Facebook laisse ouvert une faille permettant à des pirates de récolter vos données personnelles | Le Net Expert Informatique

	Facebook laisse ouvert une faille permettant à des pirates de récolter vos données personnelles

Des pirates peuvent en toute impunité obtenir le nom, la photo de votre profil et votre emplacement de votre compte Facebook vu que le réseau social n'a pas estimé que cette faille en est réellement une.

Via une faille de sécurité dans Facebook, Reza Moaiandin, un ingénieur logiciel, a réussi à obtenir les noms, les photos de profil et les emplacements des utilisateurs du réseau social, ce qui correspond tout de même à des données privées.
Pour obtenir ces données, le chercheur n'a rien piraté, il a simplement utilisé des possibilités offertes. En l'occurrence, la fonction permettant de trouver un utilisateur à partir de son numéro de téléphone, un paramètre de confidentialité méconnu est qui est par défaut autorisé pour « Tout le monde ». Cela signifie que n'importe qui peut retrouver n'importe qui simplement en connaissant son numéro de téléphone.
Futé, Reza Moaiandin a utilisé un algorithme simple pour générer des milliers de numéros mobiles possibles valables pour les États-Unis, le Royaume-Uni et le Canada. Via une API, il a ensuite simplement cherché à obtenir les données associées aux numéros.
Le fait que le système donne la possibilité de relier des profils Facebook à des numéros de téléphone à une telle échelle est une véritable de faille de sécurité vu que c'est une porte ouverte à tous les abus.
Alors que cette faille a été communiquée au réseau social au mois d'avril, Facebook ne la pas corrigée. Un ingénieur indique que cette vulnérabilité n'est pas considérée comme étant une faille de sécurité.
Si Facebook ne compte rien faire pour protéger les données personnelles de ses utilisateurs, la solution est donc que ce soient eux qui se protègent.
Pour ce faire, ils doivent limiter l'accès à leurs informations via cette fonctionnalité méconnue. Pour ce faire, il faut aller dans « Paramètres », puis « Vie privée » et chercher les personnes qui peuvent vous chercher en utilisant le numéro de téléphone fourni. Il faut modifier ce paramètre pour le mettre sur « Amis ».
Il est à souligner que Facebook s'est réfugié justement derrière le fait que chaque utilisateur peut régler la confidentialité de ses données. En clair, le réseau social ne se déclare pas responsable !

Source : http://www.linformatique.org/facebook-laisse-ouvert-une-faille-permettant-a-des-pirates-de-recolter-vos-donnees-personnelles/

L'Afrique menacée par la cybercriminalité | Le Net

Expert Informatique

L’Afrique menacée par la cybercriminalité

L'Afrique est à la traîne en matière de législation sur la cyber-sécurité, un vide juridique qui constitue un véritable danger pour le continent, où, non seulement, il engendre d'énormes pertes économiques, mais porte atteinte à la souveraineté des pays du continent, en mettant les données personnelles des Etats et des citoyens à la merci des firmes internationales du numérique.

L'Afrique n'a aucune maîtrise de la chaine numérique. Par conséquent, elle se retrouve dans un système de colonisation et de dépendance numérique, fait observer le Pr Olivier Sagna, Secrétaire Général de l'observatoire sur les systèmes d'information, les réseaux et les inforoutes au Sénégal (OSIRIS).
Sagna regrette le fait que « l'Afrique ne possède pas de point d'échange internet, tous les messages échangés passent par un point de transit, qui en fonction des accords et des coûts de droits de communications internationaux, coûte des millions de dollars » aux pays du continent noir.
Selon le Directeur associé de Performances Group au Sénégal, Mouhamed Tidiane Seck, plus de 17 millions de victimes dans le monde ont fait les frais de la cybercriminalité, entre 2012 et 2013. Soit une augmentation de 87% de cas malveillants, occasionnant des conséquences économiques évaluées à trois milliards de dollars de perte bancaire.
L'Afrique du Sud, est l'un des rares pays du continent, grâce à la force de ses lobbys, à avoir mis en place une politique de protection des données personnelles à l'endroit des firmes internationales du numérique.
Concernant l'aspect juridique sur la protection des données personnelles, le Dr Mouhamadou Lo, Président de la Commission de protection des Données Personnelles (CDP) refuse de parler de « désert juridique » en Afrique. « En Afrique, en plus de l'Afrique du Sud, il existe deux textes au niveau de la région Ouest africaine », a indiqué Dr Mouhamadou Lo.
Sur cette dynamique, il faut souligner que la Convention de l'Union Africaine sur la Cyber-sécurité et la protection des données à caractère personnel a été adoptée à Malabo en 2014. « Voter une loi est un premier pas, mais il faut la mise en place d'une commission opérationnelle », a-t-il conclu.

