Après le BYOD, voici le WYOD

	Après le BYOD (bring your own device), voici le WYOD

En ce mois de septembre, la principale nouvelle dans le secteur high-tech a été de loin l'annonce de l'Apple Watch. Disponible au début de l'année prochaine, la montre pourrait faire exploser le marché des produits vestimentaires connectés. De quoi développer le Wear Your Own Device (WYOD).

Un phénomène qui pourrait bien se généraliser

La future Apple Watch va-t-elle connaître le succès ? Difficile à dire pour le moment. Ce que nous savons par contre, c'est que de nombreux constructeurs et fabricants misent sur les objets vestimentaires connectés / intelligents. Que ce soit les bracelets sportifs de Nike et Fitbit ou encore les montres de Sony, Samsung, Motorola et bientôt Apple, la mode est au connecté.

En entreprise ou encore dans les établissements scolaires, nous connaissions déjà le BYOD (Bring Your Own Device), le BYOS (Bring Your Own Software) ou encore le BYOPC (Bring Your Own PC). Voici donc le WYOD, Wear Your Own Device. Bien entendu, un tel phénomène est loin d'être encore aussi grand que l'utilisation du smartphone en entreprise. Il n'empêche qu'il faut s'y préparer, car les logiques sont les mêmes.

Dorénavant ou tout du moins d'ici quelques mois ou années, il faudra donc veiller à ce que les montres connectées ne deviennent pas problématiques pour la sécurité des données sensibles de la compagnie. Et nous ne parlons même pas des lunettes connectées de Google qui peuvent être pires encore.

Bientôt invisibles à nos yeux

Les montres connectées ont de cela de spéciales que si l'on n'y prend pas garde, on ne la différenciera pas des autres montres, et donc on ne la remarquera pas. Même logique pour les vêtements connectés ou même les perruques connectées (oui oui). Bien plus difficiles à vérifier qu'un smartphone, une tablette tactile et bien entendu un ordinateur, tous ces nouveaux et futurs produits peuvent devenir le cauchemar des patrons et des DSI s'ils ne prennent pas les dispositions adéquates.

Comme le notait il y a quelques Kevin Noonan, analyste pour Ovum, les produits connectés comme les montres ou les lunettes pouvaient à l'époque paraître bizarres et étaient immédiatement identifiables. Aujourd'hui à force de les voir et de les côtoyer, ils risquent d'être invisibles à nos yeux.

Que faire ? Les interdire ?

Dans certains lieux vraiment sensibles, ce serait peut-être la solution la plus simple. Néanmoins, on a déjà vu que de nombreuses entreprises interdisaient le BYOD, ce qui n'empêchait pas les employés d'apporter leurs propres appareils, en le cachant aux yeux de leurs dirigeants. Une véritable catastrophe qu'il convient d'éviter pour les objets connectés.

Le contrôle avant tout

Plutôt qu'interdire, mieux vaut donc disposer d'une véritable politique propre à tous les appareils, y compris donc les objets et vêtements intelligents et connectés. Mieux vaut ainsi avoir le contrôle et la mainmise sur ce type de produits qu'en ignorer la présence, ce qui est la pire des situations.

Qui plus est, comme pour les smartphones, les entreprises doivent en tirer profit, que ce soit pour communiquer avec leurs employés ou encore trouver un moyen d'exploiter ces objets vis-à-vis des clients. Après tout, il s'agit de produits souvent compatibles avec d'autres appareils, et il n'est pas rare qu'un important espace de stockage en ligne (cloud) l'accompagne. Si cela peut devenir un problème, cela peut donc surtout être un atout.

Il faut de plus comprendre qu'à l'heure actuelle, il n'existe pas de solutions spécifiques de sécurité pour ces objets. Stephen Brown, directeur de la gestion des produits mobiles chez Landesk, expliquait par exemple en avril dernier qu'en réalité, la première préoccupation vis-à-vis de ces produits n'est pas la sécurité mais le respect de la vie privée. C'est en particulier le cas des lunettes connectées, mais pas uniquement. Est-ce que ces appareils enregistrent constamment voire à notre insu ? Répondre à ces questions est déjà un point fondamental.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

http://www.zdnet.fr/actualites/apres-le-byod-voici-le-wyod-39806705.htm

Par Nil Sanyas

Dix-huit anglicismes dans le domaine informatique ont désormais leur équivalent français

Dix-huit anglicismes dans le domaine informatique ont désormais leur équivalent français

La Commission générale de terminologie a encore sévi. Par décret, elle préconise d'utiliser une série d'équivalents français à dix-huit anglicismes dans le domaine informatique. Le back office devient un arrière-guichet et – logique – le front office un guichet. Les framework et integrated development environment (IDE) se transforment respectivement en environnement de développement et en atelier de développement.

