Est-ce que l’iPhone est vulnérable ? | Le Net Expert Informatique

Est-ce que l’iPhone est vulnérable ?

Est-ce que les iPhone sont vulnérables à l'espionnage, c'est la question que l'on peut se poser en sachant que la CIA cherche à le casser depuis sa création.

Selon la récente publication de The Intercept, on sait que la CIA a tenté de « casser », percé le chiffrement, des produits Apple depuis 2006. Cela signifie que l'agence américaine a bien évidemment aussi tenté de percer les sécurités de l'iPhone vu que la première édition est sortie en 2007. La grande question est de savoir si la CIA est arrivée à ses fins.
Sans revenir sur tous les détails de cette révélation faite sur la base des documents dévoilés par Edward Snowden, on peut comprendre de nombreuses choses à partir de cette nouvelle affaire d'espionnage des utilisateurs.
Pour commencer, il n'y avait pas que la NSA qui cherchait à collecter des données personnelles des utilisateurs de smartphones. Alors que les lois américaines empêchent normalement l'espionnage des citoyens américains, on peut sérieusement se poser la question si ces textes n'ont pas tout simplement été bafoués en essayant de casser le chiffrement des iPhone alors que les Américains sont friands de produits Apple.
Si découvrir des failles dans les systèmes Apple s'explique par le fait de vouloir obtenir des données des utilisateurs, on peut se poser la question de savoir pourquoi la CIA n'a pas averti Apple de l'existence de ces failles ? Il semble évident que cela aurait été un aveu de culpabilité. Par contre, un peu prendre cet aspect d'un autre point vu en considérant que ce que les agences américaines ont fait, d'autres agences de pays hostiles ont également pu le faire. De fait, ne pas communiquer ces failles serait une mise en danger des données personnelles des citoyens américains.
En sachant tout cela, on comprend parfaitement pourquoi les constructeurs, notamment Apple, ont renforcé la sécurité de leurs systèmes et refusent d'ouvrir des backdoors « légales » pour les autorités. En effet, comment pourrait-il exister une moindre confiance ?
En sachant tout cela, on ne comprend par contre pas la véhémence des agences américaines qui dénoncent les méthodes de cryptage mises en place par les entreprises. En effet, ces mesures ne visent que la protection des données des utilisateurs, notamment des biens appartenant à des Américains.
Au final, le débat sur la protection des données personnelles va encore faire couler beaucoup d'encre.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.linformatique.org/est-ce-que-liphone-est-vulnerable/

Les experts de la sécurité se penchent sur la Watch d'Apple | Le Net Expert Informatique

Les experts de la sécurité se penchent sur la Watch d'Apple

La firme de Cupertino a donc lancé officiellement sa montre connectée, la Watch, le 9 mars 2015 hier soir. Tout a été dit sur ce gadget déclinable en plusieurs versions dont une luxueuse au prix stratosphérique de 11 000 euros. Mais cette annonce a aiguisé la curiosité des experts en sécurité qui se sont penchés sur les faiblesses de la tocante numérique.

Nos confrères de The Register ont interrogé plusieurs spécialistes de la sécurité sur ce sujet. Ainsi, Ken Westin, chercheur chez Tripwire a indiqué que « le fait que le dispositif soit à la fois WiFi et Bluetooth va faciliter le développement des fonctionnalités supplémentaires à la montre et de s'interopérer avec d'autres équipements. Mais cela va également augmenter la surface d'attaque de l'appareil ». Pour lui, il ne fait aucun doute que « les chercheurs et les hackers ont été émoustillés pour trouver de nouvelles vulnérabilités et s'appuyer sur des attaques existantes qui profitent des faiblesses du WiFi et du Bluetooth ».

Problème de confidentialité des données
Un autre aspect de sécurité selon l'expert réside dans la confidentialité des données. « Avec ces connectivités, il sera intéressant de voir comment les données peuvent être utilisées pour suivre les personnes dans espaces physiques. Cela peut avoir un impact pour un cyberattaquant, tout comme pour des campagnes publicitaires trop ciblés ». L'arrivée d'applications tierces n'est pas faite pour rassurer le spécialiste qui y voit un risque supplémentaire pour la sécurité et la vie privée.

