Comment combattre la cyber-violence à l’école ?

Comment combattre la cyber-violence à l’école ?

La cyber-violence en milieu scolaire se développe, au collège comme au lycée. Selon une enquête du ministère de l'éducation nationale, un collégien sur cinq a déjà été la cible d'insultes, d'humiliations et de brimades par SMS ou sur les réseaux sociaux.

Catherine Blaya, professeure en sciences de l'éducation et présidente de l'Observatoire international de la violence à l'école, explique l'existence de ce phénomène et la manière de lutter contre.

Qu'est-ce que la cyber-violence ?
Catherine Blaya : La cyber-violence est une forme de harcèlement réalisé, non plus uniquement dans la cour d'école ou dans la rue, mais par le biais des nouvelles technologies et des réseaux sociaux. Il peut prendre des formes multiples : du détournement de photo à la vidéo humiliante, en passant par des brimades, des moqueries, des intimidations par SMS. La spécificité de ce harcèlement est son caractère public, amplifié par le Web, qui agit ici comme une caisse de résonance.

Avez-vous des exemples concrets de ce type de harcèlement ?
Les victimes que j'ai rencontrées ont fait état de situations diverses. Des filles prises à partie sur leur apparence physique. D'autres qui sont ostracisées par des camarades qui jalousent leur succès ou désirent briser leur popularité. Les revanches à la suite de ruptures sont nombreuses aussi, comme les humiliations pour assurer la position dominante de l'agresseur.

Les filles sont-elles plus souvent visées que les garçons ?
Elles ont 1,3 fois plus de risque d'être victimes que les garçons, car elles ont une plus grande propension à mettre en scène leur corps, en postant des photos d'elles. Cela attire les commentaires malveillants et la raillerie. Soumettre son estime de soi au regard d'autrui, c'est s'exposer au harcèlement.

Le machisme n'est-il pas la cause première ?
Bien sûr ! Un machisme auquel elles participent aussi. En critiquant leurs congénères et en utilisant le même type d'arguments que les garçons. C'est le phénomène du « slut shaming ». Elles se font, elles-mêmes, l'instrument de la domination masculine.

Pourquoi les auteurs de ces violences privilégient-ils le Web ?
Les auteurs ont besoin d'un auditoire, de spectateurs pour leur violence. Ils veulent se venger ou acquérir un statut social au sein d'un groupe. Ils cherchent donc des témoins pour faire du « buzz » et gagner des « like », afin d'asseoir leur popularité. C'est pourquoi il faut pousser les jeunes témoins à intervenir. La cyber-violence ne doit pas être banalisée. Sur les réseaux sociaux, le problème est démultiplié par un effet de viralité. Le danger supplémentaire d'Internet est que l'agresseur qui lance une rumeur sur la Toile ne peut plus la maîtriser après coup, même s'il se rétracte. Le mal est fait pour durer.

Comment réagir face aux agresseurs ?
Il ne faut pas oublier que les agresseurs sont aussi des victimes dans la plupart des cas. C'est pourquoi il est important d'expliquer aux victimes que répondre à la violence par la violence, c'est prendre le risque de devenir soi-même agresseur. Ces derniers sont souvent des jeunes en quête de popularité qui n'ont pas confiance en eux, ou sont dans une détresse psychologique. J'ai récemment eu le cas d'un jeune homme qui après une rupture difficile s'est mis à harceler son ex-compagne.

Au quotidien, comment empêcher ces violences et harcèlement ?
Il faut beaucoup informer sur le rôle primordial des témoins dans la dénonciation de ces violences. L'enquête du ministère de l'éducation nationale indique qu'un collégien sur cinq est concerné par la cyber-violence. Mais selon mes propres études, c'est plutôt 42 % des jeunes qui sont atteints au moins une fois dans l'année. Et près de la moitié d'entre eux sont à la fois victimes en ligne et dans la cour d'école. La majorité de la population collégienne est concernée par le phénomène, en tant qu'auteur, témoin ou victime.

