Quand les objets connectés contrôlent nos vies…

Quand les objets connectés contrôlent nos vies…

La sécurité est un enjeu majeur pour les objets connectés. Que ce soit dans le Quantified Self où les données relatives à la santé sont sensibles ou dans la domotique où les pirates peuvent prendre contrôle de la maison, les failles sont multiples.

Nous vous avions déjà parlé du hack du thermostat Nest lors de la Blackhat Conference, voici maintenant 5 autres cas avérés de piratage d'objets connectés. L'objectif n'est pas de vous faire peur, mais de simplement montrer que de nouveaux défis émergent pour toutes les sociétés qui s'y lancent.

Le compteur électrique qui coupe le courant
Une étude réalisée par deux experts en sécurité a montré de sérieuses lacunes dans les derniers compteurs d'électricités intelligents mis sur le marché pour répondre aux nouvelles normes du gouvernement espagnol. Les deux spécialistes ont ainsi démontré qu'il était possible de couper le courant chez les propriétaires (potentiellement pour créer un gros black out) ou trafiquer les compteurs pour fausser les factures. Grâce à un système d'infection en cascades, il serait même possible de remonter jusqu'aux centrales électriques. Sans donner le nom du fournisseur de compteurs chez qui la faille a été découverte, on sait cependant qu'il s'agirait d'un des gros acteurs du marché en Espagne que sont Endesa, Iberdrola ou E.ON.
L'Union Européenne a lancé un programme pour inciter les habitants à développer l'usage du compteur d'électricité intelligent, dans l'objectif d'économiser 3% d'énergie supplémentaires d'ici à 2020. A cette date, ce sont deux tiers des européens qui devraient en avoir installé un (sous condition qu'ils ne représentent pas de faille aussi importante…).

L'ampoule connectée qui découvre les mots de passe Wi-Fi
La société Context a exposé une faille de sécurité dans une ampoule connectée : la Lifx Wi-Fi. En parvenant à accéder à l'ampoule, elle a réussi à récupérer et décrypter les informations de configuration du réseau. L'équipe qui avait déjà trouvé des failles dans des imprimantes ou des moniteurs pour bébés a accédé au firmware de l'ampoule en étudiant le microcontrôleur afin de comprendre le mécanisme de cryptage de l'ampoule.
Le responsable recherche chez Context a déclaré « Pirater l'ampoule n'est pas simple, mais ne nécessite pas non plus d'avoir des connaissances trop complexes en matière de hack ». Il précise que ces vulnérabilités peuvent facilement être comblées en travaillant avec les développeurs Lifx. Il a déjà vu des cas plus complexes…

Le moniteur vidéo qui insulte bébé
Un couple américain habitant de l'Ohio a entendu une voix inconnue dans la chambre de leur bébé en août 2013. Il s'agissait d'un hacker qui avait réussi à prendre le contrôle de la caméra pour surveiller le bébé. Selon ABC News, la voix proférait des insultes au bébé.
Le père du bébé avait pourtant pris des précautions, notamment en donnant des mots de passe à son routeur et la caméra et en utilisant un pare-feu. La caméra était une Foscam. La société a rapidement sorti une mise à jour permettant d'éviter de nouveaux désagréments. Malheureusement, tous les utilisateurs n'ont pas mis à jour leur caméra de surveillance de bébé, à l'instar de la famille Schreck chez qui l'incident s'est reproduit en avril 2014. Les réactions en vidéo :

La box TV qui menace les grands-mères
A croire que cela ne se passe qu'aux Etats-Unis, voici l'histoire d'une grand-mère de la ville d'Indianapolis qui a eu la mauvaise surprise de voir des messages vulgaires apparaître sur sa télévision après que sa box TV AT&T ait été piratée. Alana Meeks a rapidement changé de box en n'espérant plus jamais revoir ces messages menaçants, rien n'y a fait. La police est intervenue et a pris notes des injures proférées à son encontre sur la télévision.
AT&T a immédiatement déclaré rechercher les causes de ce piratage, mais aucune nouvelle information n'a été officialisée depuis. On ne sait finalement pas si Mme Meeks a rallumé une télévision depuis.

Le frigo connecté spammeur
Le premier cas de frigo qui envoi du spam a été découvert en Californie au début de l'année. Il faisait partie d'un parc de plus de 100 000 appareils dont les pirates se servaient pour leur spam, avec des ordinateurs, des smart TV et des médias center. Plus de 750 000 emails ont été envoyés depuis ces appareils, dont 75% par les ordinateurs et le reste par des objets pour la maison reliés à internet.
Bref, autant d'exemple pour montrer que les objets connectés sont aujourd'hui vulnérables à ce genre d'attaques. Evidemment, avec le nombre de ces appareils qui va en s'accroissant, il faudra que les fournisseurs de technologie redoublent de vigilance pour assurer la sécurité de leurs clients. On se rappelle que HP a publié il y a quelques mois une étude qui montrait des résultats effarant sur les objets connectés : ce ne seraient pas moins de 250 vulnérabilités qui auraient été découvertes dans les 10 objets connectés les plus populaires du moment.

