L’accès à The Pirate Bay bloqué par les FAI français d’ici 15 jours

L’accès à The Pirate Bay bloqué par les FAI français d’ici 15 jours

The Pirate Bay a refait surface en février, sept semaines après sa fermeture. Mais suite à une décision de justice de décembre, il sera bloqué pour les abonnés d’Orange, SFR, Bouygues Telecom et Free.

The Pirate Bay et sa myriade de copies ne seront quasi-plus visibles sur le Web français d’ici quelques jours. Cette information, de NextInpact, nous a été confirmée par la SCPP. Celle qui gère les droits des producteurs de musique avait saisi le TGI de Paris en février 2014 pour obtenir ce blocage, et avait eu gain de cause le 4 décembre. Six jours plus tard, le galion pirate était coulé, rendant la décision inutile… jusqu’à son retour.

L’agrégateur de liens de téléchargement a refait surface le 2 février alors qu’entre-temps, des dizaines de miroirs s’étant procurés la base de données originelle avaient vu le jour. Il n’aura pas fallu plus de quatre jours à la représentante des majors du disque pour ajuster ses canons, refaire feu sur The Pirate Bay, et arroser les 150 sites similaires. Mais pourquoi est-ce la SCPP qui « appuie sur le bouton » pour « activer » ce blocage ?

Les nouvelles copies seront aussi visées

En fait, une décision de justice civile n’est applicable qu’à compter de la signification du jugement par une des parties à l’autre partie. « La décision a bien été notifiée aux FAI à la fin du mois de janvier 2015 », nous dit Marc Guez, le directeur de la SCPP. A partir de vendredi 6 février, les fournisseurs ont un délai de 15 jours.
Contacté, Bouygues Telecom confirme qu’il appliquera ce blocage « durant la semaine prochaine ». Les autres FAI français devront faire de même, à l’exception de Numericable, qui n’avait pas été assigné par la SCPP à l’époque. Pour ce qui est des nouvelles copies de The Pirate Bay qui échapperaient de fait à ce filtrage, « elle feront l’objet d’une demande complémentaire auprès du tribunal, dans le cadre d’une procédure rapide ».
Marc Guez souligne que d’autres actions, visant par exemple T411, sont en cours devant les tribunaux.

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

S o u r c e :
http://pro.clubic.com/legislation-loi-internet/obligations-fournisseur-acces/actualite-753139-blocage-pirate-bay.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_07/02/2015&partner=-&svc_position=853900462&svc_misc=-&crmID=639453874_853900462&estat_url=http%3A%2F%2Fpro.clubic.com%2Flegislation-loi-internet%2Fobligations-fournisseur-acces%2Factualite-753139-blocage-pirate-bay.html

---

A la Une | [Vidéo] Un clip silencieux pour lutter contre la cyberviolence

Un clip silencieux pour lutter contre la cyberviolence

Un enfant qui saute dans le lit de ses parents et qui tend, tout sourire, une carte à sa mère. Elle l'ouvre et lit, écrit d'une main d'enfant, «bonne fête des mères sale chienne» : un clip silencieux de 54 secondes veut prévenir le harcèlement et la violence des jeunes sur internet.

«Imaginez que votre enfant vous parle comme il parle peut-être déjà sur internet», poursuit alors le clip de 54 secondes.

Diffusée dans les salles de cinéma, à la télévision et sur YouTube à partir de mardi prochain, à l'occasion de la journée de l'internet sans crainte, la vidéo a pour ambition de «sensibiliser les parents à la violence des échanges de leurs pré-ados et ados sur les réseaux sociaux» et de faire «prendre conscience aux enfants que l'expression sur ces mêmes réseaux sociaux peut heurter».
Réalisé par la cinéaste Clarisse Canteloube, le film vise à démontrer en moins d'une minute que pour les jeunes, pourtant éduqués au respect et à la tolérance, internet est souvent considéré comme une «zone de non-droit».
Parallèlement au film, un label «Respect Zone» a été créé: «apposer le logo Respect Zone sur son site, sa page Facebook ou Twitter, c'est afficher publiquement son engagement citoyen et responsable contre la cyberviolence», explique son créateur Philippe Coen, président de l'association Initiative de prévention de la haine.
«Il permet de dire ouvertement que vous êtes dans un espace virtuel dans lequel le respect compte et a du sens», poursuit-il.
Ces deux initiatives ont notamment reçu le soutien de Nora Fraisse, la mère de Marion, une adolescente qui s'était suicidée en février 2013, victime d'insultes au collège et de cyberharcèlement: «par cette campagne et la diffusion du label Respect Zone, c'est un message de prévention qui est diffusé pour que chacun à son niveau prenne conscience de la dangerosité des mots».

