Vous avez eu un drone en cadeau à Noël, voici vos nouveaux droits, devoirs et obligations

Vous avez eu un drone en cadeau à Noël, voici vos nouveaux droits, devoirs et obligations

Le 23 décembre, la DGAC (Direction Générale de l'Aviation Civile) a mis en ligne les évolutions réglementaires en matière de drones, aéromodèles, etc. Elles se veulent plus lisibles et mieux adaptées aux besoins.

Si le Père Noël vous apporte un drone, voici quelque chose qui devrait vous intéresser : ce que vous avez le droit de faire ou non avec, les règles à respecter, etc.

Tout d'abord, sachez que deux textes datant du 17 décembre 2015 définissent désormais la réglementation pour l'usage de drones. Il s'agit d'un arrêté relatif à la conception, aux conditions d'utilisation et aux qualifications des télépilotes et d'un autre arrêté relatif aux conditions d'insertion dans l'espace aérien.
Comme le rappelle la DGAC, les deux textes font la distinction entre les différents pilotes : professionnels ou non. Par exemple, « lorsque cette utilisation est limitée au loisir et à la compétition, on parle d'aéromodèles ». Ce sont les drones achetés dans les grandes surfaces ou des boutiques high-tech. D'autre part, on évoque les drones réservés à une utilisation professionnelle.

Règles basiques
Si l'espace aérien est libre en-dessous de 150 mètres, il faut toutefois respecter certaines consignes basiques :
• Voler en dehors des agglomérations et des rassemblements de personnes ou d'animaux ;
• Voler en dehors des zones proches des aérodromes ;
• Et voler en dehors d'espaces aériens spécifiquement réglementés qui figurent sur les cartes aéronautiques.
• Il est également interdit de survoler des villes ou des rassemblements de personnes sans autorisation préfectorale.
• Dans tous les cas, le « télépilote d'un drone est responsable des dommages causés par l'évolution de l'aéronef ou les objets qui s'en détachent aux personnes et aux biens de la surface (article L.61613-2 du code des transports) ».

Protection de la vie privée
Le texte compte tout un tas d'autres interdits. Notamment, les personnes sourdes ne peuvent pas piloter d'aéromodèles puisqu'un pilote doit toujours être en mesure de détecter visuellement et auditivement les autres drones. Il est aussi interdit de voler la nuit, ou de piloter un drone depuis une voiture.

La DGAC rappelle aussi que la « prise de vue aérienne est réglementée par l'article D133-10 du code de l'aviation civile », afin de veiller à la protection de la vie privée. Une amende de 45 000 euros et d'un an d'emprisonnement est prévue s'il y une volonté manifeste de porter atteinte à l'intimité de la vie privée d'autrui.

Réagissez à cet article

Source : *Un drone à Noël ? Voici vos nouveaux droits et devoirs*

Vtech vend une tablette éducative tout en sachant qu'elle est défectueuse

Vtech vend une tablette éducative tout en sachant qu'elle est défectueuse

Lorsque la fille de 6 ans de Jade a développé son cadeau, le soir du réveillon de Noël, la joie a rapidement cédé la place à la déception.

«Un jouet complètement inutile», «une arnaque». C'est en ces mots que cette mère décrit la tablette Innotab max de Vtech, qui se décrit comme le chef de file mondial en jeux éducatifs électroniques pour enfants.
Le fabricant a confirmé, un peu tard aux yeux de nombreux parents, qu'il s'agissait là d'une conséquence de l'importante cyberattaque dont il a fait l'objet il y a plus d'un mois.

