

Le PSN inaccessible suite à une attaque de Lizard Squad

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<h2>Le PSN inaccessible suite à une attaque de Lizard Squad</h2>
<p>Depuis quelques heures, le PlayStation Network de Sony est inaccessible pour de nombreux utilisateurs. Il s'agirait visiblement d'une nouvelle attaque DDOS, revendiquée par le groupe Lizard Squad.</p> <p>Les problèmes touchent principalement l'Amérique du Nord, mais d'autres joueurs dans le monde ont remarqué quelques soucis depuis le milieu de la nuit. PlayStation a rapidement tenu informé ses joueurs via Twitter, sans toutefois donner trop d'informations. On ne sait donc pas vraiment quand seront réglés ces soucis, mais on sait au moins que les équipes de Sony travaillent à régler le problème, et c'est déjà une bonne nouvelle. Le groupe Lizard Squad a revendiqué cette attaque, et c'est donc visiblement le serveur d'authentification de Sony qui est visé (comme l'indique ce tweet https://twitter.com/LizardPatrol/status/541751366297743360), perturbant ainsi grandement le PSN. Espérons que tout rentrera dans l'ordre rapidement, puisque ces problèmes répétés risquent fortement d'agacer les joueurs.</p> <p>Après cette lecture, quel est votre avis ? Cliquez et laissez-nous un commentaire..</p> <p>Source : http://www.gameblog.fr/news/47390-le-psn-inaccessible-suite-a-une-attaque-de-lizard-squad</p>	

SONY : Connexion impossible au PSN



SONY
impossible Connexion
au PSN

Déjà responsable de la paralysie des serveurs du Xbox Live sur Xbox One et Xbox 360 dernièrement, le groupe de hacker Lizard Squad semble de nouveau être en train de complètement faire disjoncter le PSN, causant des messages de connexion impossible sur PS4, PS3 et PS Vita en ce lundi 8 décembre 2014. En effet, les joueurs se plaignent un peu partout de ne plus pouvoir jouer en ligne sur leur console PlayStation, et de ne plus avoir accès au PSN.

Il y a peu de temps, Lizard Squad avait annoncé une campagne visant à complètement mettre à terre les services online de Microsoft et Sony le jour de Noël 2014, et est déjà responsable de plusieurs épisodes de paralysie du PSN et du Xbox Live ces dernières semaines. Prendre en otage le PSN aujourd'hui même, alors que Sony est en pleine PlayStation Experience est-il un message d'avertissement aux deux constructeurs ? Difficile à dire, d'autant que rien n'est jamais demandé en retour. C'est alors les joueurs qui se retrouvent pénalisés avec des connexions impossible au PSN et Xbox Live. Cependant, dans l'ombre, Anonymous souhaite ne pas en rester là, et menace à son tour Lizard Squad dans une vidéo postée sur internet il y a deux jours, disponible ci-dessous.

Bien entendu, il est toujours assez délicat d'accorder de la légitimité aux nouvelles vidéos d'Anonymous, tant ce groupe est volatile, et peut être représenté par n'importe qui. Vont-ils essayer de voler dans les plumes d'un Lizard Squad qui multiplie les actions pour mettre à terre les services online de la PS4 et de la Xbox One régulièrement ? De son côté, Sony avoue être en ce moment même au travail pour rétablir les connexions à son PSN. Nous vous tiendrons bien entendu au courant de la situation, dans notre colonne d'actualité jeux vidéo, comme toujours.

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

Source :
<http://playerone.tv/news/v/6234/connexion-impossible-au-psn-lizard-squad-ddos-encore-les-services-playstation.html>

Live streaming illégal : Le revers de la médaille



vous informe...

Live streaming illégal : Le revers de la médaille :

Si depuis l'aube d'Internet, les sites pornographiques constituent le vecteur principal de propagation de virus sur la toile, les sites illégaux de live streaming représentent une concurrence de taille. Selon l'étude de l'AISP, alors que 97 % des sites de streaming illégaux sont infectés par des malwares (logiciels malveillants), faisant de cette pratique la voie d'infection la plus courante sur Internet, les plateformes illégales de live streaming représentent une grande partie de ces infections. Au point de devenir une véritable porte ouverte à la fraude et au vol de données.