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

Source : http://www.dna.fr/actualite/2015/02/06/video-un-clip-silencieux-pour-lutter-contre-la-cyberviolence

---

Attaque informatique à la Ville de Montréal | Pierre-André Normandin | Matériel

informatique

	**Attaque informatique à la Ville de Montréal**

Une attaque informatique a frappé la Ville de Montréal, hier après-midi. Près d'une vingtaine de postes de travail ont été infectés par un nouveau logiciel malveillant reçu par courriel.

« Au cours des dernières heures, plusieurs postes de travail ont été infectés par un logiciel malveillant », prévenait hier un message envoyé aux 28 000 employés de Montréal. L'avis précisait que le virus crypte les données du poste de travail infecté et des répertoires réseau connectés au poste. Du coup, les employés perdent l'accès à tous leurs fichiers informatiques.
L'ampleur des dommages causés par l'attaque n'est pas claire. Il n'a pas été possible de savoir si des données ont été volées. Le message de la Ville précisait simplement que le service des technologies s'affairait à récupérer les informations perdues et à enrayer la propagation du logiciel malveillant.
Le virus a touché « moins de 20 postes de travail répartis dans 4 édifices », a indiqué un porte-parole de la Ville, Gonzalo Nunez. Plusieurs d'entre eux se trouvaient à l'hôtel de ville, selon une source.
Les employés dont le poste de travail a été infecté ont reçu un courriel qui leur indiquait qu'ils avaient reçu une télécopie. Le fichier, identifié à leur nom afin de déjouer leur vigilance et portant une extension.zip, contenait toutefois un nouveau logiciel malveillant de type « cryptolocker ». Celui-ci bloque l'accès aux fichiers informatiques de l'ordinateur.
Les logiciels antivirus des ordinateurs infectés étaient à jour, assure la Ville, mais ils n'ont pu bloquer ce nouveau logiciel malveillant. Le fournisseur de la Ville, Symantec, a transmis en après-midi une mise à jour pour contrer le virus.
« Le service des technologies de l'information est en contrôle de la situation. », a affirmé M. Nunez.
Les informaticiens de la Ville ont invité leurs collègues à la prudence. « Pour éviter toute perte de données et préserver l'intégrité de nos infrastructures, nous vous demandons de ne pas cliquer sur les fichiers portant une extension.zip que vous recevez par courriel, peu importe que le courriel provienne de l'interne ou de l'externe. »
Il ne s'agit donc pas du même type d'attaque que celle qui avait ciblé la municipalité de Terrasse-Vaudreuil en janvier, quand son site internet avait été piraté par des sympathisants du groupe État islamique. Le service des technologies de l'information de Montréal croit d'ailleurs que la Ville de Montréal n'était pas délibérément ciblée. « Ce virus semble n'avoir aucun rapport avec la moindre organisation qui fait les manchettes actuellement », a indiqué M. Nunez.

Attaques fréquentes
Les attaques par des logiciels malveillants sont fréquentes, dit Jean-Philippe Nantel, agent de recherche senior au Centre de recherche informatique de Montréal (CRIM). « Ce type d'attaque profite d'une faille d'un programme utilisé par la Ville », résume-t-il.
Le vol de données est possible avec ce type de virus, mais il est principalement utilisé dans des tentatives d'hameçonnage, ajoute M. Nantel. Généralement, après avoir crypté les données d'un ordinateur, un pirate prend contact avec le propriétaire en demandant de l'argent pour déverrouiller les données. Une source a confirmé à La Presse que ce type de message a été reçu.
« Les organisations comme Montréal ont beaucoup de moyens pour contourner ces logiciels malveillants. En théorie, elles sont protégées. Les employés ne perdront pas des années de travail. Ils vont peut-être perdre la journée ou au pire la semaine. C'est plus un désagrément que du vol de données », dit M. Nantel.