Depuis Noël, la page Facebook de la compagnie a été prise d'assaut par des parents déçus et frustrés de ne pas avoir été mis au courant des problèmes avec la tablette d'apprentissage qu'ils ont payée 120$.
«Quelle déception!», écrit Mélyssa Guay. «Ils auraient dû faire preuve d'honnêteté depuis le début et retirer le produit ou s'assurer que les magasins publient un avertissement», renchérit Samantha Taylor.
«Comme ça coûte cher, c'était le seul cadeau pour ma fille et elle ne peut pas l'utiliser», soupire Jade, avec qui La Presse s'est entretenue. «Il y a des choses pires que ça dans la vie, mais c'est une arnaque de vendre un produit qu'on sait défectueux.»
À mi-novembre, la base de données contenue dans le «Learning Lodge» de VTech, ou «Explor@ Park» en français, a été piratée. Explor@ Park est une plateforme sur laquelle les clients téléchargent les jeux et les vidéos. Ce n'est que deux semaines plus tard, le 30 novembre, que l'entreprise établie à Hong Kong a confirmé le piratage de millions de comptes clients et de profils d'enfants.
Les noms, les dates d'anniversaire des enfants ou les mots de passe et adresses courriel des parents ont été piratés. Mais selon le site Motherboard, du groupe Vice, le pirate a aussi mis la main sur des photos des enfants et des messages. VTech n'a toujours pas confirmé ou démenti cette dernière assertion.

Pas de compte, pas de jeux

La plateforme Explor@ Park a donc depuis été suspendue, ce qui rend impossible l'utilisation de certaines applications pour les tablettes InnoTV, InnoTab MAX, InnoTab. De plus, les nouveaux clients ne peuvent créer de compte. Sans ce compte, le WiFi, les vidéos et les jeux ne sont pas accessibles, ont confirmé des parents à La Presse.
«Je savais qu'il y avait eu une brèche informatique, mais nulle part on ne m'a dit que le produit ne fonctionnerait pas», déplore Jade.
Rachelle Lowry, de Red Deer en Alberta, a acheté une tablette VTech sur le site Amazon le 27 novembre et s'est aperçue il y a deux semaines que rien ne fonctionnait.
«Je leur ai écrit à propos du problème deux semaines avant Noël et je n'ai pas reçu de réponse», a-t-elle expliqué à La Presse. Elle s'est résignée à acheter de nouveaux cadeaux à ses trois enfants pour éviter de les décevoir. «Le service à la clientèle n'a rien fait pour m'aider depuis un mois. Ce n'est qu'à Noël qu'ils ont répondu à mon message Facebook […] C'est très frustrant.»
Le 14 décembre, plus d'un mois après l'attaque informatique, VTech Canada avait écrit sur sa page Facebook un message en anglais pour s'excuser de cet «inconvénient». Le 24 décembre, le fabricant a réitéré ses excuses, ajoutant cette fois une version française.
«Nous nous excusons des inconvénients que cette cyber-attaque et la suspension temporaire à Explor@ Park ont pu vous causer», peut-on lire. Il offre maintenant une solution de rechange, soit le téléchargement d'une mise à jour de programme permettant «de débloquer certaines fonctionnalités encore bloquées sur votre tablette et de bénéficier de 3 JEUX que nous vous offrons pour nous excuser des désagréments rencontrés».
Trop peu trop tard, selon Jade, qui croit qu'un avertissement aurait dû se trouver en magasin. Au commerce Toys'R'Us où elle a acheté le jeu, une préposée lui a affirmé le 26 décembre qu'elle n'était pas au courant du problème. Dans les grandes surfaces où nous nous sommes rendues, la tablette ne se trouvait plus. «Ça s'est beaucoup vendu cette année», a indiqué une vendeuse.

Aucun avertissement

Sur les sites internet de différents détaillants, aucun avertissement n'apparaît. Un message se trouve bien sur le site de VTechkids, mais pas sur la page du produit.
La chaîne Toys'R'Us n'a pas rappelé La Presse hier, pas plus que VTech.
Sur son site internet, le fabricant affirme qu'il espère que certaines des fonctionnalités importantes de la plateforme seront utilisables vers la mi-janvier. Rachelle et Jade attendent toujours que la compagnie leur envoie la carte SD pour effectuer la première mise à jour.
«Mais sur Facebook, j'ai lu que certaines personnes se plaignaient que ça ne fonctionnait pas et je n'ai pas beaucoup d'espoir. Je n'ai plus trop confiance», soupire Jade.