Source : http://www.lemagazinedumanager.com/11300-senegal-la-cybercriminalite-une-menace-pour-lafrique.html

Bientôt un « carnet de correspondance numérique » pour les collégiens et lycéens | Le Net Expert Informatique

	Bientôt un « carnet de correspondance numérique » pour les collégiens et lycéens

Le gouvernement a publié la semaine dernière un arrêté autorisant la création d'un téléservice censé permettre aux parents « d'être informés, à distance, des événements de vie scolaire liés aux absences, aux retards, aux punitions et aux sanctions » infligées à leur(s) enfant(s). Un véritable carnet de correspondance dématérialisé se dessine ainsi, alors que le plan pour le numérique à l'école est attendu pour la rentrée 2016.

Durant toute l'année scolaire, de nombreuses informations pourront être consignées dans ce fichier concernant les élèves de la sixième à la terminale : absences, retards, retenues, exclusions de cours, blâmes, avertissements, etc. ainsi que leurs motifs et dates. Ces informations seront accessibles via Internet au jeune concerné ainsi qu'à ses parents, de même qu'aux personnels du collège et lycée en question (enseignants, assistants d'éducation, conseiller principal d'éducation, chef d'établissement). Le tout sera toutefois effacé une fois le temps des grandes vacances venu, à la fin de chaque année scolaire.

L'objectif ? Améliorer l'information des familles et la communication avec l'établissement d'enseignement, notamment afin de mieux prévenir le décrochage scolaire. Pour autant, ce dispositif ne sera pas déployé systématiquement dans tous les collèges et lycées. Si l'arrêté permet dès à présent une mise en œuvre au niveau national, ce téléservice sera uniquement proposé par les établissements volontaires. De surcroît, chaque parent aura le droit de ne pas activer le compte de son enfant.

Une phase d'évaluation dans cinq académies, avant une généralisation progressive

Contacté, le ministère de l'Éducation nationale n'était pas en mesure de répondre dans l'immédiat à nos questions concernant le calendrier de mise en place de ce téléservice. L'exécutif a cependant indiqué à la CNIL qu'un test devrait tout d'abord être mené « dans cinq académies ». Il semble ainsi fort probable que la Rue de Grenelle suive une feuille de route similaire à celle prévue pour le récent dispositif de télépaiement des frais de cantine et d'internat, dont la généralisation devrait avoir lieu à partir de la rentrée 2016, également après une phase d'expérimentations (voir ancien article Nextimpact).

Saisie pour avis, la CNIL a d'autre part prévenu le ministère de l'Éducation nationale que « les établissements devront continuer de mettre à disposition des responsables légaux qui ne seraient pas en capacité d'accéder au téléservice proposé, ou qui ne souhaiteraient pas l'utiliser, un autre moyen d'accès aux données traitées dans le téléservice ». Les explications concernant ce recours seront adossées au courrier envoyé aux parents afin de leur présenter ce dispositif « et leur attribuer un identifiant et un mot de passe provisoires », qu'ils devront changer lors de leur première connexion.

La gardienne des données personnelles a enfin invité les pouvoirs publics à être très vigilants en matière de sécurité, au-delà de l'utilisation de protocoles HTTPS et de mots de passe complexes (huit caractères minimum, avec chiffres et lettres). La CNIL souligne en effet que « l'impact sur la vie privée des élèves en cas de dysfonctionnement d'un téléservice portant sur les absences, les retards, les punitions et les sanctions pouvant être élevé, il est nécessaire que tous les établissements scolaires garantissent un niveau de sécurité satisfaisant afin d'assurer à tous les élèves du second degré une même protection ». Le ministère de l'Éducation nationale a ainsi été prié d'alerter les principaux et proviseurs sur ce point en particulier.

