Secret des conversations, Facebook Messenger bientôt chiffré

	Secret des conversations, Facebook Messenger bientôt chiffré

Non, tous les échanges sur Messenger ne sont pas chiffrés de bout en bout. Pas encore du moins. Facebook teste le procédé à travers une nouvelle fonctionnalité, #Secret Conversations. En y ajoutant un petit côté messages éphémères à la Snapchat.

Facebook chantre du chiffrement de bout en bout ? L'entreprise vient de lancer une nouvelle option pour Messenger permettant de démarrer une conversation sécurisée. Baptisée Secret Conversations, celle-ci permet de créer, via la fiche d'un contact, une conversation chiffrée entre deux utilisateurs. Derrière, on retrouve le protocole Signal, également utilisé par WhatsApp.
Mais, contrairement à #WhatsApp, Secret Conversations se veut optionnel, pour ne pas dire ponctuel. Car il s'agit là de préférer la sécurité au confort, un choix auquel Facebook n'entend pas contraindre ses utilisateurs. Ainsi, via cette fonctionnalité, on ne peut envoyer que du texte et des photos à un unique destinataire. Pas de vidéo, de GIF, de paiement ou de discussion de groupe.

Ce message s'autodétruira automatiquement dans 4…3…

Cette sobriété se conjugue avec l'absence de synchronisation entre les appareils d'un même utilisateur. Impossible donc de commencer une conversation chiffrée avec son iPhone et de passer ensuite à sa tablette : la discussion est uniquement rattachée au terminal avec lequel elle a été initiée. En outre, preuve que Mark Zuckerberg n'a toujours pas digéré le refus de son offre de rachat sur Snapchat, il est possible de définir à l'aide d'un minuteur la durée de vie d'un message. Qui s'autodétruira une fois le délai écoulé.
L'option est intégrée à l'application Messenger pour Android et iOS. Déjà disponible pour certains, elle sera déployée plus largement au cours de l'été. Pour l'heure, il semble que rien ne soit prévu pour les versions navigateur du service.

Article original de Guillaume Périssat

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Secret Conversations : Facebook Messenger en mode chiffré

Pokémon Go peut-il vraiment prendre le contrôle de votre compte Gmail ?

Pokémon Go peut-il vraiment prendre le contrôle de votre compte Gmail ?

Malgré son succès indéniable, il semblerait que l'application Pokémon Go rencontre des premiers couacs, notamment en matière de protection de la vie privée. Selon certaines informations, depuis démenties, elle pourrait accéder et composer des emails sur le compte Gmail des utilisateurs.

Après avoir soulevé certains problèmes récemment avec le cas des voleurs armés aux États-Unis qui utilisaient le jeu pour cibler leurs victimes ou celui d'une jeune adolescente qui aurait retrouvé un cadavre pendant sa « chasse » aux Pokémon. La polémique n'en finit plus autour de Pokémon Go. C'est aujourd'hui un problème d'éthique et de sécurité qui est désormais pointé du doigt.

Pokémon Go : comment le jeu a rendu fou le monde entier

En effet lorsque vous installez et que vous jouez à Pokémon Go pour la première fois, le jeu sur smartphone développé par la firme Niantic, demande deux types de connexion. La première consiste à créer un compte via l'application tandis que la deuxième exige de se connecter directement depuis son compte Google. C'est la deuxième connexion qui soulève plusieurs problèmes.

Sur son blog, l'analyste en sécurité Adam Reeve expliquait ainsi ce week-end que cette identification par Google pouvait poser plusieurs problèmes puisque l'application accédait à plusieurs paramètres de votre compte Google : « Pokémon Go et Niantic peuvent désormais lire tous vos emails, envoyer des emails de votre part, accéder à vos documents Google Drive, rechercher dans votre historique de recherche et de navigation, accéder à toutes les photos privées hébergées sur Google Photos et bien davantage ». Des accès qui ne sont, bien évidemment, pas nécessaires pour profiter de l'expérience de jeu de l'application développée par Niantic.

Des informations démenties par Google et Niantic

Cependant, interrogé par le site Gizmodo, Adam Reeve a finalement fait marche arrière sur ses affirmations, expliquant ne pas être « certain à cent pour cent » que son billet de blog est exact. Il a par ailleurs expliqué au site Internet qu'il n'avait jamais développé lui-même d'application utilisant l'identification Google et n'a pas expérimenté ce qu'il indiquait sur son blog.

Du côté de Google également, l'information a été démentie auprès de Dan Guido, expert en sécurité informatique. La firme de Mountain View explique que les autorisations de Pokémon Go ne concernent que la partie « Mon Compte » de Google et n'autorise pas d'accès spécifique à différents services.

Enfin, le studio Niantic, qui développe l'application avec The Pokémon Company, a publié ce mardi un communiqué de presse afin de rassurer les utilisateurs : « Pokémon Go n'accède qu'aux informations basiques des profils Google (votre identification et votre adresse email). Aucune autre information de votre compte Google n'est ou ne sera collectée. […] Google réduira prochainement les autorisations de Pokémon Go uniquement aux données de profil dont Pokémon Go a besoin, les utilisateurs n'auront pas besoin d'effectuer le moindre changement ».