Réagissez à cet article

Source : *Vtech vend une tablette éducative qu'il sait défectueuse | Annabelle Blais | Actualités*

Paralyser une voiture pour 90 euros | Data Security Breach

Paralyser une voiture pour 90 euros | Data Security Breach

la prise USB d'une Toyota Corolla, un chercheur en informatique, bloque la voiture à coup de DDoS.

Le monde du « sans connexion » envahi nos vies. La marche de l'IoT est lancée et rien ne l'arrêtera vue les enjeux économiques. L'important, que le client achète, on verra ensuite pour sa sécurité. **Du moins si le client est encore vivant.**

Inoue Hiroyuki, professeur en informatique à la Graduate School of Information Sciences de l'université d'Hiroshima a expliqué comment il avait « planté » une Toyota Corolla avec 90€.
Une clé USB trafiquée et un DDoS via le port USB de la voiture « Le pilote était incapable de bouger la voiture en appuyant sur l'accélérateur » explique-t-il dans le Japan Times. L'agrégé en informatique a indiqué avoir aussi été capable d'ouvrir et fermer les fenêtres de la voiture, afficher une lecture de compteur de vitesse incorrecte et geler l'accélérateur. Toyota a annonçait qu'il allait continuer « à faire des efforts » pour améliorer la sécurité de ses véhicules.

Il serait peut-être temps d'arrêter de nous prendre pour des idiots ?
En juillet 2015, une Jeep Cherokee, et un mois plus tard, une Corvette étaient elles aussi malmenées. Le piratage des voitures ne fait que débuter ! Pour le moment, il ne se déroule officiellement que dans des laboratoires.

Réagissez à cet article

Source : *Paralyser une voiture pour 90 euros | Data Security Breach*

Les objets connectés doivent-ils vraiment recueillir autant de données personnelles pour fonctionner correctement ?

	Les objets connectés doivent-ils vraiment recueillir autant de données personnelles pour fonctionner correctement ?

Télévision, pèse-personne, thermostat et autres hubs domotiques… les objets connectés tentent d'envahir nos maisons et de s'infiltrer au coeur même de leur réseau numérique.

Pourtant, malgré leur objectif de nous simplifier la vie, leur développement semble encore assez poussif ; en raison sans doute de leur manque criant de sécurité. C'est ce que révèle une étude menée par la division Sécurité de Hewlett Packard : rien de moins que 250 vulnérabilités ont été relevées par les experts d'HP Fortify au sein des 10 objets connectés les plus populaires.

Ces failles de sécurité seraient, selon Mike Amistead, le manager général d'HP Fortify, le symptome de la ruée des entreprises sur le créneau des objets connectés. Il estime en effet que les start-ups se lançant sur ce marché tenteraient de commercialiser leur produit le plus rapidement possible avant la concurrence… au mépris de la garantie d'un niveau de sécurité suffisant des réseaux et des données personnelles.

Vos données personnelles en clair sur la toile

Parmi les failles de sécurité relevées, HP a constaté que :

– 90 % des objets connectés étudiés solliciteraient une information personnelle sensible (ex : adresse email ou postale, nom, date de naissance, etc) ; une information ensuite véhiculée en clair sur la toile ;

– 70 % des objets connectés ne crypteraient pas les données échangées avec le réseau ;

– 80 % des objets connectés ne nécessiteraient pas de mot de passe complexe pour identifier les demandes de connexion tierces ;

– 60 % des objets connectés seraient vulnérables aux attaques dites de « cross-site scripting » (type de faille de sécurité permettant d'injecter du contenu dans une page, et provoquant ainsi des actions sur les navigateurs web visitant la page).