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

Source : http://techno.lapresse.ca/nouvelles/materiel-informatique/201502/05/01-4841461-attaque-informatique-a-la-ville-de-montreal.php
Par Pierre-André NORMANDIN

Plusieurs entreprises visées par des hackers

Plusieurs entreprises visées par des hackers

La prudence doit être de mise lorsque vous ouvrez vos e-mails. Une dizaine de cas de «ransomware», une arnaque informatique qui tente de soutirer une rançon aux victimes, ont été recensés cette semaine par le CIRCL, le Computer Incident Response Center Luxembourg. Ce type d'attaque est «techniquement très avancé depuis quelques semaines», a indiqué le CIRCL.

Ces piratages prennent la forme d'un e-mail dans lequel un lien ou une pièce jointe contient un logiciel malveillant qui prend en otage les données personnelles contenues sur l'ordinateur. Une fois les fichiers bloqués, les hackers invitent les victimes à payer de 500 à 1 000 euros pour, soi-disant, résoudre le problème.

Restaurer ses fichiers
Parmi les cas recensés ces derniers jours au Luxembourg, ce sont principalement des entreprises qui ont été touchées. Un ordinateur infecté peut alors bloquer les fichiers de tous les ordinateurs connectés au réseau de l'entreprise. Les données sont ensuite quasiment impossibles à récupérer vu la complexité du code utilisé actuellement par les hackers.
Le CIRCL suggère à toutes les entreprises de bien vérifier leur back-up. «Souvent les entreprises sauvegardent leurs fichiers mais ne vérifient pas que leur back-up est bien fait», explique-t-on au CIRCL. Il faut donc vérifier que les fichiers sauvegardés peuvent bien être restaurés et qu'ils disposent d'une période de conservation adéquate. Du côté des particuliers, sauvegarder ses données personnelles sur un disque dur externe est un bon réflexe. «Mais il ne faut pas laisser le disque dur branché à l'ordinateur», insiste-t-on encore au CIRCL, faute de quoi les fichiers contenus sur le disque dur externe seront aussi accessibles aux hackers

Comment reconnaître un «ransomware»?
Ce type d'attaque informatique circule via les liens ou les pièces jointes d'un e-mail. Souvent, il s'agit de courriers électroniques demandant de payer une facture. L'adresse du destinataire ne paraît à première vue pas suspecte.

Comment les éviter?
Pour éviter de se faire hacker, il faut donc garder en tête les précautions de base. Par exemple, ne pas cliquer sur un lien ou ouvrir un fichier .pdf, .zip ou .doc de la «Deutsche Telekom» si vous n'avez pas de facture à recevoir de cet opérateur. De même avec un e-mail pour un colis que vous n'attendez par, par exemple.
Le CIRCL recommande aussi de mettre à jour vos logiciels, y compris les plug-ins des navigateurs (comme Flash, Java, Silverlight, etc.) et de vous assurer que votre anti-virus est bien à jour.

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

Source : http://www.lessentiel.lu/fr/news/story/15460014

Des rebelles syriens piratés grâce à de faux profils Skype et Facebook

Des rebelles syriens piratés grâce à de faux profils Skype et Facebook

Victimes de «femmes fatales» sur les réseaux, ils se sont fait dérober des informations militaires ou personnelles.
La recette est vieille comme l'espionnage, mais elle fonctionne toujours à l'ère numérique : pour soutirer des informations à la rébellion syrienne, un groupe de pirates informatiques encore non identifié a utilisé de faux profils féminins sur les réseaux Skype et Facebook. C'est ce qu'a découvert une équipe de chercheurs travaillant pour la société américaine de sécurité informatique FireEye, dont le rapport, intitulé «Derrière les lignes de front numérique du conflit syrien», a été publié ce 2 février.

