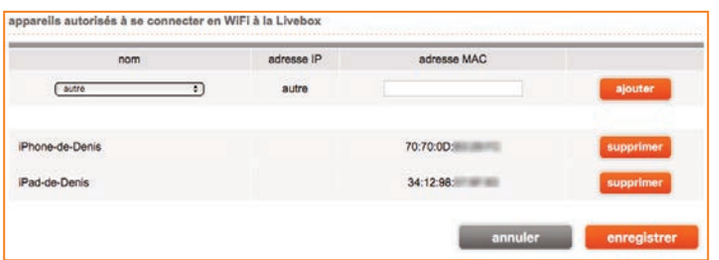
Il est recommandé de renouveler régulièrement la clé de sécurité Wifi de votre box. Au moins deux fois par an, car vous êtes juridiquement responsable de l'utilisation qui est faite de votre réseau Wi-Fi, même par un tiers non autorisé (un voisin par exemple). À ce titre, **vous avez le devoir légal de le protéger convenablement**.
Il est vrai que le simple fait que la clé de sécurité soit imprimée sur l'étiquette de certaines box **[5]** n'incite pas a son changement. Cela laisse supposer, à tort, qu'elle est gravée dans le marbre et qu'il ne faut surtout pas la modifier. **Il n'en est rien**, c'est juste une facilité pour les clients étourdis et le SAV de l'opérateur.
La modification s'effectue dans l'interface de configuration de votre box.
Connectez votre Mac à la box via **un câble Ethernet**, car vous perdrez provisoirement la connexion sans fil. Cochez la case **Afficher le mot de passe** pour ne pas commettre d'erreur de saisie et **entrez une nouvelle clé entre 8 et 63 caractères**. Une fois la modification enregistrée, il vous faudra reconfigurer la connexion Wi-Fi de tous les matériels sans fil !
Note : la clé de sécurité qui se trouve sur l'étiquette de votre box ne sera plus utile.

FILTRER GLOBALEMENT ET AUTORISEZ SÉLECTIVEMENT

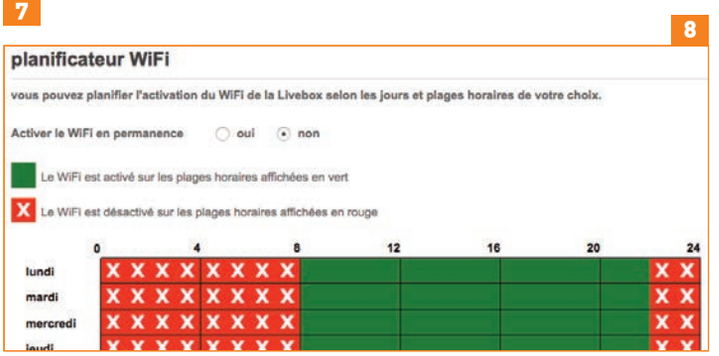
L'adresse MAC correspond à l'identifiant physique unique d'une carte réseau ou d'une interface réseau.
Allez dans **les réglages Wifi de la box**, à la section **Filtrage MAC [6]**.
La **Livebox** permet de sélectionner directement les appareils détectés sur le réseau dans une liste déroulante, évitant la saisie fastidieuse des adresses MAC (Media Access Control). Cette fonction restreint l'accès au réseau Wifi aux seuls matériels que vous aurez approuvés en ajoutant leur adresse MAC dans la liste **[7]** des équipements autorisés. Vous devrez donc préalablement noter les adresses MAC de vos différents appareils. L'adresse MAC de vos appareils se trouve :
▶ **iOS** : **Réglages > Général > Informations > Adresse Wi-Fi**
▶ **macOS** : **Menu Pomme > À propos de ce Mac > Rapport système**…
puis **Réseau > Wi-Fi**.
▶ **Android** : **À propos de l'appareil > État des paramètres > Adresse MAC Wi-Fi**
Il est aussi possible de modifier une adresse MAC, mais cette solution n'est pas suffisante en elle-même pour empêcher un accès non autorisé par une personne expérimentée.