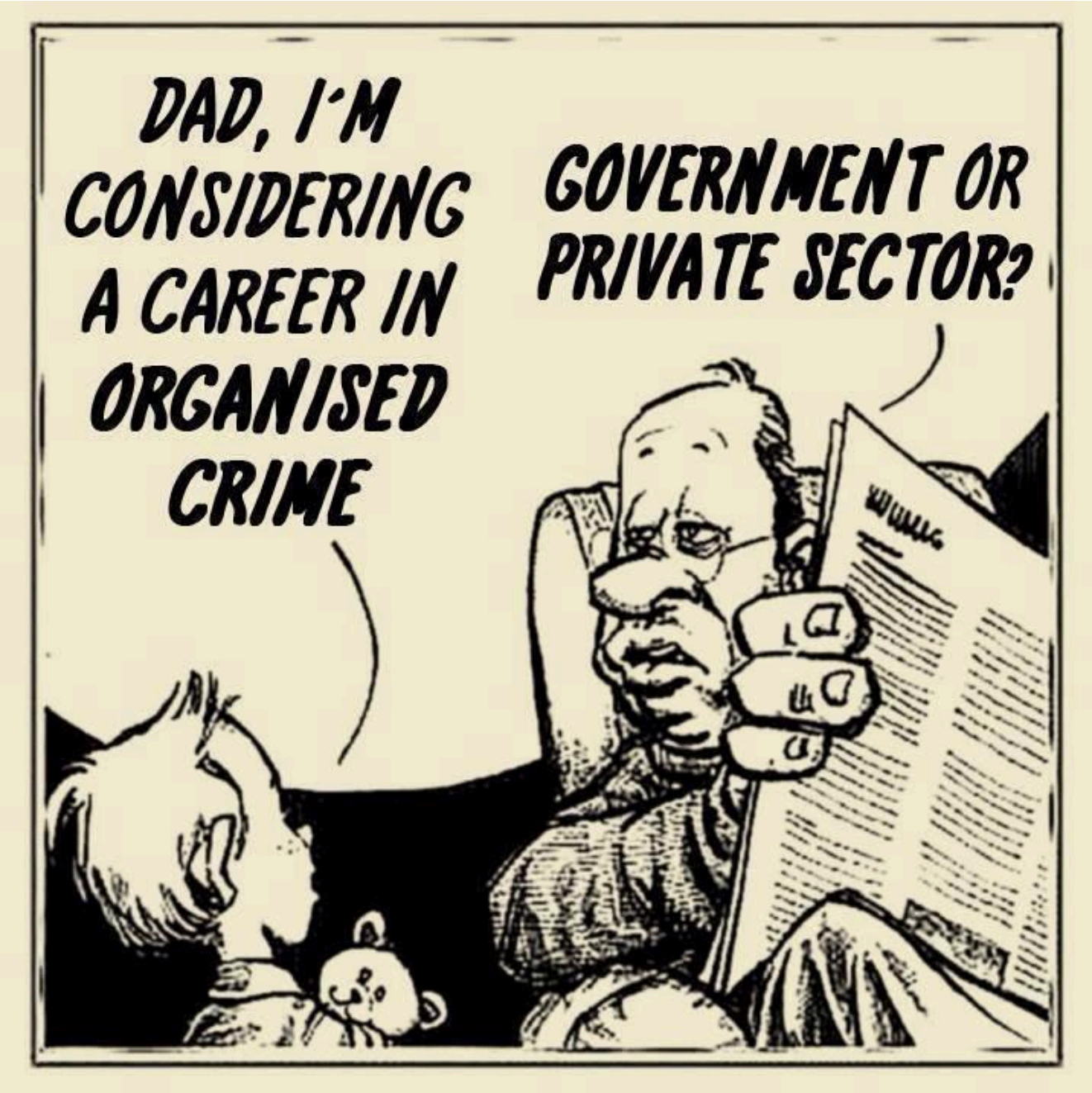
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.stuffi.fr/objets-connectes-exemples-piratages-insolites/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Stuffi+(Stuffi+-+L%27actualit%C3%A9+des+objets+connect%C3%A9s

---

Faire carrière dans la

cybercriminalité ?



Faire carrière dans la cybercriminalité ?

The People's Voice

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

Source : https://www.facebook.com/thepeoplesvoicetv/photos/a.287874141360034.1073741844.219195584894557/386748201472627/?type=1

Pickpocket numérique, une nouvelle activité saisonnière

	« Pickpocket » numérique, une nouvelle activité saisonnière

La cybercriminalité est un marché… comme un autre. Avec ses foires, ses codes et même ses monnaies.

« Pickpockets » numériques

Appelons les « pickpockets » numériques. Le soi-disant « hameçonnage » numérique, ou phishing. Le premier marché pour ce type de cybercriminalité est l'Amérique du Nord, à savoir États-Unis et Canada. Suivi par le Royaume-Uni. Ce marché, en plus de son organisation, est un marché saisonnier. En novembre, les attaques augmentent ; l'activité diminue à partir de décembre, au moment de Noël. Il y a une explication très simple à ce phénomène étrange : une fois les données volées… les criminels doivent aller faire du shopping ! Selon Daniel Cohen, un des responsables de cette question chez RSA (la division sécurité d'EMC), les attaques augmentent de nouveau en avril, saison du paiement des taxes aux États-Unis et, bien évidemment, en août, pour les vacances.

La complexité de ce marché ne fait que s'accroître. Ainsi, les pirates, les cybercriminels qui volent des données, ne savent la plupart du temps pas quoi faire desdites données, et les vendent à des experts qui savent comment les utiliser et les transformer en argent réel. « Il faut savoir comment faire des emplettes dans le monde numérique sans laisser de traces », explique Daniel Cohen. En effet, ce marché est si organisé qu'il existe des 'places de marché' undeground où on peut trouver des données de cartes de crédit. Avec des garanties. Si la carte de crédit a expiré ou a été annulée par l'utilisateur, la place de marché va rembourser l'acheteur ou remplacer la carte inutilisable.

