INTERNET, RÉSEAUX SOCIAUX, WINDOWS…

PROTÉGEZ VOTRE VIE PRIVÉE

Comment stopper l'utilisation abusive de vos données personnelles

Dès lors que vous êtes inscrit sur un service Internet, une version officielle de Windows ou un réseau social en vogue, toutes vos informations personnelles sont collectées, dans le seul but de vous proposer des produits ou des extensions. Dites enfin stop au fichage virtuel de votre identité réelle.

Dossier réalisé par Stéphane Philippon

Dans la vraie vie, nous sommes tous plus ou moins fichés, pardon, connus et identifiés. Cela commence par notre date de naissance, notre adresse postale, notre numéro de contribuable et ainsi de suite. Parfois même, nos habitudes de consommation sont relevées par de courts sondages effectués par les établissements qui vous ont proposé une carte de fidélité en magasin. Hélas, notre existence virtuelle fait l'objet d'encore plus d'attention, sans que l'on en prenne tout le temps conscience. Vous êtes Inscrit sur un réseau social tel que Facebook, disposez d'une adresse Gmail ou avez choisi d'utiliser Windows 10 au quotidien ? Et bien, vous êtes alors reconnu autant de fois que nécessaire. La question ne se pose même plus de savoir qui vous êtes, car ces différents services le savent dès le départ. Pour envisager concrètement de n'être rien d'autre qu'un utilisateur anonyme d'Internet et de Windows, vous devez retrousser vos manches et suivre nos conseils pas à pas pour chacun des domaines concernés. S'il n'est pas ici question de naviguer de manière anonyme (c'est presque illusoire sans mettre en œuvre des solutions payantes qui réclament en outre quelques connaissances techniques), il est possible d'éviter que vos informations personnelles ne vous suivent à la trace au moindre clic ou à la moindre mise à jour automatique. Au final, vous vous sentirez un peu moins espionné et donc un peu plus libre de profiter de tout ce qu'offrent Internet et votre ordinateur. Chance toutefois, cet article ne se détruira pas après lecture ! ■

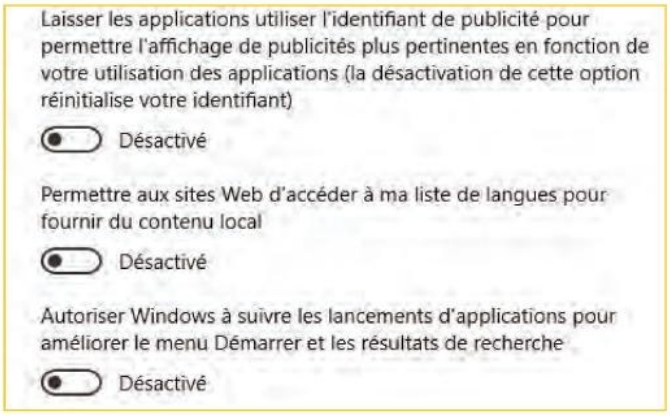
A SAVOIR

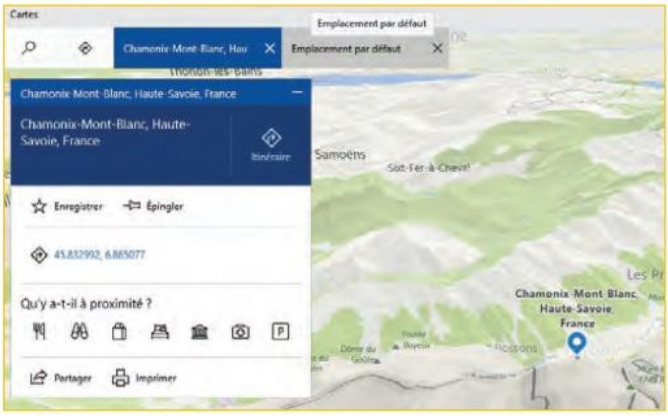
Pour éviter que quiconque ne tombe sur votre profil Google+ lorsqu'il effectue une recherche sur Internet, allez dans les paramètres, partie Profil et désactivez le curseur *Autoriser l'affichage de mon profil* dans les résultats de recherche. Dans ce même menu Paramètres, partie Confidentialité, cliquez sur *Effacer l'historique des recherches*.

La suppression pure et simple de toutes vos coordonnées prend du temps mais ce jeu en vaut la chandelle.

Procédez aux réglages de confidentialité dans Windows 10

Vie privée et Windows 10 ne font pas vraiment bon ménage. Pour preuve, des réglages de confidentialité positionnés par défaut sur la collecte intensive des données personnelles, la publicité ciblée, etc. Il y a moyen de revenir sur ces failles béantes.





1 Désactivez les réglages généraux

Vous êtes passé à Windows 10 voilà quelques temps sans vous préoccuper des réglages en matière de confidentialité des données. Il n'est jamais trop tard pour bien faire ! Cliquez sur l'icône *Windows*, la roue crantée *Paramètres, Confidentialité*. Dans Général, désactivez les 3 curseurs (identifiant publicitaire, liste de langues, lancements d'applications). Cliquez en colonne gauche sur *Informations sur le compte* et désactivez le curseur associé. Faites de même avec les curseurs Caméra, Microphone et Contacts pour éviter d'être espionné par les applis.

2 Renseignez une fausse localisation

Cliquez sur *Localisation* en colonne gauche. La dernière mouture de Windows 10 permet d'indiquer un emplacement par défaut au système, applis et services lorsque votre localisation est approximative. Il est donc possible d'indiquer un faux emplacement. Cliquez sur *Définir par défaut* dans Emplacement par défaut et sur *Modifier*. Renseignez une fausse adresse de localisation et cliquez sur *Modifier*. Windows se référera désormais à ce nouveau lieu lorsqu'il aura du mal à vous situer. Quittez l'appli Cartes et revenez aux paramètre de confidentialité.

3 Minorez l'espionnage de votre compte

En colonne gauche, cliquez sur *Informations sur le compte* puis sur le lien *Déclaration de confidentialité*. Si vous y tenez, prenez connaissance des explications fournies par Microsoft sur la collecte des données. On y apprend notamment que tout est remonté vers les serveurs Microsoft puis décortiqué afin d'afficher des publicités ciblées. Il n'est pas possible de totalement stopper cette espionnite aiguë. Contentez-vous de désactiver le curseur d'informations de compte pour éviter que les applis accèdent à vos données personnelles.