Source : http://www.nextinpact.com/news/96066-bientot-carnet-correspondance-numerique-pour-collegiens-et-lyceens.htm

---

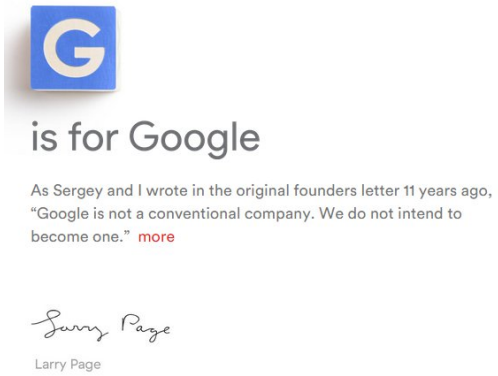
Google devient Alphabet | Le

Net Expert Informatique

	**Google devient Alphabet**

Les deux fondateurs de Google annoncent une importante restructuration donnant naissance à une nouvelle société, Alphabet, laquelle englobera le moteur de recherche, les activités satellite historiques et tous les projets initiés par le duo.

Larry Page et Sergey Brin ont annoncé lundi 10 août la plus profonde restructuration financière jamais entreprise par Google depuis son introduction en bourse en 2004. Dans une lettre commune, ils indiquent que le groupe qu'ils ont fondé sera désormais englobé au sein d'une nouvelle société, baptisée Alphabet.



Un nom à dimension holistique, qui recouvrira les activités historiques du moteur de recherche ainsi que les nouveaux projets lancés au sein de ses laboratoires qui deviendront autant de nouvelles entités, de Life Sciences et ses lentilles connectées pour diabétiques à Calico, dont l'objectif consiste à prolonger la vie de l'homme en passant par la livraison par drone promise par Wing. Google ne sera donc plus désormais que le « G » de l'Alphabet selon Page et Brin.
« Qu'est donc Alphabet ? Alphabet consiste principalement en une collection de sociétés. Dont la plus importante est bien sûr Google. Ce nouveau Google est un peu allégé, dans la mesure où les sociétés qui sont éloignées de nos principaux produits liés à Internet sont maintenant contenus dans Alphabet », expliquent les deux hommes.
L'explication appelle à la logique, partant du principe qu'il n'est pas forcément aisé de mener un moteur de recherche, la première régie publicitaire en ligne au monde et le développement de voitures autonomes ou la recherche en biotechnologies à l'aide de rênes uniques. « Fondamentalement, nous pensons que (cette nouvelle structure) nous permettra de mieux adapter notre gestion dans la mesure où nous conduisons de façon indépendante des choses qui ne sont pas liées ». Chaque entité au sein d'Alphabet sera menée par son propre chef d'orchestre, Page et Brin assurant le pilotage général, le premier en tant que CEO et le second au poste de président.
La direction du nouveau Google reviendra quant à elle à Sundar Pichai. Il englobe la recherche, la publicité en ligne, YouTube, la cartographie, Android et l'ensemble des infrastructures techniques associées, qui constituent aujourd'hui le bras armé de Google sur le plan financier.
Nest (thermostat connecté), Fiber (fournisseur d'accès) et les différentes entités dédiées à l'investissement (Google Ventures, Google Capital), activités moins « stables » dans le sens où elles induisent des investissements importants associés à une certaine part de risque, appartiendront en revanche à l'ensemble Alphabet.
Au Nasdaq, Alphabet Inc. remplacera Google Inc. en tant qu'entité publique, et l'ensemble des actions sera automatiquement convertis, à valeur et droits équivalents.
En attendant de mesurer l'accueil des marchés boursiers face à ce changement inédit, Page et Brin renouvellent leur profession de foi : cette nouvelle organisation devrait selon eux permettre d'accomplir des tâches toujours plus importantes, inscrites dans une vision à long terme, tout en favorisant le développement de l'ensemble de l'écosystème, de façon toujours plus transparente… pour in fine « améliorer la vie d'autant de personnes que possible ».
Derrière la portée symbolique et les accents humanistes de la déclaration, difficile de ne pas supposer en arrière plan des manœuvres plus terre à terre, visant à redonner de l'agilité sur le plan financier à celle qui fut un jour une start-up et pèse aujourd'hui parmi les plus importantes capitalisations boursières de la planète.