Article original de GEOFFROY HUSSON

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

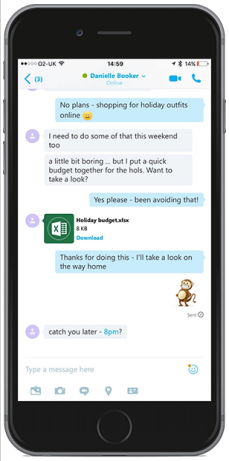
Original de l’article mis en page : Pokémon Go peut-elle vraiment prendre contrôle de votre compte Gmail ?

Envoyez désormais des fichiers aux contacts hors ligne avec Skype

Envoyez désormais des fichiers aux contacts hors ligne avec Skype

---

La mise à jour de Skype permet de transmettre des fichiers aux contacts hors ligne. En outre, la limite maximale par fichier a été relevée à 300 Mo.
Si vous avez l'habitude d'envoyer des fichiers par Skype, voilà une nouvelle qui devrait vous satisfaire : en récupérant la version la plus récente du logiciel de téléphonie et de messagerie instantanée, vous pouvez partager des contenus lorsque les destinataires ne sont pas connectés au moment de l'envoi.
Cette fonctionnalité implique manifestement un stockage du fichier sur les serveurs de Microsoft – la maison-mère de Skype – afin que le service puisse être en mesure de le faire suivre quand le destinataire se reconnectera. L'envoi peut concerner un seul contact ou tout un groupe de discussion.



Attention, néanmoins. Une limite à 300 Mo par fichier est appliquée par Microsoft. Si celle-ci suffit amplement dans la plupart des cas, vous ne pourrez pas envoyer une vidéo trop lourde. Il faudra procéder autrement si vous tenez absolument à envoyer ce fichier qui contient « 2016.TRUEFRENCH.EXTENDED.BDRip.XViD.AC3 » dans le titre…
Une autre évolution appréciable de Skype figure dans l'accès à un fichier depuis de multiples appareils. Maintenant, vous pouvez lire le même document depuis votre smartphone, votre tablette ou votre ordinateur, sans avoir besoin de demander à votre interlocuteur de vous le renvoyer.

Article original de Julien Lausson

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Skype vous permet d'envoyer des fichiers aux contacts hors ligne – Tech – Numerama

---

Eleanor, nouvelle menace sur la planète Mac

Eleanor, nouvelle menace sur la planète Mac

Alors que beaucoup d'utilisateurs de Mac se montrent parfois négligents en matière de sécurité, les équipes de BitDefender ont détecté un nouveau backdoor baptisé Eleanor qui ciblent les Mac et qui peut causer d'importants dégâts sur les machines. En effet, il offre la possibilité aux pirates de prendre le contrôle d'une machine à distance.

Le backdoor Eleanor à l'assaut des Mac

Comme souvent, c'est l'éditeur BitDefender qui a identifié la nouvelle menace qui pèse sur les Mac. Eh oui, même si les dangers sont généralement moindres sur Mac que sur PC, voilà que ceux qui ont choisi les ordinateurs d'Apple doivent se montrer vigilants.

En effet, dès lors que ce backdoor silencieux est parvenu à infecter une machine, il a la capacité de permettre à un attaquant de prendre le contrôle du Mac à distance. Ainsi, les hackers peuvent s'en servir pour voler des données présentes sur la machine piratée, télécharger des applis frauduleuses ou même pour détourner la webcam, une pratique de plus en plus courante.

Reste que l'infection du Mac ne se produit pas toute seule et qu'elle est l'une des conséquences du téléchargement de l'application malveillante Easy Doc Converter. En effet, lors du démarrage d'OS X, cette appli va installer sur le Mac trois composantes : un service Tor, un service web capable de faire tourner PHP et un logiciel dédié. Autrement dit le matériel indispensable pour que s'installe, sur Mac, un backdoor silencieux comme Eleanor.

L'intégralité des Mac concernée par Eleanor ?

Si BitDefender a tenu à alerter sur sa découverte, il semblerait tout de même que tous les Mac ne soient pas tous concernés par cette menace.

En effet, parce que le logiciel Easy Doc Converter n'est pas signé numériquement avec un certificat approuvé par Apple, les risques d'infection sont réduits. D'ailleurs, la marque à la pomme a tenu à le préciser en rappelant que tous les Mac dotés de la protection Gatekeeper n'avaient rien à craindre.

Article original de Jérôme DAJOUX

Réagissez à cet article

Original de l’article mis en page : Eleanor, nouvelle menace sur la planète Mac

---

Peut-on vraiment forcer les collectivités locales d’utiliser un « cloud souverain » ?