Un thumbnail (image réduite par rapport à l'original) prend le joli nom d'imagette et le lurker (internaute qui suit les échanges sur le web sans y participer) celui de fureteur. Proches des termes originaux, le blogue, le microblogue ou la cyberconférence ont plus de chances de remplacer, dans l'usage courant, le blog, le microblogging ou la web conference.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.01net.com/editorial/626898/ne-dites-plus-back-office-mais-arriere-guichet/#?xtor=EPR-1-NL-01net-Actus-20140916

Le système de reconnaissance biométrique du FBI est

opérationnel

Le système de reconnaissance biométrique du FBI est opérationnel

Grâce aux outils du système NGI, le FBI pourra retrouver des criminels dans tous les Etats-Unis grâce à une empreinte, un scan d'iris ou une photo.

Le système NGI sera disponible dans tous les Etats-Unis d'ici à la fin 2014.
Après trois années de développement, le nouveau système de reconnaissance biométrique Next Generation Identification system) du FBI est opérationnel a annoncé le Bureau le 15 septembre 2014. Il a été conçu pour améliorer les possibilités d'identification biométriques explique le FBI dans son communiqué.
Il comporte deux nouveaux outils qui viennent s'ajouter aux bases de données d'empreintes digitales et de scans d'iris. Le premier concerne la reconnaissance faciale, l'Interstate Photo System (IPS) et le second, Rap Back, fournit des notifications écrites.

La base contiendra à terme 52 millions de photos.

Rap Back permet à toutes les autorités habilitées de recevoir des informations sur l'historique criminel de toute personne occupant un poste de confiance : un professeur, un conseiller bancaire…, explique le FBI dans son communiqué. Plus question de passer sous silence une arrestation pour conduite en état d'ivresse à 19 ans. Quant à IPS, il permet d'accélérer la recherche de criminels grâce à une base de données qui comptera 52 millions de photos d'ici à 2015.

En avril dernier, l'ONG Electronic Frontier Foundation émettait déjà quelques réserves sur cet outil. En premier lieu, elle dénonçait le mélange des genres puisqu'en plus des photos de criminels, celles de citoyens lambdas se trouvaient dans cette base. Elle s'inquiétait également du risque de « faux positif » compte tenu du taux de fiabilité du système qui n'est que de 85 %.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.01net.com/editorial/626932/le-systeme-de-reconnaissance-biometrique-du-fbi-est-operationnel/#?xtor=EPR-1-NL-01net-Actus-20140916

Cécile Bolesse

Droit à l'oubli : Une vue générale des demandes de désindexation à Google

Droit à l'oubli : Une vue générale des demandes de désindexation à Google

Google reste assez évasif sur les demandes qui lui sont adressées chaque jour au titre du droit à l'oubli, instauré par la décision prise par la CJUE en mai. On sait certes que le nombre de demandes traitées par le géant des moteurs de recherche est important, au moins 120.000 requêtes ont été adressées à Google depuis l'ouverture de son formulaire. Mais derrière les chiffres officiels se cache une vraie bataille politique menée par Google autour de ce droit à l'oubli et la firme de Mountain View distille ses informations sur le sujet avec précaution.

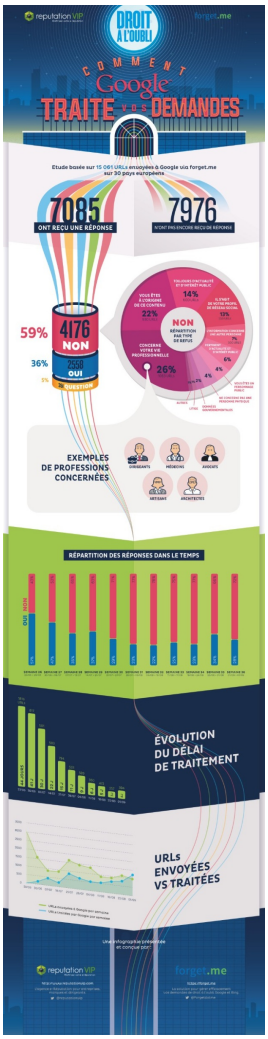
Forget.me est un site qui se propose comme un intermédiaire entre l'utilisateur lambda et le formulaire de Google.
Au total, depuis le lancement de son service, Forget.me a reçu plus de 15.000 demandes (depuis 30 pays d'Europe) dont environ la moitié a été traitée par Google. L'entreprise a donc compilé ses résultats et publie une étude retraçant leur vision de ce phénomène.