Le streaming vidéo, qui constitue aujourd'hui 91 % du trafic Internet mondial, est depuis quelque temps déjà ancré dans le paysage virtuel mondial. Son pendant « en direct », le live streaming, est quant à lui entré dans les mœurs il y a peu. Développées en 2008 par des entreprises comme Youtube ou Google, les technologies permettant le visionnage et le partage de vidéos en direct sur Internet ont plus ou moins stagné depuis. Il faudra attendre la Coupe du monde de football 2014 au Brésil pour démocratiser la pratique dans le monde entier, mais surtout pour voir un véritable marché noir du live streaming se développer en parallèle. Du 12 juin au 13 juillet dernier, plus de 20 millions de personnes à travers le monde ont regardé les matches de la Coupe du monde en live streaming sur des sites illégaux.

Une question d'informations

Leur gratuité, si elle a permis à ces sites de se démocratiser, est aussi la cause principale de l'émergence des pirates dénoncée par l'AISP. Comme n'importe quelle marchandise ou service, un site peut être gratuit soit parce qu'il bénéficie de subventions ou de dons – une hypothèse peu probable pour les sites illégaux de live streaming – soit parce qu'il a minoré ses investissements dans son développement, le plus souvent au détriment de sa sécurité.

Faire sauter les pare-feu des sites illégaux de live streaming est ainsi bien souvent un jeu d'enfants pour pirates et hackers. Toujours selon ce rapport de l'AISP, certains d'entre eux vont même jusqu'à créer et développer leurs propres sites de live streaming illégal, infectés et porteurs de chevaux de Troie dès leurs créations, afin d'augmenter leurs chances d'attraper un internaute dans leur toile. Ainsi, alors que 160 000 nouveaux malwares sont créés par jour, les sites illégaux de live streaming ont envahi les moteurs de recherche et représentent une pierre de plus à l'édifice de menaces que constitue Internet aujourd'hui.

La toile est en effet souvent pointée du doigt comme la source de dangers toujours plus nombreux et variés. Des accusations parfois exagérées qui ne doivent pas faire oublier la responsabilité de l'internaute. Pour Anton Korobkov-Zemlianski, un membre de la commission de la science et des innovations de la Chambre publique de Russie, également expert en médias, Internet « présente moins de dangers que d'autres objets que nous utilisons. Les voitures causent la mort de beaucoup plus de monde qu'Internet (...) Beaucoup commencent à voir dans Internet une panacée appelée à simplifier leur vie. Le web ne simplifie pas notre vie, il crée des conditions nouvelles et exige que les gens changent et évoluent ».

Une réglementation comme le Code de la route est cependant impossible à mettre en place sur la toile, l'anonymat étant à la portée de tous sur Internet. La diffusion de l'information et la responsabilisation des usages apparaissent alors comme la plus fiable des solutions. Et tandis qu'il suffit d'ajuster son comportement aux risques et aux menaces d'Internet, « il vaut mieux prévenir que guérir » n'a jamais été aussi adapté.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.generation-nt.com/live-streaming-illegal-donnees-actualite-1909470.html>
par Julien Hatier

Après le piratage, les employés de Sony reçoivent un email de menaces – L'Express avec L'Expansion



Après le
piratage,
les
employés de
Sony
reçoivent
un email de
menaces –
L'Express
avec
L'Expansion

Une semaine après s'être fait pirater, la société Sony Pictures a indiqué que ses employés avaient reçu un email de menaces d'un groupe de pirates informatiques. Le FBI enquête sur le dossier.

Les attaques viennent de toutes parts. Des employés de Sony Pictures, qui a fait l'objet la semaine dernière d'une attaque informatique massive, ont reçu un email de menaces qui se dit être du groupe de pirates informatique GOP (« Guardians of Peace ») a indiqué un porte-parole de la société américaine. Il assure par ailleurs être « au courant du problème et travailler avec les forces de l'ordre ». Le FBI, la police fédérale américaine, enquête sur le dossier.