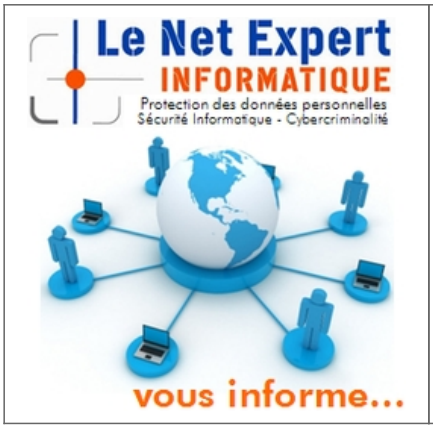
Ces sites ont même des centres d'appels pour aider les escrocs utilisant de cartes frauduleuses à appeler la banque du possesseur légal de la carte, afin de changer d'adresse par exemple. Imaginez que vous achetiez une carte dans ce monde souterrain et que vous vouliez modifier l'adresse qui y est associée. Évidemment, la banque se montrerait suspicieuse si la carte était émise au Texas par exemple, et que votre accent semblait plutôt correspondre à la Caroline du Nord. Ou à l'Angleterre. Un des services offerts par les magasins du crime online est précisément de mettre à disposition des hommes et femmes avec des accents différents afin d'appeler – et de tromper – les banques. Et ceci n'est qu'un exemple des services fournis…

En savoir plus sur http://www.silicon.fr/plongee-monde-cybercriminels-103081.html

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

Source : http://www.silicon.fr/plongee-monde-cybercriminels-103081.html#dV0OWrskHOYXcst5.99

Les experts de Symantec présentent leurs prédictions de sécurité pour 2015 – Global Security Mag Online



Des experts présentent leurs prédictions de sécurité pour 2015

Compte tenu du nombre d'incidents survenus cette année, depuis les campagnes de cyber-espionnage et de cyber-sabotage jusqu'aux vulnérabilités identifiées dans les fondements mêmes du Web, il est difficile de hiérarchiser les événements marquants de l'année 2014. On peut cependant s'interroger sur la signification de certains d'entre eux et sur ce qu'ils laissent présager pour l'année à venir.

L'équipe Symantec Security Response a récemment listé les 4 événements marquants de l'année 2014 en matière de sécurité. Laurent Heslault, directeur des stratégies de sécurité chez Symantec, s'est penché sur ce que 2015 nous réserve et présente aujourd'hui ses conclusions.

Les moyens de paiements électroniques en ligne de mire
Il est peu probable que des attaques à grande échelle similaires à celles qui ont ciblé les équipements de points de vente aux États-Unis se produisent en Europe. En effet, notre système de carte à puce associé à un code confidentiel ne facilite pas la récupération des données de carte bancaire. Cela dit, ces cartes à puce et à code confidentiel peuvent être subtilisées et utilisées pour effectuer des achats sur Internet. L'adoption grandissante des cartes de paiements sans contact, accompagnée du paiement sans contact via les mobiles, augmentera le risque d'attaques ponctuelles.

Les attaques de cyber-espionnage et de cyber-sabotage ne devraient pas faiblir en 2015
En 2015, les campagnes de cyber-espionnage et de cyber-sabotage financées par des États, telles que les opérations DragonFly et Turla observées en 2014, ou encore le spyware très récemment analysé et rendu public Regin, constitueront toujours des menaces pour la sécurité des infrastructures nationales et stratégiques dans le monde entier. Face à de telles campagnes visant à soutirer des renseignements et/ou à saboter des opérations, les entreprises et administrations devront revoir leur politique de cyber-sécurité et donner la priorité à la sécurité, qui deviendra un investissement stratégique plutôt que tactique.

Les secteurs publics et privés devront davantage collaborer pour lutter contre la cyber-criminalité
Fortes des différents démantèlements de groupes de cyber-criminels tels que les opérations Gameover Zeus, Cryptolocker ou encore Blackshades menées en 2014 , les autorités internationales adoptent une approche plus active et plus agressive vis-à-vis de la cyber-criminalité en renforçant leur collaboration avec l'industrie de la sécurité en ligne. Cette collaboration entre le secteur privé et les forces de police se poursuivra en 2015 afin d'avoir un impact durable et de stopper les cyber-criminels dans leur élan.

De nouvelles réglementations pour les entreprises européennes
À l'heure où l'Europe souhaite appliquer sa nouvelle législation sur la protection des données, la confidentialité et l'utilisation des informations demeureront au centre des préoccupations en 2015. Contraintes de garantir le respect des nouvelles réglementations, mais aussi de suivre le rythme de l'économie mondiale en exploitant leurs énormes volumes de données pour créer de nouveaux services et de trouver d'autres sources de revenu, les entreprises européennes vont devoir relever un certain nombre de défis en 2015.

En 2015, les plates-formes Open Source seront le maillon faible
L'année 2015 apportera son lot de vulnérabilités dans les bases de données Open Source et les plates-formes de services Web, que les pirates exploiteront en toute impunité. À l'instar de Heartbleed et Shellshock, ces vulnérabilités constituent une cible potentiellement juteuse pour les pirates, le plus gros risque continuant d'être lié aux failles connues ; entreprises et particuliers n'appliquent pas toujours les patchs correctifs appropriés.

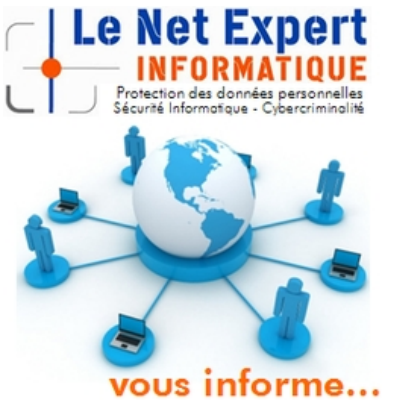
L'Internet des objets restera l'Internet des vulnérabilités, mais les attaques seront limitées et ponctuelles
L'« Internet des objets » étant essentiellement lié à la génération de données, les cyber-criminels redoubleront d'imagination pour exploiter les failles logicielles des appareils connectés. Seront notamment concernés les technologies portatives, les équipements domestiques connectés, comme les téléviseurs connectés et les routeurs, et les applications automobiles connectées. Cela dit, nous ne devrions pas observer d'attaques à grande échelle sur l'Internet des objets, seulement des attaques ponctuelles.