4 Interdisez aux appareils de fouiner dans votre vie privée

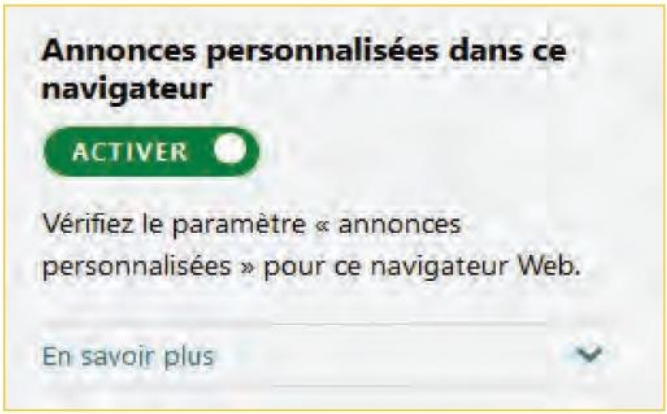
En plus de l'OS Windows 10, des applis et services, les appareils connectés au PC (USB, Bluetooth, etc.) peuvent être source d'espionnage. Dans les paramètres de confidentialité, cliquez tour à tour sur *Caméra, Microphone, Radios, Autre appareils*, puis désactivez tous les curseurs associés. Par ailleurs, sans être alarmiste, nous vous conseillons de déconnecter la webcam du PC lorsque vous ne l'utilisez pas. Enfin, dans les paramètres généraux, cliquez sur *Périphériques* puis supprimez les appareils que vous ne reconnaissez pas.

LA SÉCURITÉ ET LA VIE PRIVÉE EXISTENT AUSSI SOUS WINDOWS 7 !

Si vous avez décidé de demeurer sous Windows 7, il est bien évidemment possible là aussi d'optimiser certains paramètres de confidentialité. Accédez au Panneau de configuration, partie Paramètres de contrôle de compte utilisateur dans Centre de maintenance. Positionnez le curseur sur *Toujours m'avertir*. Vous serez notifié lorsqu'un programme tente de modifier votre ordinateur à votre insu. Désactivez ensuite l'envoi d'infos à Microsoft en allant dans Microsoft Default Manager depuis le menu Démarrer et cochez la case *Non, je ne souhaite pas participer*. Cela étant, les options de confidentialité sont bien moins développées dans 7 que dans 10.

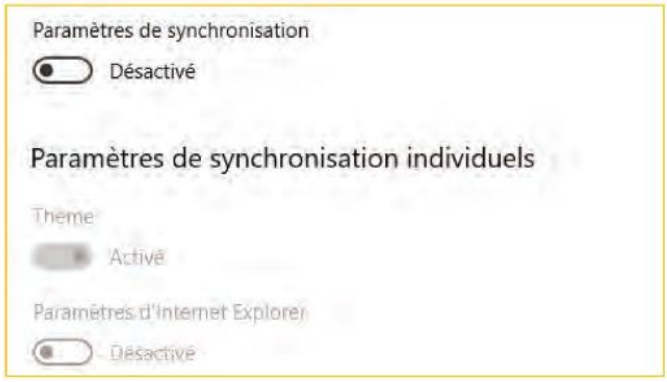
5 Désactivez la publicité ciblée

Chaque PC sous Windows 10 possède un identifiant unique. Cela permet à Microsoft de connaître l'administrateur de tous les appareils fonctionnant sous Windows et de leur proposer de la publicité ciblée, en relation avec des partenaires tiers. Pour désactiver ce ciblage nominatif et recevoir à la place des annonces génériques, accédez à cette page : **https://goo.gl/0RAeZr**. Dans la partie à droite nommée Annonces personnalisées, cochez le curseur de manière à ce qu'il soit vert et qu'il soit nommé Activer.



6 Interdisez la synchronisation des paramètres

Par défaut, Windows 10 autorise la synchronisation de ses paramètres avec les autres appareils utilisant l'adresse mail de l'administrateur du PC. Il peut s'agir de synchroniser des éléments avec votre smartphone par exemple lorsque vous utilisez cette même adresse mail en mobilité. Cliquez sur l'icône *Windows*, la roue crantée *Paramètres, Comptes, Synchroniser vos paramètres* en colonne gauche. Désactivez l'intégralité des synchronisations au moyen du curseur Paramètres de synchronisation. Tout sera désactivé et notamment Autres paramètres Windows.

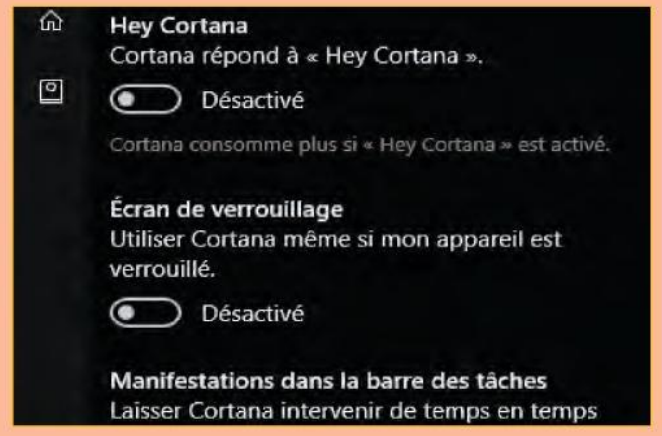


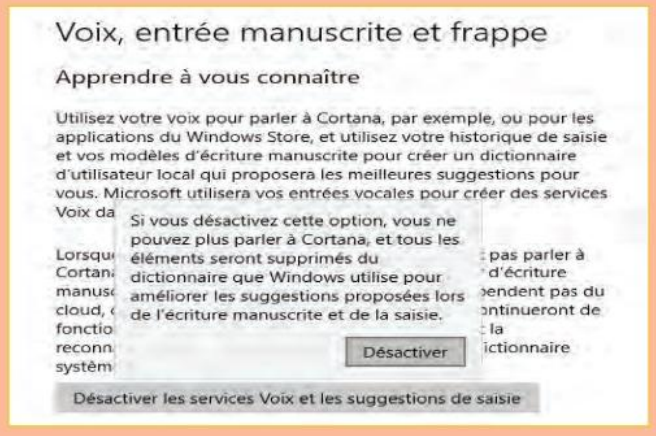
MINOREZ LA SOIF DE L'ASSISTANT VIRTUEL CORTANA