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'intérieur
Direction générale des collectivités locales
Sous-direction des compétences et des institutions locales

Ministère de la culture et de la communication
Direction générale des patrimoines
Service interministériel des Archives de France

Note d'information du 5 avril 2016 relative à l'informatique en nuage (*cloud computing*)

Références : DGP/SIAF/2016/006
~~DGCL~~
NOR: MCCA6143540

Ministère de la Culture et de la Communication
05 AVR. 2016 – 2016/004
SAFIG/SDAIG/MPDOC

Le directeur général des collectivités locales et le directeur chargé des archives de France

à

Mesdames et Messieurs les préfets de région
et Mesdames et Messieurs les préfets de département

Peut-on vraiment forcer les collectivités locales d’utiliser un « cloud souverain » ?

---

par Emilien Ercolani

Une circulaire d'avril dernier, qui sert à rappeler le cadre légal applicable, écrit noir sur blanc qu'il est illégal d'utiliser « un cloud non souverain » pour les documents créés et gérés par les collectivités territoriales. Au-delà d'être illusoire, la mesure est en plus ubuesque.

C'est une circulaire du 5 avril 2016 qui a remis le sujet sur le tapis. Relative à l'informatique en nuage, elle explique tout d'abord que les documents et données numériques produits par les collectivités territoriales « *relèvent du régime juridique des archives publiques dès leur création* ». Les archives publiques sont considérées comme « *des trésors nationaux* », et les données numériques ne font pas exception.
Le raisonnement est donc le suivant : pour protéger les « *trésors nationaux* », il convient de les conserver sur le territoire national pour ainsi dire garantir leur préservation. « *Un trésor national ne peut pas sortir du territoire douanier français sinon à titre temporaire* », souligne encore le texte. Pour les données numériques, il faut donc qu'elles soit traitées et stockées en France. Raisonnement logique… pour qui ne connaît pas vraiment le monde de l'informatique.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'intérieur
Direction générale des collectivités locales
Sous-direction des compétences et des institutions locales

Ministère de la culture et de la communication
Direction générale des patrimoines
Service interministériel des Archives de France

Note d'information du 5 avril 2016 relative à l'informatique en nuage (*cloud computing*)

Référence : DGCL/SIAF/2016/006
NOR : INTB1607913N

Le directeur général des collectivités locales
et le directeur chargé des archives de France

à

Ministère de la Culture et de la Communication
05 AVR. 2016 - 2016/004
SAFIG/SDAIG/MPDOC

Mesdames et Messieurs les préfets de région
et Mesdames et Messieurs les préfets de département

Les conséquences de la loi appliquée à la lettre

Concrètement, cela voudrait dire qu'une collectivité territoriale doit donc traiter et stocker ses données, anciennes et futures, sur le territoire. Et donc, dans des data centers installés sur le sol français. Ce qui implique que toutes les suites d'outils logiciels et bureautiques en mode cloud sont désormais interdites : Office 365 et les Google Apps (pour ne citer que les plus connues) sont désormais bannies puisque ni l'une ni l'autre ne sont en mesure de garantir un stockage sur le territoire national.

« *L'utilisation d'un cloud non souverain (…) est donc illégale pour toute institution produisant des archives publiques* », poursuit la circulaire. A savoir que la définition d'un cloud souverain pour la direction générale des collectivités locales (DGCL), qui dépend du ministère de l'Intérieur, est la suivante :

Modèle de déploiement dans lequel l'hébergement et l'ensemble des traitements effectués sur des données par un service de cloud sont physiquement réalisés dans les limites du territoire national par une entité de droit français et en application des lois et normes françaises.

Une circulaire « politique »

*La **circulaire** s'appuie toutefois sur des textes de loi, et notamment sur les articles L211-1 et L211-4 du Code du Patrimoine, utilisés dans le **Référentiel général de gestion des Archives**. Mais, concrètement, cela traduit d'une part une méconnaissance de l'informatique en règle générale, d'autre part des mesures qui ne sont pas réalistes.*
Responsable juridique du Syntec Numérique, Mathieu Coulaud nous explique tout d'abord que cela ne pénalise pas que Google ou Microsoft, mais aussi des acteurs européens ; l'Allemand T-Systems héberge par exemple de nombreuses données des collectivités territoriales françaises. D'autre part, il s'étonne « qu'aucune consultation et d'étude d'impact n'aient été réalisées ». Pour lui, cette circulaire est donc purement politique dans le sens où :
• Rien n'a été fait pour ouvrir le dialogue et s'informer des conséquences d'une telle mesure
• Cela dénote une incompréhension de la part des pouvoirs publics mais aussi les dissonances entre les différents ministères
« Nous avons écrit au directeur du SIAF (Service Interministériel des Archives de France) en 2015. Nous avons reçu sa réponse en janvier 2016, qui était en somme une fin de non-recevoir », poursuit Mathieu Coulaud. « Pour nous, ils confondent sécurité et localisation des données ». Effectivement, car même l'Anssi ne semble pas avoir été consultée, elle qui prépare un label « Secure Cloud » sensé garantir la souveraineté des données hébergées.