Source : http://pro.clubic.com/entreprises/google/actualite-776160-google-restructure-sein-maison-mere-alphabet.html
Par Alexandre Laurent

On peut voler des identifiants Active Directory depuis Internet via SMB | Le Net Expert Informatique

On peut voler des identifiants Active Directory depuis Internet via SMB

Deux chercheurs ont montré sur la conférence Black Hat 2015 qu'une attaque via le protocole de partage de fichiers SMB connue pour s'effectuer au sein d'un réseau local peut en fait servir à attaquer des serveurs Windows hébergés dans le cloud.

Lors de la conférence Black Hat 2015 (Las Vegas, du 1er au 6 août), deux chercheurs ont montré qu'une technique d'attaque via le protocole de partage de fichiers SMB que l'on croyait ne fonctionner que sur les réseaux locaux peut en fait être exécutée sur Internet. Avec cette attaque, dite de relais SMB, un ordinateur Windows appartenant à un domaine Active Directory laisse apparaître les informations d'identification de l'utilisateur quand celui-ci consulte une page web, un courriel dans Outlook ou regarde une vidéo dans Windows Media Player. L'attaquant peut ensuite détourner ces identifiants pour s'authentifier au nom de l'utilisateur sur des serveurs Windows où il dispose d'un compte, y compris ceux hébergés dans le cloud.
Dans un réseau Active Directory, les ordinateurs Windows retournent automatiquement leurs informations d'identification pour accéder aux différents services de partage de fichiers à distance, aux serveurs de messagerie Microsoft Exchange ou aux outils de collaboration SharePoint. Ces informations d'authentification – en l'occurrence le nom de l'ordinateur, le nom de l'utilisateur, tous deux en texte clair, et un hash cryptographique dérivé du mot de passe de l'utilisateur – sont envoyées à l'aide du protocole d'authentification NTLMv2. En 2001, des chercheurs en sécurité avaient déjà mis au point une attaque dite par relais SMB : en se positionnant entre un ordinateur Windows et un serveur, les attaquants pouvaient intercepter les informations d'identification, puis les relayer vers le serveur et s'authentifier à la place de l'utilisateur légitime. Mais à l'époque, tout le monde pensait que l'attaque ne fonctionnait qu'en local.

Authentification configurée par défaut dans IE
Sauf que, dans Internet Explorer, l'authentification de l'utilisateur est configurée par défaut avec l'option « ouverture de session automatique réservée à la zone intranet ». Or, les chercheurs en sécurité Jonathan Brossard et Hormazd Billimoria, ont constaté que cette option était ignorée et qu'il était possible de duper le navigateur pour que celui-ci laisse fuiter vers Internet les informations Active Directory de l'utilisateur – c'est à dire son nom et la séquence de code cryptographique basée sur son mot de passe – pour les transmettre à un serveur SMB distant contrôlé par les pirates. Les chercheurs ont pu suivre le trajet d'un fichier DLL propre à Windows, utilisé aussi bien par Internet Explorer que par de nombreuses applications pouvant accéder aux URL, comme Microsoft Outlook, Windows Media Player ou d'autres programmes tiers. « Quand l'application veut accéder à une URL, le fichier DLL vérifie les informations d'authentification dans le registre, mais tout en les ignorant », ont expliqué les chercheurs pendant leur présentation.

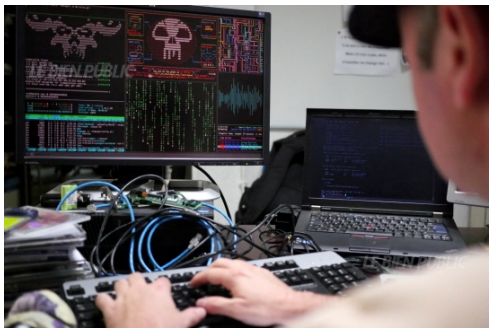
Toutes les versions actuelles de Windows et d'Internet Explorer (ou encore supportées) sont concernées par le problème. « C'est la première attaque à distance capable de compromettre potentiellement Windows 10 et le nouveau navigateur Microsoft Edge », a alerté Jonathan Brossard. « Nous sommes au courant de ce problème et nous enquêtons à ce sujet », a déclaré jeudi un représentant de Microsoft par courriel.