Réagissez à cet article

Source : http://www.archimag.com/vie-numerique/2014/07/30/objets-connectes-internet-failles-securite

Objets connectés : les Français sont séduits mais restent méfiants

Objets connectés : les Français sont séduits mais restent méfiants

---

L'internet des objets, terrain de jeu de nombreuses start-up et d'entreprises industrielles, entre doucement dans les habitudes de consommation des Français.

Réalisé par le Credoc pour le compte du Conseil général de l'économie (CGE) et de l'Autorité de régulation des communications électroniques et des postes (Arcep), le baromètre du numérique 2015 vient de paraître.
Cette enquête, destinée à faire le point sur la diffusion des technologies de l'information dans la société française, s'est notamment portée sur l'accueil réservé par les consommateurs aux objets connectés.
Il en ressort que 6 % des Français utilisent déjà des outils leur permettant de commander à distance des appareils électroniques présents à leur domicile. Un chiffre qui reste modeste et qui n'a augmenté que de deux points depuis la dernière étude réalisée en 2011.
Sans surprise, les jeunes adultes (8 %), les plus diplômés (8 %), les cadres supérieurs (13 %) et les habitants de la région parisienne (10 %) sont les plus friands de ces solutions domotiques. Quant à leur adoption prochaine, 33 % des Français déclarent l'envisager (contre 25 % en 2011). Les 12 à 17 ans (60 %), les hauts revenus (40 %) et les habitants de la région parisienne (40 %) sont sur ce point les plus catégoriques.

Un frein sur les objets connectés « santé »
La santé est un des principaux axes de développement de l'Internet des objets. Interrogés sur ces solutions, les Français les considèrent comme intéressantes lorsqu'elles sont destinées à recueillir des données permettant d'améliorer leur état de santé (28 %), à mieux gérer leur poids (24 %) ou bien leur sommeil (21 %).
En revanche, ils font preuve, à une écrasante majorité, d'une réelle défiance vis-à-vis des entreprises qui fabriquent et commercialisent ces objets connectés. 83 % estiment ainsi qu'elles feront un usage commercial des informations recueillies sur leur santé. Une opinion très ancrée chez les cadres supérieurs (92 %) et les plus diplômés (91 %). En outre, 78 % considèrent que ces entreprises sont incapables de garantir une parfaite protection de ces données personnelles et privées.

-

Réagissez à cet article
Source : http://business.lesechos.fr/entrepreneurs/web/7000261-objets-connectes-les-francais-sont-seduits-mais-restent-mefiants-205224.php

---

Objets connectés : une moyenne de 5 failles par objet

Objets connectés : une moyenne de 5 failles par objet

9271 vulnérabilités majeures découvertes dans le firmware de 185 « objets de l'internet », principalement des routeurs, modems DSL/câble, téléphone IP, caméras de surveillance sous IP etc.

C'est le résultat brut de l'étude signée Andrei Costin et Aurélien Francillon d'Eurecom avec le concours d'Apostolis Zarras de l'Université de Bochum.
Réduire l'étude de ces trois chercheurs en quelques chiffres ne rend pas justice au travail effectué. En fait, son aspect le plus intéressant porte surtout sur l'automatisation et le travail à grande échelle de cette chasse au bug, grâce à la mise en place d'un environnement d'émulation.
La machine virtuelle est adaptée aux principaux systèmes et matériel du commerce, et les firmware chargés puis épluchés de manière dynamique les uns après les autres. Une sorte de « VM de torture » reproduisant au mieux l'environnement d'exécution.
Autre point important, cette recherche s'est limitée (sic) aux simples interfaces Web d'administration et de paramétrage qui sont en général intégrées dans le moindre des objets IoT. Et qui, pourrait-on ajouter, constituent le ventre mou de ces systèmes embarqués depuis des lustres. En d'autres mots, il n'est pas question ici des failles matériel, des trous Wifi/bluetooth/DECT, bref, de ce qui sort du volet « httpd » de ce travail. Il y a fort à parier que si l'analyse avait pu s'étendre à ces aspects, le nombre de défauts recensés aurait été probablement doublé.
Mais ce genre de tests est nettement moins susceptible de pouvoir être automatisé. Les armes de chasse sont classiques : Arachni, Zed Attack Proxy, w3af, ce qui n'interdit pas à tout chercheur souhaitant continuer ce travail d'y ajouter Metasploit ou Nessus.
L'environnement lui-même, Qemu, a été retenu en raison du nombre important de processeurs supportés : Arm, Mips, Mipsel, Axis Cris, bFLT, PowerPC, X86 et même Nios II d'Altera.
Certains cœurs échappent à ce crible, tels les processeurs spécifiques de Dlink ou un Risc 32 bits peu répandu, le Arctangent A5.
Plus de la moitié des objets utilisant un ARM ont été vulnérables à un Chroot et une attaque Web, entre 17 et 21 % pour les systèmes à base de MIPS, et un peu moins de 30 % pour les IoT avec moteur Mipsel.
Les vulnérabilités les plus fréquemment rencontrées sont : XSS (5000 sur les 9271 recensées), manipulation de fichiers (1129), exécution de commandes arbitraires (938), ajout de fichiers (513), divulgation de fichiers (461), injection SQL (442)…