«MATA HARI NUMÉRIQUES»
La récolte est considérable. En remontant le fil de documents PDF contenant des logiciels malveillants (ou malwares), les chercheurs ont découvert un ensemble de 7,7 GB de données «révélant la stratégie de l'opposition syrienne, des plans de bataille, des besoins d'approvisionnement, et une foule d'informations personnelles et de sessions de messagerie instantanée appartenant aux hommes qui combattent les forces du président syrien Bachar al-Assad». Le piratage, qui se serait déroulé a minima de novembre 2013 à janvier 2014, a visé aussi bien des rebelles liés à l'Armée syrienne libre que des membres de groupes islamistes armés et des personnes sans affiliation précise. Parmi la soixantaine de cibles directes identifiées – un chiffre minimal, qui correspond au nombre de comptes Skype compromis –, l'équipe a notamment repéré un chef d'unité combattante, un ex-officier de haut rang ayant déserté les services de sécurité d'Assad, un coordinateur local d'une ONG turque, ou encore un membre d'un centre de presse basé en Syrie.
Lors de leurs échanges avec les «femmes fatales», les opposants au régime syrien se voyaient demander s'ils utilisaient Skype «sur un ordinateur ou sur [leur] téléphone», avant de recevoir une photo abritant le malware adéquat, grâce auquel les attaquants pouvaient ensuite accéder à l'ordinateur de leur cible. Les profils Facebook correspondants étaient, eux, truffés de liens malveillants, cachés derrière des discours favorables à l'opposition et des invitations à utiliser des outils de sécurisation des communications, tels que des réseaux privés virtuels ou le réseau d'anonymisation Tor.
Une stratégie de «Mata Hari numérique», comme l'a noté Martin Gropp, journaliste à la Frankfurter Allgemeine Zeitung :

DES OUTILS «SUR MESURE»
L'utilisation de faux profils féminins sur les réseaux sociaux à des fins d'espionnage n'est pas une nouveauté. Nicolas Arpagian, directeur scientifique à l'Institut national des hautes études de la sécurité et de la justice, fait notamment état d'une opération du même genre attribuée au Hezbollah : d'après un article du Spiegel paru en mai 2010, un faux profil Facebook aurait permis de soutirer des informations à quelque 200 soldats ou réservistes de l'armée israélienne. Il y a deux ans, une étude du département de la Défense australien a accusé les talibans d'user de la même méthode pour espionner ses soldats.

Dans le cadre du conflit syrien, en revanche, le déploiement à cette échelle de la méthode est inédit. «C'est la première fois que nous constatons un tel degré de sophistication dans l'utilisation de faux profils, et dans cet objectif», explique John Scott-Railton, chercheur associé au Citizen Lab de l'université de Toronto et l'un des auteurs du rapport de FireEye. Le mode opératoire – qui repose en grande partie sur «l'ingénierie sociale», autrement dit l'exploitation des failles humaines – n'est pas la seule différence avec ce qu'il a pu examiner jusqu'à présent (1). «Ces acteurs ont utilisé une boîte à outils plus diversifiée que ce que nous avions observé de la part de hackers pro-gouvernement ou dans l'attaque liée à l'EI, poursuit Scott-Railton. Ils ont des outils « sur mesure ». Et ils ont clairement ciblé des informations de nature militaire.» Au final, souligne le rapport, la moisson d'informations récoltées avait de quoi offrir «un avantage immédiat sur le champ de bataille».
L'attaque reste néanmoins assez peu technique, estime Raphaël Vinot, chercheur en sécurité au CERT (2) national du Luxembourg. La plupart des logiciels utilisés reprennent du code qui circulait déjà sur Internet. Le logiciel de prise de contrôle des ordinateurs à distance, dénommé «Darkcomet», existe depuis 2008 – son créateur, un programmeur français, a même cessé de le développer face aux utilisations malveillantes qui en étaient faites. «C'est un outil lourd, vraiment pas discret, estime le Luxembourgeois. Mais les antivirus ne le détectent pas, donc cela fonctionne dans la majorité des cas.»