Cortana, l'assistant virtuel de Microsoft implémenté dans Windows 8.1 et 10, offre de précieux services comme des requêtes web, des recherche de documents sur le PC, des chansons, des lieux, des rendez-vous, etc. Pour cela, il scanne méthodiquement les données personnelles dont les mails, les contacts, l'historique de navigation, les commandes tapées au clavier. Ceci afin de vous proposer toujours plus de conseils et suggestions. Sachez que vous ne pourrez jamais totalement annihiler sa soif de savoir, mais tout au plus la minorer. En appliquant nos solutions, soyez également conscients que vous n'aurez plus accès à Cortana mais uniquement à la zone de recherche matérialisée par l'icône Rond. Cliquez sur l'icône *Cortana* dans la barre des tâches. Pour débuter la désactivation de l'assistant, cliquez sur la roue crantée *Paramètres* et décochez les curseurs *Hey Cortana, Écran de verrouillage, Manifestations dans la barre des tâches, Raccourci clavier, Partager les notifications, Historique de mon appareil, Mon historique de recherche.*

Données personnelles et centres d'intérêt

Cliquez sur l'icône *Cortana* dans la barre des tâches puis sur l'icône située sous l'icône Maison en colonne droite. Le Carnet de notes s'ouvre. Cliquez sur *Autorisations*. Vérifiez que les curseurs Emplacement, Contacts et Historique de navigation sont tous désactivés, sinon faites-le. Au bas de cette fenêtre, cliquez sur *Paramètres de confidentialité*. Les paramètres Voix, entrée manuscrite et frappe s'affichent. Cliquez sur la commande *Désactivez les services Voix et les suggestions de saisie*. Refermez cette fenêtre. Revenez à Cortana en cliquant sur son icône dans la barre des tâches puis sur la roue crantée Paramètres et sur *Modifier ce que Cortana sait de moi dans le cloud*. La page des informations personnelles s'affiche. Déroulez-la vers le bas et cliquez sur *Effacer*. Cela permet de supprimer vos données personnelles, favoris, centres d'intérêt et autres éléments enregistrés dans MSN et dans le moteur de recherche Bing. Redémarrez le PC.





Profitez de multiples outils et services anti-espionnage

Dès que vous vous connectez à Internet et touchez à votre messagerie ou navigateur, vous voilà pisté. Sans en arriver à débrancher la prise Ethernet ou couper le Wi-Fi, il existe des solutions qui vont contribuer à préserver votre confidentialité.

En parallèle des réglages de confidentialité de Windows 10, il existe de nombreux outils et services spécialisés dans la maîtrise de sa vie privée en ligne. Chrome, Firefox et Edge offrent tous des paramètres de confidentialité plus ou moins développés, mais mieux vaut tout de même en passer par le moteur de recherches français Qwant, qui affirme ne jamais transmettre les données de navigation. Si vous ne souhaitez pas lâcher votre navigateur habituel (préférez Firefox à Chrome, bien moins fouineur), habillez-le de quelques extensions visant à masquer votre surf et à bloquer les mouchards de toutes sortes. Quant aux messageries, par défaut, tout ce que vous envoyez et recevez peut-être intercepté et consulté. Là encore, il existe des solutions faciles à mettre en œuvre simplement en cryptant vos mails à base de clés de cryptage.

Connaissance zéro

Par ailleurs, si vous avez besoin d'envoyer, de partager ou de stocker de gros fichiers ou dossiers personnels, tous les clouds ne sont pas logés à la même enseigne. Evitez Dropbox, Google Drive et OneDrive et préférez soit le cloud français hubiC qui localise les données dans l'hexagone, ou le cloud américain SpiderOak, l'un des seuls à crypter puissamment les éléments sauvegardés sans même que son personnel n'y ait accès. C'est ce qu'on appelle dans le jargon la "connaissance zéro". Et si ces solutions ne vous satisfont pas entièrement, il reste une ultime chose à mettre en œuvre, moyennant un abonnement mensuel, à savoir la mise en place d'une connexion VPN qui va anonymiser l'intégralité de vos échanges de données en modifiant votre adresse IP et en la géolocalisant dans le pays de votre choix. La grosse cavalerie certes, mais au moins vous serez assuré de surfer sans être pisté ! ■

Habillez votre navigateur favori de quelques extensions visant à masquer votre surf et à bloquer les mouchards.

QUELLE MESSAGERIE INSTANTANÉE POUR MA VIE PRIVÉE ?

Tout le monde envoie des SMS chaque jour depuis son smartphone Android. Attention car toutes les messageries instantanées ne se valent pas en terme de vie privée. Facebook Messenger, Hangouts, WhatsApp, Signal, Telegram, Android Messages, etc., bien malin qui saurait dire laquelle est la mieux sécurisée. Et pourtant, il n'y a pas photo puisque seulement deux d'entre elles chiffrent tous les messages et en plus respectent de bout en bout la vie privée, l'éditeur n'ayant pas accès aux données échangées. Il s'agit des applis Telegram Messenger et Signal Private Messenger, cette dernière étant utilisée par Edward Snowden, cet ancien employé de la CIA et de la NSA qui a révélé l'espionnage de masse. C'est dire si Signal est sécurisé !

4 solutions anti mouchards efficaces

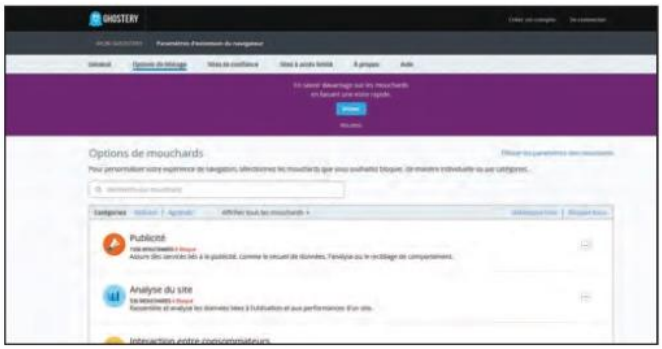
Impossible de passer à côté de ces 4 outils si vous souhaitez réduire votre empreinte en ligne et amoindrir les éléments que vous donnez gratuitement aux espions de tout poil !