Les organisations reconnaîtront que le système identifiant/mot de passe classique a ses limites
À une époque où les organisations cherchent des solutions pour prévenir les intrusions et protéger leurs utilisateurs, elles seront heureuses d'apprendre que des alternatives à l'ancien système se profilent à l'horizon. Notamment, l'authentification à deux facteurs, qui n'exige pas seulement une information que seul le véritable propriétaire connaît (mot de passe, etc.), mais aussi une information que lui seul est censé détenir (numéro de téléphone portable, etc.). Toutefois, alors que chaque service commence à prendre ce genre de mesures, le consommateur va devoir de plus en plus composer avec des applications, numéros de téléphone et questions de sécurité multiples (et ce sur différentes plates-formes), risquant ainsi de lui compliquer la tâche.

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

Source : http://www.globalsecuritymag.fr/Les-experts-de-Symantec-presentent,20141201,49146.html

Le pirate Informatique ayant attaqué Sony enfin démasqué ?



Le pirate Informatique ayant attaqué Sony enfin démasqué ?

Ce serait la première fois qu'un studio d'Hollywood – en l'occurence Sony – soit la victime d'une cyberattaque venue de la Corée du Nord, et pourtant. Selon le site d'informations technologiques Re/code, Pyongyang a mené une attaque informatique pour pirater les bureaux de Sony Pictures à Los Angeles.

La vengeance est un plat qui se mange froid, même en Corée du Nord. En juin dernier, les autorités de Pyongyang avaient annoncé qu'une réponse sans merci serait adressée à «l'acte de guerre» que constituait la sortie du film «L'interview qui tue!» d'Evan Goldberg, dans laquelle deux agents de la CIA se font passer pour des journalistes afin d'assassiner le dictateur nord-coréen Kim Jong-un.

Les menaces n'avaient pas été prises au sérieux: le film est une comédie avec Seth Rogen dans le rôle principal, et personne ne se doutait que la Corée du Nord puisse réellement prendre la mouche devant ce qui n'est qu'une parodie potache. C'était oublier le caractère absurde de la dictature nord-coréen. De mystérieux «Gardiens de la paix» ont mené une attaque informatique en début de semaine dernière contre le réseau informatique de Sony Pictures – qui distribue le film. Les employés du studio américano-nippon (deux pays ennemis de la Corée du Nord, Ndlr) ont été renvoyés chez eux, mardi avec la consigne de ne pas se connecter au réseau informatique de la société, selon Next web.

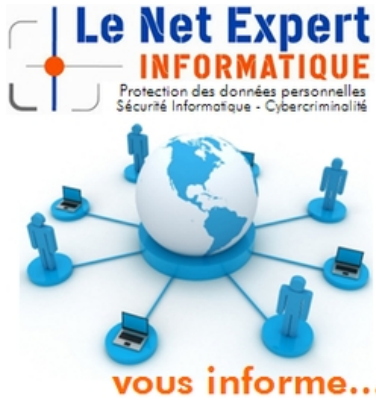
CINQ FILMS PIRATÉS

Cinq films ont été piratés et puis jetés en pâture sur le Web: «Annie», nouvelle version de la comédie musicale, avec Quvenzhané Wallis et Jamie Foxx, «Mr. Turner» de Mike Leigh, «Still Alice», drame avec Julianne Moore and Alec Baldwin, ou encore «Fury» avec Brad Pitt, déjà sorti en salles. Selon «Variety», les films ont été téléchargés illégalement par plus de 1,2 millions d'utilisateurs… Les pirates auraient pu également volés de nombreuses données personnelles de stars liées à Sony comme Angelina Jolie, Cameron Diaz et Jonah Hill. Pas sûr que cet épisode de guerre cyber se retrouve dans le bonus DVD de «L'interview qui tue!».

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

Source : http://www.parismatch.com/Culture/Cinema/Kim-Jong-un-dictateur-susceptible-660458

Recherche en ligne : le Parlement européen prône le démantèlement



Recherche en ligne : le Parlement européen prône le démantèlement

Le Parlement européen a appelé les états membres de l'Europe ainsi que la Commission européenne à éliminer les obstacles qui freinent la croissance du marché unique du numérique en Europe dans une résolution votée le 28 novembre 2014.

Dans un projet qui vise clairement Google, les députés du Parlement européen ont mis l'accent sur le besoin d'empêcher les entreprises du Web d'abuser de leurs positions dominantes en imposant la mise en application des lois en place en matière de concurrence et en dissociant les moteurs de recherches des autres services commerciaux.
Le marché unique du numérique pourrait générer quelque 260 Md€ par an pour l'économie européenne et renforcer la concurrence, soutient cette résolution, qui a été approuvée par 384 votes contre 174.
Toutefois, elle tire la sonnette d'alarme sur certains problèmes, comme la fragmentation du marché, le manque d'interopérabilité et les inégalités régionales et démographiques en matière d'accès aux technologies, qui doivent être résolus pour libérer tout le potentiel de la région.
La résolution souligne que « le marché de la recherche en ligne est clé pour garantir les conditions de la concurrence dans le marché unique du numérique » et salue les engagements de la Commission européenne à enquêter davantage sur les pratiques des sociétés agissant sur le segment de la recherche. Le texte appelle également la Commission à « empêcher tout abus marketing en relation avec des services interconnectés chez les opérateurs de moteurs de recherche », marquant le degré d'importante d'une recherche en ligne non discriminatoire. Selon les députés, « l'indexation, l'évaluation, la présentation et le ranking par les moteurs de recherche doivent être impartiaux et transparents. »
Cette résolution suit quatre années d'enquête de Bruxelles sur la prétendue position dominante de Google sur le marché de la recherche en Europe et sur de possibles détournements de trafic en faveur de ses propres services.
La Commission a rejeté toutes les propositions du Californien visant à répondre aux allégations portant sur des pratiques commerciales anti-concurrentielles. On estime à 90% les parts de marché de Google sur le marché de la recherche en ligne en Europe.

