Vous et Votre Mac

Vous et Votre Mac

N° 133 • Mai 2017 100 % Mac en pratique

- 10 utilitaires gratuits et pratiques
- Votre premier bloc-notes avec OneNote
- Les nouveautés d'iWork 2017
- 2 caméras pour surveiller la maison

Fantastical, BusyMac et Pagico pour rester maître de son temps

Les astuces secrètes du Finder de Sierra

10 choses à faire *dès que l'on achète* un nouveau Mac !

14 applications *pour remplacer* les apps d'Apple

Tout savoir des extensions pour Photos Mac

Comprendre tous les réglages du système pour préserver votre vie privée !

iOS

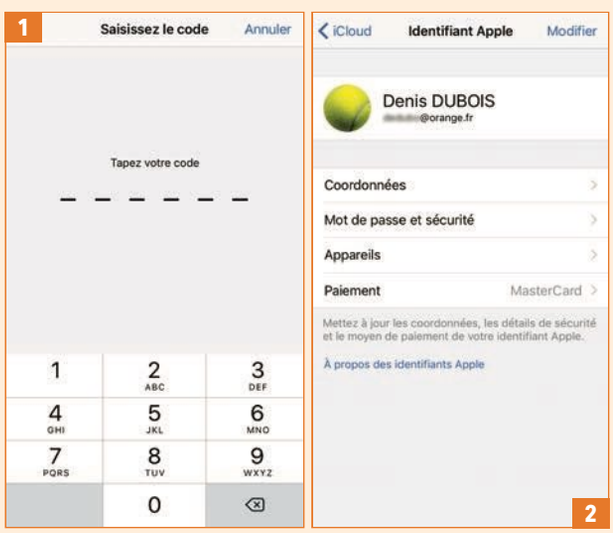
FRANCE métropolitaine : 5,90 € • SUISSE : 9,90 FS
DOM - BEL - MUX - PORT CONT : 6,90 € • CANADA 10,99 $
L 11206 - 133 - F : 5,90 € - RD

Maîtriser les réglages de **vie privée sur**

Lors de la première utilisation de votre nouvel appareil iOS, comme dans le cadre d'une mise à jour du système, il est indispensable de prendre le temps de bien le paramétrer. Il s'agit d'assurer la sécurité de vos données en cas de perte ou de vol, et la confidentialité de vos informations personnelles. On distingue deux types de paramètres. Les paramètres de sécurité d'abord, dont la mise en œuvre est indispensable pendant la phase d'installation du système. Ensuite, les paramètres relatifs au respect de la vie privée, qui peuvent être réglés après l'installation. Ces derniers permettent de contrôler les données sortantes des appareils, de définir au cas par cas quelles informations on accepte de fournir en échange d'un service rendu (informations qui iront nourrir les bases de données des éditeurs d'application et des annonceurs publicitaires sur vos habitudes et vos goûts). Je vous propose de faire un tour des réglages les plus importants. DENIS DUBOIS (TWITTER @DEDUBO)

LES PARAMÈTRES DE SÉCURITÉ

Il est impératif de définir **un code d'accès** (ou code PIN) sur votre appareil afin de protéger l'accès au contenu, en cas de perte ou de vol. Ce dernier est passé de 4 à 6 chiffres depuis iOS 9, permettant un million de combinaisons ! De quoi décourager d'éventuels opportunistes.
On peut éventuellement lui substituer un code alphanumérique personnalisé.
Vous pouvez utiliser vos empreintes digitales (fonction Touch ID) à la place du code d'accès. Ces dernières sont sauvegardées chiffrées et elles permettent un contrôle d'accès à la fois efficace et moins contraignant. Je ne peux que vous le recommander. Ça se passe dans, **Réglages > Touch ID et code** [1].
Choisissez un mot de passe complexe et unique pour votre identifiant Apple et demandez le mot de passe (ou via une validation Touch ID) pour chaque achat sur iTunes ou l'App Store.
Activez l'identification à deux facteurs pour votre identifiant Apple en allant sur **Réglages > iCloud > Mot de passe et sécurité** [2]. Cette fonction protège efficacement l'accès à votre compte. Même si une tierce personne apprenait votre mot de passe, elle ne serait pas en mesure d'accéder à votre compte depuis un appareil inconnu, sans la saisie d'un code de vérification à six chiffres envoyé sur vos appareils de confiance (iPhone, iPad, iPod touch ou Mac).