1 Naviguez tranquille avec Qwant

C'est écrit noir sur blanc dans la partie Vie privée du moteur de recherche français Qwant : la philosophie de Qwant repose sur ne pas tracer les utilisateurs et ne pas filtrer le contenu d'internet. Les données qui transitent sur les serveurs Qwant ne sont ni divulguées ni revendues. De plus, les utilisateurs peuvent effectuer une demande de droit à l'oubli. **www.qwant.com**

2 Oubliez les mouchards avec Ghostery

Disponible sur Chrome, Firefox et Edge, l'extension Ghostery permet de bloquer les mouchards lors de la navigation. Il commence par les repérer grâce à une bibliothèque de mouchards constamment mise à jour. Vous éviterez d'être espionné dans vos faits et gestes, que ce soit par les réseaux sociaux, la publicité ou les administrateurs de sites Web. **www.ghostery.com**

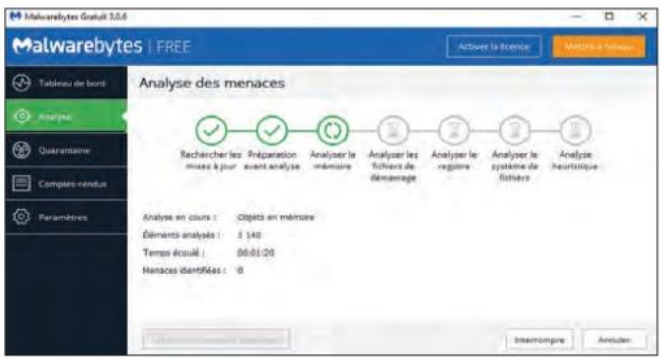


3 Correspondez en privé avec Mailvelope

Pour protéger efficacement l'échange de mails, voici une autre extension qui se greffe à Chrome ou Firefox. Si vous utilisez un webmail de type Gmail, Yahoo ou Outlook, Mailvelope va générer des clés de cryptage et les associer au chiffrement des envois. Le contact pourra lire votre missive depuis sa propre clé. Personne d'autre ne pourra en prendre connaissance. **www.mailvelope.com**

4 Éradiquez les logiciels espions

Même si vous êtes précautionneux, il y a des chances que votre PC finisse par être infecté par un logiciel espion sans que vous ne vous en aperceviez. Pour les traquer et les éliminer, rien ne vaut la version gratuite de Malwarebytes. Après la fin de la version d'essai, vous pourrez continuer à l'utiliser mais c'est à vous de l'activer au moins une fois par mois. **https://fr.malwarebytes.com**



OPTIMISEZ LES RÉGLAGES DU NAVIGATEUR ET ÉVITEZ LE PISTAGE

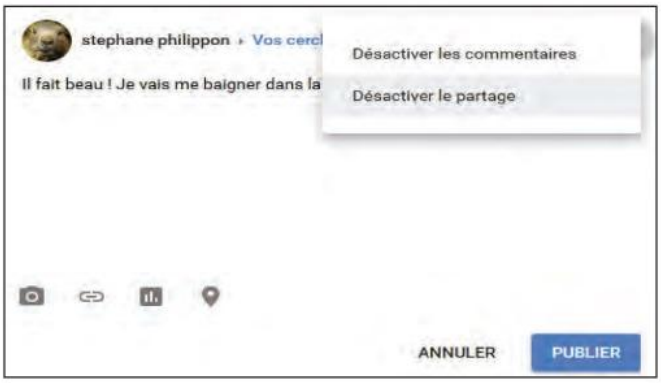
Edge, Google et Firefox disposent d'outils anti-pistage dont le but consiste à dire aux sites sur lesquels vous accédez de ne pas mémoriser votre navigation. Pour Edge, cliquez sur les points en haut à droite, *Paramètres, Afficher les paramètres avancés* et activez le curseur Envoyer des demandes Do Not Track. Pour Chrome, cliquez sur les points en haut à droite, *Paramètres, Afficher les paramètres avancés*. Dans Confidentialité, cochez *Envoyer une demande interdire le suivi pendant la navigation*. Pour Firefox, cliquez sur l'icône *Hamburger* en haut à droite, *Options*. En colonne gauche, cliquez sur *Vie privée*. Cochez la case *Pistage*. Cliquez sur *Gérer les paramètres Ne pas me pister* et cochez la case associée.

Gérez votre vie privée sur Google+

Google+ offre des possibilités de partage, d'envoi automatisés de photos, etc. Autant d'éléments qui, s'ils sont mal réglés, vous exposent à la vue du plus grand nombre.

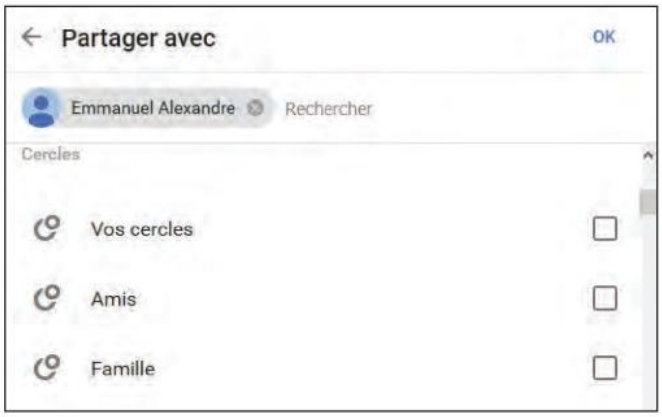
1 Maîtrisez le partage de nouvelles

A l'instar de Facebook, Google+ permet de poster des nouvelles à chaque instant via la zone de saisie supérieure. Lorsque vous écrivez un post, cliquez sur les points à droite pour désactiver les commentaires et le partage afin que ce que vous dites ne soit pas relayé indéfiniment. Cliquez sur *Vos cercles* pour sélectionner votre audience et évitez de cocher Public.



2 Sélectionnez précisément les destinataires

Cliquez sur *Plus de détails*. Le dossier Partager avec permet de sélectionner précisément à qui envoyer vos nouvelles. Déroulez le menu vers le bas et décochez la case *Vos cercles* puis cochez celles des destinataires qui la recevront. Il s'agit du seul moyen offert par Google+ d'envoyer des posts à un seul individu identifié. Cliquez sur *OK* puis sur *Publier*.



3 Restreignez notifications et commentaires

Cliquez sur l'icône *Hamburger* à gauche, *Paramètres*. Dans Général, vous pouvez décider qui est en mesure de notifier et commenter vos publications. Déroulez les menus à droite, cliquez sur *Personnaliser* et sélectionnez précisément les seuls contacts autorisés. Faites de même avec le menu Activité +1 pour choisir les amis habilités à voir à qui vous attribuez des +1.

4 Privatisez vos contenus multimédia

Lorsque vous publiez une photo ou vidéo sur Google+, elle est accessible à tous. Pour conserver un simili droit à l'image, rendez-vous dans les paramètres, partie Photos et vidéos partagées. Désactivez les deux curseurs de géolocalisation et d'autorisation de téléchargement par tous puis activez le curseur inférieur pour que Google ne se les approprie pas.

RÉGLAGES DE CONFIDENTIALITÉ À ACTIVER DE TOUTE URGENCE !