Etant donné le rôle des moteurs de recherche dans l'exploitation commerciale des résultats obtenus, et la nécessité de faire appliquer les lois de la concurrence en Europe, les députés européens ont également demandé à la Commission de « réfléchir à des propositions visant à séparer les activités de moteur de recherche de celles liées à des services commerciaux » sur le long terme.
« Le trafic internet dans son ensemble doit être traité de façon équitable, sans discrimination, restriction ou interférence », ont souligné les députés européens. Pour prendre effet, la résolution doit encore être approuvée par la Commission. Pourtant certains observateurs prétendent que le vote en faveur d'une séparation des activités commerciales pourrait bien donner à Google de bonnes sueurs froides.
Le vote met en avant les inquiétudes des européens quant à une éventuelle position dominante de Google et pourrait donner le coup d'envoi d'une nouvelle série d'enquêtes des régulateurs en Europe.

Même si l'Europe n'a pas le pouvoir de démanteler Google, si approuvée par le Commission, la résolution pourrait forcer le Californien, ainsi que les autres moteurs de recherche, à restructurer ses activités en Europe. Bruxelles devrait donner à Google la possibilité de répondre avant de prendre sa décision.

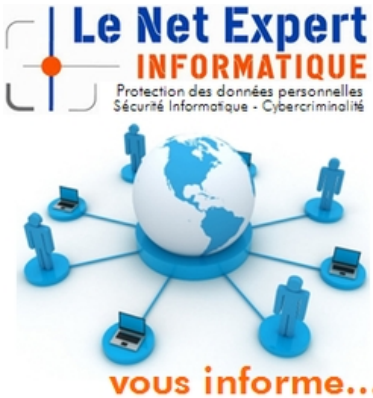
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemagit.fr/actualites/2240235624/Recherche-en-ligne-le-Parlement-europeen-prone-le-demantelement

---

Les consommateurs réclament

transparence, pertinence et simplicité dans l’utilisation des données en ligne



Les consommateurs réclament transparence, pertinence et simplicité dans l’utilisation des données en ligne

Les consommateurs se disent prêts à partager leurs données personnelles si c'est fait avec transparence et à condition qu'ils en retirent un intérêt.
Pour offrir une expérience captivante en ligne, une marque doit savoir quelles sont les attentes des clients et comment les satisfaire. Pour se démarquer de la concurrence, les entreprises ont compris l'importance de nouer une relation d'engagement et d'être en capacité de la traduire rapidement en action. Mais une stratégie basée sur de bonnes idées, sur l'intuition ou même ce qui a fonctionné par le passé ne suffit plus. Les consommateurs d'aujourd'hui sont complexes et exigeants. Ils veulent être compris et traités individuellement mais se montrent intraitables quant à leur sphère privée. Pour attirer et garder leur attention, les entreprises doivent pouvoir se procurer la bonne information au bon moment et de la bonne façon.
Nous avons interrogé 2 000 adultes britanniques pour obtenir leur point de vue dans le débat qui oppose personnalisation et protection de la vie privée. Il ressort de cette étude que les consommateurs acceptent volontiers de partager des données personnelles avec les marques, du moment que cet échange virtuel de bons procédés respecte trois valeurs fondamentales : la transparence, la pertinence et la simplicité.
84 % des 18-34 ans partagent volontiers leurs données personnelles avec les marques en utilisant pour se connecter les identifiants de leur compte sur les réseaux sociaux. Dans ce contexte, voici trois pistes à suivre par les marques pour rassurer les consommateurs et se distinguer de la concurrence en instaurant des relations privilégiées.

Transparence, des gages de protection de la vie privée des consommateurs
Les consommateurs rechignent à partager des données personnelles avec les marques de peur que celles-ci en fassent un mauvais usage. Il est important de réaffirmer aux consommateurs l'importance que vous accordez à la confidentialité des données et de leur dire clairement quelle utilisation vous faites de leurs données. Chaque fois que vous avez besoin d'accéder à des données personnelles, énoncez clairement l'utilisation que vous allez en faire et l'intérêt pour vos clients de jouer le jeu.
Les clients interrogés sur ce qui les inciterait à communiquer davantage d'informations les concernant à une entreprise ou une marque ont cité deux conditions majeures : être certains que la société ne partagera pas leurs données avec un tiers et savoir quels usages la société s'engage à faire des informations ainsi collectées. Chaque entreprise devrait se doter d'une politique claire qui réaffirme son approche vis-à-vis du respect de la confidentialité des données. Plutôt que de contraindre vos clients à faire l'effort de comprendre votre approche de la gestion des données, prenez les devants et publiez une déclaration d'engagement brève et formelle. Insistez sur la volonté de votre entreprise de respecter les dernières préconisation en matière de sécurité des données et envoyez un message clair à vos clients et à vos prospects qui souligne le sérieux de votre approche de protection de la confidentialité et de la sécurité des données.
En proposant aux utilisateurs de se connecter à votre site via un tiers, à savoir le compte de leur choix sur les réseaux sociaux (Facebook, Twitter, Google, etc.), vous leur permettez de décider quelles informations ils sont d'accord de partager ou non. Vous les dispensez aussi de devoir se remémorer plusieurs combinaisons d'identifiants et de mots de passe et vous-même n'aurez pas besoin de stocker ces données et les maintenir à jour.