La confiance dans l'IoT, ça se mérite. Toutefois, précisent les trois chercheurs, il est des domaines où la sécurité est prise nettement plus au sérieux.
C'est notamment le cas de boîtier de télévision payante, par câble ou satellite. Probablement en raison des conséquences de pertes économiques directes qu'un défaut de sécurité provoquerait immédiatement, certainement aussi conséquemment aux multiples hacks qui, depuis plus de 20 ans, ont conduit ces intégrateurs à s'engager dans une course au blindage antipirates.
Comme quoi, c'est pas la sécurité qui manque, dans le domaine de l'Internet des Objets, c'est la menace financière.

Réagissez à cet article
Source : http://www.cnis-mag.com/iot-une-moyenne-de-5-failles-par-objet.html

Objets connectés, des cadeaux aussi pour les pirates informatiques

Objets connectés, des cadeaux aussi pour les pirates informatiques

Les pirates informatiques pourraient se frotter les mains avec l'arrivée des fêtes de fin d'année et parmi les cadeaux, des millions de nouveaux et potentiellement vulnérables appareils connectés à internet.

Drones, bracelets de fitness, montres et appareils électroménager « intelligents »… n'importe quel appareil connecté « peut être un point d'entrée pour accéder à votre réseau informatique.
Même si s'introduire dans un accessoire vestimentaire connecté ou un drone ne semble pas apporter grand chose aux pirates, cela peut ensuite servir de porte d'entrée à un smartphone et aux appareils auxquels il se connecte…
Une fois l'accès ouvert aux ordiphones, ordinateurs ou smartphones, les pirates pourraient facilement y installer des virus qui aspirent tous les mots de passe qui transitent sur votre réseau et les renvoient directement au pirate…
Beaucoup des gadgets électroniques proposés aux consommateurs , lorsque les sécurités sont activées, utilisent malheureusement des connexions peu sécurisées et recourent souvent de manière minimale à des mots de passe ou autres moyens d'authentification peu difficiles à percer.
Quand on reçoit ces nouveaux jouets qui brillent pour Noël, on veut juste commencer à s'en servir.
Avec la frontière de plus en plus floue entre travail et loisirs, les salariés risquent davantage de ramener des documents d'entreprise sensibles chez eux et que parfois, rien qu'en se connectant au réseau wifi de la maison, ils exposent des documents sur tout internet.
Le cabinet de recherche Gartner estime que 6,4 milliard d'objets connectés seront utilisés dans le monde en 2016, soit 30% de plus que cette année, et que leur nombre grimpera à 20,8 milliards d'ici 2020.
Juniper Research prédit pour sa part que les ventes de « jouets intelligents » atteindront 2,8 milliards de dollars cette année, tout en notant que « les vendeurs se reposeront probablement sur l'expertise de fournisseurs extérieurs de logiciels pour éviter des désastres en termes de relations publiques causés par des pirates ».