Les familles des employés aussi menacées

L'attaque informatique, qui s'est traduite par le vol de données personnelles d'employés de Sony, dont leurs adresses, dates de naissance et numéro de sécurité sociale, et la mise en ligne illégalement de cinq films du studio, a touché quelque 47 000 personnes, selon des experts informatiques.

L'email adressé aux employés est reproduit par Variety. Il ordonne à son destinataire d'envoyer son nom à une adresse email « si vous ne voulez pas faire l'objet de représailles ». « Si vous ne le faites pas, non seulement vous mais votre famille serez en danger », précise le message.

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

Source

http://lexpansion.lexpress.fr/high-tech/apres-le-piratage-les-employes-de-sony-recoivent-un-email-de-menaces_1629800.html :

L'attaque informatique de Sony Pictures a touché 47.000 personnes

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<h2>L'attaque informatique de Sony Pictures a touché 47.000 personnes</h2>
---	--

Les pirates informatiques responsables de la cyberattaque géante de Sony Pictures ont dévoilé des informations confidentielles de 47.000 individus dont des personnalités, ont affirmé vendredi des experts en sécurité informatique.

Les noms, adresses, numéros de sécurité sociale et dates de naissance ont ainsi été dérobés, autant d'informations permettant des usurpations d'identité, selon la société Identity Finder.

« Le plus inquiétant est le nombre très élevés de copies des numéros de sécurité sociale retrouvés dans les dossiers que nous avons analysés », a fait remarquer le président de cette société, Todd Feinman.

Il a précisé que ces numéros apparaissaient dans plus de 400 documents différents, « offrant aux pirates la possibilité de causer davantage de dégâts ». Selon lui, quelques 15.000 personnes, actuels ou anciens employés de Sony, ont eu leur numéro de sécurité sociale dérobé.

Sony Pictures a confirmé cette semaine avoir été victime d'un vol « très important de données confidentielles » fin novembre. En plus de ces informations confidentielles, cinq films, y compris des films pas encore sortis, avaient été piratés.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source :

<http://www.jeanmarcmorandini.com/article-329895-l-attaque-informatique-de-sony-pictures-a-touche-47000-personnes.html>

Le porno devient le 6e usage depuis un smartphone

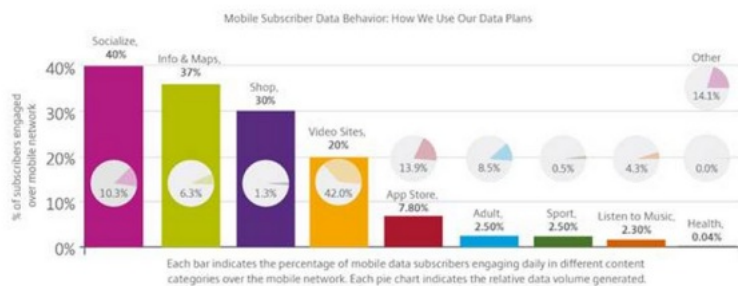


Le porno devient le 6e usage depuis un smartphone

Si les réseaux sociaux et l'information sont en tête des usages, les contenus « pour adultes » se classent devant la musique et la santé, selon une étude de Citrix.

Une nouvelle étude sur les usages depuis un smartphone confirment les grandes tendances que l'on connaissait déjà. Ainsi, selon le dernier rapport de Citrix sur la question (basé sur le trafic 3G/4G dans le monde), les abonnés utilisent principalement leurs terminaux pour se connecter aux réseaux sociaux (40%), pour s'informer et consulter des cartes (37%) et réaliser des achats en ligne (30%).

Derrière ce trio inamovible, on trouve la consommation de vidéos (20%), les visites dans les app stores (7,8%) et désormais les contenus adultes qui se hissent à 2,5% des mobinautes, et qui passent devant la musique (2,3%).