Plusieurs scénarios possibles
« Une fois que les attaquants ont mis la main sur les informations d'identification de l'utilisateur, ils peuvent les utiliser de différentes façons », a précisé Jonathan Brossard. Un premier scénario consisterait à monter une attaque par relais SMB pour s'authentifier à la place de la victime sur des serveurs hébergés hors du réseau local en utilisant une fonctionnalité appelée « NTLM over http », ajoutée pour étendre le périmètre des réseaux dans les environnements cloud. Les pirates pourraient notamment accéder à un shell distant sur le serveur qu'ils utiliseraient ensuite pour installer des logiciels malveillants ou exécuter des programmes exploitant des failles. Si le serveur distant est un serveur Exchange, les attaquants pourraient télécharger toute la boîte aux lettres de l'utilisateur.

Un autre scénario impliquerait de casser la séquence de code cryptographique et de l'utiliser pour accéder à un serveur Remote Desktop Protocol. Des pirates peuvent y arriver en utilisant des plates-formes spécialisées ou des services donnant accès à une grosse puissance de calcul. Un mot de passe de huit caractères ou moins peut être craqué en deux jours environ. « Et, déchiffrer toute une liste de hashs volés ne serait pas plus long, puisque le processus teste toutes les combinaisons à la fois », a ajouté le chercheur. Des identifiants Windows volés via Internet seraient également utiles à des attaquants qui ont déjà réussi à se faufiler dans un réseau local, mais ne disposent pas des privilèges d'administration. En envoyant un simple message électronique à l'administrateur légitime, ils pourraient récupérer ses identifiants dans Outlook et utiliser le hash volé pour mener une attaque par relais SMB contre les serveurs connectés au réseau local.

Source : http://www.lemondeinformatique.fr/actualites/lire-black-hat-2015-on-peut-voler-des-identifiants-active-directory-depuis-internet-via-smb-62000.html
Par Jean Elyan et IDG News Service

Alerte à partager : Vigilance face au logiciel malveillant Didrex | Le Net Expert Informatique

	Alerte à partager : Vigilance face au logiciel malveillant Didrex

Vols d'identifiants et d'informations personnelles, transferts de fonds non autorisés… devant la multiplication du nombre d'ordinateurs infectés par le logiciel malveillant Dridex, la gendarmerie nationale lance une mise en garde à tous les utilisateurs d'Internet et distille quelques conseils pour se prémunir de la menace.

Depuis le début du mois de juin 2015, la France fait face à une campagne massive de dissémination de logiciel malveillant (malware) par le biais de courriers électroniques non sollicités (Spam). Ce logiciel connu sous le nom de «Dridex» a pour vocation d'infecter les postes informatiques utilisant le système d'exploitation Microsoft Windows (toutes versions allant de Windows XP à Windows 8.1). Actuellement, 28 000 postes sont infectés en France.

Un mail trompeur sous forme de facture
Le but de ce logiciel est de prendre le contrôle de la machine à des fins crapuleuses. En effet, après avoir été infecté, le poste informatique compromis va servir, à la fois, à la collecte de données personnelles (numéro de compte, identifiants et mot de passe de connexion, numéro de carte bancaire, historique de navigation, etc.) ainsi qu'à la réalisation de manœuvres frauduleuses (transfert d'argent, connexion à des sites Internet, envoi de message, relais mandataire, etc.) et ce, à l'insu du légitime propriétaire de la machine. La victime, particulier ou entreprise, est destinataire d'un message électronique contenant une pièce jointe, le plus souvent, un document au format Microsoft Word/Excel, voire dans certains cas, au format portable Document File (.pdf). Cette pièce jointe est souvent intitulée «Invoice» ou «facture» et l'objet du message est souvent en lien avec un paiement ou une facture.

Tous vos codes et données collectés
L'ouverture de cette pièce jointe entraîne, lorsque l'activation des macros est autorisée, le téléchargement d'un logiciel malveillant qui va permettre la prise de contrôle à distance de la machine. Par la suite, lorsque la victime se connecte au site de sa banque en ligne, le malware, va récupérer toutes les informations intéressantes (identifiant, mot de passe, nom, prénom, numéro de téléphone, numéro de compte, numéro de carte bancaire, solde du compte, etc.). Muni de l'ensemble de ces données, l'escroc va alors réaliser des transferts de fonds depuis le compte de la victime vers celui d'une tierce personne pouvant se trouver en France, mais plus généralement à l'étranger.