Lors de la mise en place de son service, en juin, Forget.me a ainsi reçu environ 1800 demandes de déréférencement. A l'époque, Google répondait en moyenne à une demande en 44 jours mais aujourd'hui, soit environ 3 mois plus tard, le nombre de demande par semaine semble stabilisé aux alentours de 300 et Google répond en moyenne en moins de 4 jours.

Autre statistique relevée par Forget.me : Google semble bien plus difficile sur les demandes que lors du lancement du service. En juin, le taux de refus de la part du moteur de recherche était autour de 50%, aujourd'hui celui-ci flirte plus souvent avec les 70%. Le moteur de recherche s'appuie pour cela sur 11 typologies de refus. La plus fréquente étant « Concerne votre vie professionnelle » avec 26% des URL concernées.

« Plusieurs facteurs entrent en jeu, et Google n'est pas le seul en cause dans ce durcissement » précise Bertrand Girin « Il est possible que Google ait volontairement durci ses critères, mais ce droit est encore jeune et ses équipes ont probablement eu besoin de s'adapter et de se former pour le maitriser totalement. Et cela prend évidemment un peu de temps. » Même constat pour les différentes Cnils européennes, qui doivent bientôt publier leurs directives sur le sujet, le droit va s'adapter à cette nouvelle régulation et les usages vont se stabiliser.

Pour visualiser ces indicateurs, Reputation VIP a eu la bonne idée de créer une infographie synthétique :



Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/droit-a-l-oubli-vers-une-stabilisation-des-demandes-a-google-en-europe-39806691.htm

Google et Dropbox tentent eux aussi de simplifier la cybersecurité

Google et Dropbox tentent eux aussi de simplifier la cybersecurité

Les deux entreprises ont initié une alliance dédiée à la cybersecurité, nommée Simply Secure. Google et Dropbox entendent s'atteler au défi séculaire du monde de la cybersecurité : la simplicité d'accès et d'usage de ces outils.

Si l'on devait compter le nombre de start-ups et de projets qui promettent d'offrir un service garantissant à la fois la plus haute confidentialité des données et une simplicité d'utilisation inégalée, on pourrait probablement passer un moment à établir la liste.
En effet, les récentes révélations Snowden et autres fuites multiples de photos de stars dénudées n'ont fait que rappeler à la communauté des chercheurs en cybersecurité le douloureux problème qui frappe le secteur : les solutions existent, simplement personne ne sait vraiment les utiliser. Mais quand deux géants tels que Google et Dropbox s'allient autour du développement de solutions simples et faciles d'accès pour protéger la vie privée des utilisateurs, l'initiative mérite d'être notée. C'est l'objet de Simply Secure, le consortium dévoilé par les deux entreprises la semaine dernière.

Beaucoup de bruit pour rien ?
Si pour l'instant, Simply Secure n'a pas grand-chose à offrir, il promet beaucoup. Simply Secure l'explique ainsi sur son site « nous voulons aider la communauté de cybersecurité open source à faire mieux. Nous ne voulons pas racheter, nous ne voulons pas inventer » mais simplement apporter un soutien dans le domaine de la recherche. Leur cible : le taux d'adoption des outils déjà existant, qui reste particulièrement bas, comme le rapporte le Guardian.