La fraude au paiement
En disposant d'une capacité NFC, l'Apple Watch peut servir pour le paiement mobile. Les risques de fraudes existent donc. Une récente étude de Drop Labs montre que le niveau de fraude sur les paiements avec Apple Pay est de 6% contre 1% en moyenne pour les transactions par carte bancaire. Pour la défense d'Apple, le problème vient surtout d'un niveau d'authentification faible de la part des banques. Une affaire récente a démontré ce risque. Certains spécialistes s'interrogent sur la fiabilité de la technologie NFC avec la capacité de la contourner.

Une révision des politiques de BYOD ?
Phil Barnett, directeur général EMEA de Good Technology, préfère souligner les menaces que les montres connectées et plus généralement les « wearables technology » impliquent dans le monde du travail. Elles s'inscrivent dans les politiques de BYOD (Bring Your Own Device) qui selon lui doivent être révisées. « Le BYOD a déjà connu les smartphones et des tablettes, les accessoires connectés arrivent comme les prochains véhicules de la donnée. Ils représentent une immense opportunité pour la productivité, mais ils nécessitent avant leur arrivée en entreprise de les sécuriser. »
Cela passe pour lui par plusieurs axes : « Chiffrement des données transitant sur le Bluetooth et la conteneurisation des données de l'entreprise. Par ailleurs, un contrôle plus granulaire des politiques de sécurité devrait permettre de trouver un équilibre entre risques et productivité. » A condition qu'il n'y ait pas de défaut dans la cuirasse, comme le montre la faille Freak qui affaiblissait le chiffrement des navigateurs Apple et Android. La firme de Cupertino vient d'ailleurs de publier iOS 8.2 qui règle ce problème.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.silicon.fr/les-experts-de-la-securite-se-penchent-sur-la-watch-dapple-110567.html

Réglementation des drones et droit des robots | Le Net Expert Informatique

source : http://live.orange.com/drones-parrot-amazon-zephyr/

Réglementation des drones et #droit des robots

Le survol des drones au dessus des centrales nucléaires [1] ainsi que d'autres sites sensibles et parisiens [2] représente une menace face à laquelle les réponses, notamment réglementaires, semblent encore insuffisantes.

En effet, la détection par radar militaire mais également l'interception de ces engins volants se révèlent difficiles de par la furtivité des drones et l'incapacité actuelle des autorités à les tracer et à les écarter.

Au niveau réglementaire, l'utilisation des drones ou plus exactement d' « aéronefs qui circulent sans monde à bord » civils, à distinguer des drones militaires, est encadrée par deux arrêtés d'avril 2012 [3], un arrêté relatif aux conditions de navigabilité et de télépilotage et un autre relatif aux exigences liées à l'espace aérien.

Le principe est le suivant :
sauf autorisation particulière, les drones doivent survoler un espace bien précis délimité en volume et en temps, en dehors de toute zone peuplée. De plus, en fonction de deux catégories de critères (finalité d'utilisation et poids du drone), des règles particulières s'appliquent. Ainsi, les drones civils professionnels utilisés par exemple par les agriculteurs ou les photographes doivent notamment se faire connaître auprès des autorités.
Concernant l'utilisation de drone de loisirs qui est en vente libre, il faut également respecter des règles spécifiques qui sont rappelées dans une notice rédigée par la Direction Générale de l'Aviation Civile (DGAC) en décembre 2014 [4] et qui interdisent notamment le vol de nuit, le survol des sites sensibles ainsi que de l'espace public en agglomération.
Au final, la violation des conditions d'utilisation des drones est passible d'un an d'emprisonnement et de 75000 euros d'amende en vertu de l'article L.6232-4 du code des transports.
Autre point d'importance à souligner, même si la prise de vue aérienne est réglementée par l'article D. 133-10 du code de l'aviation civile, il n'en demeure pas moins que la captation et l'enregistrement d'images relatives aux personnes relèvent également de la loi « Informatique et Libertés »[5].
En effet, il est important de souligner également le risque de collecte de données à caractère personnel par les drones. Un facile parallèle peut être établi entre le survol des drones et le passage dans nos rues des « Google cars ». La CNIL avait constaté lors de contrôles effectués fin 2009 et début 2010 que la société Google, via le déploiement de véhicules enregistrant des vues panoramiques des lieux parcourus, récoltait, en plus de photographies, des données transitant par les réseaux sans fil Wi-Fi de particuliers, et ce à l'insu des personnes concernées. Cette collecte déloyale de très nombreux points d'accès Wi-Fi constitue un réel manquement à la loi « Informatique et Libertés ».
Concernant les drones, il faudra donc s'attacher à vérifier qu'ils ne récupèrent pas également des données à caractère personnelle de façon illégale. En effet, les drones sont des machines qui peuvent embarquer une quantité importante de capteurs divers et variés tels un appareil photo, une caméra ou un dispositif de géolocalisation permettant de collecter et diffuser des données à caractère personnel avec pour conséquence l'atteinte manifeste à la vie privée des individus.
Consciente de ces enjeux depuis 2012, la CNIL, en liaison avec le Groupe des 29 CNIL européennes (G29) réfléchit activement à l'amélioration de la réglementation à ce sujet.