Pertinence, l'importance de la personnalisation
Dans un monde où les consommateurs sont confrontés à des centaines de messages de marketing par jour, la clé est de leur délivrer des annonces pertinentes et de leur faire vivre des expériences qui leur parlent. Mais pour que ces expériences reflètent les attentes et les souhaits des consommateurs d'une façon authentique et respectueuse, les entreprises ont besoin des données des personnes concernées (first-party data). Les techniques de ciblage traditionnelles, comme les cookies de traçage, relèvent d'un jeu de devinette : ce que vous apprendrez dépend des pièces du parcours de navigation que vous allez pouvoir associer. Ces techniques ne permettent pas de dépeindre le profil complet de l'utilisateur.

Les informations les plus importantes restent de côté : les loisirs, les centres d'intérêts, les marques préférées et les relations. Et si plusieurs utilisateurs se partagent le même appareil, ces données sont encore plus diluées.

De plus, les cookies ne permettent pas de faire un suivi de l'activité sur terminaux mobiles. Maintenant qu'ils sont sensibilisés à la question de la protection de leur confidentialité, de plus en plus d'utilisateurs se protègent au moyen de logiciels qui bloquent les publicités (ad blockers) et d'applications anti-tracking, au détriment des marketers qui ont recours à ces méthodes. Ceux-ci obtiennent les données du consommateur directement qui donne son accord pour recevoir des informations par e-mail, en s'abonnant à un service, ou en se connectant via un réseau social, etc. Selon les prévisions mondiales de Bloomberg, deux milliards de personnes posséderont un smartphone en 2015.

Les entreprises doivent se familiariser avec ce nouveau paysage multicanal, veiller à soigner leur présence sur les canaux les plus stratégiques et apprendre à lisser leur image de marque et la cohérence de l'expérience qu'elles proposent, du PC fixe au terminal mobile au point de vente. Dans cette démarche d'engagement des clients sur les différents canaux, la compagnie aérienne KLM Royal Dutch Airlines a développé le programme Meet & Seat auquel les voyageurs acceptent de se connecter pour partager les infos de leurs profils Facebook ou LinkedIn avec les autres passagers.
Tous ceux qui le souhaitent ont ainsi accès aux profils sociaux des autres utilisateurs du service et peuvent choisir à côté de qui ils veulent voyager.

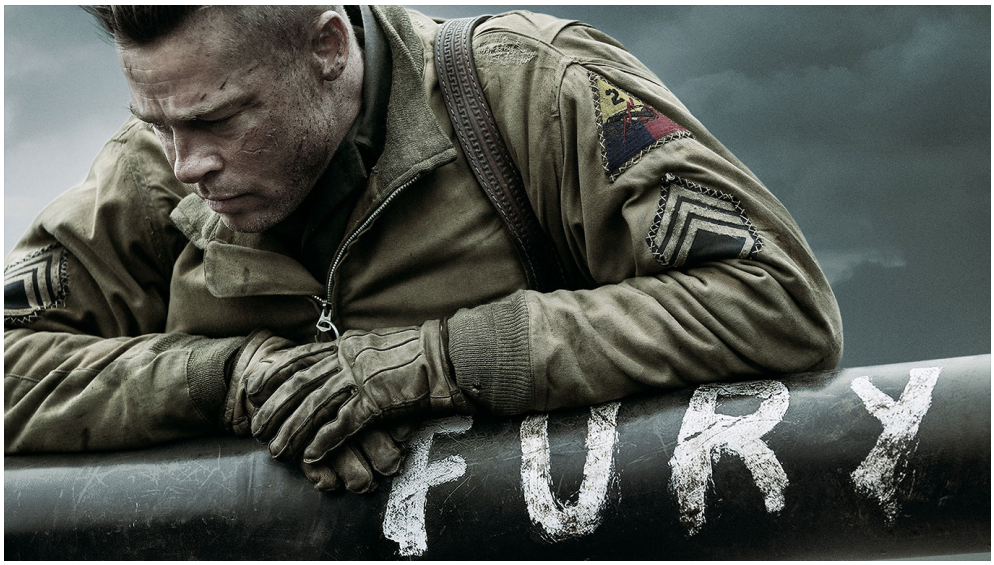
Simplicité, le confort pratique avant tout
Dès que vous invitez des utilisateurs à s'identifier, il faut que la procédure soit pratique et transparente. Notre étude montre que 59,4 % des adultes britanniques se connectent à leurs sites préférés via leur profil sur des réseaux sociaux pour gagner du temps et éviter d'en perdre à devoir remplir des formulaires.
Et plus ces consommateurs utiliseront des terminaux mobiles, plus ils chercheront à éviter les processus d'authentification longs et alambiqués pour s'inscrire et se connecter à des sites Web et à des applications. Ceux d'entre vous qui se sont arraché les cheveux à se remémorer leur mot de passe d'accès à un site se reconnaissent probablement dans les 62 % de consommateurs qui ont quitté un site Web faute d'avoir pu retrouver leur identifiant et/ou mot de passe.