Comment se prémunir de Didrex
-> Observez une grande vigilance vis-à-vis de la messagerie électronique et ayez un esprit critique sur l'origine des messages qui vous parviennent
– Supprimez tous les e-mails suspects prospectifs (spam) reçus dans la boîte de messagerie, surtout s'ils contiennent des pièces jointes.
– N'ouvrez surtout pas les documents en pièce jointe contenus dans un spam; il suffit de les supprimer.
– Si vous avez des suspicions sur un courriel prétendant provenir d'organisations légitimes (banques, administrations, sites de ventes, etc…), il vaut mieux avant, vérifier auprès de ces organisations en question, la véracité de l'envoi du message et l'authenticité de la pièce jointe.
– Installez une solution antimalware qui protège également des spams. En premier lieu, cela devrait du moins réduire ou au mieux éliminer le risque d'ouvrir accidentellement un de ces pourriels et pièces jointes malveillantes
– Désactivez les macros exécutables automatiquement dans Microsoft Word et Excel
– S'il y a soupçon d'infection, changez immédiatement le mot de passe d'accès au compte bancaire en ligne, pour ce faire veuillez contacter rapidement votre établissement bancaire et l'alerter d'un risque potentiel de fraude. DRIDEX étant capable de dérober d'autres types d'identifiants de connexion, il est vivement recommandé pour tous autres accès à des services en ligne, de modifier les « logins et mots de passe ». ATTENTION : faites ceci en utilisant un autre moyen de connexion que l'ordinateur suspecté d'infection
– Procédez à la même mesure concernant tous autres comptes de services internet dont vous êtes titulaires (fournisseur d'accès internet, vente en ligne, réseaux sociaux, etc…). Dridex vole aussi ce genre d'information
– Surveillez l'activité de vos comptes bancaires et vérifiez la légitimité de vos transactions.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.bienpublic.com/actualite/2015/08/06/la-gendarmerie-appelle-a-la-vigilance-face-a-didrex

---

Une faille de sécurité de Hacking Team a été utilisée par un important groupe de pirates | Le Net Expert Informatique

Une faille de sécurité de Hacking Team a été utilisée par un important groupe de pirates

Des groupes de pirates informatiques ont utilisé, peu après leur publication, le contenu des fichiers volés à l'entreprise Hacking Team pour se livrer à des tentatives de piratage, révèle l'entreprise de sécurité Kaspersky. Selon Kaspersky, le groupe « Darkhotel », notamment, a utilisé des vulnérabilités qui avaient été employées par Hacking Team, une entreprise spécialisée dans la vente de logiciels de surveillance.

« Darkhotel » s'est notamment signalé par le passé pour avoir utilisé des méthodes élaborées pour placer des logiciels espions – par exemple en prenant le contrôle des réseaux wifi utilisés dans de grands hôtels. Parmi ses cibles figurent des dirigeants de très grandes entreprises, dans la chimie, les cosmétiques ou la pharmacie, des militaires et des responsables d'ONG, dans plusieurs pays d'Europe, d'Asie et d'Afrique, toujours selon Kaspersky. Des cibles et un niveau de sophistication qui laissent supposer à Kaspersky qu'il s'agit d'un groupe étatique ou soutenu par un Etat.
Hacking Team, société italienne à la réputation sulfureuse, est spécialisée dans la vente de logiciels espions et de dispositifs de surveillance électronique. L'intégralité des données de l'entreprise a été publiée en ligne après un piratage, y compris le contenu des messageries de la société. Des associations et des élus européens ont demandé l'ouverture d'une enquête sur les pratiques commerciales de la société, soupçonnée d'avoir notamment vendu des logiciels au Soudan, et une réforme de la législation sur l'exportation de ces technologies.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemonde.fr/pixels/article/2015/08/10/une-faille-de-securite-de-hacking-team-a-ete-utilisee-par-un-important-groupe-de-pirates_4719735_4408996.html

---

Démonstrations de piratages au salon de «hackers» de Las Vegas | Le Net Expert Informatique

Démonstrations de piratages au salon de «hackers» de Las Vegas

Des pirates informatiques ont fait aussi bien que la bande de George Clooney dans Ocean's eleven en arrivant samedi, lors d'un salon à Las Vegas, à ouvrir un coffre-fort et à tromper la vigilance des caméras de surveillance sans être repérés.