DÉSACTIVEZ LE WIFI QUAND IL N'EST PLUS NÉCESSAIRE

Toutes les box permettent de **définir des plages d'activation du réseau Wi-Fi selon les heures et les jours de la semaine [8]**. Inutile de le laisser allumer toute nuit, ou le week-end si vous n'êtes pas là. C'est prendre un risque inutile d'intrusion malveillante.
La Livebox présente un bouton physique très pratique pour allumer/éteindre le Wi-Fi à tout moment, indépendamment des plages programmées.
Lorsque vous partez en vacances, vous pouvez laisser la box allumée pour accéder à distance à vos contenus multimédias ou pour programmer des enregistrements d'émissions ou de films, **mais pensez à éteindre le Wi-Fi dans la console d'administration web**.



7



8

FERMEZ LES ACCÈS À DISTANCE

Les box récentes peuvent être utilisées comme de véritables NAS pour accéder à vos contenus multimédias à distance. Si vous n'utilisez pas ces fonctions, ni la programmation TV à distance, **désactivez l'accès à distance**. Cela évitera les risques d'intrusion malveillante en fermant une porte d'accès à votre box.

N'UTILISEZ PAS L'APPAIRAGE WPS

Certaines box (Freebox, Livebox) proposent **un bouton WPS (Wi-Fi Protected Setup)** d'appairage rapide et sécurisé de périphériques au réseau domestique. Cette fonction simplifie au maximum la configuration de la sécurité du réseau via le protocole WPA.
Il suffit d'appuyer sur le bouton physique (ou virtuel) WPS présent sur les deux appareils pour appairer la box à une imprimante sans fil, par exemple, sans avoir besoin d'entrer la clé de sécurité Wi-Fi. Le standard WPS comprend également une méthode de vérification par code PIN proposé par certaines box (SFR). Un numéro présent sur l'appareil à connecter au réseau sans fil est à reporter sur le point d'accès.
Quelle que soit la méthode employée, le standard WPS fait l'objet de graves vulnérabilités, il est fortement déconseillé de recourir à cette facilité.

RememBear
sur Mac, iOS…

J'AIME
L'interface plaisante, claire et animée ; l'extension pour Safari ; le niveau de sécurité.

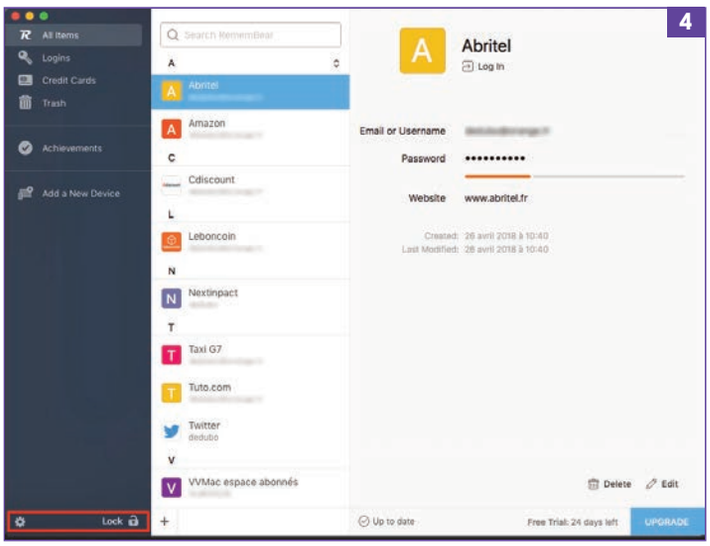
J'AIME MOINS
Le code source non disponible ; distribué sous forme d'abonnement pour plus d'un matériel ; en anglais.

ANGLAIS
Prix : gratuit si utilisation sur un seul matériel ; sinon version Premium à 35 €/an pour synchronisation entre matériels et sauvegarde.
Config. : macOS 10.12+ et iOS 11
Éditeur : TunnelBear
Mac App Store, iOS App Store
https://www.remembear.com

Placez-vous sous la protection d'un ours

Après avoir proposé un des meilleurs services de VPN sur Mac, l'éditeur TunnelBear se lance sur le marché des gestionnaires d'identifiants/mots de passe, avec un produit de qualité, disponible entre autres sur Mac et iOS, et très sécurisé.