Si cette part peut paraître marginale, le trafic généré l'est beaucoup moins. Toujours selon Citrix, le porno représente 8,5% du trafic, contre 4,3% pour la musique ou 13% pour le shopping. Dans ce domaine, la vidéo représente 42% des données mobiles générées.



Le spécialiste confirme également que le très haut débit mobile (4G) incite à consulter des contenus riches. « Il y a 1,5x plus de requêtes de vidéos sur les réseaux 4G que sur les réseaux 3G. La résolution des vidéos mobiles augmente de 20% sur les réseaux 4G par rapport à la 3G. Cela implique une augmentation du nombre de données générées, 5x plus élevé sur les réseaux 4G que sur la 3G », peut-on lire.

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

Source :

<http://www.zdnet.fr/actualites/le-porno-devient-le-6e-usage-depuis-un-smartphone-39805969.htm>

Sécurité des données : Quid des risques liés aux nouveaux usages ?

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p>  <p>vous informe...</p>	<p>Sécurité des données : Quid des risques liés aux nouveaux usages ?</p>
---	---

Une étude Hiscox/IFOP révèle que si 3/4 des actifs interrogés se considèrent bien sensibilisés à la protection des données professionnelles, une majorité d'entre eux ont toujours des pratiques risquées... Pourquoi ?

C'est un fait, les appareils mobiles sont complètement intégrés au sein des entreprises et les frontières entre le professionnel et le privé s'en trouvent fortement diminuées. Qu'en est-il de la sécurité des données des entreprises ? Hiscox s'est interrogé sur le sujet avec l'institut IFOP et les résultats sont pour le moins surprenants !

La sécurité des entreprises est exposée

Les salariés équipés d'au moins un appareil mobile professionnel sont les plus concernés par ces pratiques risquées puisqu'ils sont 77% à déclarer transporter des fichiers professionnels sur une clé USB ou un disque dur externe (contre 63% pour l'ensemble) et la moitié partage des fichiers en ligne via un service de cloud (contre 39% pour l'ensemble). 54% estiment que le partage de fichiers via le cloud n'a pas d'incidence sur la sécurité.

Si les salariés des petites structures sont les mieux équipés en appareils mobiles, ce sont ceux qui utilisent le plus leur matériel professionnel à titre personnel. 82% des salariés de ces entreprises se connectent à Internet au moins une fois par semaine pour des raisons personnelles à partir de leur appareil professionnel.

Des techniques de sécurisation non adaptées

Mais ce n'est pas tout ! Pour assurer leur protection, 9 entreprises sur 10 s'appuient sur un mot de passe. Et là, tout commence, 18% des actifs doivent changer leur mot de passe tous les mois alors que 34% déclarent devoir le changer moins de 2 fois par an. Quant à l'élaboration du mot de passe, 70% des entreprises imposent au moins une règle à leurs salariés pour le choix du mot de passe, on arrive à 51% dans les structures de moins de 10 salariés.

Parmi les autres techniques, 35% des actifs interrogés déclarent disposer d'outils de cryptage des données mais 22% ne savent pas s'ils peuvent bénéficier de cette technique dans leur entreprise.

Enfin, 63% laissent leur ordinateur allumé lorsqu'ils quittent le bureau en fin de journée ou ne le verrouillent pas en quittant leur poste.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source

<http://www.itpro.fr/n/securite-donnees-quoi-risques-lies-nouveaux-usages-20899/>

Attention, la CNIL contrôle votre site Web sans vous en informer et rédige des PV

 **Attention, la CNIL contrôle votre site Web sans vous en informer et rédige des PV**

La CNIL peut désormais contrôler des sites web hors la présence de l'organisation concernée. Le responsable du traitement n'est informé qu'après coup. En octobre dernier, la CNIL a publié le mode d'emploi pour ce nouveau type de contrôle. Analyse de Bénédicte Querenet-Hahn, associée, et Grit Karg, collaborateur au sein du cabinet d'avocats GGV.

La loi du 17 mars 2014 relative à la consommation, également appelée loi Hamon, a introduit à l'article 44 de la loi Informatique et Libertés un nouveau mode de contrôle. Elle prévoit que la CNIL procède à toute constatation utile, en dehors des contrôles sur place et sur convocation.