Alors, avant de profiter de votre nouveau joujou, prenez un peu de temps et assurez-vous d'avoir suffisament de sécurité en place sur votre appareil, vos communications, votre réseau… car une fois que vous aurez mis en route l'appareil et commencé à échanger des données, il sera trop tard pour faire marche arrière. Vous vous serez plutôt concerntré sur son utilisation.

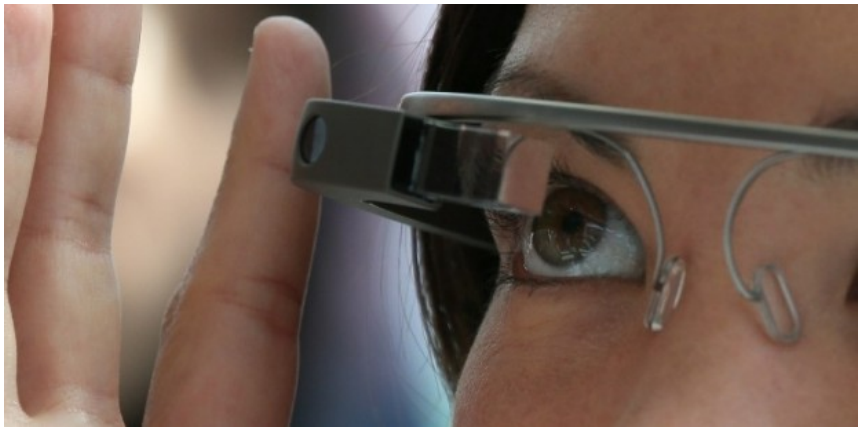
Réagissez à cet article
Source : Denis JACOPINI

https://www.lesnewseco.fr/2015/11/21/science-high-tech/les-pirates-informatiques-pourraient-sinviter-pour-noel-5359.html

Google Glass : Google prévoirait trois nouvelles versions

Google Glass : Google prévoirait trois nouvelles versions

Après la débâcle de l'an dernier, Google a décidé de repartir de zéro pour la conceptualisation de ses Google Glass et prévoirait désormais trois nouvelles versions de ses lunettes de réalité augmentée.



Le géant du Web, qui a été contraint de repartir de zéro après avoir analysé les premiers retours sur son prototype de lunettes de réalité augmentée, travaillerait aujourd'hui sur trois nouvelles versions du produit selon le site The Information.
La première serait destinée aux entreprises, et pourrait dès lors venir dans une forme plus brute, avec une batterie supplémentaire qui se porterait par exemple à la taille, et des fonctionnalités dédiées aux professionnels.
Une version plus "grand public" serait également en cours de conceptualisation. Probablement plus accessible, plus élégante et surtout davantage axée sur une utilisation quotidienne, cette version sera probablement la vitrine de la marque Google Glass.
Enfin, Google prévoirait également une version qui serait dépourvue du micro-écran et qui pourrait donc prendre la forme d'une simple oreillette Bluetooth, bardée de capteurs.
Pour l'heure, difficile de dire son utilité exacte, mais il semblerait encore une fois que ce modèle soit destiné aux professionnels.
Malheureusement, Google ne donne toujours aucune précision sur la nouvelle version de Google Glass, dont la date de sortie reste la grande inconnue.

Source : http://geeko.lesoir.be/2015/11/17/google-glass-google-prevoirait-trois-nouvelles-versions/

Une journée avec des objets connectés : ça change quoi ?

Une journée avec des objets connectés : ça change quoi ?