Nous avons tous des dizaines de mots de passe à gérer pour accéder à nos services dématérialisés. Dans mon article sur les mots de passe (VVMac 145), je vous recommandais d'en créer un nouveau pour chacun de ces services et de les stocker dans un gestionnaire de mots de passe. Pas dans votre navigateur ! Des gestionnaires, il en existe de nombreux. Dans VVMac 142, je vous avais parlé de la solution libre Bitwarden. Un nouveau venu, RememBear, a fait depuis son entrée sur le marché. C'est une solution propriétaire, tout comme 1Password, l'un des plus connus. Son éditeur est déjà connu pour son application de VPN, TunnelBear, qui jouit d'une bonne réputation. Une des rares applications mobiles à ne disposer d'aucun tracker, même sous Android ! La sécurité est au cœur des préoccupations de l'éditeur.

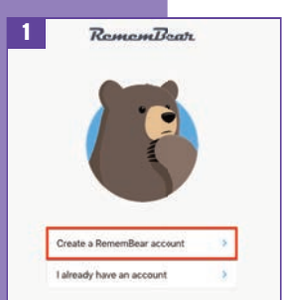


4

UNE INSTALLATION TRÈS SIMPLE

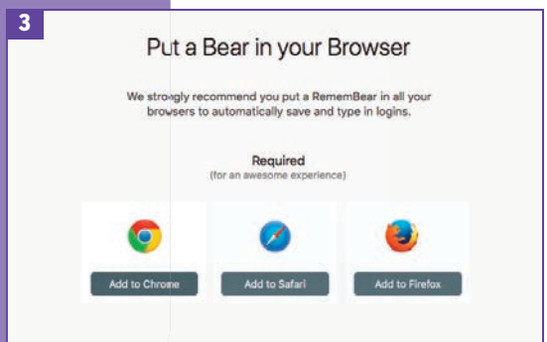
Après avoir téléchargé la version Mac sur le site de l'éditeur, on lance l'application et on suit les instructions d'installation. Commencez par cliquer sur *Create a RememBear account* [1]. Une adresse mail valide suffit. Il faut créer aussi un mot de passe maître. Choisissez-le avec soin. Toute la sécurité du contenu du coffre-fort repose sur lui. Une longueur de 12 à 16 caractères assurera une bonne sécurité. Ensuite, il vous est proposé de créer un *Backup Kit* [2], un document à imprimer ou à sauvegarder en PDF, qui contient les informations nécessaires pour récupérer l'accès à votre compte en cas d'oubli du mot de passe ou de perte de tous vos appareils. Vous y noterez manuellement le mot de passe maître au bas du document (cadre rouge) ; par sécurité, mentionnez plutôt un indice. Stockez le Backup Kit en lieu sûr et ne communiquez ces informations à personne.

L'installateur propose ensuite d'importer les identifiants stockés dans le navigateur ou dans le Trousseau d'Apple. Ceci fait, on le supprime du navigateur. Ensuite, on importe les données d'autres gestionnaires de mots de passe (*import from another password manager*) que l'on aura préalablement exportées au format .csv (fichier texte dont chaque valeur est séparée par une virgule). Enfin, l'installeur suggère d'installer les différentes extensions pour les navigateurs Safari, Chrome et Firefox [3]. Le support de Safari est un vrai plus par rapport à Bitwarden.