Le programme de l'alliance Simply Secure est donc de s'ouvrir aux acteurs déjà existant et de mettre en place plusieurs partenariats. Pas vraiment de concret à l'horizon donc, et l'alliance s'attaque à un problème pour le moins épineux que beaucoup auparavant ont tenté d'aborder, sans réel succès.
Mais la question de la cybersecurité n'a jamais été aussi significative aux yeux du grand public, et cette initiative de la part de Google et Dropbox vient réaffirmer leur engagement en faveur d'un internet plus sécurisé. Pas sur que cela soit un réel souci pour la NSA, mais c'est l'intention qui compte.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/google-et-dropbox-tentent-eux-aussi-de-simplifier-la-cybersecurite-39806679.htm
Par Louis Adam | Lundi 22 Septembre 2014

Rapport 2013 DU GIABA : trafic de drogue, fraude fiscale, cybercriminalité constituent les infractions les plus fréquentes au Sénégal

Rapport 2013 DU GIABA : trafic de drogue, fraude fiscale, cybercriminalité constituent les infractions les plus fréquentes au Sénégal

Le Groupe intergouvernemental d'action contre le blanchiment d'argent en Afrique de l'Ouest (Giaba) vient de publier son rapport annuel pour l'année 2013, dans lequel, il souligne que le trafic de drogue, la fraude fiscale, les autres investissements et la cybercriminalité ont été les infractions sous-jacentes les plus fréquentes en 2013.

Le rapport annuel 2013 du Groupe intergouvernemental d'action contre le blanchiment d'argent en Afrique de l'Ouest (Giaba) vient d'être publié. En ce qui concerne notre pays, le Giaba a signalé que «le rapport national du Sénégal répertorie le trafic de drogue, la fraude fiscale, les autres investissements et la cybercriminalité comme infraction sous-jacentes les plus fréquentes en 2013». Il a aussi rappelé que «le rapport de l'Organe international de contrôle des stupéfiants (Incsr) 2013 du développement d'Etat américain étend la liste pour y inclure les fraudes bancaires et de dépôt, la falsification de documents, la revente de voitures volées et les combines de la Ponzi. Un taux de corruption élevé a également été signalé dans le pays, un phénomène qui frappe tous les niveaux de gouvernance et le commerce, selon le rapport ».
Le Giaba a souligné que «le Sénégal a de plus en plus démontré son engagement à lutter contre les crimes financiers, y compris le Bc/Ft» surtout en prenant des mesures pour renforcer son dispositif de lutte contre le blanchiment des capitaux et de lutte contre le financement du terrorisme (Lbc/Ft). Cependant, «Un projet de stratégie national de Lbc/Ft est actuellement en attente d'approbation par les autorités, conformément à la loi de Lbc/Ft».
Le rapport annuel renseigne aussi que, chez nous, «plusieurs décisions de justice ont été rendues, y compris des peines d'emprisonnement, des amendes et confiscations, suite à des accusations de blanchiment de capitaux». Et en 2013, la Cellule de renseignement financier a reçu 109 déclarations d'opérations suspectes liées au blanchiment, 14 des cas analysés ont été envoyés aux autorités d'exécution, aux fins d'enquête et de poursuite et 3 condamnations ont été prononcées. Il faut dire que dans les premières lignes de la partie du rapport consacré à notre pays, la traduction en justice, pour enrichissement illicite de Karim Wade, a été rappelée : «En 2013, la répression de la corruption a conduit à la mise en accusation devant les tribunaux de plusieurs ministres dans le gouvernement du Président Wade, dont son fils, Karim Wade, pour corruption» y lit-on.
Même si le Sénégal a fait des progrès d'envergure dans le renforcement de son système de Lbc/Ft, les lacunes suivantes demeurent, selon le Giaba «l'adoption d'un cadre approprié de l'approche fondée sur les risques, la mise en oeuvre de mesures de vigilance pour la surveillance continue des relations et transaction avec les clients, la conduite de l'application de mesures renforcées de vigilance pour les clients à risques élevés».
Egalement, «le renforcement de l'obligation de déclarer les tentatives d'opération et un mécanismes pour la mise en oeuvre des résolutions 1267 et 1373 du conseil de sécurité de l'Onu et les résolutions qui les ont suivies».

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.dakaractu.com/Rapport-2013-DU-GIABA-trafic-de-drogue-fraude-fiscale-cybercriminalite-constituent-les-infractions-les-plus-frequentes_a73269.html

Osmose Radio – Emission Da vici Code du 16/09/2014 – La CNIL, la Loi I&L et la protection des données à caractère personnel

	Osmose est une Web Radio que l'on peut écouter sur www.osmose-radio.fr **Emission du 16/09/2014 :La CNIL, la Loi Informatique et Libertés et la protection des données à caractère personnel** Emission d'une série sur le Numérique, présentée par Paula SAUDEZ et co-animée avec Denis JACOPINI et Maître ABENSOUR, avocat au barreau d'Avignon.