***Exclusif** : ce mercredi 6 juillet a lieu une réunion interministérielle qui réunit notamment Bercy, Matignon et le ministère de la Culture. Les administrations vont donc se parler et le sujet sera vraisemblablement à l'ordre du jour.*
« Nous avons déjà été reçus par différents ministères (Economie, Culture, etc.) mais sans rien obtenir. Plusieurs recours sont possibles, notamment concernant l'accès à la commande publique. Nous estimons qu'il existerait avec cette circulaire une vraie discrimination entre les acteurs, ce qui est contraire à la loi. Le ministère de la Culture assure que tout est viable juridiquement, mais je n'ai rien pu vérifier », ajoute Mathieu Coulaud qui souligne : « nous nous réservons des actions possibles d'influence et de droit ».

Une double lecture

Le rappel du cadre légal a rapidement fait réagir de toutes parts. « Je ne peux m'empêcher de penser qu'il s'agit de fausses bonnes nouvelles pour les prestataires de services comme pour les collectivités locales », estime Christophe Lejeune, directeur général de l'entreprise nantaise Alfa Safety qui persiste : « Enfermer dans un cadre strictement national un service innovant comme le cloud est un contre-sens ». Pour le Syntec Numérique, la circulaire va à rebours du projet de loi République Numérique, crée des barrières protectionnistes et freinera la transformation numérique. Sans compter qu'elle ne dit rien sur la nature des données en elles-mêmes. « Si un DSI envoie un smiley, cela devient un trésor national !« , ironise Mathieu Coulaud.
Mais à bien y regarder, la circulaire en question n'est-elle pas fondamentalement positionnée pour défendre les enjeux nationaux ? Et pourquoi pas faire émerger un nouveau « cloud souverain » français, voire des alternatives logicielles en mode cloud ? Opportuniste, l'hébergeur du Nord OVH rappelle non seulement son implantation en France mais aussi ses certifications et finalement qu'il est un « acteur national responsable, capable d'héberger sans risque les données issues du travail et des archives des différentes institutions publiques ; créant ainsi un Cloud véritablement souverain et fonctionnel ».

Original de l'article mis en page : Les collectivités locales forcées d'utiliser un « cloud souverain » ?

Microsoft stocke 200 Mo de données informatiques sous forme d'ADN

Microsoft stocke 200 Mo de données informatiques sous forme d'ADN

L'université de Washington a collaboré avec Microsoft pour écrire 200 Mo de données informatiques sur un bout d'ADN. Le but est d'optimiser au maximum l'espace de stockage et sa durabilité en allant vers un stockage biologique.

Écrire 200 méga-octets de données informatiques sur de l'ADN de synthèse. C'est la prouesse réalisée par des scientifiques de l'université de Washington en collaboration avec Microsoft. Les informations inscrites sur les molécules contiennent la Déclaration universelle des droits de l'homme en plus de 100 langues, les 100 livres électroniques les plus téléchargés sur la bibliothèque Projet Gutenberg, une partie des bases de données de Crop Trust, un groupe consultatif international pour la recherche agricole et un clip musical du groupe américain Ok Go,
« *Nous utilisons l'ADN comme un espace de stockage de données numériques* », explique le professeur Luis Ceze dans une vidéo. « *La raison pour laquelle nous faisons cela est parce que l'ADN est très dense et que l'on peut mettre énormément d'informations dans un très petit volume* », ajoute-t-il.

LA TOTALITÉ DE L'INTERNET POURRAIT TENIR DANS UNE BOÎTE À CHAUSSURES
Il affirme également que la totalité de l'Internet pourrait tenir dans une boîte à chaussures grâce à ce procédé. L'autre motivation des scientifiques est aussi le fait que l'ADN peut être conservé très longtemps. « *Dans les bonnes conditions, il peut durer des milliers d'années tandis que les technologies de stockages ne tiennent que quelques décennies* ».

L'ADN est fait de différentes séquences de quatre molécules : l'adénine (A), la guanine (G), la cytosine (C) et la thymine (T).Les scientifiques ont réussi à encoder les données qu'ils voulaient stocker sur les quatre molécules de base de l'ADN synthétisé.
En analysant l'ADN, ils peuvent lire les informations et les rétablir à leur état original.
Les 200 Mo de documents sont enregistrés sur un bout d'ADN qui fait la taille de quelques grains de sucre. Celui-ci a été encapsulé pour éviter toute dégradation.
Les capacités de stockage de l'ADN sont énormes. Malheureusement, lire les données dessus prend beaucoup de temps – jusqu'à plusieurs heures. Aussi, ce procédé n'est pas prêt d'être démocratisé, d'autant plus qu'il coûte encore très cher. Mais cela serait apparemment en train de changer. « *La technologie pour lire l'ADN est en train de se développer rapidement et pourrait devenir suffisamment rapide et bon marché pour être commercialisée* », explique Luis Ceze à The Register.
Le scientifique pense que les premiers clients seront probablement les centres de données pour qui l'optimisation de l'espace de stockage est un enjeu permanent.