Pour éviter que quiconque ne tombe sur votre profil Google+ lorsqu'il effectue une recherche sur Internet, allez dans les paramètres, partie Profil et désactivez le curseur *Autoriser l'affichage de mon profil dans les résultats de recherche*. Dans ce même menu Paramètres, partie Confidentialité, cliquez sur *Effacer l'historique des recherches*. Cliquez ensuite sur *Gérer le partage de position* dans Partage de position et désactivez-le. Dans Autre, désactivez les recommandations partagées afin de ne pas recevoir de recommandations d'autres personnes utilisant les services Google. Enfin, si vous n'utilisez plus Google+, mieux vaut supprimer votre compte. Dans Compte, cliquez sur *Supprimer votre profil Google+* et suivez la procédure.

Limitez la publicité en ligne

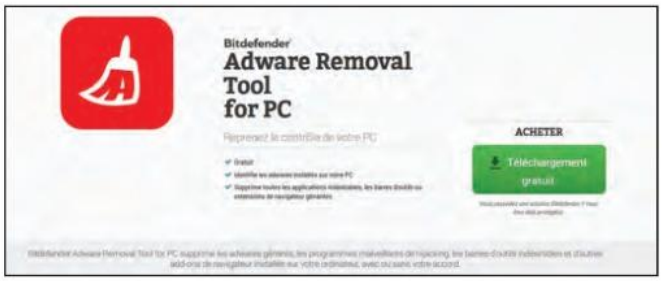
Sur Internet la publicité est partout et, comme tout est gratuit, c'est vous le produit ! S'il est impossible de la supprimer totalement, il existe des moyens d'y être moins exposé.

1 Construisez une barrière anti-pub

Que vous utilisiez Edge, Chrome ou Firefox, mieux vaut installer le module complémentaire AdBlock qui permet de supprimer les publicités sur les sites que vous visitez. Non seulement vous serez moins exposé aux annonces, pop-ups et malwares de toutes sortes mais en plus votre navigateur ne subira plus d'éventuels ralentissements dûs à ces ajouts non sollicités. **https://adblockplus.org**

2 Supprimez les mouchards publicitaires

Les adwares sont des programmes de toutes sortes qui s'installent à votre insu pour ensuite afficher des publicités. Pour les traquer et les supprimer, connectez-vous au site Bitdefender : **https://goo.gl/7pw1Bu**. Cliquez sur *Téléchargement gratuit* et installez le soft anti-pub. Celui-ci va scanner le PC à la recherche de tout programme malveillant et les supprimer.

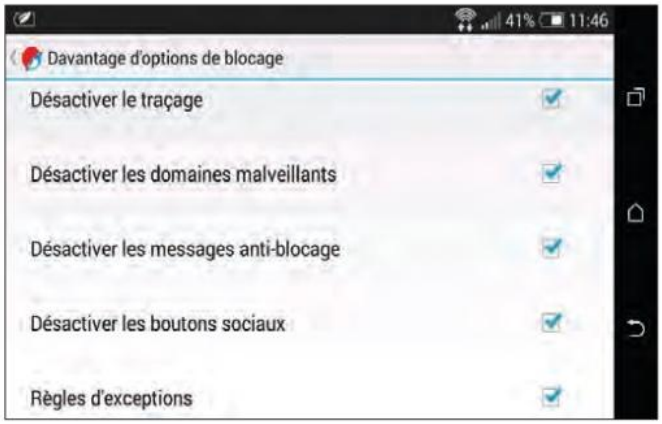


3 Ne conservez que les bons cookies

Votre navigateur conserve en mémoire les cookies utilisés par les sites Web pour vous authentifier, stocker une information ou des contenus personnels. Il est possible de sélectionner ceux à conserver. Installez CCleaner et cliquez sur *Options, Cookies*. Passez en revue la liste à gauche et passez en colonne droite uniquement ceux dont les noms vous sont familiers.

4 Surfez en mobilité sans publicité

AdBlock a conçu un navigateur qui bloque les publicités sur Android. Vous pouvez le télécharger ici : **https://goo.gl/zU1mMz**. Une fois installé, cliquez sur les points en haut à droite, *Paramètres, Blocage de publicités, Davantage d'options de blocage* et cochez toutes les cases. Vous pouvez aussi autoriser les publicités non intrusives dans Publicités acceptables.



RÉGLEZ LE NIVEAU DES PUBLICITÉS DE GOOGLE

Google permet de régler le type de publicité que les internautes souhaitent voir. Ce qui ne veut pas dire que vous allez pouvoir bloquer leurs annonces mais plutôt les configurer en fonction de vos attentes ou pas. Connectez-vous à votre compte et accédez à cette page : **https://goo.gl/9VyTPC**. Dans Informations personnelles et confidentialité, cliquez sur *Paramètres des annonces, Gérer les paramètres des annonces*. Désactivez le curseur des annonces par centre d'intérêt pour éviter que Google ne fouine dans votre historique de recherche et ne se base sur vos données personnelles pour vous servir des publicités ciblées. Attention, le curseur doit être positionné sur Activer de couleur verte.

Maîtrisez votre confidentialité sur Facebook

Facebook est un réseau extraordinaire pour retrouver d'anciens amis et s'en faire de nouveaux. Mais c'est aussi un voyeur de la pire espèce ! Pour préserver sa vie privée, il est impératif de bien paramétrer les options de confidentialité.

Facebook, le gigantesque réseau social mondial aux quelque 1,86 milliard d'utilisateurs actifs mensuels (chiffres Facebook), est depuis longtemps déjà devenu une aubaine pour les publicitaires et escrocs de tout poil. Les vies privées de millions de personnes s'y exposent impunément sans que celles-ci ne se rendent compte de l'impact de leurs publications, clic sur la mention J'aime et autres petits jeux à croquer. Bref, un monstrueux puits de données à ciel ouvert que Facebook se fait fort de revendre aux spécialistes en marketing. D'où son bénéfice financier en 2016 estimé à plus de 10 milliards de dollars. Alors, afin d'être un peu moins le produit de ce monstre numérique et aussi pour conserver un semblant de vie privée en ligne, il est impératif de paramétrer judicieusement quelques fonctionnalités internes à Facebook.

Réputation en ligne

Il est également possible de mettre en place des outils externes qui vont vous aider à faire le ménage dans les publications et amis et à trouver rapidement un élément posté voilà plusieurs années. Car qui dit vie privée dit aussi réputation en ligne, les annonceurs n'hésitant pas à aller pêcher des informations sur des candidats à l'embauche ou les autorités à utiliser le réseau pour leurs enquêtes. Bref, mieux vaut donc prendre le temps de gérer quelques réglages. D'ailleurs, la dernière version de Facebook propose désormais un assistant de confidentialité, basique certes, mais qui permet déjà de régler quelques options, comme le fait de restreindre ses publications à ses seuls amis plutôt qu'aux millions de membres. Un bon début mais qui ne suffit pas à totalement maîtriser sa vie privée en ligne. Nous allons donc plus loin en vous conseillant des outils et services de surveillance et de confidentialité de pointe. ■

Facebook est un gigantesque puits de données privées à ciel ouvert qu'il revend aux spécialistes en marketing.