La réalité a fini par dépasser la fiction. Eric Van Albert et Zach Banks, deux chercheurs en informatique, ont fait dans la vraie vie ce que Hollywood a déjà accompli à moult reprises. Ils ont détourné le flux vidéo de caméras de sécurité pour injecter à la place leurs propres images et ainsi tromper la vigilance des surveillants en leur faisant croire que tout était normal. En général, au cinéma, c'est là que les cambrioleurs en profitent pour amasser leur butin et s'enfuir ni vu ni connu. Dans les faits, il ne s'agit que d'une simple démonstration, réalisée à l'occasion de la Def Conf, un célèbre salon de «hackers» à Las Vegas.
«Nous avons mis sur pied notre dispositif en restant le plus fidèle possible à ce qui se fait dans les films», a déclaré Eric Van Albert. «Nous voulions voir à quel point ce type d'attaque était plausible», a-t-il ajouté. Lui et son acolyte ont dépensé environ 500 dollars pour fabriquer l'outil qui permet de pénétrer le câble reliant les caméras aux écrans des gardiens. Le flux est ensuite passé à la moulinette d'un programme informatique qui restitue des images inoffensives.

Ouvrir un coffre-fort avec une clef USB
Les deux chercheurs pourraient s'associer avec Daniel Petro et Oscar Salazar de Bishop Fox, une entreprise de sécurité informatique qui a réussi à ouvrir un coffre-fort avec une clé USB. Le coffre n'était pas une boîte en métal épais «toute bête» mais était équipé pour compter les billets et créditer les comptes de dépositaires par internet. Les deux hommes ont indiqué qu'ils avaient choisi la prise USB parce qu'elle leur permettait d'utiliser un ordinateur plus puissant pour ouvrir le coffre. Mais Daniel Petro a souligné que, de toute façon, il fallait accéder physiquement au coffre pour pouvoir en retirer l'argent.
Pour éviter que ce scénario hollywoodien ne se répète, les deux hommes ont prévenu la compagnie qui fabrique les coffres-forts, et qui a déjà trouvé une parade à ce type d'attaque.

Source : http://www.lefigaro.fr/secteur/high-tech/2015/08/09/32001-20150809ARTFIG00158-des-hackers-s-inspirent-de-hollywood-pour-piller-des-coffres-forts.php

---

Vie privée et données personnelles sous Windows 10 : les astuces de la Cnil pour vous protéger | Le Net Expert

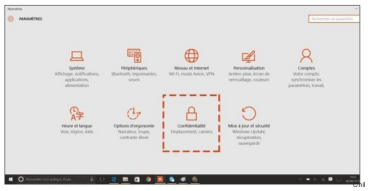
Informatique

Vie privée et données personnelles sous Windows 10 : les astuces de la Cnil pour vous protéger

La Commission nationale de l'informatique et des libertés (Cnil) a diffusé lundi 10 août un communiqué pour aider les utilisateurs du flambant neuf Windows 10 à protéger leurs données personnelles.

Au cœur d'une polémique depuis l'adoption d'une nouvelle politique sur la collecte des données privées, le dernier système d'exploitation de Microsoft s'est vu attaqué ces derniers jours par des utilisateurs mais aussi par Marine Le Pen qui dénonçait « l'espionnage généralisé des ordinateurs des Français ».
La présidente du FN avait d'ailleurs interpellé la Cnil « pour analyser les conséquences de Windows 10 sur la vie privée des Français » et demandé des mesures « afin que Microsoft se conforme à la loi française sur la protection de la vie privée. »
Rien de tel pour l'heure mais l'organisme propose à défaut la série de réglages ci-dessous pour « limiter la communication de vos informations à l'éditeur et à ses partenaires. »

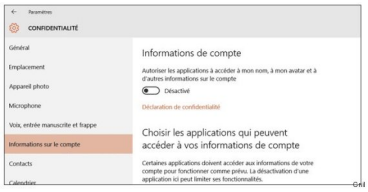
• Cliquez sur le logo Windows en bas à gauche puis sur » Paramètres « . Sélectionnez alors le menu » confidentialité » où vous pourrez modifier les principales fonctionnalités qui collectent des données :



Cnil

• Pour limiter le plus l'envoi de vos données, vous pouvez systématiquement tout désactiver.