Les données imprudemment accessibles

La CNIL peut à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations.

La CNIL n'a pas besoin de se déplacer pour effectuer le contrôle, qui peut être effectué sans que l'organisme contrôlé en ait connaissance, à tout moment, et sans que le responsable des locaux puisse s'y opposer.

Procès verbal

Une fois un contrôle effectué, la CNIL rédigera un procès-verbal factuel décrivant la méthodologie appliquée et précisant l'environnement technique du contrôle ainsi que les éléments vérifiés. Ce procès-verbal sera ensuite adressé au responsable du traitement qui disposera alors d'un délai fixé par la CNIL afin de faire part de ses observations.

Un contrôle à distance peut être combiné avec tout autre moyen dont dispose la CNIL, telles que les auditions ou visites. En cas d'infraction à la réglementation constatée, un contrôle en ligne peut donner lieu à une mise en demeure ou, le cas échéant, à l'ouverture d'une procédure de sanction.

Finalités de la collecte de données

Les vérifications en ligne portent notamment sur la pertinence des données collectées au regard des finalités pour lesquelles elles sont collectées, les mentions obligatoires relatives à la collecte de données à caractère personnel, la sécurité des données collectées et traitées, le respect des formalités déclaratives auprès de la CNIL.

Selon la CNIL, un accent est également mis sur la vérification du respect des règles relatives aux « cookies » et à d'autres traceurs. La CNIL vérifiera le nombre et la nature des cookies déposés sur le poste informatique de l'internaute, les modalités d'information à destination du public en matière de cookies, la qualité et la pertinence de l'information et les modalités de recueil du consentement de l'internaute.

Répression des fraudes

Par ailleurs, la loi Hamon renforce la coopération de la CNIL avec les agents de la DGCCRF (la direction générale de la concurrence, de la consommation et de la répression des fraudes). Tout manquement constaté par l'autorité sera en effet transmis à la CNIL pour qu'elle puisse prendre les mesures nécessaires.

La communication systématique d'informations entre la CNIL et la DGCCRF a déjà été mise en place dans le domaine du e-commerce par la signature, le 6.1.2011, d'un protocole de coopération afin d'améliorer l'échange d'informations relatif à la protection des données personnelles.

Eviter tout risque de sanction

Au regard de ce renforcement des moyens de contrôles et de la volonté affichée de la CNIL de vérifier systématiquement les sites web, il appartient aux marchands s'assurer de la conformité de leurs sites avec la réglementation en vigueur, afin d'éviter tout risque de sanction.

Pour en savoir plus, nous vous recommandons notre article « Nouvelles exigences de la loi Hamon – Comment mettre à jour votre site e-commerce » : http://www.francoallemand.com/fileadmin/ahk_frankreich/Dokumente/recht/publications-droit/DF/4-2014-F-D-Nouvelles-exigences-de-la-loi-Hamon.pdf.

Contrôles dans l'entreprise

Pour rappel, selon l'article 44 de la loi Informatique et Libertés, les agents de la CNIL sont habilités à effectuer des contrôles au sein des entreprises. Ces contrôles sont en général réalisés suite à une plainte auprès de la CNIL et en présence d'une personne responsable des locaux, éventuellement assisté d'un conseil.

Le responsable des locaux doit par ailleurs être informé de son droit d'opposition à la visite. En cas d'exercice de ce droit, la visite ne peut avoir lieu qu'avec l'autorisation du juge des libertés et de la détention du TGI (Tribunal de Grande Instance) compétent. En cas d'urgence toutefois ou de risque de destruction de documents, la CNIL peut procéder à la visite, sur l'autorisation du juge, sans que l'entreprise ne puisse s'y opposer.