Pour lui, l'outil le plus évolué pourrait être le malware ciblant le système d'exploitation pour smartphones Android. Ce qui est également, selon les chercheurs de FireEye, une nouveauté dans le contexte syrien. Or les smartphones sont une mine d'informations, en particulier dans une zone où, explique le rapport, «les pannes de courant régulières peuvent pousser les gens à se fier encore plus aux mobiles pour communiquer».

LA PISTE LIBANAISE
Quant à savoir qui se cache derrière cette opération, mystère. Les auteurs de l'étude avancent prudemment avoir «des indications selon lesquelles le groupe pourrait être financé et/ou situé en dehors de la Syrie». Ils font néanmoins état de multiples références au Liban, que ce soit dans les faux profils ou sur le site web mis en ligne par le même groupe, présenté comme émanant de l'opposition syrienne et lui aussi truffé de logiciels malveillants. Par ailleurs, deux versions de test des malwares utilisés ont été mises en ligne depuis le Liban. Vraie ou fausse piste ? «Avec Internet, tout est possible, rappelle John Scott-Railton. Mais si ce groupe a fait preuve d'une certaine sophistication dans l'attaque, peut-être qu'en matière de sécurité opérationnelle, il n'était pas en capacité de mettre en place une énorme « fausse bannière ».»

«C'est à juste titre que le rapport reste prudent, juge Eva Galperin, analyste à l'Electronic Frontier Foundation, qui a travaillé sur une précédente étude de cyberattaques en Syrie. Attribuer une attaque informatique est très difficile, et je ne vois rien, pour l'instant, qui indique de manière définitive un acteur originaire du Liban.» A ce stade donc, difficile d'aller plus loin que les conjectures. D'autant qu'à la différence de l'Armée électronique syrienne, qui s'illustre depuis près de trois ans par des coups d'éclat prioritairement orientés vers les médias – et dont Le Monde a été la plus récente victime –, ce groupe-ci a agi dans la plus grande discrétion.

Avant de rendre public leur rapport, les chercheurs ont contacté quelques-unes des victimes du piratage. Lesquelles ont eu une réaction assez fataliste : «Les groupes syriens ont tellement l'habitude que leurs communications soient espionnées, conclut Scott-Railton, qu'ils ne sont pas vraiment surpris d'avoir été piratés. En général, ils estiment qu'ils ont d'autres problèmes plus urgents.» Non seulement le cyberespionnage se démocratise très manifestement, mais il a en prime de beaux jours devant lui.

(1) Voir notamment les deux précédentes études auxquelles il a participé : l'une sur les attaques menées par des pirates informatiques pro-gouvernement («Quantum of Surveillance», rapport conjoint du Citizen Lab et de l'Electronic Frontier Foundation), l'autre consacrée à une attaque par malwareliée à l'État islamique.

(2) Computer Emergency Response Team, le centre d'alerte et de réaction aux attaques informatiques.

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

Source : http://www.liberation.fr/monde/2015/02/04/des-rebelles-syriens-pirates-grace-a-de-faux-profils-skype-et-facebook_1194718

Statut de l’hébergeur : nouvelles passes d’armes en prévision

Statut de l’hébergeur : nouvelles passes d’armes en prévision

Ce n'est pas la première fois qu'une reforme du statut des hébergeurs est évoquée et ça ne sera surement pas la dernière : le coup vient cette fois de la ministre de la Culture Fleur Pellerin qui appelle dans une interview du journal Les Echos à une réévaluation du statut juridique de l'hébergeur. « Ces statuts datent de la loi de confiance dans l'économie numérique, de 2004, qui transpose elle-même une directive européenne de 2000. Internet a évolué depuis ! ».