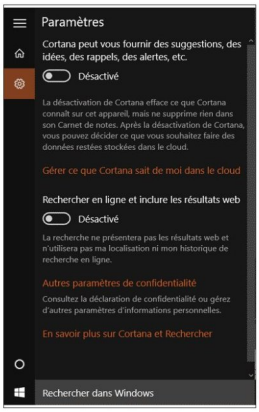
• Par défaut la géo-localisation de votre poste est activée. Il est recommandé de la désactiver depuis l'onglet » Emplacement « .



Cnil

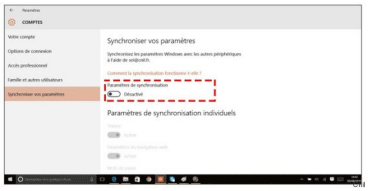
• Vous pouvez désactiver complètement la collecte de données ou empêcher certaines applications d'y accéder. Notamment pour l'Appareil photo, le Microphone, les Informations de Compte, les Contacts, lu Calendrier, la Messagerie, les communications Radio et la synchronisation avec les Autres appareils.

• Cortana, l'assistante embarquée dans Windows 10, a besoin d'accéder à plusieurs types d'informations pour fonctionnet. Vous pouvez désactiver Cortana soit en cliquant sur l'icone de Cortana (le cercle) soit directement depuis la barre des taches, soit depuis le menu démarrer. En cliquant sur le livre puis sur » Paramètres » de Cortana.



Cnil

• Si vous disposez d'un compte connecté qui synchronise vos paramètres entre les différents terminaux équipés de Windows 10, vous pouvez désactiver cette synchronisation (et la collecte des données associées), en allant dans la fenêtre de » Paramètres » et en cliquant sur » Comptes « .



Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.huffingtonpost.fr/2015/08/10/vie-privee-donnees-personnelles-windows-10-astuces-cnil_n_7965788.html

Données biométriques au travail : les employeurs dans le flou | Le Net Expert Informatique

	**Données biométriques au travail : les employeurs dans le flou**

Les données biométriques sont à nouveau au cœur du débat. Il n'est pour l'heure pas interdit aux entreprises de réclamer ces données à leurs employés. Mais la situation est-elle sur le point de changer ? C'est la question qui se pose après que l'ICT Appeal Tribunal a donné raison à Amanda Jones, à titre posthume, ce mercredi 5 août. Celle-ci avait refusé de donner ses empreintes digitales alors qu'elle était employée à la Clavis Primary School, à Moka. Elle aurait été renvoyée à la suite de son refus.

Le jugement de l'ICT Appeal Tribunal soulève de nouveau la question du droit des employés de refuser de donner leurs empreintes digitales. Pour l'instant, comme l'explique Pradeep Dursun, président de la Mauritius Employers' Federation (MEF), donner ses empreintes digitales fait partie des conditions d'emploi dans certaines entreprises.

Mais depuis les contestations de la part, entre autres, d'employés de la Cargo Handling Corporation Ltd et d'Alteo Limited, les employeurs sont dans le flou. La MEF attend que la Cour suprême tranche dans l'affaire opposant des syndicats de l'industrie sucrière à Alteo Limited sur cette question. Elle sera alors fixée. Mais, précise Pradeep Dursun, ce n'est pas seulement le privé qui est concerné, mais aussi le secteur public.

De leur côté, les syndicats maintiennent la pression sur cette question de protection des données personnelles. Des syndicalistes du privé, ainsi que Radhakrishna Sadien de la Government Services Employees' Association, souhaitent que les données biométriques soient détruites au même titre que celles de la carte d'identité nationale.

Une employée obtient gain de cause à titre posthume

Amanda Jones, une ex-enseignante de la Clavis Primary School, avait fait appel au Data Protection Office (DPO) à la suite de son renvoi. Celui-ci avait réclamé une enquête de la police. La plaignante, qui est décédée le 17 juin 2014 en Australie, a ensuite obtenu gain de cause auprès du DPO. La Clavis Primary School a fait appel auprès de l'ICT Appeal Tribunal, qui a rejeté cet appel. Dans son jugement, le tribunal a indiqué qu'à aucun moment il n'y a eu d'accord explicite de l'employée. Mais l'institution primaire privée pourrait saisir le recours en appel de la décision de l'ICT Appeal Tribunal, a indiqué à l'express l'avocat de la Clavis Primary School, Me Hervé Duval Jr.

Source : http://www.lexpress.mu/article/266939/donnees-biometriques-au-travail-employeurs-dans-flou