Article original de Omar Belkaab

Réagissez à cet article

Original de l'article mis en page : Microsoft stocke 200 Mo de données informatiques sous forme d'ADN – Sciences – Numerama

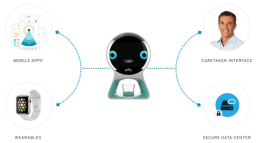
Pillo, un robot intelligent et connecté en guise de pilulier

Pillo, un robot intelligent et connecté en guise de pilulier

Pillo est un petit robot à placer dans le foyer, qui reconnait les membres de la famille pour distribuer à chacun les pilules dont ils ont besoin, et délivrer des conseils médicaux adaptés.

Pillo ne sera disponible qu'en 2017, toutefois, ce petit robot pilulier se dévoile déjà à l'occasion de son financement participatif sur IndieGogo. Un crowd-funding presque intégralement réussi ce lundi (près de 75 000 dollars levés) alors-même que le robot n'a été mis en ligne qu'il y a une semaine. Le petit pilulier aura réussi à convaincre des backers en très peu de temps.

Il a pour cela quelques arguments : le petit assistant domestique se propose d'être une interface afin de monitorer et gérer au quotidien la santé des foyers. Pillo distribue quotidiennement aux membres d'une famille les pilules qui lui sont nécessaires et pour cela le robot est équipé d'une technologie de détection des visages, afin de rendre le pilulier totalement autonome et faciliter nos quotidiens. Seulement, là où le robot convainc vraiment, c'est qu'en dehors de son rôle de distributeur, il parvient à trouver un vrai rôle en tant qu'objet .



En plus de surveiller votre consommation de médicaments et de vous demander d'en recommander quand il risque de vous en manquer, Pillo répond également à de nombreuses questions sur votre santé et les aliments que vous consommez et s'ambitionne comme une véritable interface pour les consultations à distance par exemple. Or, c'est là qu'on trouve la valeur ajoutée du Pillo face au pilulier de mamie ; le robot exécute une tâche essentielle chaque jour, mais en plus de répondre à un besoin, il introduit assez de composants et de possibilités pour s'ambitionner comme un véritable hub de la health tech à la maison.

Ses concepteurs ont promis que le produit serait commercialisé, peu importe la réussite de la campagne IndieGogo qui comme souvent sert d'opération publicitaire pour une startup. Le robot était disponible à partir de 256 $ sur la plateforme et sera commercialisé plus de 600 $ en 2017, dans un premier temps uniquement aux USA.
Mieux vaudra en tout cas être sûr de sa fiabilité et de sa sécurité, pour accepter de reposer sur un robot connecté pour distribuer ses pilules au petit déjeuner…
Article original de Corentin Durand

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

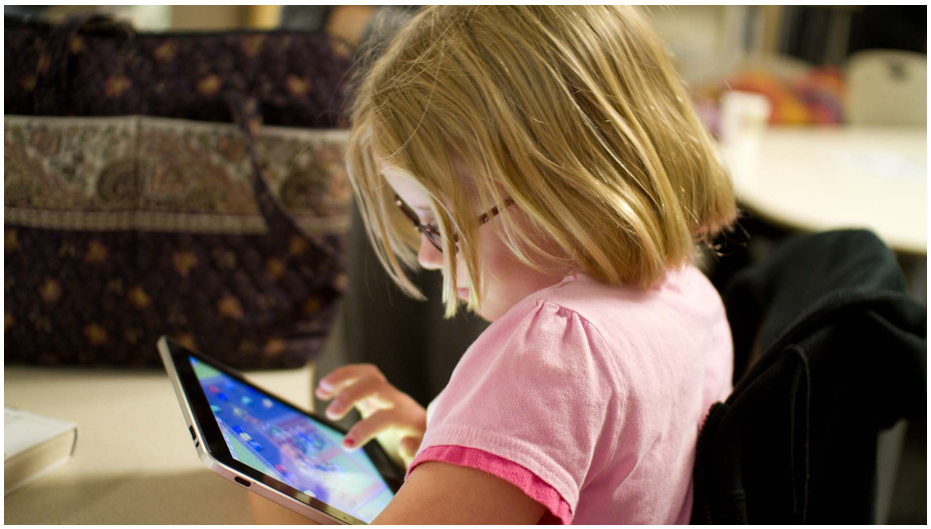
Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Pillo : un robot en guise de pilulier intelligent et connecté — Tech — Numerama

---

Attention aux ondes des tablettes et smartphones pour les enfants !



Attention aux ondes des tablettes et smartphones pour les enfants !

Un rapport publié par l'agence de la sécurité sanitaire met en garde les parents sur l'exposition des enfants aux ondes. Elle recommande un usage modéré et encadré des technologies sans fil. Elle suggère aussi une révision de la réglementation.

Attention aux technologies sans fil ! Telle est la mise en garde que vient de formuler l'agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses) ce vendredi, dans un rapport portant sur le sujet hautement sensible de l'exposition aux radiofréquences et à la santé des enfants. Dans celui-ci, elle note « des effets possibles sur les fonctions cognitives et le bien-être » et recommande de limiter et d'encadrer l'usage de ces technologies.