La CNIL, la Loi Informatique et Libertés et la protection des données à caractère

personnel

1 Introduction de l’émission par Paula SAUDEZ

Accueil des auditeurs et accueil de l’invité Denis JACOPINI qui se présente.

2. Présentation de Denis JACOPINI

Expert judiciaire en Informatique,

Consultant en sécurité informatique et cybercriminalité

Consultant en mise en conformité avec la Loi Informatique et Libertés

Correspondant CNIL (CIL)

Membre de la Compagnie nationale des experts de justice en informatique et techniques associées et membre de l’Association Française des Correspondants à la protection des Données à caractère Personnel.

Par rapport au sujet de cette émission, Denis JACOPINI accompagne les entreprises à se mettre en conformité avec la CNIL par rapport à la Loi Informatique et Libertés.

3. Introduction du sujet par Paula SAUDEZ du sujet de l’émission

Pause Musicale

4. Avant de démarrer sur le sujet, le débât

09/09/2014 Depuis quelques mois, un groupe sur Facebook fait parler de lui.
Créé il y a deux ans, le « Groupe qui te dit où est la police en Aveyron » compte plus de 10000 membres. C'est un groupe Facebook qui alerte les conducteurs de la localisation de contrôles routiers dans la région. Cette page Facebook est dans le viseur du procureur de Rodez. Le procès a eut lieu mardi 9 septembre au tribunal correctionnel de Rodez (Aveyron). Quinze personnes membres du groupe Facebook ont comparu pour avoir divulgué les emplacements des radars de leur département sur le réseau social. Aux yeux du procureur de la République, elles se sont *"soustraites à la constitution des infractions routières"*.

L'article R-413-15 du Code de la route interdit les "appareils, dispositifs ou produits" qui pourraient empêcher de constater une infraction ou aider à ne pas s'y soustraire. Mais pour Rémy Josseaume (Avocat au Barreau de Paris qui défend ce groupe), les pages Facebook ne peuvent être assimilées à de tels détecteurs de radars.

Le verdict, le 3 décembre prochain à 14h00.

J'aurais aimé savoir si vous étiez d'accord ou pas et avoir votre avis sur cette affaire.

Vous pouvez nous appeler à la radio au 04 90 88 22 56.

4. Le sujet de l’émission

Présentation par Denis JACOPINI du contenu avec intervention de Paula, des auditeurs et des intervenants éventuels.

Lien vers notre dossier du mois

Pause Musicale

5. Les Actus du Net Expert

Depuis le 13 mai 2014, Google n’a pas le choix.
Il doit mettre à disposition des internautes un formulaire leur permettant de pouvoir désindexés du moteur de recherche des contenus qu’ils jugeraient non pertinents, inexacts, incomplets ou encore excessifs.
Google, a été sommé, depuis mai d’accéder aux demandes des internautes voulant désindexer un contenu.
Pour répondre à cette sommation, Google a mis en place une commission pour trancher entre respect de la vie privée et droit à l’information des internautes car c’est le fond du problème qui se cache derrière chaque demande.
Une commission mise en place par Google a tenu mardi dernier, le 9/9/2014, la première d’une série de réunions publiques s’est déroulée à Madrid et a donné le coup d’envoi d’un total de sept réunions dans des capitales européennes au moment où Google doit faire face à des milliers de demandes par mois de retrait de résultats de recherche.

A titre d’exmple, Google déclare avoir reçu plus de 90 000 demandes entre juin et mi-juillet. Probablement plus de 100 000 demandes aujourd’hui.

Publication du 19/08/2014 dans le blog « LeNetExpert.fr »
A partir du 12/08, un correctif Windows (installé automatiquement pour la plupart des ordinateurs fonctionnant sous Windows 7, 8 et 8.1) créait, une fois installé des ralentissements, plantages, des écrans bleus. Le 18/08 a pris en compte les retour des utilisateurs et à retiré la mise à jour de sécurité Microsoft Windows (KB2982791) du processus de mise à jour automatique. Si cette mise à jour a été installée avant le 28/08 est à supprimer de toute urgence. Si elle été installée après 28/08, pas de soucis, car Microsfot aurait corrigé depuis le prblème.