Lire la synthèse : Un collégien sur cinq a été victime de « cyber-violence »
http://campus.lemonde.fr/campus/article/2014/11/27/un-collegien-sur-cinq-a-ete-victime-de-cyber-violence_4530528_4401467.html

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

Source et la suite sur :
http://campus.lemonde.fr/campus/article/2014/12/02/comment-combattre-la-cyber-violence-a-l-ecole_4532343_4401467.html

Cybercriminalité : le jeu en vaut-il la chandelle ?

Crédit Photo : Shutterstock

Cybercriminalité : le jeu en vaut-il la chandelle ?

Faire réaliser une page web factice pour faire du hammeçonnage ne coûte que 150 dollars

Attention, il n'est pas là question de dire qu'être un cybercriminel c'est bien… comme toute activité criminelle elle est punie par la loi avec des amendes et des peines de prison, nous y reviendront. Mais, tout de même, selon une étude Kaspersky, il semblerait que le ratio investissement/gains soit plus qu'intéressant… ce qui explique l'augmentation exponentielle de ce nouveau type de criminalité 2.0 qui ne nécessite plus du tout de courage. Assis tranquillement devant un ordinateur, les criminels n'ont plus rien à voir avec les gangsters des années 30.

Mais avant tout, une petite précision : tous les cybercriminels ne sont pas des hackers… et tous les hackers ne sont pas des cybercriminels. Bon nombre de cybercriminels ne font qu'acheter des logiciels préconçus par des hackers, les « Black Hats »… et il y a des hackers, les « White Hats », qui luttent justement contre ce derniers.

Le vol de données : peu d'investissement pour beaucoup de gain
Les cybercriminels qui ne veulent pas investir beaucoup dans un logiciel malveillant peuvent tout simplement faire du phising (hammeçonnage) de données. Pour 150 dollars, selon Kaspersky Lab, il est possible de se faire créer une page web similaire à celle visée (réseau social, site institutionnel, société…), de l'héberger et d'envoyer des spams (du style « Insérez vos données pour qu'on vous rembourse 450 euros de trop payé sur vos factures » et autres…)

Ce type de campagne de phising est souvent facilement décelable puisque de grossières fautes de grammaire et d'orthographe se glissent dans le texte. Mais malgré tout ça peut rapporter gros : en revendant les données ainsi captées (ne serait-ce que nom, prénom et adresse), le pirate peut toucher 100 dollars par personne touchée… avec 100 personnes touchées, les gains montent en flèche : 10 000 dollars.

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

Source : http://www.economiematin.fr/news-cout-cybrecriminalite-enjeu-gain-piratage-revente-donnees

---

Données personnelles L'Europe prépare sa loi anti-Gafa

Données personnelles L'Europe prépare sa loi anti-Gafa

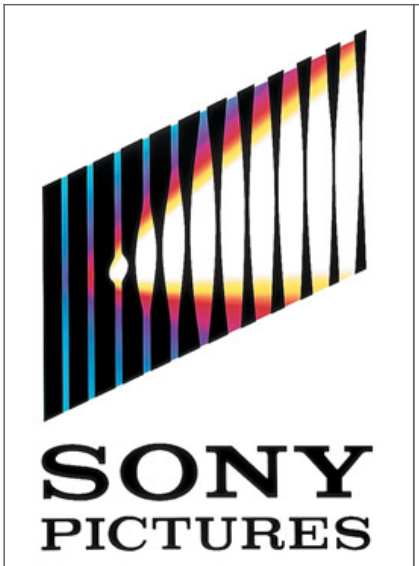
La bataille est relancée entre l'Europe et les géants américains de la Toile. Après la résolution symbolique adoptée par les députés européens pour le démantèlement des activités de Google, Paris et Berlin s'attaquent désormais au référencement payant au sein des moteurs de recherche. Les deux capitales ont adressé un texte à Bruxelles dans lequel ils réclament la création d'une loi pour imposer une plus grande transparence dans l'accès aux sites internet de Facebook, Google, Amazon et Apple, surnommés «GAFA».