Dans le cadre de ce travail, ce sont les enfants de moins de six ans qui ont fait l'objet d'un suivi particulier. L'Anses avait été saisie par les pouvoirs publics afin de vérifier si les dispositions réglementaires à propos des appareils radioélectriques destinés aux plus jeunes sont suffisamment protectrices en matière de santé et de sécurité. Il ressort que « les enfants pouvaient être plus exposés que les adultes » du fait de leurs spécificités morphologiques et anatomiques.

C'est ce que détaille à France Info Olivier Merckel, chargé de l'évaluation des risques. « Les enfants sont plus exposés que les adultes aux champs électromagnétiques : l'épaisseur du crâne chez les enfants est plus petite que chez les adultes donc on a une exposition globale plus importante ». En outre, les « caractéristiques de certains de leurs tissus » contribuent à cette vulnérabilité accrue. Il faut donc redoubler de vigilance quant à l'exposition des petits.
Le problème, c'est la généralisation des équipements de transmissions sans fil dans leur environnement. « Les données disponibles sur l'exposition montrent une forte expansion de l'usage des nouvelles technologies sans-fil, notamment chez les très jeunes enfants », relève le rapport. Il y a le smartphone, il y a la tablette, il y a les objets connectés, il y a le babyphone, il y a les jouets radiocommandés… et beaucoup d'autres appareils dédiés à la surveillance du petit ou à l'occuper.

LES ENFANTS SONT PLUS EXPOSÉS QUE LES ADULTES
Or, on le devine aisément : plus la source émettrice est proche, plus l'intensité et la quantité du rayonnement sont élevées. En la matière, des appareils comme des smartphones ou des babyphones peuvent légitimement constituer une source d'inquiétude, car ils sont en général très près de la tête — que ce soit pour parler au téléphone ou bien pour entendre les bruits de bébé et s'assurer que tout va bien.

QUELS EFFETS POTENTIELS ?
L'Anses souligne toutefois que « les données actuelles ne permettent pas de conclure à l'existence ou non d'un effet des radiofréquences chez l'enfant sur le comportement, les fonctions auditives, les effets tératogènes et le développement, le système reproducteur, les effets cancérogènes, le système immunitaire, la toxicité systémique ». Des études plus approfondies seront sans doute nécessaires.
L'Anses mentionne toutefois deux cas où à un effet des radiofréquences est possible : les fonctions cognitives d'abord. « Les résultats montrant des effets aigus se basent sur des études expérimentales dont la méthodologie est bien maîtrisée », note le rapport. Un effet négatif sur le bien-être peut aussi être envisagé, même s'il « pourrait cependant être lié à l'usage du téléphone mobile plutôt qu'aux radiofréquences qu'ils émettent ». Bref ce serait plus ce serait la manière dont on s'en sert le problème.

UN USAGE RAISONNABLE
Est-ce que cela veut dire qu'il faut tenir les enfants loin de ces sources d'émission ? En clair, faut-il les priver de portable jusqu'à un âge avancé, retirer les jouets high tech et vérifier que la chambre n'est pas trop exposée ? Pour Olivier Merckel, il faut prendre quelques mesures, mais ne pas non plus exagérer. Les jeunes de moins de 13 ans peuvent passer « quelques appels, quelques SMS par jour » mais « certainement pas plusieurs heures ».
Un usage maitrisé. Tel est donc le conseil général donné par l'Anses à l'attention des parents. « L'Agence recommande aux parents d'inciter leurs enfants à un usage raisonnable du téléphone mobile, en évitant les communications nocturnes et en limitant la fréquence et la durée des appels ». Mais des actions doivent aussi être engagées du côté des pouvoirs publics, au niveau français ou européen.

UNE RÉGLEMENTATION À REVOIR
Pour l'Anses, il convient d'actionner plusieurs leviers, à commencer par l'obligation de soumettre l'ensemble des dispositifs radioélectriques, et notamment ceux destinés aux enfants, « aux mêmes obligations réglementaires en matière de contrôle des niveaux d'exposition et d'information du public que celles encadrant les téléphones mobiles ». L'agence demande aussi de reconsidérer les niveaux de référence visant à limiter l'exposition environnementale.
Les pouvoirs publics doivent également « réévaluer la pertinence du débit d'absorption spécifique (DAS) ». Il s'agit d'un indicateur utilisé pour l'établissement des valeurs limites d'exposition des personnes, à des fins de protection contre les effets sanitaires connus et avérés (effets thermiques) des radiofréquences. Il convient également de « développer un indicateur représentatif de l'exposition réelle des utilisateurs de téléphones mobiles », « quelles que soient les conditions d'utilisation ».