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

Source : http://www.journaldunet.com/ebusiness/expert/59273/utilisation-des-donnees-en-ligne–les-consommateurs-reclament-transparence–pertinence-et-simplicite.shtml par Patrick Sayler – Directeur Général, GIGYA

Sony : plusieurs films

piratés avant même leur sortie dans les salles



Sony : plusieurs films piratés avant même leur sortie dans les salles

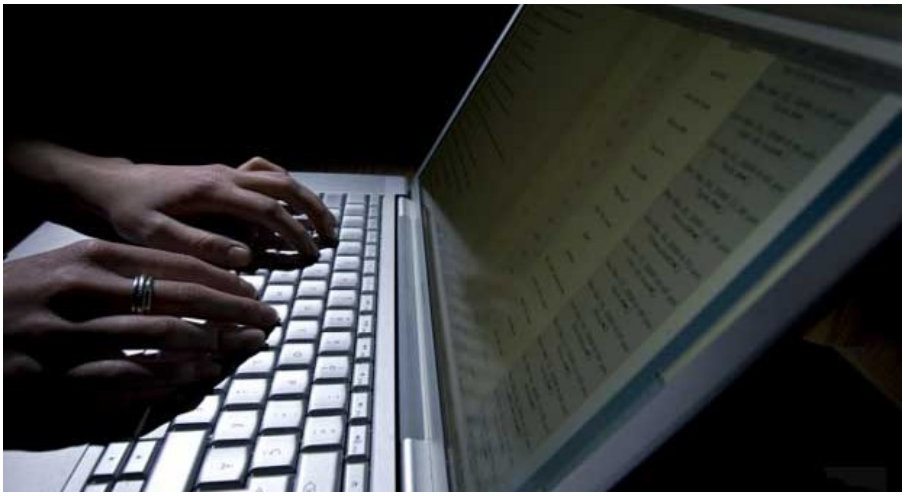
Victime d'une attaque informatique d'envergure, Sony Pictures a vu ses activités tourner au ralenti la semaine dernière. Dimanche, des hackers publiaient plusieurs copies des grosses productions à venir sur la toile, compromettant le lancement de plusieurs films.

Victime de plusieurs attaques informatiques la semaine passée, l'intranet de Sony Pictures est tombé peu après que la sécurité de l'un des serveurs de la firme ait été compromise. Les hackers, qui ont pénétré dans le système, ont menacé Sony Pictures de diffuser les dernières superproductions de Sony sur la toile si le distributeur ne répondait pas aux exigences des pirates, lesquelles n'ont pas été dévoilées publiquement.
Dimanche, le groupe de pirates menait ses menaces à exécution en diffusant plusieurs copies de films récents ou à venir comme Fury, Annie, Mr. Turner ou encore Still Alice, en version DVD.
En quelques heures, Fury, le dernier film de Brad Pitt, était déjà le second film le plus téléchargé sur Pirate Bay.
La diffusion de ces copies DVD de films pas encore sortis ou tout juste disponibles dans les salles est une grande première sur la toile. Si plusieurs films ont déjà fait les frais d'une diffusion à grande échelle avant leur sortie, comme The Expendables 3 ou X-Men, c'est la première fois que tout le catalogue de films d'un distributeur est diffusé simultanément. Un fiasco qui pourrait bien sûr affecter les résultats de Sony Pictures au cours des prochains mois mais aussi pousser les distributeurs à investir davantage dans la sécurité informatique.
Le distributeur, qui a très peu communiqué sur le piratage de son intranet, a réagi à la diffusion de son catalogue de films sur Pirate Bay en évoquant un "crime". Elle a également indiqué travailler avec les forces de l'ordre pour retrouver les auteurs des attaques.

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

Source : http://geeko.lesoir.be/2014/12/01/sony-plusieurs-films-pirates-avant-meme-leur-sortie-dans-les-salles/

Le nombre d’incidents de sécurité informatique a augmenté de 48% en 2014 !



Le nombre d’incidents de sécurité informatique a augmenté de 48% en 2014 !

D’après l’enquête The Global State of Information Security Survey, le nombre d’incidents de sécurité informatique dans le monde a augmenté de 48 % cette année.

C’est à l’instigation de PwC, CIO et CSO que le sondage The Global State of Information Security Survey a été réalisé auprès 9700 chefs de direction et gestionnaires en finances, en informatique et en sécurité informatique dans le monde, 35% en Amérique du Nord, 34% en Europe, 14% de l’Asie-Pacifique, 13% d’Amérique du Sud et 4% du Moyen-Orient et d’Afrique.

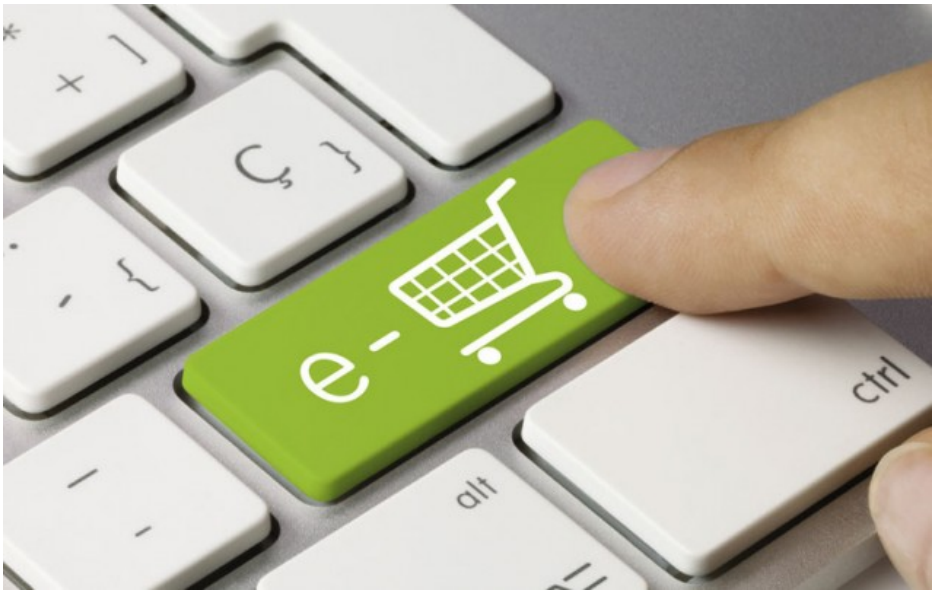
Publiés ce jeudi, les résultats sont que le nombre d’incidents de sécurité informatique à l’échelle internationale a augmenté de 48% en 2014 pour atteindre près de 43 millions d’incidents, soit un peu plus de 117 000 attaques par jour.