Lors de tels contrôles, la CNIL peut demander la communication de tous les documents nécessaires, en prendre copie, recueillir tout renseignement utile, et accéder aux programmes informatiques et aux données.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.larevuedudigital.com/2014/12/expert/attention-la-cnil-controle-votre-site-web-sans-vous-en-informer/>

74% des réseaux domestiques français sont fortement exposés à la cybercriminalité



74% des réseaux domestiques français sont fortement exposés à la cybercriminalité

Près de trois ménages français sur quatre connectés à internet sont susceptibles d'être victimes d'une cyberattaque via leur routeur sans fil, estime Avast Software, qui vient de publier une étude sur ce domaine. La vulnérabilité des routeurs et la faiblesse des mots de passe permettent aux pirates informatiques d'accéder facilement aux réseaux domestiques.

« Les routeurs non-sécurisés sont des points d'entrée très faciles d'accès pour les hackers, qui sont dès lors capables de pirater des millions de réseaux domestiques en France, déclare Vince Steckler, Directeur Général d'Avast. Notre enquête révèle que la vaste majorité des routeurs domestiques en France ne sont pas sécurisés. Et si un routeur n'est pas correctement sécurisé, un cybercriminel pourra facilement accéder aux informations personnelles d'un particulier, comme par exemple à ses données financières, ses identifiants et mots de passe, ses photos et son historique de navigation. »

D'après l'étude, plus de la moitié des routeurs seraient mal sécurisés par défaut ou ne seraient équipés d'aucune protection, avec des combinaisons login/mot de passe beaucoup trop évidentes telles que admin/admin ou admin/mot de passe, voire admin/. Au terme de cette enquête réalisée auprès de plus de 20 000 ménages en France, Avast met également en avant que 24% des consommateurs utilisent comme mot de passe leur adresse, leur nom, leur numéro de téléphone, le nom de leur rue ou d'autres mots faciles à deviner.

L'un des principaux risques auxquels un réseau Wi-Fi est exposé est le piratage du système de noms de domaine (DNS). Les logiciels malveillants sont utilisés pour exploiter les failles de sécurité d'un routeur insuffisamment protégé et pour rediriger subrepticement l'utilisateur depuis un site connu, comme par exemple un site web bancaire, vers une fausse page identique à l'original. Lorsque l'utilisateur s'y connecte, le pirate peut ainsi capturer ses identifiants et les utiliser pour accéder à son compte sur le véritable site.

« Le manque de sécurisation actuel au niveau des routeurs rappelle fortement la situation des PC dans les années 1990, où les tendances laxistes des utilisateurs en matière de sécurité et l'explosion du nombre de menaces avaient rendu les environnements informatiques largement exploitables. La grande différence, c'est que les utilisateurs stockent aujourd'hui bien plus d'informations personnelles sur leurs appareils qu'ils n'en avaient auparavant. Les consommateurs ont besoin d'outils à la fois simples d'utilisation et capables de prévenir toute cyberattaque ciblant leurs données », explique Vince Steckler.

Toujours selon le sondage, moins de la moitié des français interrogés sont persuadés que leur réseau privé est sécurisé, tandis que 20% d'entre eux déclarent avoir déjà été victimes d'un pirate informatique. Les participants précisent être pleinement conscients de la gravité des conséquences d'une faille de sécurité, et confient que leurs principales craintes concernent le vol de leurs données bancaires ou financières (34%), la perte de leurs informations personnelles (34%), le piratage de leurs photos (17%) et le vol de leur historique de navigation (13%).

Afin de répondre à ces problèmes, Avast a récemment lancé Avast 2015, qui inclut la première solution de sécurisation de réseaux privés (Home Network Security), capable de protéger les utilisateurs face au piratage des réseaux domestiques, tant au niveau du système de noms de domaine que dans le cas de mots de passe trop simples. Avast 2015 est disponible gratuitement et en version payante via www.avast.com.

L'« internet des objets » est présent dans les ménages français : 96% des ménages français possèdent six appareils ou plus connectés à un réseau Wi-Fi. En marge des ordinateurs de bureau et portables, les utilisateurs possèdent des appareils mobiles (28%), des imprimantes et scanners (18%), des Smart TV (5%), et des lecteurs DVD ou Blu-ray (3%) connectés à leur réseau Wi-Fi.