UN DÉBAT PERMANENT
La question des ondes et de leurs effets potentiels sur la santé a donné lieu à une littérature scientifique abondante. L'Anses elle-même publiait déjà en octobre 2013 un avis dans lequel elle notait à l'absence d'effets avérés sur la santé mais suggérait quand même de prendre des mesures de précaution, en particulier du côté des enfants et des utilisateurs intensifs. La publication avait toutefois fait l'objet de critiques dans la société civile, au sein d'associations spécialisées.
Deux ans auparavant, le centre international de recherche sur le cancer déclarait que les champs électromagnétiques de radiofréquence sont peut-être cancérogènes. Mais là encore, les conclusions avaient été discutées. Ainsi, des organisations professionnelles avaient estimé que le risque soulevé par les experts n'avait pas été clairement démontré par un lien évident de cause à effet et, que de ce fait, la poursuite des travaux scientifiques est indispensable.
Article original de Julien Lausson

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Ondes : les enfants doivent moins utiliser les tablettes et smartphones

---

Le chiffrement des smartphones Android incassable ?

Le chiffrement des smartphones Android incassable ?

Un chercheur en sécurité décrit comment faire sauter la protection par chiffrement des données sur les smartphones Android équipés de puces Qualcomm.

Chiffrer l'ensemble de ses données sur un support de stockage est un bon moyen de les protéger en cas de perte ou vol du dit support. Néanmoins, il n'est pas infaillible. Particulièrement sur les smartphones Android équipés de processeurs Qualcomm. C'est ce que démontre le chercheur en sécurité Gal Beniamini. Dans un document très détaillé, il indique comment contourner les systèmes de protection. Et plus particulièrement, *« comment l'exécution du code TrustZone du noyau peut être utilisé pour briser efficacement le schéma de l'Encryption Full Disk d'Android »*, précise le chercheur.

Le Full Disk Encryption (FDE), la technique de chiffrement du disque d'Android, est proposé par Google depuis la version 5.0 de l'OS mobile. Il permet de générer des clés de chiffrement maître et esclave de 128 bits. La clé maître, également appelée DEK (pour Device Encryption Key) est protégée par chiffrement à partir du mot de passe, du code PIN ou du schéma de déverrouillage choisi par l'utilisateur. La DEK est stockée sur le smartphone (ou la tablette) dans un espace non chiffré de l'appareil, le *crypto footer*. Et c'est là que le problème survient. A cause d'une faille dans les processeurs de Qualcomm.

Utiliser une Trustlet

Pour comprendre pourquoi, il faut savoir que Android dispose, comme iOS, de mécanismes de temporisation et de blocage de l'appareil pour interdire les attaques par force brute (essais successifs de saisie des identifiants). Ces mécanismes sont liés au module KeyMaster qui s'exécute dans un environnement séparé de l'OS et considéré comme sécurisé, le Trusted Execution Environment (TEE). Le KeyMaster peut ainsi générer des clés de chiffrement sans les révéler au système d'exploitation. Une fois générées, ces clés sont à leur tour chiffrées et communiquées à l'OS. Quand ce dernier les sollicite, un bloc de données (le Blob, Binary Large OBject, un type de données qui permet l'intégration d'un pilote, souvent propriétaire, dans le code du noyau Linux) est fourni au KeyMaster sous forme d'une clé RSA de 2048 bits.

Mais le KeyMaster dépend de l'implémentation qu'en fait le fabricant sur son matériel. En l'occurrence, Qualcomm exploite bien le KeyMaster dans la TrustZone. Sauf que le TEE fourni par le constructeur, le QSEE (Qualcomm Secure ExecutionEnvironment), autorise des appliquettes (Trustlets) a s'exécuter dans cette zone sécurisée. Et, selon le chercheur, il est possible d'exécuter sa propre Trustlet dans la TrustZone en exploitant potentiellement une vulnérabilité Android. A partir de là, l'attaquant peut obtenir des privilèges administrateur et accéder au Blob qui contient les clés générées. Il ne reste alors plus qu'à lancer une attaque par force brute pour retrouver le code secret de l'utilisateur et disposer ainsi de la clé de déchiffrement du support de stockage.

Une correction difficile

Certes, la manœuvre n'est pas à la portée du premier venu. Et nécessite de disposer du terminal en main. Mais le déchiffrement d'un disque peut visiblement être exécuté par le fabricant des puces. Lequel peut avoir à se plier à une requête judiciaire comme on l'a vu avec Apple dans l'affaire de l'attentat de San Bernardino. Qui plus est, selon Qualcomm, le « bug » n'est pas facile à corriger. La correction demandera probablement une modification de l'architecture des processeurs. Lesquels équipent aujourd'hui une majorité de smartphones Android de la planète.

Néanmoins, le chercheur reste optimiste. *« J'espère qu'en jetant la lumière sur le sujet, cette recherche va motiver les équipementiers et Google à se réunir pour penser à une solution plus robuste pour le FDE*, écrit-il. *[…] Je crois qu'un effort concentré des deux côtés peut aider à rendre la prochaine génération d'appareils Android vraiment « inviolable ». »*

Article original de Christophe Lagane

Original de l'article mis en page : Le chiffrement des smartphones Android n'est pas incassable

---

Les géants d'internet contrôlent de plus en plus l'information

Les géants d'internet contrôlent de plus en plus l'information

Entre les médias et les lecteurs, l'information passe aujourd'hui le plus souvent par les algorithmes des géants d'internet, qui contrôlent de fait ce flux et une bonne partie des revenus qu'il génère. Au point de susciter des inquiétudes.