Les deux capitales réclament un «traitement transparent et non discriminatoire» des sites. La nouvelle loi, qui sera tout sauf symbolique, ciblera également Facebook qui vient de modifier ses conditions d'utilisation en élargissant l'usage de données personnelles des utilisateurs pour mieux cibler les publicités.
Elle veut rendre le contrôle sur leur vie digitale et leurs données aux utilisateurs et leur redonner la liberté de choix pour l'utilisation d'applications ou de services sur ces plates-formes. Dans un texte adressé à la Commission européenne, les deux capitales, sans jamais citer le nom des sociétés mises en cause, désignées comme les «plates-formes indispensables» de l'Internet, réclament un «traitement transparent et non discriminatoire» des sites. Et ce en référence aux accusations de pratiques anti-concurrentielles dont Google fait l'objet de la part des deux pays. Ainsi, les deux États demandent à Bruxelles de lancer, dès l'année prochaine une consultation publique. Une mesure que la Commission européenne se dite prête à prendre.
Parallèlement, les établissements européens de protection des données personnelles passent eux aussi à la charge. Ils ont publié un ensemble de règles encadrant le droit à l'oubli. Parmi leurs doléances, le groupement réclame l'extension du droit à l'oubli à tous les noms de domaine, y compris en «.com». Le droit à l'oubli ne doit plus seulement concerner les déclinaisons nationales de Google, mais l'universaliser.

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

Source : http://www.leconomiste.com/article/962737-donnees-personnellesl-europe-prepare-sa-loi-anti-gafa par M. L.

Piratage de Sony Pictures : le FBI met en garde contre un malware « destructeur »



Piratage de Sony Pictures : le FBI met en garde contre un malware « destructeur »

Le piratage massif de Sony Pictures Entertainment la semaine dernière a motivé le FBI à tirer la sonnette d'alarme. Le bureau fédéral, qui enquête sur l'affaire, met en garde les entreprises concernant un logiciel malveillant « destructeur » utilisé par les pirates.

De toute évidence, le FBI ne prend pas le piratage de Sony Pictures à la légère. Le bureau fédéral d'investigation a communiqué par voie de presse pour mettre en garde les entreprises contre un nouveau malware. Ce dernier est décrit comme étant « destructeur », et serait à l'origine des déboires de Sony, dont plusieurs films encore inédits aux Etats-Unis ont été mis en ligne dans des versions piratées. Il faut cependant préciser que, dans son rapport d'alerte, le FBI ne cite jamais le nom de Sony. Néanmoins, pour des experts en sécurité interrogés par l'agence Reuters, il ne fait aucun doute que les autorités évoquent bien cette affaire.
Selon le FBI, « il s'agit de la première cyber-attaque destructrice menée contre une entreprise sur le sol américain ». Des manœuvres similaires ont été constatées en Asie et au Moyen-Orient, mais jamais aux USA jusqu'à aujourd'hui.

Concrètement, le logiciel malveillant remplace petit à petit les données présentes sur le disque dur, y compris dans les secteurs d'amorçages qui permettent à l'ordinateur de démarrer. Le système se retrouve donc bloqué, à la merci des pirates qui contrôlent le malware.
« Le FBI conseille régulièrement le secteur privé de divers indicateurs de cyber-menaces observés au cours de ses enquêtes » explique le porte-parole du bureau, Joshua Campbell. « Ces données sont fournies afin d'aider les administrateurs systèmes à se protéger des actions permanentes des cyber-criminels. » Les entreprises victimes de ce type d'attaques sont invitées à contacter les autorités au plus vite.

Du côté de Sony, si un porte-parole a récemment déclaré que l'entreprise avait d'ores et déjà restauré « un certain nombre de services importants », de nombreux documents ont été récupérés par les pirates durant l'intrusion, et pas seulement des films du studio. Des contrats de tournage et des papiers d'identité de certains comédiens font partie des fichiers volés. Quant à l'origine de l'attaque, elle reste toujours à confirmer, même si les soupçons sont tournés vers la Corée du Nord, qui n'aurait pas apprécié la sortie du film « L'Interview qui tue », comédie qui prend pour cible le régime politique du pays.

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

Source :
http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-742501-piratage-sony-fbi-garde-malware-destructeur.html?estat_svc=s%3D223023201608%26crmID%3D639453874_766966538

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

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/