Au final, la réglementation relative aux drones qui, d'une part, a le mérite d'exister et, d'autre part, est relativement souple et adaptable en prévoyant plusieurs scénarii spécifiques, apparaît même novatrice au niveau international. Les Etats Unis par l'intermédiaire de la Federal Aviation Association (FAA) n'ont dévoilé que le 15 février 2015 et pour la première fois des recommandations pour encadrer l'utilisation des drones civils commerciaux sur le sol américain [6].
Toutefois, la DGAC a prévu quand même de réviser prochainement la réglementation des drones afin de mieux prendre en compte la massification de l'utilisation de drones civils. Cette révision devra si possible prendre en compte une future réglementation européenne à ce sujet.

Plus largement, ce focus juridique sur les drones peut élargir son horizon en s'intéressant à la problématique du droit des robots qui, au regard de la vitesse de création des inventions technologiques, constitue indéniablement un des enjeux majeurs juridiques mais également éthiques des années à venir.
Certes pour les objets connectés, les enjeux juridiques ont déjà été identifiés mais il semble qu'il faille pousser le cadre juridique plus loin pour les futures générations de robot doté d'une certaine forme d'intelligence artificielle.
La vente du robot, comme tout bien, entraine pour le vendeur une obligation de garantie et engage sa responsabilité délictuelle du fait d'un défaut de sécurité de l'un de ses produits ou services entraînant un dommage à une personne. Cependant, il est probable que l'autonomie des robots grandissante, il faille réfléchir à la responsabilité propre du robot. De prime abord, la responsabilité juridique repose sur la notion de discernement, actuellement les machines restent sous la responsabilité de son gardien soit de l'usager ou encore de son fabricant par le biais de la responsabilité des produits défectueux.
Il est possible que, dans un futur plus ou moins proche, le législateur décide de mettre en place une personnalité juridique spécifique du robot. Cette dernière, se distinguant du régime juridique lié aux animaux et des biens, devra être encadrée afin de prévoir la sécurité des utilisateurs mais également la sécurité du robot lui-même. Pour commencer, il pourrait même s'agir de la reprise des trois règles de la robotique édictée par Isaac Asimov [7]!

[1] Dix-sept centrales nucléaires sur les dix-neuf que compte le parc français ont été survolées par des drones depuis début octobre. Six l'ont été simultanément dans la nuit du 31 octobre.
[2] http://www.liberation.fr/societe/2015/02/24/paris-survole-par-des-ovnis_1209273
[3]Les arrêtés du 11 avril 2012 relatifs d'une part à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord et d'autre part à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent constituent le socle réglementaire d'utilisation des drones civils.
[4] Règles d'usage d'un drone de loisir : http://www.developpement-durable.gouv.fr/IMG/pdf/Drone-_Notice_securite-2.pdf
[5] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.
[6] « Drones civils – les Etats-Unis avancent sur leur législation : les différences avec le modèle français » par Emmanuel de Maistre, président de Redbird : http://www.infodsi.com/articles/154099/drones-civils-etats-unis-avancent-legislation-differences-modele-francais-emmanuel-maistre-president-redbird.html?key=a0a42d0bc78aa63d
[7] http://nte.mines-albi.fr/SystemiqueSudoku/co/v_regle_vie_Azimov.html

---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://securitedessystemesjuridiques.blogspot.fr/2015/03/reglementation-des-drones-et-droit-des.html

---

La NSA et sa consœur

britannique surveillent aussi les cartes SIM

Crédit : Fotolia

La NSA et sa consœur britannique surveillent aussi les cartes SIM

Aucun vecteur informatique ne semble échapper aux radars de l'agence de sécurité américaine. Cette fois, la NSA (et la GCHQ) s'est offert un accès aux clients de 450 opérateurs, via les cartes SIM.