L'objectif affiché par Fleur Pellerin est ici de permettre une meilleure lutte contre la contrefaçon en ligne d'œuvre de l'esprit. Si la ministre exclut la possibilité de rendre ces « plateformes » entièrement responsables du délit, elle appelle à la mise en place d'un statut « hybride » afin de garantir une meilleure défense du droit d'auteur et une plus grande réactivité face à ces contenus illégaux.
Des propositions qui s'inspirent librement des recommandations émises par le conseil d'état comme le souligne Nextinpact, qui avait dans son rapport annuel 2014 consacré au numérique évoqué la mise en place d'un principe de « loyauté des plateformes » qui se traduirait par une série d'obligations et de contraintes venant limiter la marge de manœuvre des éditeurs vis-à-vis des contenus qu'ils diffusent via leurs services.

L'Afdel craint les effets de rebonds
La reforme du statut des hébergeurs est un thème qui revient régulièrement dans les projets législatifs et autres rapports du gouvernement. Mais celui-ci ne manque pas de faire réagir l'Afdel, qui a publié par voie de communiqué une longue tribune mettant en garde le gouvernement à l'égard de ces mesures. Si l'Association des éditeurs de logiciels ne parait pas opposée sur le principe à de nouvelles mesures visant à protéger plus efficacement les œuvres de l'esprit, elle s'inquiète des éventuels ricochets que pourrait provoquer une reforme du statut de l'hébergeur.
L'association souligne ainsi que « le statut juridique de l'hébergeur ne fait pas la différence entre différents types d'hébergeurs (B2C, B2B…) » Un point à clarifier pour l'Afdel, qui s'inquiète d'un impact possible de ce nouveau statut sur les entreprises proposant des services en mode Saas ou « qui stockent des données à la demande du destinataire du service ».
Le gouvernement reste pour l'instant évasif sur les prochaines mesures concrètes visant à matérialiser cette volonté affichée. Mais la grande loi sur le numérique promise par Axelle Lemaire pour 2015 est encore dans les cartons et sera peut être l'occasion pour le gouvernement de détailler leurs intentions.

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

Source : http://www.zdnet.fr/actualites/statut-de-l-hebergeur-nouvelles-passes-d-armes-en-prevision-39814102.htm
Par Louis Adam

Denis JACOPINI est intervenu au Salon du numérique 2015 le

3 février et a coanimé une conférence avec Orange

Denis JACOPINI est intervenu au Salon du numérique 2015 le 3 février et a coanimé une conférence avec Orange

Imaginez un instant que vous soyez consommateur. Vous découvrez soudain que vos données (coordonnées personnelles, bancaires ou encore médicales) se trouvent diffusées sur le net, sans votre accord, à cause de la négligence d'un professionnel.

Imaginez maintenant que ce professionnel c'est vous, malgré la mise en application imminente du projet de règlement Européen sur la Protection des données personnelles, le risque d'anéantir votre réputation et de vous sanctionner lourdement. Certes, le mal est fait mais pire, les Cybercriminels sauront en profiter !
Comment ne pas être ce professionnel négligeant en protégeant le patrimoine le plus précieux de votre entreprise : Votre réputation
Cette conférence était présentée par Denis JACOPINI (Le Net Expert Informatique) et Eric Wiatrowsi (Orange Business Services)

Présentation pdf de Denis JACOPINI Le Net Expert Informatique
Présentation pptx de Hervé JUHEL Crédit Agricole
Les infos pratiques du salon
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Remise des trophées du 1er concours EDUCNUM Opération Vie privée à la CNIL

	Remise des trophées du 1er concours EDUCNUM Opération Vie privée à la CNIL

Le 28 janvier 2015, lors de la journée européenne de protection des données, le collectif Educnum a remis à la CNIL les prix aux lauréats du premier concours Educnum en présence de Mme Najat Vallaud-Belkacem, Ministre de l'Education nationale, de l'Enseignement supérieur et de la Recherche.

L'ambition des trophées
Pour que le web reste un espace d'échange et d'inspiration, mais aussi de respect de la vie privée, le collectif pour l'éducation au numérique a lancé le 13 octobre 2014 un concours pour les étudiants.

Son objectif :
• sensibiliser les plus jeunes, de l'école primaire au lycée, aux bons usages du web, par un dialogue intergénérationnel ;
• susciter et valoriser la créativité des étudiants ;
• mettre en lumière et donner vie à des projets innovants.