Les utilisateurs craignent que des « espions » ne se cachent dans leur voisinage, mais certains aiment aussi épier les autres : 60% des répondants seraient très mal à l'aise s'ils apprenaient qu'un voisin ou une tierce personne se connecte en cachette à leur réseau Wi-Fi privé. 5% indiquent avoir eux-mêmes déjà utilisé le réseau Wi-Fi d'un voisin sans le lui avoir signalé ou lui en avoir demandé la permission...

Malgré leurs inquiétudes, les utilisateurs manquent de clairvoyance en matière de protection : 23% des répondants ignorent s'ils disposent d'une solution de protection sur leur réseau domestique, alors que 12% sont sûrs de ne pas en posséder une seule. 25% des personnes interrogées utilisent toujours le même nom d'utilisateur et le même mot de passe, aussi bien pour leur routeur que sur les sites web protégés par mot de passe. 34% ont conservé le mot de passe par défaut de leur routeur, tandis que 6% des utilisateurs sont incapables de répondre à cette question. Seuls 38% ont pris des mesures supplémentaires pour protéger leur réseau, en marge de leur pare-feu de base.

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

Source :

<http://www.lavienumerique.com/articles/152544/74-reseaux-domestiques-francais-sont-fortement-exposes-cybercriminalite.html>

Les Français demandent des boutiques et des vendeurs connectés

x	Les Français demandent des boutiques et des vendeurs connectés
---	--

Les magasins doivent-ils accélérer leur transformation numérique ? Selon cette étude d'OpinionWay, les Français sont agacés par le manque de connaissance client et les lacunes des vendeurs sur le conseil.

Le b.a.-ba de la relation-client est de reconnaître les personnes qui ont déjà acheté dans sa boutique, et quels produits. La pratique est répandue dans les petits commerces auprès de la clientèle la plus fidèle. Elle l'est aussi, de façon moins chaleureuse, sur les sites e-commerce, notamment grâce aux cookies. Toujours est-il que lorsqu'on fait une moyenne, les consommateurs regrettent de ne pas être reconnus en boutique.

Extrait du film Minority Report

Ce constat est fait par OpinionWay au travers d'une étude auprès d'un millier de personnes pour le vendeur de meubles en ligne Miliboo – précisons que ce dernier a lancé cet automne une boutique ultra-connectée à Paris. Selon cette étude, tout juste 13% des consommateurs interrogés ont ainsi le sentiment que les magasins se souviennent des problèmes qu'ils ont rencontrés lors de leurs derniers achats, 22% pensent que les magasins se rappellent de la dernière fois qu'ils sont venus et 24% ont l'impression que les magasins les connaissent.

« Les Français attendent des vendeurs plus d'implication. Il est important pour eux qu'ils puissent répondre à leurs questions immédiatement, sans hésitation ni délais », argumente Aline Buscemi, co-fondatrice de miliboo.com. Les consommateurs attendent également « un service toujours plus poussé et personnalisé ».

Avoir un meilleur conseil

Autre constat : six Français sur dix veulent gagner du temps en boutique – cet argument est souvent avancé par les personnes préférant acheter sur Internet. Plus de six personnes sur dix demandent une accélération du passage en caisse, et près de huit sur dix aimeraient récupérer en boutique un achat effectué en ligne.

Les trois quarts, enfin, voudraient connaître l'état des stocks des magasins en temps réel afin d'éviter de se déplacer pour rien. C'est dans cette optique que des sites de Web-to-store comme Socloz se développent.

Dernier constat accablant – et sévère, disons-le – pour les commerçants en dur : les deux tiers des Français interrogés déclarent que les vendeurs ne savent pas donner de conseils en boutique. Ils sont, du reste, 57% à en appeler à un équipement des vendeurs en smartphones ou tablettes afin de pêcher des informations à même de les renseigner. Si bien qu'un Français sur cinq serait même prêt à payer un peu plus cher pour cela.

Visite de la boutique du futur par Cegid
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source :
<http://pro.clubic.com/actualite-e-business/actualite-743139-magasins-connectes-etude.html>