Une nouvelle révélation sur la NSA démontre, si ce n'était pas déjà suffisant, l'étendue de la portée de l'agence de sécurité américaine. Selon le site The Intercept, l'organisation accompagnée par son homologue britannique, le GCHQ, ont toutes deux pénétré dans les réseaux informatiques du premier fabricant de cartes SIM dans le monde, le franco-néerlandais Gemalto, qui produit plus de deux milliards de cartes par an.

A ce stade, la société ciblée ne peut pas « confirmer ces informations » et souligne qu'elle n'avait « aucune connaissance préalable que ces agences gouvernementales conduisaient cette opération », rejetant donc une quelconque complicité. Gemalto indique prendre cet article « très au sérieux » et met en œuvre « tous les moyens nécessaires pour investiguer et comprendre l'étendue de ces techniques sophistiquées ».
Selon The Intercept, qui se base sur des documents fournis par le lanceur d'alertes Edward Snowden, la NSA et le GCHQ ont mis la main sur des clés de chiffrement après avoir installé un malware sur des ordinateurs de Gemalto. Pour cela, l'agence américaine aurait fait appel à son programme de surveillance XKeyscore, qui lui donne accès aux e-mails, conversations Facebook et historiques Internet, lui aussi mis au jour, en août 2013.
Ces clés, utilisées pour protéger la confidentialité des communications téléphoniques, permettent aux deux organisations d'intercepter les échanges vocaux, les SMS et les données Internet des clients mobiles.

Les clients de 450 opérateurs écoutés
En visant Gemalto, les deux consœurs ont pu toucher les clients de 450 opérateurs de téléphonie mobile dans 85 pays. « En possédant ces clés de chiffrement, les agences de renseignement peuvent surveiller les communications mobiles sans demander l'autorisation des opérateurs télécoms ni des gouvernements étrangers », écrit l'auteur de ces révélations. Il ajoute que « c'est aussi un moyen de se passer de mandat, tout en ne laissant aucune trace sur le réseau qui révéleraient que des personnes ont été mises sur écoute ».
La révélation de ce nouvel avatar de la surveillance américaine intervient alors que que le ministre de l'Intérieur, Bernard Cazeneuve, est en déplacement aux États-Unis, où il tente de mobiliser les grands acteurs comme Google et Facebook dans la lutte anti-terroriste sur Internet. S'il leur est demandé une collaboration plus étroite avec le gouvernement sur les enquêtes en cours, et une meilleure réactivité sur la suppression du contenu appelant au terrorisme, rien ne semble empêcher le travail en tâche de fond de la tentaculaire NSA.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://pro.clubic.com/it-business/securite-et-donnees/actualite-755133-sim-gemalto.html
Par Thomas Pontiroli

Gemalto a bien été attaqué, mais ses réseaux sécurisés seraient restés étanches

Gemalto a bien été attaqué, mais ses réseaux sécurisés seraient restés étanches

Oui des attaques ont bien été détectées, mais Gemalto précise que ses réseaux sécurisés n'ont pas été pénétrés. Le vol massif de clés de SIM ? Impossible en 2010 du fait du chiffrement des échanges avec les opérateurs. Et d'autres facteurs permettent de pondérer les conséquences de ces attaques.

Un peu moins d'une semaine après la publication par The Intercept de documents décrivant des attaques contre des fournisseurs de cartes SIM, Gemalto, un des acteurs ciblés, a présenté les conclusions de ses investigations.
Et cette analyse semble effectivement confirmer le scénario d'une opération conjointe de deux agences de renseignement étrangères, la NSA et le GCHQ.

Des attaques « graves et sophistiquées », mais sur des réseaux périphériques
« Nous avons analysé la méthode décrite dans les documents et les tentatives d'intrusion sophistiquées que nous avions détectées sur notre réseau en 2010 et 2011 rendent l'information qui est décrite probable » déclare Olivier Piou, le directeur général de Gemalto.
Pour étayer cette conclusion, l'entreprise s'appuie sur la détection de « deux attaques particulièrement sophistiquées qui pourraient effectivement être liées à cette opération ». Le directeur de la sécurité de Gemalto, Patrick Lacruche, décrit ces deux attaques précises en 2010.
La première a été identifiée en juin de cette année. « Nous avons identifié une activité suspecte sur un de nos sites français. Un tiers a essayé de se connecter à un de nos réseaux que nous appelons Office, c'est-à-dire le réseau de communication des employés entre eux et avec le monde extérieur. »
Toujours en 2010, un second incident est détecté par l'équipe de sécurité : « Il s'agissait de faux emails envoyés à un de nos clients opérateurs mobiles en usurpant des adresses email authentiques de Gemalto. Ces faux emails contenaient un fichier attaché qui permettait le téléchargement d'un code malveillant. » Le client sera alerté et l'attaque signalée aux autorités.
Suivront sur la « même période » plusieurs « tentatives d'accès aux ordinateurs » de salariés de l'entreprise, ciblés en raison vraisemblablement de leurs « contacts réguliers » avec les clients de Gemalto.