Les étudiants avaient carte blanche pour participer : application mobile, dataviz, goodies ou kit de survie sur les réseaux sociaux, tous les projets étaient les bienvenus.

Les lauréats
25 projets ont été présentés à l'issue de 3 mois de concours.
Le Grand Prix du Jury avec une dotation de 7000 euros est remis à l'équipe du Master 2 « Droit, économie et gestion de l'audiovisuel » à la Sorbonne, pour le projet Les aventures croustillantes de Prince Chip.
Le Prix Spécial du Jury avec une dotation de 3000 euros est attribué à l'équipe de l'Ecole Boulle pour le projet Data Fiction, le site dont vous êtes le héros. Vivre l'aventure, faire réfléchir, accompagner sont au cœur de ces projets qui placent le jeune public au cœur de l'action.

Les projets récompensés
« Prince Chip » Appelle à la vigilance des « âges » pour les 6/10 ans
La pédagogie sur les bonnes pratiques à adopter sur le web passe ici par un divertissement dans l'univers familier des fruits et légumes. Elle repose sur l'identification à un personnage attachant et l'utilisation d'une technique moderne, le stop motion. Le webdocumentaire Les Aventures croustillantes de Prince Chip offre aux adultes un outil d'accompagnement pour parler aux plus jeunes, dès leurs premiers pas sur le net. Unanimité du jury pour remettre le Grand Prix à une fiction qui donne la frite !
Visionner le projet
Pour Serge Tisseron, psychiatre et co-auteur de l'avis de l'Académie des Sciences « L'enfant et l'écran » et membre du jury : « C'est un bonheur de découvrir comment, sur Internet, un méchant poivron peut se faire passer pour une jolie tomate ! Je fais le pari que les autres épisodes sauront toucher avec une égale efficacité la part d'enfance qui existe chez chacun, et à tout âge. »

Devenir héros de son propres site avec « Data fiction » pour les 12/18 ans
Le serious game Data Fiction fait de l'internaute un héros. En partant des outils et services numériques utilisés par les jeunes au quotidien, le projet révèle à l'utilisateur l'exposition de ses données. Ce jeu en trois étapes (découverte, appropriation, tutoriel) fait le pari de l'expérience pour sensibiliser : incité à dépasser ses limites, le jeune devient acteur. Les compétences-métier des étudiants en design de l'Ecole Boulle ont été particulièrement saluées par le jury, « une véritable œuvre d'art ! ».
Visionner le projet

Pour Stéphane Distinguin, Président de Cap Digital et membre du jury, : « Le projet de l'école Boulle m'a particulièrement impressionné, par sa créativité, ses angles, très bien choisis, et la qualité remarquable de sa réalisation. Très cohérent et utile, je l'ai trouvé particulièrement juste ».

Et après ?
Lors de la soirée de remise des prix organisée à la CNIL, les lauréats ont pu rencontrer des membres du collectif Educnum et de la CNIL, la Présidente d'Universcience, la Direction du numérique pour l'éducation. Autant de bons conseils à échanger pour faire grandir ces projets et transmettre les bonnes pratiques au plus grand nombre.
« L'éducation au numérique est une responsabilité partagée qui nécessite une mobilisation générale. Les membres du collectif s'engagent à valoriser les projets retenus sur leurs supports de communication : sites Internet, réseaux sociaux.C'est le moyen pour ces étudiants d'avoir une très bonne visibilité et de pouvoir bénéficier d'une aide dans la réalisation future de leurs projets. », indique Isabelle Falque-Pierrotin, Présidente de la CNIL.

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

Source : http://www.cnil.fr/linstitution/actualite/article/article/remise-des-trophees-du-1er-concours-educnum-operation-vie-privee/

Attention à vos comptes Gmail, cibles de pirates…

	Attention à vos comptes Gmail, cibles de pirates…

Un nombre croissant de comptes piratés est actuellement signalé au Luxembourg. Cela commence toujours par un vol des données de connexion. Dans certains cas, cela passe par un faux message d'erreur qui nous informe que certains e-mails n'ont pas pu être transmis. L'utilisateur est alors prié de cliquer sur un lien qui mène à une prétendue adresse web de Google. C'est ici qu'il devra saisir ses données de connexion.