LES PARAMÈTRES DE CONFIDENTIALITÉ

Une étude du magazine *Que Choisir* d'octobre 2014 (« *Applications mobiles – Tous espionnés* » http://bit.ly/2mILzU9) a démontré que si les applications iOS sont généralement bien moins « bavardes » que les apps Android, **elles ne sont pas silencieuses pour autant**. Nombre d'informations personnelles sont envoyées, parfois à votre insu, à des sites tiers (jusqu'à plusieurs dizaines pour une seule application !). Parmi ces sites on trouve des prestataires techniques légitimes, nécessaires au fonctionnement de l'application, mais surtout des services marketing et publicitaires. Ces flux de données (comme vos identifiants et mots de passe) sont parfois envoyés en clair – et même sous chiffrement SSL, ils peuvent s'avérer facilement déchiffrables en cas d'interception. D'où la nécessité de bien paramétrer les autorisations d'accès aux ressources des applications et du système lui-même pour limiter, autant que faire se peut, les fuites de données.

Limitez les publicités ciblées

Apple affiche des publicités ciblées dans l'App Store et Apple News, en fonction des informations collectées à partir de l'historique de vos recherches et de vos lectures sur le lecteur de médias. **Chaque appareil se voit attribuer un identifiant de publicité** qui est utilisé par les centrales publicitaires pour le reconnaître de manière unique et être au courant des actions réalisées, des sites visités…

Vous pouvez refuser la collecte et l'exploitation de ces informations à des fins publicitaires. Dans **Réglages > Confidentialité > Publicité** activez l'option **Suivi publicitaire limité** [3]. Vous verrez toujours l'affichage de publicités mais celles-ci ne seront pas personnalisées.

Vous pouvez dans ce même écran **Réinitialiser l'identifiant de publicité** de temps en temps, ce qui aura pour effet de remettre à zéro le suivi (pistage) de votre appareil.

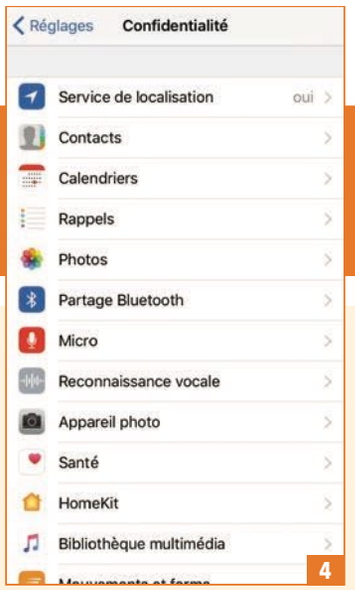
Restez vigilant sur la géolocalisation

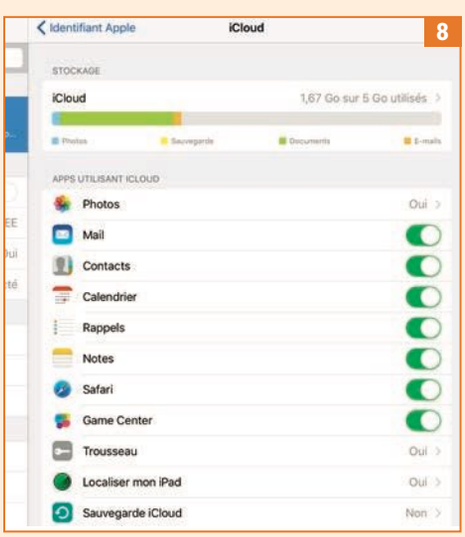
À cause de la puce GPS de vos appareils, vous pouvez être tracé en permanence. La CNIL estime que 30 % des applications vous géocalisent, parfois plusieurs fois par minute !
Ces informations permettent de cerner vos déplacements et donc vos habitudes de vie. Bien sûr, vous pouvez désactiver cette fonction en basculant l'interrupteur dans **Réglages > Confidentialité > Service de localisation** [4] mais vous restreignez alors l'intérêt de nombreuses applications. Apple prévient que *ces*

informations de localisation peuvent être utilisées en cas d'appel d'urgence […] que vous ayez activé la fonction ou non !
Cependant, l'avantage appréciable d'iOS sur Android est que l'**on peut paramétrer la géolocalisation application par application** [5].
Pour chacune d'elles, vous pouvez choisir entre trois options : **Toujours**, **Si l'app est active** (même en arrière-plan) ou l'option radicale **Jamais**.
Si vous doutez de l'utilité, pour une application donnée, d'accéder aux fonctions de géolocalisation n'hésitez pas à désactiver l'accès à ce service.
La géolocalisation permet également de vous envoyer des publicités en fonction du lieu où vous vous trouvez.
Rendez-vous dans **Réglages > Confidentialité > Service de localisation > Services système** [6] et désactivez **Publicité Apple selon le lieu**.
Vous pouvez également désactiver les fonctions **Alertes selon le lieu**, **Suggestions selon le lieu** et **Partager ma position**, ainsi que **Lieux fréquents** fonction qui mémorise les lieux que vous fréquentez régulièrement pour renseigner certaines applications.
Si vous êtes perdu, vous pouvez restaurer tous les paramètres par défaut dans **Réglages > Général > Réinitialiser**, puis sélectionnez **Réinitialiser localisation et confidentialité** [7].