Des vols de clés ? Possibles dans des « cas exceptionnels »
Si les attaques, qualifiées de « graves et sophistiquées », semblent avérées, le fournisseur de cartes SIM exclut en revanche qu'elles aient pu aboutir à la compromission de ses produits de sécurité ou à l'interception massive de clés de chiffrement.
Patrick Lacruche l'assure, ces attaques n'ont affecté « que des parties externes des réseaux Gemalto ». Or les « clés de cryptage et plus généralement les données clients ne sont pas stockées sur ces réseaux ».
Car, poursuit-il, « nous n'avons rien détecté d'autre, que ce soit dans les parties internes du réseau de notre activité SIM » ou « dans les parties du réseau sécurisé d'autres produits comme les cartes bancaires ». Ces « réseaux sont isolés entre eux et ne sont pas connectés au monde extérieur » indique encore le responsable sécurité.
L'entreprise reconnaît cependant que des interceptions de clés ont pu, dans des « cas exceptionnels », éventuellement être réalisées. Pour le justifier, Gemalto fait savoir qu'il avait « dès avant 2010 », mis en place un système d'échange sécurisé avec ses clients. Ce chiffrement empêcherait donc que les clés, en cas d'interception, puissent être exploitées ensuite pour des écoutes.

Au pire, seuls les réseaux 2G seraient affectés par des écoutes
Serge Barbe, le vice-président de Gemalto en charge des produits et services, a apporté d'autres informations permettant selon lui de relativiser les conséquences de ces attaques et les risques d'espionnage pour les clients des opérateurs.

Ainsi, si des clés de chiffrement de SIM avaient effectivement été dérobées, celles-ci ne permettraient de procéder à des écoutes que sur des communications 2G. Or, la faiblesse de cette technologie, « pensée dans les années 80 », était déjà connue.

« Donc si les clés de cryptage de cartes SIM 2G étaient interceptées par des agences de renseignement, il leur était techniquement possible d'espionner les communications » reconnaît Serge Barbe, qui précise toutefois que ces cartes étaient pour la plupart des cartes prépayées, c'est-à-dire dont le cycle de vie était réduit.

Mais qu'en est-il alors des SIM des générations suivantes ? Le vol auprès du fournisseur ou de l'opérateur des clés permet-il des opérations d'espionnage des communications ? Non selon Gemalto pour qui la faiblesse des carte 2G a été « éliminée » par la suite.

La sécurité a « encore été largement renforcée, je dirais même repensée, avec l'arrivée des cartes SIM de troisième et quatrième générations » revendique Serge Barbe. « L'interception et le décryptage en cours d'échange entre le fournisseur et l'opérateur ne permettrait pas aux pirates de se connecter aux réseaux 3G ou 4G et donc par conséquent d'espionner les communications ».

« Les cartes 3G et 4G ne pouvaient pas être affectées par l'attaque qui est décrite » dans les documents attribués aux GCHQ. Malgré tout, « ces produits plus récents ne sont toutefois pas utilisés universellement dans le monde » tient à préciser le représentant de Gemalto.

Pour le patron de Gemalto, Olivier Piou, une conclusion s'impose dans cette affaire d'espionnage : « l'encryptage systématique des échanges et l'utilisation de cartes de dernière génération, couplés à des algorithmes personnalisés pour chaque opérateur, sont la meilleure réponse à ce genre d'attaque. » Bref, une bonne opportunité finalement pour l'entreprise de faire la promotion de ses produits et pratiques de sécurité.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/gemalto-a-bien-ete-attaque-mais-ses-reseaux-securises-seraient-restes-etanches-39815336.htm
Par Christophe Auffray

Inquiétudes : Chez Samsung, c’est la télé qui vous regarde

	Inquiétudes : Chez Samsung, c’est la télé qui vous regarde

Attention à ce que vous dites lorsque vous êtes confortablement assis devant votre téléviseur, puisque cela pourrait se retourner contre vous. Si Big Brother vous regardait, la SmartTV de Samsung, elle, vous écoute.