1

2



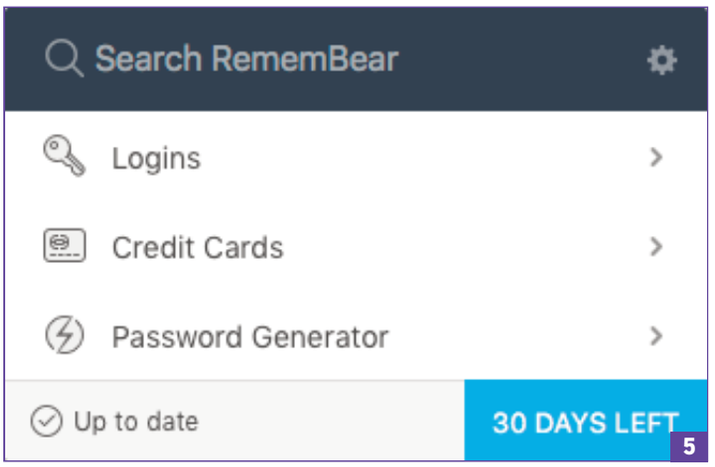
3

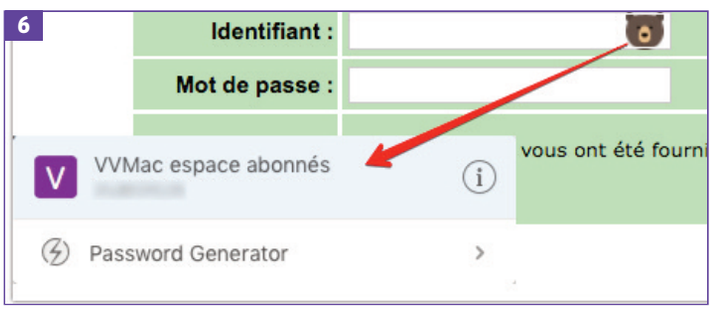
On bénéficie alors de la version Premium pendant 30 jours. Elle assure la synchronisation d'un nombre illimité d'éléments sur un nombre illimité de matériels, ainsi qu'une sauvegarde sécurisée de l'espace RememBear personnel et un accès prioritaire au service client. À l'issue des 30 jours, à défaut de s'abonner, l'application ne peut être utilisée que sur un seul matériel sans aucune synchronisation, ni sauvegarde sécurisée.

UNE VERSION MAC CLAIRE ET ÉPURÉE

L'interface de l'application sur macOS [4] propose une section pour les identifiants (*Login*) et une autre pour les cartes bancaires (*Credit Cards*) qui devront être ajoutées à la main. On retrouve l'indispensable Corbeille et une rubrique Add a New Device pour enregistrer un nouvel appareil mobile ou de bureau. Nous y reviendrons. Le menu *Achievements* différencie les fonctions activées de celles restant à activer.

En face de chaque champ, un bouton propose de copier son contenu et de le révéler en clair, s'il s'agit d'un mot de passe. Au bas de la version de bureau, on trouve des icônes donnant accès à des fonctions présentes dans l'application Desktop et dans l'extension. *Lock*, un cadenas, verrouille le coffre et déconnecte tous les





services, y compris sur les extensions de navigateur. Les *Préférences* (engrenage) sont structurées en deux onglets. *Security* permet le verrouillage du coffre sous certaines conditions et *Account* propose des options avancées.

L'extension du navigateur **[5]** offre un champ de recherche des identifiants, une rubrique Login pour les identifiants et d'une autre pour les cartes de paiement. Enfin, un générateur de mots de passe est proposé.

UNE UTILISATION PLUTÔT TRANSPARENTE

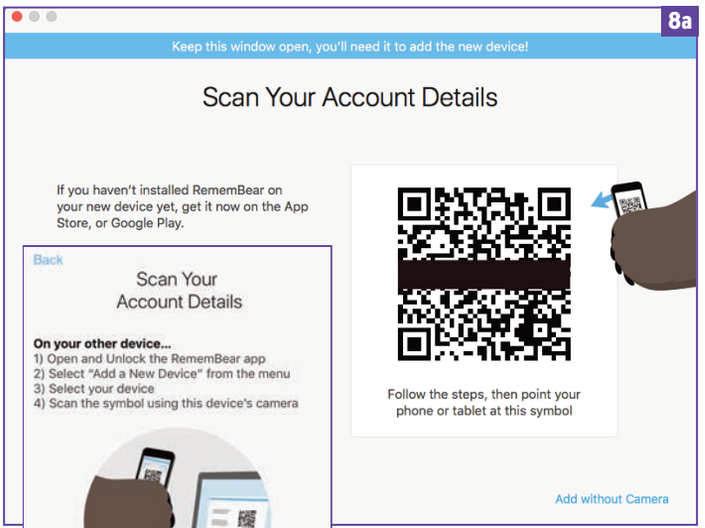
La connexion automatique à un site Internet s'effectue via l'interface de l'application en cliquant *Log In* ou, de façon plus pratique, via *l'extension du navigateur*. Dans la page web de connexion à un site Internet, on clique la tête de l'ours **[6]** présente devant le champ d'identification. Un menu apparaît.