FACEBOOK FAIT ÉVOLUER SES CONDITIONS D'UTILISATION

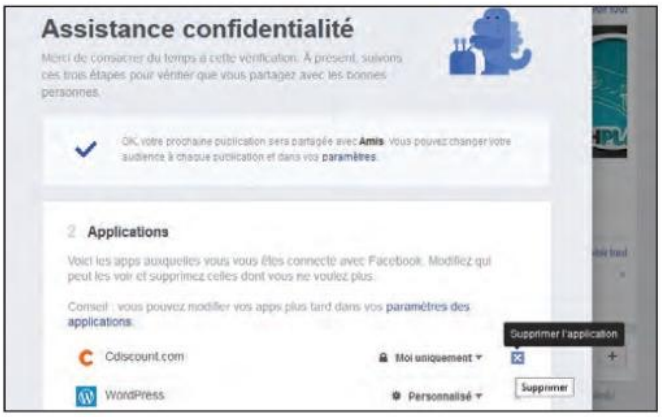
Depuis mars dernier, tout utilisateur actif sur Facebook est désormais protégé contractuellement contre l'espionnage et la surveillance de son compte. Rob Sherman, le chargé de la protection de la vie privée explique que les développeurs créant des logiciels utilisant les données de Facebook ne doivent plus les utiliser *« pour créer un outil à des fins de surveillance »* Un pas de plus dans le respect de la vie privée. En effet, auparavant, ces développeurs pouvaient espionner n'importe qui par le biais d'API, et géolocaliser les usagers Facebook, connaître leurs styles musicaux, etc. *« Nous sommes engagés dans la construction d'une communauté où les gens peuvent se sentir en sécurité lorsqu'ils s'expriment »*, ajoute Rob Sherman. Croyons-le sur parole.

4 options à ne pas sous-estimer

Facebook se bonifie avec un assistant de confidentialité. Mais pour mieux se protéger, des options de vie privée supplémentaires doivent être activées.

1 Profitez de l'assistant de confidentialité

Cliquez sur l'icône *Point d'interrogation* dans le menu supérieur, *Assistance confidentialité*. Suivez la procédure en sélectionnant d'abord qui peut voir vos publications (nous vous conseillons Amis). Cliquez sur *Suite* et découvrez ensuite les applications connectées à votre profil. Celles-ci vous espionnent constamment. Si vous ne les utilisez pas, cliquez sur X.

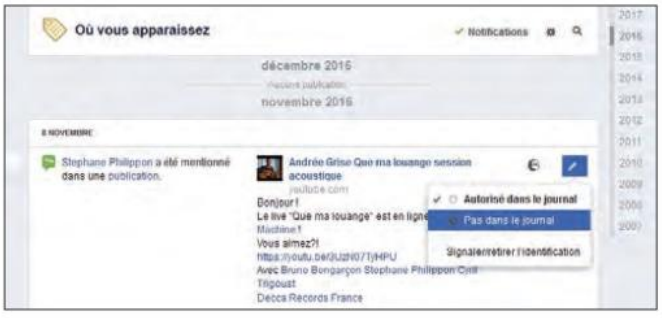


2 Paramétrez qui peut voir votre contenu

Cliquez sur la flèche pointant vers le bas dans le menu supérieur, *Paramètres, Confidentialité* en colonne gauche. Dans Qui peut voir mes contenus, optez pour *Amis*. Cliquez sur *Limiter l'audience des anciennes publications* pour limiter les contacts ayant accès à vos anciennes annonces. Ce paramètre est important pour protéger votre historique personnel sur Facebook.

3 Sachez qui vous identifie

Pour savoir qui a mentionné vos publications ou vous a identifié sur une photo, cliquez sur votre prénom, *Afficher l'historique personnel, Où vous apparaissez* en colonne gauche. Les publications vous mentionnant s'affichent. Pour les faire disparaître de votre journal, cliquez sur l'icône *Crayon* et sur *Pas dans le journal*. Revenez aux paramètres de confidentialité.



4 Restez caché aux yeux de Google

Pour éviter que quiconque ne puisse trouver votre page Facebook en renseignant votre nom dans un moteur de recherche comme celui de Google ou Bing, cliquez sur *Modifier* dans la partie Voulez-vous que les moteurs de recherche... Décochez la case *Autoriser les moteurs de recherche*, cliquez sur *Désactiver, Fermer*. Positionnez Qui peut me contacter sur Amis pour terminer.

NETTOYEZ VOTRE HISTORIQUE AVEC QSEARCH

Dans la zone de saisie Cherchez des personnes de Facebook, entrez *Qsearch* et cliquez sur *Qsearch* (App). Cliquez sur *Login With Facebook, OK, Renvoyer* (si demandé). La page Qsearch s'affiche dans Facebook. Utilisez la zone de saisie pour rechercher n'importe quel élément (nom, lieu, événement, etc.). Qsearch est bien plus puissant que la recherche Facebook qui est loin d'afficher tous les résultats. De plus, avec Qsearch, il est possible de trier les résultats en fonction du type de contenu via les onglets Photo, Link (liens web), Video. De plus, la flèche bleue en haut à droite de chaque résultat permet d'accéder à la publication d'origine pour la supprimer ou modifier son degré de visibilité.

Tweetez en paix !

Onze ans déjà que ce réseau de microblogage où chacun raconte sa vie en 140 signes existe. Au fil des ans, Twitter a su développer de multiples outils de confidentialité.

1 Paramétrez l'identification visuelle et la localisation

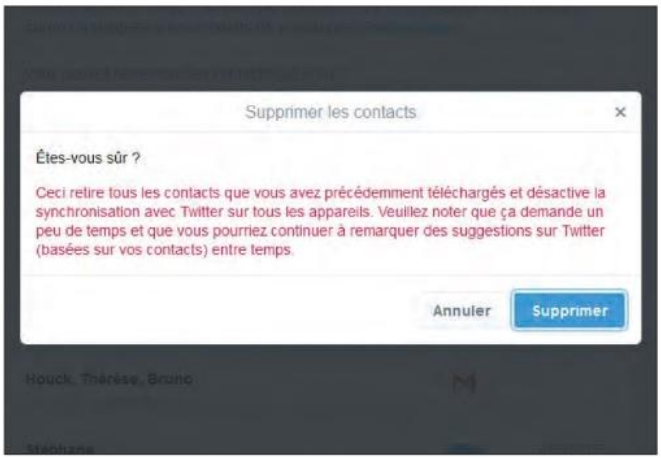
Depuis la page d'accueil, cliquez sur la vignette de votre personne dans le menu supérieur, *Paramètres et confidentialité* puis, en colonne gauche, sur *Confidentialité et sécurité*. Dans la partie Identification de photo, cochez la case *N'autoriser personne à m'identifier*. Vérifiez ensuite que la coche Localisation soit désactivée. Cela évitera que l'on vous géolocalise.