Grâce à sa commande par reconnaissance de la parole, la SmartTV, ce nouveau téléviseur connecté à internet de Samsung peut effectivement enregistrer ce que vous dites et le transmettre à une tierce partie, rapporte The Daily Beast.
Seule une petite mise en garde, noyée quelque part dans la version anglaise de la politique de confidentialité de la SmartTV, informe d'ailleurs les consommateurs quant à cette fonctionnalité permettant au téléviseur d'enregistrer vos conversations.
« **Veuillez prendre note que si vos paroles contiennent des informations personnelles ou sensibles, ces paroles peuvent faire partie des données enregistrées et transmises à une tierce partie.** » La version française de la politique de confidentialité n'en fait d'ailleurs pas mention, souligne Fabien Deglise, dans Le Devoir.
Ainsi, l'appareil de Samsung ne collecte pas seulement les mots que lui dictent les téléspectateurs, mais aussi des bribes des conversations que tiennent les personnes qui sont assises devant l'écran.
Si vous êtes trop paresseux pour utiliser votre télécommande, vous feriez peut-être mieux de vous limiter dans vos sujets de conversation. Comme le remarque The Daily Beast, entre deux épisodes de votre série préférée, ne discutez surtout pas d'évasion fiscale ou de consommation de drogue, parce que cela pourrait se retourner contre vous.
En s'immisçant de la sorte dans les conversations des téléspectateurs, **Samsung pourrait compromettre la vie privée de ses consommateurs**, affirme d'ailleurs le Daily Beast. Les consommateurs devraient pouvoir savoir à qui – et sous quelle forme – leurs informations sont transmises. Si les données transmises ne sont pas codées, les téléviseurs pourraient effectivement se transformer en de véritables postes d'écoute.
En réponse aux inquiétudes soulevées par certains consommateurs, Samsung a dit prendre la vie privée de ses consommateurs très au sérieux. Le géant de l'électronique sud-coréen se veut également rassurant et affirme avoir recours à des techniques d'encodage des données afin d'assurer la confidentialité des informations émises par ses consommateurs.
Samsung insiste aussi sur le fait que la fonctionnalité de commande par reconnaissance de la parole peut être désactivée en tout temps. De plus, la commande vocale ne fonctionne pas si la télévision n'est pas connectée à internet.
Par ailleurs, comme le rappelle Business Insider, le système Siri, qui transmet aussi de l'information à une tierce partie, a déjà fait l'objet de telles inquiétudes.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.egaliteetreconciliation.fr/Chez-Samsung-c-est-la-tele-qui-vous-regarde-31023.html

Bill Gates met en garde au sujet des futurs progrès de l’intelligence artificielle

	Bill Gates met en garde au sujet des futurs progrès de l’intelligence artificielle

Après le chercheur Stephen Hawking et l'entrepreneur Elon Musk, c'est au tour de Bill Gates de demander à ce que chacun réfléchisse aux progrès de l'intelligence artificielle. Le fondateur de Microsoft confie son inquiétude sur le sujet.

« Science sans conscience n'est que ruine de l'âme ». La formule de Rabelais trouve une nouvelle résonance aux yeux de certains chercheurs, entrepreneurs et personnalités reconnues du monde des Sciences. Plusieurs d'entre eux n'hésitent désormais pas à témoigner de leurs inquiétudes au sujet de l'évolution de l'intelligence artificielle.
Bill Gates s'interroge à ce sujet et considère que l'utilisation de ce type de technologie doit provoquer des réflexions en chacun de nous. L'ancien dirigeant de Microsoft rejoint des questionnements déjà entamés par Stephen Hawking ou même par le fondateur de PayPal, SpaceX et Tesla, Elon Musk.