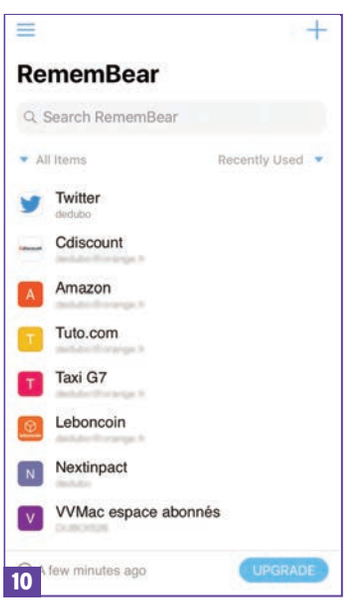
Si le site est déjà enregistré dans RememBear, les champs sont alors automatiquement renseignés d'un clic. Sinon, un message demande si l'on souhaite enregistrer. Classique.

Le générateur de mots de passe **[7a][7b]** permet de choisir un mot de passe constitué de caractères aléatoires ou d'une suite de mots du dictionnaire (anglais). Il prend en compte les nouvelles recommandations concernant la composition des mots de passe (VVMac 145).

ET SUR IOS ?

Pour enregistrer un nouvel appareil mobile, cliquez sur le menu *Add a New Device* dans l'application Mac **[8a]**. Avec l'appareil mobile, on scanne le code QR d'appairage **[8b]**. Ensuite, les données du coffre seront synchronisées entre les appareils du même compte. Il vous sera demandé si vous souhaitez autoriser l'utilisation de Touch ID pour déverrouiller votre coffre, très pratique, ainsi que d'installer *l'extension RememBear dans Safari Mobile*. Cette dernière sera accessible via *le bouton Partage d'iOS* **[9]**. Mais vous pouvez aussi choisir d'utiliser *Bear-owser*, le navigateur intégré à l'application. Bien entendu, l'application **[10]** recense identifiants et cartes, et offre les mêmes fonctions que la version de bureau.





LA SÉCURITÉ AVANT TOUT

La sécurité est essentielle dans ce type d'application. L'éditeur a travaillé à trouver un équilibre entre une approche de sécurité sans concession et une expérience utilisateur fluide et agréable. Le résultat est tout à fait convaincant.

RememBear utilise un chiffrement de bout en bout (AES-256 bits) pour la sauvegarde et la synchronisation des données. Les données sont chiffrées en local sur chaque matériel, à l'aide du mot de passe maître, avant que d'être transférées sur les serveurs de l'éditeur qui ne peut pas lire vos informations (dans le futur, il pourrait y avoir aussi une option de stockage local).

Le mot de passe maître est renforcé par l'ajout d'une chaîne de caractères aléatoire (New Device Key ou nouvelle clé de périphérique) qui rend presque impossible le succès d'une attaque par la force brute (qui teste toutes les combinaisons possibles).

De plus, la synchronisation des données ne s'effectue qu'avec des matériels que vous avez dûment autorisés. Même avec votre mot de passe maître, un hacker ne pourra pas accéder à votre compte RememBear puisque ses appareils ne seront évidemment pas autorisés à se connecter.

À l'usage RememBear s'avère très agréable et redoutablement efficace. Assurément, l'un des meilleurs produits de sa catégorie.

DENIS DUBOIS