2 Protégez vos tweets

Si vous activez la coche Protéger mes Tweets, vos prochains tweets ne seront plus visibles de tous mais uniquement de vos contacts Twitter. Décochez les deux cases Détectabilité pour ne pas être repéré par votre mail ou n° de téléphone, ainsi que les deux cases Messages privés pour interdire à une personne que vous ne connaissez pas de vous envoyer des tweets.

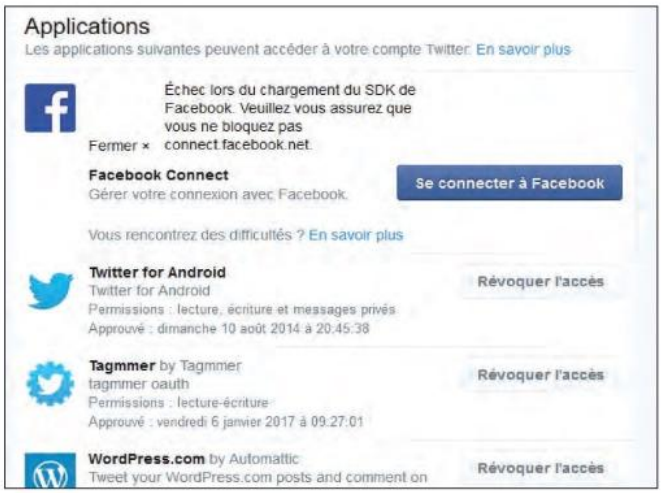
3 Faites le ménage dans les contacts

Cliquez sur *Gérer vos contacts* dans Carnet d'adresses. S'affiche la liste des contacts importés de vos boîtes mail. Cliquez sur *Supprimer tous les contacts*. Vos contacts Twitter ne seront pas effacés mais vous empêcherez Twitter de se faire trop voyeur. Revenez aux paramètres de confidentialité et décochez la case *Contenu sponsorisé* pour éviter la publicité ciblée.



4 Vérifiez quelles applis accèdent au compte

Dans les paramètres, cliquez sur *Applications* en colonne gauche. Les applis accédant à votre compte s'affichent. Cliquez sur *Révoquer l'accès de celles que vous n'utilisez pas avec Twitter*. Cela permettra de gagner en confidentialité. N'oubliez pas de changer de mot de passe périodiquement en cliquant en colonne gauche sur *Mot de passe* pour protéger le compte.



NE SOYEZ PLUS IMPORTUNÉ

Les filtres de notification permettent de ne pas recevoir de messages d'abonnés n'ayant pas totalement complété leur identification vis-à-vis de Twitter. Ce qui peut vous éviter d'être trouvé et traqué par des personnes pouvant avoir des perspectives malveillantes. Allez dans les paramètres et cliquez en colonne gauche sur *Notifications*. Cochez les 4 cases *Masquer les notifications de personnes* et cliquez sur *Enregistrer les modifications*. Par ailleurs, si une personne vous envoie des tweets sans raison, mieux vaut la bloquer en cliquant sur la flèche pointant vers le bas à droite du tweet, *Bloquer NomDuCompte*. Vous pouvez retrouver les comptes bloqués dans les paramètres, Comptes bloqués à gauche.

Privatisez votre chaîne YouTube

YouTube attire plus de 4 millions de visiteurs par jour rien qu'en France ! Cette grand-messe vidéoludique dispose heureusement de nombreuses options de confidentialité.

1 Réduisez le pistage des applis tierces

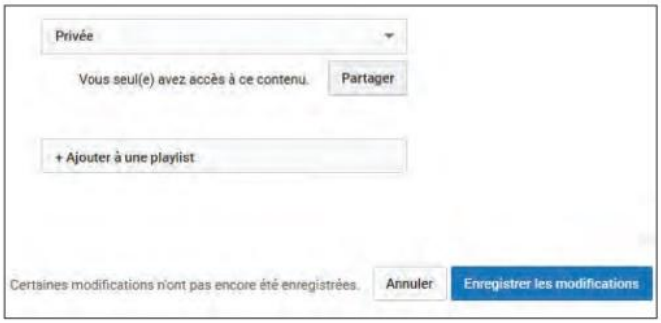
Connectez-vous à votre compte YouTube. Cliquez sur la vignette vous représentant en haut à droite puis sur la roue crantée et sur le lien *Options avancées, Sites autorisés à être utilisés avec votre compte Google*. Sélectionnez les applis et/ou services que vous ne souhaitez plus être reliés avec entre autres YouTube puis cliquez sur *Supprimer*. Vous serez moins pisté.

2 Désactivez pubs et recommandations

Dans les paramètres généraux, cliquez sur *Afficher les fonctionnalités supplémentaires* sur Options avancés (partie Chaîne). Si vous avez créé une chaîne, vous pouvez désactiver les annonces ciblées en cochant la case associée. Cochez la case n'autorisant pas les recommandations de chaîne ainsi que la case masquant votre nombre d'abonnés. Cliquez sur *Enregistrer*.

3 Paramétrez l'audience

Les vidéos que vous publiez sont publiques et visibles par tous. Pour qu'elles ne soient vues que par certains contacts, cliquez sur *Ma chaîne* en colonne gauche, *Gestionnaire de vidéos* et sur la flèche à droite de la vidéo à paramétrer, *Infos et paramètres*. Cliquez sur *Publique* puis sur *Privée, Partager*. Renseignez les adresses mail des contacts avec qui la partager.



4 Débarrassez-vous des publicités

YouTube est une plate-forme appréciée des annonceurs. Pour mettre fin aux pubs qui se lancent parfois avant une vidéo ou prennent la forme de bannière, installez l'extension Chrome Adblock pour YouTube ici : **https://goo.gl/cwwo7U**. Il est possible de trouver l'équivalent pour Firefox avec le module AdBlocker for YouTubeVideo à installer ici : **https://goo.gl/bHG3ZO**.