« Je ne comprends pas pourquoi certaines personnes ne s'en préoccupent pas »
Interrogé dans le cadre d'une session de questions/réponses organisée sur le site Reddit, Bill Gates explique : « Je suis dans le camp de ceux qui se préoccupent de l'évolution des super intelligences. Tout d'abord, les machines exécuteront de nombreuses tâches à notre place et n'auront pas besoin d'être réellement dotées d'une intelligence redoutable. Ce doit donc être un mouvement positif si nous les gérons correctement. Mais plusieurs décennies après, cette même intelligence sera suffisamment puissante pour qu'elle représente un problème. Je suis donc totalement en accord avec les propos d'Elon Musk et d'autres à ce sujet, et je ne comprends d'ailleurs pas pourquoi certaines personnes ne s'en préoccupent pas ».
L'ancien dirigeant de Microsoft souhaite donc que les progrès futurs de l'intelligence artificielle puissent être observés et éventuellement interrogés. Il considère cependant la technologie comme un élément important de nos sociétés.
Au cours de la même session ouverte de questions/réponses, Bill Gates précise : « la technologie ne rend pas les gens moins intelligents. […] Elle leur permet de mieux répondre à certaines de leurs questions afin qu'ils demeurent encore plus curieux. De nos jours, il est plus facile d'en savoir plus sur de nombreux sujets importants, ce qui nous permet de résoudre des problèmes complexes ».

Des inquiétudes déjà formulées par Stephen Hawking ou Elon Musk
Dans une tribune co-signée avec trois autres scientifiques, le physicien Stephen Hawking a formulé cette année des inquiétudes similaires au sujet du développement des intelligences artificielles. Leurs propos, repris dans la presse britannique, évoquaient les réalisations actuelles comme des éléments qui « feront sans doute pâle figure par rapport à ce que les prochaines décennies apporteront ».

Elon Musk

« On peut imaginer que cette technologie soit capable de déjouer les marchés financiers, de dépasser les scientifiques humains, de manipuler les dirigeants et développer des armes qu'on ne puisse pas comprendre. L'incidence à court terme de l'intelligence artificielle dépend de celui qui la contrôle, mais, à long terme, cela dépend de la possibilité concrète de la contrôler », ajoutaient les chercheurs.

Plus récemment, Elon Musk, a également livré ses inquiétudes à ce sujet. Le dirigeant de Tesla et SpaceX expliquait qu'avec l'intelligence artificielle, « nous invoquons un démon. Dans toutes les histoires mettant en scène un type avec un pentagramme et de l'eau bénite, il est sûr et certain qu'il va pouvoir contrôler le démon. Sauf qu'il n'y arrive pas. » Là encore, l'entrepreneur en appelait à la prudence.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.clubic.com/mag/culture/actualite-752143-bill-gates-intelligence-artificielle.html

2020 : 1% des objets connectés seront des…voitures

2020 : 1% des objets connectés seront des…voitures

Les équipements sans fil s'immiscent dans les véhicules. En 2020, 250 millions de voitures seront connectées au réseau avertit le Gartner. Un véritable écosystème est en train de se créer sur ce mouvement.

En 2020, 250 millions de voitures connectées parcourront les routes du monde avertit le Gartner. Dans les 5 années qui viennent, les nouveaux véhicules équipés de capacités de conduite automatique vont devenir un segment majeur de l'Internet des objets, assure le cabinet d'étude.
Cette année, le Gartner prévoit unparc de 4,9 milliards d'objets connectés, en croissance de 30% par rapport à 2014. En 2020, il devrait y avoir 25 milliards d'objets connectés. Les voitures connectées devraient donc représenter 1% des objets connectés dans 5 ans.

Un levier de croissance économique
« La voiture connectée est déjà une réalité, et la connectivité sans fil dans les véhicules est en expansion rapide, des modèles de luxe et des marques haut de gamme, au modèles de milieu de gamme » explique James F. Hines, du Gartner. L'Idate confirmait déjà cette tendance en juin dernier.
Par ailleurs, la prolifération de la connectivité automobile doit avoir des implications majeures sur des secteurs tels que la télématique, la conduite automatique, ou encore la mobilité, assure le Gartner.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/2020-1-des-objets-connectes-seront-desvoitures-39813698.htm

Le NFC est-il vraiment utile pour le paiement ?

Le NFC est-il vraiment utile pour le paiement ?

Un sondage rapporte que les Français ne considèrent pas le NFC comme utile pour réaliser des paiements. Les banques se sont pourtant massivement dirigées vers cette technologie, notamment avec leurs cartes de paiement.