Alors que ce chiffre donne déjà des frissons, il est estimé que plus de 70% des incidents informatiques ne sont pas détectés en raison des méthodes de plus en plus sophistiquées qui sont utilisées par leurs auteurs.
Ce constat a vraiment de quoi inquiété vu qu’il est estimé que le coût global de la cybercriminalité cette année dépasse les 23 milliards de dollars, et cela uniquement pour les incidents détectés. Le coût global réel des atteintes à la sécurité informatique est « impossible à établir » selon les auteurs de l’enquête. En soulignant qu’il est particulièrement difficile de chiffrer la valeur de certains types d’informations, par exemple la propriété intellectuelle et les secrets commerciaux.
L’enquête révèle par ailleurs qu’un tiers des incidents sont imputables aux employés, un autre tiers aux ex-employés et un quart aux pirates informatiques. Les attaques des États, le crime organisé et de la concurrence font partie des incidents les moins fréquents.

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

Source : http://www.linformatique.org/le-nombre-dincidents-de-securite-informatique-augmente-de-48-en-2014/

Sites e-commerce: Le contrôle commence



Sites e-commerce: Le contrôle commence

Seulement 22% des sites web affichent une mention relative à la protection des données personnelles conforme aux exigences de la loi.

Le gendarme de l'e-commerce a commencé ses opérations de contrôle. La Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), la CNIL au Maroc, a passé sous la loupe plusieurs catégories de sites web.

Des sites d'annonces, voyage et hôtellerie, cabinets de recrutement et emploi, vente en ligne, deals, marketing, organismes publics, organismes de prévoyance sociale, jusqu'aux concessionnaires de services publics, en passant par l'immobilier, les banques et les sociétés de financement, les assurances, le transport et logistique, la santé, les télécoms et même la location de voitures. Cette opération de contrôle a montré que seulement 22% des sites web au Maroc affichent une mention relative à la protection des données personnelles conforme aux exigences de la loi. «La mention est présente, mais incomplète dans 28% des cas», a indiqué la CNDP qui a mené cette première campagne de contrôle, précisant que 50% des sites contrôlés n'affichent pas de mention relative à la protection des données à caractère personnel.
Les résultats du contrôle, publiés en septembre dernier, démontrent que «très peu de sites web au Maroc, à peine 1%, se soucient de recueillir le consentement des internautes à collecter et traiter leurs données personnelles. Dans 80% des cas, le site web n'évoque nulle part la demande de consentement, et dans 19% des cas, la présence de la demande est aléatoire, puisqu'elle ne figure pas sur la totalité des formulaires de collecte des données», selon la CNDP.
L'opération de contrôle de la CNDP montre que l'obligation d'informer les personnes concernées au moment de la collecte de leurs données personnelles dans les termes prévus par la loi est très rarement respectée avec 1%.
Une lettre, accompagnée de la fiche de synthèse et du document, a été adressée aux responsables de traitement, afin de les inviter à procéder à la mise en conformité de leur site web, selon la CNDP. Et à l'expiration du délai fixé par la Commission, les sites web seront à nouveau contrôlés afin de permettre à la CNDP de prendre les mesures légales qui s'imposent. Il s'agit notamment de la relance du responsable du traitement, la mise en demeure et, en l'absence d'une réponse positive, l'ouverture d'une procédure disciplinaire qui pourrait déboucher sur un avertissement, un avertissement public, un blâme, ou même le transfert du dossier à la justice.
Créée par la loi n° 09-08 du 18 février 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, la CNDP est chargée de vérifier que les traitements des données personnelles sont licites, légaux et qu'ils ne portent pas atteinte à la vie privée, aux libertés et droits fondamentaux de l'Homme. Cette loi a pour objectif de doter l'arsenal juridique marocain d'un instrument juridique de protection des particuliers contre les abus d'utilisation des données de nature à porter atteinte à leur vie privée, et d'harmoniser le système national de protection des données personnelles à celles de ses partenaires, tel que défini par les instances européennes.
Pour mieux protéger les internautes, la loi n° 09-08 du 18 février 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel a prévu des sanctions. Ainsi, et sans préjudice de la responsabilité civile des personnes ayant subi des dommages du fait de l'infraction, est puni d'une amende de 10.000 à 100.000 dirhams quiconque aura mis en œuvre un fichier de données à caractère personnel sans la déclaration ou l'autorisation exigée ou aura continué son activité de traitement de données à caractère personnel malgré le retrait du récépissé de la déclaration ou de l'autorisation.

Aussi, est puni d'une amende de 20.000 à 200.000 dirhams par infraction, tout responsable de traitement de données à caractère personnel refusant les droits d'accès, de rectification ou d'opposition. La loi n° 09-08 a également prévu une peine d'emprisonnement de trois mois à un an et d'une amende de 20.000 à 200.000 dirhams ou de l'une de ces deux peines seulement, quiconque effectue un transfert de données à caractère personnel vers un Etat étranger.

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

Source :
http://www.aujourdhui.ma/geeks/nouvelles-technologies/sites-e-commerce-le-controle-commence-114695#.VHxhLNKG8t4
Par Atika Haimoud