7h, la lumière du jour vous réveille en douceur. Pourtant, dehors, il fait encore nuit. Vous vous glissez hors de la couette sans trop de difficulté car l'air ambiant de votre chambre est juste comme vous aimez. Pourtant, dehors, il fait très froid.
Vous vous sentez en forme. Un coup d'œil à vos cycles de sommeil sur votre téléphone vous confirme que vous avez bien dormi.
Et c'est aussi grâce à lui, votre téléphone, que vous vous êtes réveillé en douceur. Connecté à votre réveil, à votre thermostat et à votre capteur de sommeil, il a dialogué avec eux pendant que vous dormiez paisiblement. Grâce à une ou plusieurs applications, vous aviez au préalable donné vos instructions à cet écosystème intelligent : vous réveiller à 7h avec une température ambiante de 20°c.
Votre chauffage s'est automatiquement mis en route et votre réveil lumineux vous a éveillé progressivement au meilleur moment de votre cycle de sommeil.Matin facile !Vous regardez sur votre téléphone si votre petit dort toujours. Oui, vous avez donc le temps de filer prendre une douche… Vous avez envie d'écouter les infos, en un rien de temps la radio est lancée sur l'enceinte de votre salle de bain.
Le fil d'info vous suivra ensuite de la chambre à la cuisine. Entre temps votre enfant s'est réveillé, vous allumez à distance la petite veilleuse de sa chambre pour le faire patienter quelques instants.

La maison connectée Et il en va ainsi…
Au fil de votre journée, vos objets intelligents continuent de vous faciliter le quotidien. A peine sortie de chez vous, votre système de sécurité est activé. Votre maison est protégée et vous veillez à distance. Vous serez aussi informé quand votre ado sera bien rentré du collège.
Dans l'après-midi, vous avez un doute : vous avez pensé à mettre le linge dans la machine mais l'avez-vous bien programmée ? Et non, mais voilà chose faite à l'instant grâce à votre smartphone et votre lave-linge des temps modernes.
Une alerte : votre montre ou votre bracelet connecté qui analyse votre activité et compte vos pas depuis ce matin vous signale que vous ne vous êtes pas suffisamment dégourdi les jambes aujourd'hui. C'est décidé, vous prendrez les escaliers et vous irez chercher le pain à pied. C'est déjà ça !

Une soirée connectée
Une fois rentré à la maison, vous adaptez l'ambiance du salon à votre humeur en quelques clics sur votre écran tactile : morceau rythmé et lumière colorée ? Ou musique douce et lumière tamisée ?
Une notification sur votre smartphone vous rappelle que vous devez arroser vos plantes. Mission accomplie, voilà que votre mobile vous signale que votre plat a fini de mijoter dans votre cocotte. Et oui, elle aussi est connectée !
Après le repas, vous pourrez vérifier que vos enfants se sont bien brossés les dents. S'achèvera alors une journée bien remplie…
Mais parfaitement normale !

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !
Source : http://www.darty.com/darty-et-vous/high-tech/objets-connectes/une-journee-avec-des-objets-connectes-ca-change-quoi

Les cybercriminels ciblent le paiement mobile | Le Net Expert Informatique

Il y a quelques semaines, nous avons traité, du e-Commerce. C'est un registre si vaste et varié que nous choisissons, cette semaine aussi, d'y consacrer quelques réflexions, histoire de susciter chez nos lecteurs quelque intérêt pour une problématique appelée à devenir incontournable. Malgré l'essor du e-Commerce, les modes de paiement mobile peinent à décoller dans de nombreux pays développés. En cause, le conservatisme et la peur de l'inconnu.

L'inconnu, selon de nombreux spécialistes, c'est la cybercriminalité qui donne des sueurs froides aux fournisseurs de solutions. Dans un excellent article au titre très évocateur publié récemment, « Le paiement mobile, nouvel eldorado des escrocs », Benoît Huet de la rédaction de lemondeinformatique.fr nous amène faire une immersion dans les méandres d'un secteur pourtant promu à un bel essor. Les résultats du paiement mobile, il faut bien le concéder, sont assez modestes.

Dans son article, Benoît Huet écrit : « Selon l'institut d'études GFK, qui a mené une enquête dans 17 pays auprès de 17 000 consommateurs, seulement 5% des transactions mondiales sont réellement effectuées avec un appareil mobile ». Presqu'un désert ! Dans un pays comme la France, notre référence à tous, « les transactions via le paiement mobile sont souvent estimées à moins de 1% par les différents cabinets d'études ».