Régler un achat en passant simplement sa carte sur une borne ne semble pas intéresser outre mesure les Français. En dehors des défauts et qualités inhérents au NFC, un sondage réalisé par Odoxa pour le compte du Syntec Numérique, montre que l'utilité de cette technologie reste encore à démontrer.
Selon l'étude réalisée en janvier dernier auprès d'un échantillon de 1 008 personnes représentatif de la population, pas moins de 57% des sondés « trouvent le paiement sans contact inutile. Ce désintérêt pour le sujet semble toucher toutes les catégories de population interrogée ».
L'institut nuance ce résultat par le fait que certaines personnes interrogées vivent en milieu rural et ne disposent pas de moyens d'utiliser le NFC au quotidien. Malgré ce point, le désintérêt envers ce type de technologie, en particulier pour le paiement, est clairement affirmé.
Cette étude (.pdf) vient s'ajouter à d'autres sondages montrant des résultats identiques. En février dernier, une analyse réalisée par Statista expliquait que seulement 22% des Français étaient à l'aise avec le paiement sans contact. Ces derniers précisaient qu'ils préféreraient de loin l'usage traditionnel de la carte de paiement (insertion dans la fente d'un terminal puis code à taper).

Le paiement NFC n'a pas décollé en France
La carte à puce semble donc avoir encore de beaux jours devant elle. C'est pourquoi les banques se sont massivement dirigées vers le NFC en proposant à leurs clients des cartes compatibles avec la technologie. Le succès n'est, malgré tout, pas au rendez-vous puisque les transactions réalisées par ce biais ne représentent qu'une infime partie du volume global.
Le sondage réalisé pour le Syntec Numérique confirme ce mouvement. Il indique que 44% des personnes interrogées ont connaissance de la fonction paiement sans contact de leur carte bancaire, mais seulement 15% l'ont déjà utilisée. Pire, 29% des sondés affirment ne pas se servir de cette option tout en sachant que leur carte est compatible NFC.
Pour tenter d'inverser la tendance, les professionnels entendent communiquer davantage sur l'intérêt de la technologie. Dans ce cas, ils devront également informer des risques que peut représenter le NFC en termes de sécurité.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://pro.clubic.com/e-commerce/paiement-en-ligne/actualite-751153-nfc.html
Etude : http://www.syntec-numerique.fr/sites/default/files/cp_sondage_odoxa_paiement_sans_contact_22janv2015.pdf

Obsolescence programmée – Dénoncez et ne soyez plus complice

Obsolescence programmée – Dénoncez et ne soyez plus complice

L'obsolescence programmée regroupe l'ensemble des techniques visant à réduire la durée de vie ou d'utilisation d'un produit afin d'en augmenter le taux de remplacement.La demande ainsi induite profitera au producteur, ou à ses concurrents, ce qui explique certains cas de cartels. Le secteur bénéficie alors d'une production plus importante, stimulant les gains de productivité et le progrès technique, qui accélère l'obsolescence des produits antérieurs.Cette stratégie n'est pas sans risques car elle implique un effort de recherche et développement, n'allant pas toujours dans le sens d'une amélioration du produit.

Il y a également un impact écologique direct. L'obsolescence programmée visant la surconsommation, elle est la cause d'un surplus de déchets, indépendamment de l'état de fonctionnement effectif des produits techniques mis au rebut ou de l'état d'usure des objets d'usage. Les circuits de recyclage ou de conditionnement des matières plastiques et des métaux, en particulier, ne prennent pas en charge le stockage des déchets informatiques, malgré l'abondance de matières premières de valeur qu'ils peuvent contenir comme le fer, l'aluminium, les métaux rares, etc.

L'exportation en masse de déchets des pays de grande consommation vers des zones géographiques où le stockage est négociable à moindre coût est d'autant plus problématique et expose classiquement les pays receveurs à des pollutions spécifiques sur les sites de décharge de grande envergure.

L'enquête de Cash Investigation dévoile la face cachée de l'obsolescence programmée, ou comment les fabricants d'électroménagers, de téléphones portables ou d'ordinateurs font souvent tout pour limiter la durée de vie de leurs produits. Pourquoi ? Pour que les consommateurs en rachètent toujours plus, et toujours plus rapidement.

Cash Investigation a notamment enquêté sur le géant Apple et d'autres grandes marques. Vous découvrirez que les techniques de l'obsolescence programmée sont variées et sophistiquées. Les conséquences sont claires, une surconsommation généralisée et au bout de la chaîne, de gros dégâts environnementaux pour la planète.

Cash Investigation – La mort programmée de nos appareils
Emission diffusée sur France 2 le 22 Octobre 2012
présentée par Elise LUCET

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.inexplique-endebat.com/article-cash-investigation-la-mort-programmee-de-nos-appareils-le-lobby-du-sel-106398577.html