Info du 1er septembre parue dans le blog « LeNetExpert.fr »
Près de 20% des entreprises sont victimes d’escroqueries bancaires. La dernière ruse en vigueur est celle qui profite de la norme SEPA, l’espace de paiement unique européen.
Après « l’arnaque à la nigériane », « l’arnaque au président » appelée aussi « l’arnaque à la directions », voici maintenant « l’arnaque au videment SEPA » (Single Euro Payments Area)

Selon une étude parue le 2 septembre faite par le célèbre cabinet Kindsight Security Labs du groupe Alcatel Lucent, 15 millions de terminaux mobiles seraient infectés d’un malware.
Rassurez-vous, car sur l’ensemble des appareils en circulation l’on estime que 0,65% d’entre eux (sur les 2 307 692 300 en circulation) sont infectés d’un malware.

Le 3 septembre 2014, j'ai fais paraître une publication dans mon blog « le net expert.fr » intitulé : « 5 conseils pour protéger ses photos et données perso dans le cloud ».

1) Evitez le cloud pour stocker des données confidentielles.
2) Utilisez un bon mot de passe.
3) Chiffrez vos données. Si vous avez des données confidentielles et que vous voulez quand même utiliser le cloud, il y a une solution : le chiffrement préalable.
4) Analysez la sécurité de votre fournisseur (https, authentification renforcée, serveurs configurés pour supporter le PFS (Perfect Forward Secrecy) – en français « confidentialité persistante »
5) Ne partagez pas tout avec n'importe qui.

Le 9/9/2014 Apple a présenté son nouveau téléphone : l'iPhone 6 équipé d'un écran impossible à rayer, et l'Apple Watch, sa montre connectée . Outre son bracelet original avec un fermoir magnétique, ses capteurs permettent de mesurer très précisément les paramètres vitaux. En fait l'Apple Watch est un boîtier bourré de capteurs qui détectent les mouvements (nombre de pas) et les paramètres vitaux au poignet du porteur : pression artérielle, le niveau d'hydratation, la fréquence cardiaque, des données comme la glycémie.
Selon deux employés cités par le New York Times, Apple aurait investi une quantité astronomique de temps et d'argent pour concevoir d'aussi précis capteurs à tel point qu'ils seraient largement plus précis que ceux des objets connectés déjà commercialisés.

Publication du 15/09/2014 dans le blog « le net expert.fr »
Le site internet de la Région Provence-Alpes-Côte d'Azur (http://www.regionpaca.fr) a été victime d'un piratage

informatique le mercredi 10 septembre. Après avoir été mis hors-ligne, le site est à nouveau accessible.

6. Conclusion et présentation de la prochaine émission avec LeNetExpert :

Comment bien sécuriser son ordinateur

Données personnelles : la Cnil épingle l’opacité des applis mobiles

	**Données personnelles : la Cnil épingle l’opacité des applis mobiles**

Près de 15% de 121 applications examinées ne fournissent aucune information sur le traitement des données collectées et la moitié rendent ces infos peu accessibles.

La collecte de données personnelles par les applis mobiles téléchargées ne donne pas lieu à beaucoup d'informations de la part de leurs éditeurs. C'est le constat issu d'une démarche initiée, en mai 2014, par la Cnil et 26 de ses homologues dans le monde. Celles-ci ont mené un audit en ligne simultané de plus de 1 200 applications mobiles gratuites et payantes.
Leurs vérifications ont porté sur le type de données collectées par les applications, le niveau d'information des utilisateurs et la qualité des explications données par l'application concernant le motif de la collecte de ces données.
Pour la France, la Cnil a examiné 121 applications parmi les plus populaires pour les trois principaux systèmes d'exploitation mobiles (iOS, Android, Windows Phone). Ses conclusions ne diffèrent pas du constat général effectué à l'échelon mondial.
La CNIL a passé au crible 121 applications mobiles les plus populaires en France
Ainsi, 15% des applications examinées ne fournissent aucune information sur le traitement des données collectées. Et même lorsqu'une information est fournie sur la politique de collecte, près de la moitié des applications concernées ne la rendent pas facilement accessible.
La Cnil déplore qu'on impose à l'utilisateur une recherche active sur le site internet de l'éditeur ou dans les différents onglets de l'application : « Il a ainsi été constaté que les mentions d'information de certaines applications à destination d'utilisateurs français ne sont disponibles qu'en anglais. »
Fort des de constat, la Commission recommande aux utilisateurs d'être à la fois curieux, vigilants et exigeants. « Il existe un large choix d'applications offrant des services similaires, détournez vous de celles qui en demandent le plus et en disent le moins ! » conclut-elle.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.01net.com/editorial/626952/donnees-personnelles-la-cnil-epingle-lopacite-des-applis-mobiles/#?xtor=EPR-1-NL-01net-Actus-20140917
Frédéric Bergé 01net.le 16/09/14 à 19h50