« Ces 18 derniers mois, (ces géants d'internet) qui avaient jusqu'ici une relation distante avec le journalisme sont devenus des acteurs dominants de l'écosystème de l'information », résume le Tow Center for Digital Journalism de l'Université américaine de Columbia, dans une étude publiée en juin 2016. Beaucoup proposent aux éditeurs de presse de publier directement leur contenu sur leurs plateformes, à l'instar des canaux Instant Articles de Facebook ou Discover de Snapchat, et sont*« désormais directement impliqués dans tous les aspects du journalisme »*, fait valoir l'étude. La plupart des médias nouent des partenariats avec ces nouveaux acteurs de l'information pour maintenir ou développer leur exposition sur les moteurs de recherche et les réseaux sociaux, mais les perspectives financières restent incertaines.
« Il y a des gens qui font de l'argent sur internet, mais pas les médias, qu'ils soient tous supports ou uniquement en ligne », affirme une autre étude, du centre indépendant Pew Research Center, publiée mi-juin. Elle souligne ainsi qu'en 2015, 65% des revenus publicitaires en ligne étaient concentrés par cinq places fortes du web, Google, Facebook, Microsoft, Yahoo et Twitter, une proportion en hausse par rapport à 2014 (61%). Tout comme le modèle économique, c'est aussi le contenu et sa hiérarchie qui leur échappent, soumis au filtre des algorithmes. *« L'impact que ces sociétés technologiques ont sur le secteur du journalisme va bien au-delà de l'aspect financier, jusqu'à ses composantes les plus essentielles »*, considère l'institut Pew.
Désormais, les géants d'internet *« supplantent les choix et les objectifs des sites d'information et leurs substituent (les leurs) »*, affirme l'étude. Si certains y voient l'occasion d'une démocratisation de l'information, d'autres s'inquiètent d'une altération de sa qualité. *« Vous n'avez aucune idée de ce que les gens vont voir et il se peut tout à fait que (ce soit) quelque chose d'assez léger plutôt que des informations majeures »*, prévient Dan Kennedy, professeur de journalisme à l'Université Northeastern.

Le secret des algorithmes

Une étude réalisée par Nic Newman du Reuters Institute a fait état de*« préoccupations liées à la personnalisation des informations et une sélection algorithmique qui pourraient passer à côté de nouvelles importantes et de points de vue différents »*, selon le blog de son auteur. Mais *« les jeunes préfèrent les algorithmes aux éditeurs »* qui organisent l'information, constate-t-il. Ce pouvoir croissant des incontournables d'internet a attiré l'attention début mai lorsque le site d'information Gizmodo a accusé, témoignages à l'appui, Facebook d'avoir manipulé son fil de tendances. Après enquête interne, le plus grand réseau social du monde a conclu qu'il n'y avait pas eu de démarche concertée ou de manipulation, mais s'est engagé à préserver la neutralité de sa plateforme.
« Nous sommes une entreprise technologique, pas un média », a expliqué récemment la directrice d'exploitation de Facebook, Sheryl Sandberg, lors d'une table ronde à Washington. *« Nous n'essayons pas de recruter des journalistes ou de rédiger des nouvelles »*, a-t-elle martelé. Pour autant, l'intervention humaine reste nécessaire, selon elle, *« parce que sans cela, tous les jours à midi, le déjeuner serait une tendance »*. Même si la hiérarchisation des informations est largement automatisée sur ces plateformes, les programmes qui régissent ce processus sont bien rédigés par des humains qui opèrent, pour ce faire, des choix. Cela pose, dès lors,*« des questions quant à la transparence »* de l'ensemble, souligne Nicholas Diakopoulos, professeur de journalisme à l'université du Maryland. *« Il pourrait être intéressant de savoir de quelles données se nourrit le logiciel ou quels sites il suit »*, estime l'universitaire, pour qui *« il faut réfléchir à des normes de transparence ».*
Une étude publiée l'an dernier a révélé que le trafic des principaux sites d'information en provenance de Facebook avait chuté de 32% après une modification des algorithmes du réseau social. *« Il est vrai que Facebook peut faire décoller ou tuer un site d'information selon la façon dont il calibre son algorithme »*, reconnaît Nikki Usher, professeure de nouveaux médias à l'Université George Washington. *« D'un autre côté, les médias n'ont jamais eu à rendre de compte sur les décisions qu'ils prenaient »* en matière éditoriale, fait-elle valoir.

Article original de Joël Ignasse

Réagissez à cet article

Original de l'article mis en page : Les géants d'internet contrôlent de plus en plus l'information – Sciencesetavenir.fr