Limitez l'accès à vos données

En 2013 et 2014, la CNIL et l'INRIA (institut de recherche en informatique) ont mené une grande enquête pour analyser les données personnelles enregistrées, stockées et diffusées par les smartphones et leurs applications. L'étude Mobilitics a été mise en œuvre en deux temps.
La saison 1 portait sur iOS (**http://bit.ly/2ndeeys**) ; la saison 2 sur Android (**http://bit.ly/2nmkZ09**).
L'étude avait mis en évidence les capacités intrusives et l'ampleur du recueil des données personnelles des applications mobiles. Alors même qu'une étude récente de 2017 des cabinets d'audit KPMG et 3Gem sur la sensibilité des utilisateurs sur la collecte de leurs données personnelles révèle que 82 % des consommateurs ne souhaiteraient pas voir leurs données personnelles cédées à des tiers, même en échange de services supplémentaires (**http://bit.ly/2fymDLO**).
À la lecture de l'étude, il paraît sage de ne conserver sur les mobiles que les seules applications utilisées et de désinstaller régulièrement celels que vous délaissez.
Sous iOS, on peut affiner les autorisations d'accès application par application et il ne faut surtout pas s'en priver ! Après chaque installation, faites un tour dans les Réglages de l'application et ajustez finement les droits d'accès aux données.
Dans **Réglages > Confidentialité**, vous trouverez une liste des types de données disponibles et des applications ayant fait une demande d'accès.
Si l'accès à la fonction ne vous paraît pas justifié, compte tenu de la finalité de l'application, n'hésitez pas à le désactiver.
Le mode **Avion** peut également être mis à contribution pour éviter l'affichage de publicités dans les apps gratuites et dans les jeux.





LES SERVICES D'ICLOUD

Le cloud d'Apple fédère les données de nombreuses applications comme Calendrier, Contacts, Rappels, Notes, Photos, Signets, Mail… On peut donc légitimement se poser la question de la confidentialité des données qui transitent par iCloud.
Les données transférées sur iCloud sont chiffrées pendant leur transport et protégés une fois sur les serveurs d'Apple par un chiffrement (relativement) fort (AES 128 bits).
Les fonctions **Localiser mes amis** ou **Localiser mon iPhone, iPad ou iPod touch**, qui nécessitent des données de localisation, offrent suffisamment de garanties pour que l'on puisse raisonnablement faire confiance à Apple. Les données sont en effet délivrées à la demande et pas en continu ; de plus, elles sont **chiffrées** puis définitivement effacées au bout de deux heures.
Vous pouvez laisser actives toutes les fonctions d'iCloud [8] sur vos appareils sans craindre pour votre vie privée. Elles se trouvaient dans **Réglages > iCloud** sous iOS 10 et désormais dans **Réglages > Votre fiche d'utilisateur > iCloud** dans iOS 10.3.
Le Trousseau iCloud qui stocke notamment identifiants, mots de passe et informations de carte bancaire, est **chiffré (AES 256 bits)** en local et les clés de chiffrement restent sur vos appareils approuvés, seules les données chiffrées sont transférées sur les serveurs d'Apple et seulement si la récupération du trousseau est activée. Vous pouvez refuser que les données de votre Trousseau soient sauvegardées dans le nuage d'Apple. Il suffit de ne pas créer de code de sécurité iCloud lors de la configuration du trousseau. Les données seront alors stockées localement.

>>>

À PROPOS DE SAFARI…

Sous iOS, Safari offre quasiment les mêmes réglages que sur macOS. Vous pouvez utiliser le mode de **navigation privée** de Safari qui empêche certains sites de récupérer des informations ; de plus, votre historique de navigation et les pages consultées ne sont pas gardés dans le cache de l'application. **Ouvrez Safari puis touchez l'icône Double carré puis Privée et Terminé.**

A posteriori, vous pouvez effacer vos traces en supprimant votre historique, les fichiers téléchargés, et en vidant votre cache… dans **Réglages > Safari > Effacer historique, données de site** [9].