Et pourtant, précise l'article de notre confrère, ce n'est pas faute d'avoir essayé. De nombreuses applications permettant de payer avec un smartphone existent : le service PayByPhone pour payer le stationnement et le parking à Boulogne, Nice et dans d'autres villes, ainsi que des commerces qui ont mis en place un terminal NFC (Paiement Sans Contact) pour régler diverses courses.

La première raison, et nous l'évoquions plus haut, le conservatisme culturel : « Si le paiement mobile a encore du mal à percer en France, c'est déjà parce que les moyens de paiement sont très liés à la culture des pays. La France est par exemple un pays fortement tourné vers l'usage de la carte bleue Visa alors qu'en Belgique, c'est la Mastercard qui règne, quant à l'Allemagne, le paiement en liquide est encore très courant ».

Sans vouloir défier la technologie, « Les français ne sont pas encore prêts à payer avec leur mobile, c'est à la fois un problème culturel et un manque de confiance dans les technologies, ils préfèrent donc payer en caisse avec une carte, de l'espèce ou en chèque ».

La seconde raison qui plombe l'essor du paiement mobile vient d'être lâchée : le manque de confiance dans les technologies. Par instinct de survie, la majorité des français boudent le paiement mobile, moins sécurisé à leurs yeux, de peur d'être victime des cyberescrocs qui ont plus d'un tour dans leur sac.

Sans l'affirmer, les conclusions de l'étude donnent raison aux cyber-sceptiques qui semblent se perdre dans la jungle des technologies de communication sans contact comme les balises (Beacons utilisant le Bluetooth) ; le RFID ; le NFC (qu'utilise Apple, entre autres, avec Apple Pay et Google avec Google Wallet) ; le QR code (comme le Flash'NPay créé par Auchan) ; la transmission magnétique (Samsung Pay exploite la technologie transmission magnétique suite au rachat de LoopPay mais aussi le NFC) ; les systèmes de portefeuilles électroniques mobiles comme Orange Cash (Orange et Visa) ; PayPal Mobile et Paylib (initié par les banques françaises). Jungle, il faut bien l'admettre, est vraiment un doux euphémisme pour évoquer cet univers ! Face à un tel environnement, banques et entreprises n'ont d'autres choix que de perfectionner la sécurité des systèmes de paiement mobiles afin de donner davantage d'assurance aux consommateurs. Cette assurance semble passer par des systèmes de cryptage des données très évolués et les dispositifs de détection prédictive de malwares. Notre confrère cite PayPal qui vient de racheter la start-up israélienne CyActive qui a mis au point une technologie capable d'anticiper les futures attaques grâce à des algorithmes permettant d'analyser et de comprendre les processus de piratage.

En parallèle, les fournisseurs ne ménagent pas leurs efforts en apportant, au niveau du terminal, des mécanismes à double authentification comme Apple qui exploite l'empreinte digitale en plus d'un code de sécurité unique et des quatre derniers numéros de la carte de sécurité sociale de l'utilisateur. On le voit bien, il y a de gros efforts en cours pour tendre vers le risque zéro, même s'il n'existe pas.

Les entreprises du secteur et les banques gagneraient à collaborer plus étroitement pour améliorer la sécurité des transactions au plan national et international, tout comme elles sont condamnées à imaginer des standards qui détectent à mille lieues les criminel et les neutralisent sans coup férir.

Enfin, chaque entreprise qui propose des solutions de paiement mobile devrait assortir son plan d'expansion d'une campagne de communication qui permettrait aux utilisateurs d'éviter de tomber dans les pièges, de plus en plus perfectionnés, des cybercriminels.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

Source : http://malijet.com/la_societe_malienne_aujourdhui/139922-chronique-du-web-les-cybercriminels-ciblent-le-paiement-mobile.html
Par Serge de MERIDIO