GÉREZ FINEMENT LES PRINCIPALES OPTIONS DE VIE PRIVÉE

Pour que personne ne puisse voir les chaînes auxquelles vous êtes abonné, rendez-vous dans Mes paramètres (roue crantée) et cliquez sur *Confidentialité* en colonne gauche. Dans Vidéos, cochez *Garder mes abonnements privés*. Profitez-en aussi pour cocher *Garder privées mes vidéos "J'aime"* pour que personne ne puisse voir les vidéos que vous avez notées comme aimé. Cliquez sur *Enregistrer*. Vous pouvez également masquer l'intégralité de votre chaîne pour que personne ne puisse y accéder et voir vos vidéos. Accédez aux options avancées des paramètres du compte et cliquez sur *Supprimer la chaîne*. Déroulez le menu Je souhaite masquer ma chaîne. Cochez les cases des données que vous souhaitez masquer et cliquez sur *Masquer ma chaîne*.

Que faire des données personnelles après son décès ?

Pas facile de se projeter après sa propre mort. Pourtant, tout ce que nous avons partagé en ligne demeure sur Internet. Comment gérer cette mémoire numérique ?

En 2012, environ 3 millions de profils Facebook sont passés de vie à trépas. S'il est difficile de se projeter après sa propre mort, il est encore plus complexe de savoir ce que vont devenir tous nos écrits, photos, vidéos et musiques mémorisés sur Internet. Aujourd'hui, le droit français n'apporte pas de réponse à ce qu'il convient de faire des données numériques d'un proche qui vient de décéder. Celles-ci étant généralement sauvegardées sur le sol américain par des groupes étrangers, on doit se tourner avec l'aide de son notaire vers Google, Facebook ou encore Microsoft pour pouvoir accéder au compte du défunt dans le but d'en prendre connaissance et le clôturer, si bien que l'on fait face au droit américain. Facebook exige par exemple un document écrit prouvant que ce dernier souhaitait de son vivant *« remettre spécifiquement ses communications électroniques entre vos mains ou celles d'un tiers »*. Google, lui, exige un certificat de décès ainsi qu'une ordonnance d'un tribunal des Etats-Unis. En fait, la vie numérique privée demeure privée même après la mort, étant donné que nous confions de plus en plus de documents à notre micro, ouvrons parfois des comptes sur des sites de rencontre,

FAITES RESPECTER VOTRE DROIT À L'OUBLI

Si vous souhaitez faire table rase après votre mort, il existe des solutions permettant d'effacer une grande partie de vos traces numériques. Commencez par en informer vos proches et laissez-leur vos codes d'accès à vos boîtes de messagerie, réseaux sociaux et autres webmarchands afin qu'ils puissent clôturer vos comptes. Ils peuvent aussi en passer par des services spécifiques d'effacement comme Reputation.com, Agence CSV (**www.agence-csv.com/e-nettoyeurs**) ou bien Zen-reputation.com. Tous proposent, moyennant finance, de supprimer des pages Web vous concernant. Suivez aussi les préceptes de la Cnil à cette adresse : **http://goo.gl/VSnrdv**. Ils permettent d'éradiquer vos données sur les moteurs de recherche.

établissons des fils de discussion avec des ex dont on ne souhaite pas divulguer la teneur, achetons toutes sortes de biens, etc. Autant d'actes pouvant avoir des conséquences post-mortem pour la famille, le conjoint.

Coffre-fort numérique

Voilà pourquoi mieux vaut, si on le souhaite, remettre à son notaire l'ensemble de ses codes d'accès et mots de passe et coucher sur papier ce qu'il doit en faire une fois décédé. Ce dernier peut par exemple transmette à la famille ce patrimoine numérique ou au contraire imposer sa suppression, en fonction de la volonté du défunt. Ces codes peuvent aussi servir à récupérer des documents, musiques, vidéos et autres photos qui viendront chérir le souvenir du défunt. Vous pouvez également vous offrir les services d'un coffre-fort numérique à l'image d'Edeno (**https://secure.edeneo.fr**) qui entrepose vos informations personnelles puis les transmet aux personnes que vous aurez désignées après votre mort. Coût d'un tel service ? 300 € à vie. En attendant d'y passer à votre tour, vous pouvez aussi chérir la mémoire d'un proche qui détenait un profil Facebook puisque ce réseau social propose depuis 2009 un mode commémoratif où famille et amis peuvent venir se recueillir sur une page qui rend hommage à la personne décédée. Une bonne solution pour faire son deuil, tout en conservant une trace indélébile de ce qu'aura été la vie de la personne sur ce réseau social. Emouvant souvenir en définitive où il est possible de laisser des messages post-mortem comme on le fait déjà depuis des années avec les carnets du souvenir lors d'un enterrement. ■

Il est très difficile de récupérer ses données personnelles, même après sa disparition.

Pensez à vos proches

3 solutions numériques post-mortem

1 Sanctri Echangez autour du défunt

Sanctri est une application Facebook permettant de créer un mémorial virtuel et personnel autour de la personne disparue. Les proches et la famille peuvent échanger des souvenirs, textes et photos pour chérir le souvenir du disparu. N'importe qui peut créer un mémorial et y poster des témoignages privés ou publics. Leur publication s'affiche ensuite sous la forme d'un scrapbook. **www.sanctri.com**

2 La vie d'après Constituez votre héritage numérique

Ce service vous permet de constituer tout au long de votre vie un héritage numérique à travers un espace privé et crypté. Vous pourrez y glisser des messages à destination de vos amis, rédiger vos mémoires, stocker vos codes d'accès à vos réseaux sociaux et gérer vos contacts. A votre mort, la personne que vous aurez désignée pourra ouvrir le coffre-fort. **www.laviedapres.com**

3 Social Mausoleum Elevez un mausolée

Pourquoi ne pas élever un mausolée à votre image une fois enterré ? C'est ce que propose Social Mausoleum avec la constitution d'un espace que vous nourrissez en préparant un message d'anniversaire à vos petits-enfants, un message d'adieu à vos amis Facebook, un livre d'or, etc. Une fois décédé, Social Mausoleum se propose de clôturer les comptes de vos réseaux sociaux. **www.socialmausoleum.com**

APRÈS MOI LES SOUVENIRS

Avec After Me, vous avez la possibilité de laisser une trace sur cette Terre qui a déjà vu plus de 100 milliards d'humains y vivre et mourir. Pour sauvegarder votre ego et permettre à vos descendants d'entretenir la flamme, cette plate-forme sauvegarde votre vie à partir de documents, photos, vidéos et musiques. Libre à vous, après votre décès, de partager tel ou tel souvenir avec tel ou tel proche. Vous organisez comme bon vous semble cet espace à partir de modèles de pages. Après votre mort, After Me se chargera de transmettre votre message pour l'éternité ! **www.after-me.com**