Choisissez **DuckDuckGo comme moteur de recherche par défaut**, le seul de la liste qui a un engagement explicite en matière de respect de la vie privée de ses utilisateurs. **Désactivez les suggestions du moteur de recherche, les suggestions Safari et les sites fréquemment visités**. Les suggestions proposent des liens vers des sites en rapport avec la requête effectuée par l'utilisateur. Les termes saisis dans Safari ou un moteur de recherche, même DuckDuckGo, sont transmis aux serveurs d'Apple souvent accompagnés d'autres informations.

Touchez **Ne pas me suivre** [9] pour envoyer l'information, qui sera prise en considération ou non, selon le bon vouloir des sites visités. Positionnez Cookies sur **Oui pour les sites visités** pour ceux des sites tiers. Le menu **Avancé** permet de supprimer les données des sites consultés et de désactiver JavaScript, à utiliser au coup par coup (cela risque d'affecter le fonctionnement de certains sites).

Apple autorise dorénavant le contrôle du contenu publicitaire directement dans le système.

Depuis iOS 9, une interface permet aux développeurs de proposer des bloqueurs de pub dans Safari comme 1Blocker (payant) ou Safari Blocker (gratuit). Si un bloqueur est installé, une nouvelle ligne **Bloqueurs de contenu** apparaît dans les réglages de Safari, pour les activer ou les désactiver individuellement.

Enfin, l'utilisation d'un tunnel chiffré (VPN) pour sécuriser vos connexions passe par **Réglages > Général > VPN** [10]. La configuration peut s'avérer un peu technique, à moins d'utiliser un client VPN qui vous affranchira de toute complexité, comme l'excellent Opéra VPN (gratuit).

9

10

ATTENTION À LA SANTÉ !

S'il est un domaine où la vie privée doit être maximale, c'est bien celui de la santé tant les conséquences peuvent être désastreuses si ces informations sensibles sont transmises à des tiers. Le refus d'un crédit, des primes d'assurance qui flambent, un accès à l'emploi plus difficile… peuvent en être la conséquence. Déjà des mutuelles françaises commencent à s'y intéresser et envisagent de mettre en place un système de bonus-malus en fonction de votre hygiène de vie.

11

L'application Santé d'Apple propose de suivre les informations relatives à votre activité physique, à votre sommeil et à votre santé y compris au travers des capteurs de santé compatibles. Elle va même jusqu'à proposer l'importation et la consultation de vos dossiers médicaux ! Toutes ces informations sont stockées dans une base de données médicale centralisée nommée HealthKit. Toute app qui souhaite accéder à vos informations de santé *doit disposer d'une politique de confidentialité […], qu'il vous faudra consulter, […] et toutes vos informations de santé sont chiffrées avec le code d'accès de votre appareil* (dixit Apple).

Apple a mis en place des garde-fous interdisant aux développeurs l'exploitation commerciale des données médicales et leur stockage dans iCloud. Cependant, au moment de la sauvegarde de votre appareil, les informations de santé sont également enregistrées dans iCloud où elles sont chiffrées (transfert inclus).

Pour une sauvegarde locale via iTunes, il est fortement conseillé d'activer le chiffrement [11] ! Si vous créez une Fiche médicale, certaines informations utiles en cas d'urgence (allergies, traitements, etc.) seront par défaut accessibles aux services de secours à partir de l'écran verrouillé, sans nécessiter votre code d'accès, sauf à désactiver l'option **Afficher en mode verrouillé**.

Que vous le vouliez ou non, l'app **Santé** compte automatiquement vos pas et mesure les distances que vous parcourez [12]. Elle va même jusqu'à mesurer votre activité sexuelle, si vous le souhaitez !

Vous pensez vos données de santé inaccessibles, bien au chaud dans votre appareil ? Détrompez-vous ! Les dernières révélations de WikiLeaks (Vault 7) dévoilent que la CIA (et probablement d'autres agences) aurait accès à l'intégralité des informations contenues dans n'importe quel smartphone iOS ou Android (**http://bit.ly/2m1IQlw**) en exploitant des vulnérabilités non dévoilées du système (Zero Day).

Autre risque de voir vos données de santé quitter votre appareil : en cliquant sur votre fiche dans **Données Santé**, un lien vous propose **Exporter les Données Santé** sous la forme de fichiers au format XML.

Quelques utilitaires comme l'application gratuite QS Access de Quantified Self Labs ou Health Export de Lybron Sobers (2 €) proposent d'en afficher le contenu dans votre tableur (Numbers, Excel…).

Tous les paramétrages concernant l'app Santé s'effectuent directement dans l'application. Rentrez les informations avec parcimonie, et réfléchissez bien aux conséquences éventuelles si ces informations arrivaient à « fuiter » un jour.

12