Il y a désormais plus d'un milliard de sites Web en ligne…

Il y a désormais plus d'un milliard de sites Web en ligne…

Chiffre symbolique, le Web qui a fêté ses 25 ans en mars viendrait de passer le cap du milliard de sites Web en ligne. En revanche, on ne sait pas combien sont à l'abandon…
Il y a eu les pages perso, puis les blogs, puis les Myspace, Tumblr et autres espaces personnalisés, petits bouts de 0 et de 1, colonisés à la sueur du clavier. Le Net et le Web sont des espaces d'expression jamais vus auparavant et leur succès est colossal, à l'échelle de l'humanité.

25 ans et toutes ses dents
Selon le site spécialisé Internet Live Stats, il y a désormais plus d'un milliard de sites Web, et ce chiffre augmente en permanence, selon les derniers relevés établis en temps réel mardi. Le Web a fêté ses 25 ans en début d'année et le compteur d'internetlivestats.com indiquait que la toile comptait plus d'1,06 milliard de sites mercredi peu avant minuit.
L'idée du Web, interface « graphique » du Net, a été développée dans les années 1980 par le Britannique Tim Berners-Lee, qui n'était alors qu'un jeune ingénieur en informatique dans un laboratoire de physique en Suisse. Il a présenté son idée par écrit le 12 mars 1989, un jour en général considéré comme la date de naissance du Web. Les militaires américains avaient étudié l'idée de connecter des ordinateurs en réseau dans les années 1950, et avaient lancé Arpanet en 1969, une sorte de précurseur d'Internet.

Le Web a gagné son premier milliard à seulement 25 ans…
Explosion de l'information
Mais grâce au système de « Sir Tim », aujourd'hui âgé de 59 ans, les gens ont été en mesure de publier ce qu'ils souhaitaient sur des ordinateurs reliés entre eux par internet, ouvrant la porte à un gigantesque partage d'informations et à une explosion du nombre de sites.
Des moteurs de recherche comme Yahoo! ou Google ont ensuite été créés pour aider les internautes à trouver les pages qui les intéressaient parmi la profusion d'informations postées. Ainsi, rien que pour la journée du mardi 16 septembre 2014, Google a enregistré plus de 3,1 milliards de recherches sur ses serveurs selon internetlivestats.com. Et près de 170 milliards d'e-mails avaient aussi été envoyés au cours des dernières 24 heures.

Tout n'est pas vert…
Toujours selon le compteur d'internetlivestats.com, la barre des 3 milliards d'internautes devrait aussi être franchie prochainement. Le revers de la médaille est que l'électricité consommée pour faire fonctionner internet a généré au moins 2,17 millions de tonnes de dioxyde de carbone (CO_2) rejetées dans l'atmosphère rien que pour la journée de mardi, selon internetlivestats.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.01net.com/editorial/626966/il-y-a-desormais-plus-d-un-milliard-de-site-web-en-ligne/#?xtor=EPR-1-NL-01net-Actus-20140917

Chine : première hausse des infections aux virus informatiques en cinq ans

Chine : première hausse des infections aux virus informatiques en cinq ans

Plus de la moitié des ordinateurs en Chine sont infectés par des virus, indique une récente enquête, précisant que ce nombre est en hausse pour la première fois en cinq ans.

Ce taux a augmenté de 9,8% en glissement annuel en 2013, mettant fin à une baisse successive de cinq ans, a annoncé mardi le Centre national des mesures d'urgence face aux virus informatiques.
D'après une enquête menée par le centre, 54,9% des ordinateurs examinés étaient touchés par des virus.
Les sites bancaires et les méthodes de paiement en ligne restent les principales cibles des virus, et les pirates tentent de dérober à la fois des fonds et des informations privées. Les utilisateurs de Weibo sont aussi vulnérables aux attaques de virus, selon le centre.
Chen Jiamin, directeur adjoint du centre, a affirmé que les failles de sécurité mettaient en lumière les manques en matière d'administration des sites Internet et de technologies de sécurité des réseaux dans plusieurs organisations.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://french.people.com.cn/n/2014/0917/c31357-8783700.html