Une fois qu'ils ont mis la main sur les données de connexion, les criminels convertissent le compte en arabe. Ensuite, une nouvelle adresse e-mail est créée sur Yahoo, très semblable à l'adresse originale (par exemple: pit.luxi@yahoo.com à la place de pit.luxi@gmail.com).
Tout le courrier entrant sur l'adresse gmail est ensuite redirigé vers la nouvelle adresse e-mail contrôlée par les criminels. L'adresse de réponse des e-mails sortants est également sur le compte Yahoo, de sorte que la victime ne se rend pas compte de ce qui se passe. En outre, les criminels copient la liste entière des contacts de la victime et les suppriment du compte Gmail, pour empêcher la victime de communiquer. Ils vident aussi toute la boîte de réception, ainsi que tous les contenus des différents dossiers.

Une fraude perfide
Pendant que la victime se débat avec le rétablissement de la langue d'origine, les escrocs peuvent tranquillement commencer à envoyer des e-mails de phishing ou des demandes d'argent à la liste de contacts des victimes. Si la victime insouciante réinitialise son compte dans les 7 jours, dans sa langue, il verra une notification lui indiquant que tous ses messages sont transférés à l'adresse xxx@yahoo.com. Passé ce délai de 7 jours, la notification disparaît.
Si votre compte Gmail se retrouve subitement dans une autre langue, c'est le signe indubitable qu'il a été piraté et que votre identité à été usurpée.

Les bons réflexes
La police, Bee Secure et CASES vous conseillent de réagir de la manière suivante:
• faites repasser votre compte dans la langue d'origine ;
• désactivez la redirection automatique de vos e-mails ;
• ensuite, modifiez votre mot de passe sans attendre. Un mot de passe solide doit comporter 10 caractères au minimum, avec des caractères spéciaux, des majuscules, des minuscules et des chiffres, de manière à ce qu'il ne figure dans aucun dictionnaire ;
• restaurez vos listes de contacts;
• récupérez vos e-mails disparus (suivez le tutoriel vidéo de la police);
• prévenez vos contacts que votre compte à été piraté et qu'ils ne doivent en aucun cas répondre aux e-mails provenant d'une autre adresse (Yahoo en l'occurrence). Dans la mesure du possible, cette adresse doit être signalée et bloquée par le fournisseur.

☞ La police a réalisé un tutoriel video qui vous guide pour les étapes 1 à 5:

D'un point de vue préventif, les mesures suivantes sont toujours valables:
activez la double authentification sur vos comptes e-mail;
ne saisissez jamais de données personnelles (login, mot de passe, numéro de carte de crédit..) sur une page web que vous avez ouverte en cliquant sur un lien dans un e-mail ;
suivez les bonnes pratiques e-mail (https://www.cases.lu/fr/e-mail-bonnes-pratiques.html).
suivez les conseils donnés dans l'article clever clicks for safer business (https://www.cases.lu/arnaques.html)
Si un ami ou une connaissance vous demande de lui envoyer de l'argent pour l'aider à se sortir d'une situation difficile, il s'agit très probablement d'une arnaque. En cas de doute, appelez votre ami pour prendre de ses nouvelles.
Si vous pensez que le compte e-mail d'un de vos contacts a été piraté, prévenez-le.
Cette vague de phishing vise pour l'instant les comptes Gmail, mais elle pourrait se produire avec tout autre fournisseur de messagerie. Ouvrez l'oeil!
Pour plus d'information, consultez la chaîne TV de la Police. Bee Secure y a participé à l'émission du 15 janvier sur la Cybercriminalité:

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

Source : https://www.cases.lu/fr/comptes-gmail-pirates-copies-et-convertis-en-arabe.html

L’obligation de notification des violations de données à caractère personnel à la CNIL

L’obligation de notification des violations de données à caractère personnel à la CNIL

A l'occasion de la révision des directives « Paquet télécom » en 2009, le législateur européen a imposé aux fournisseurs de services de communications électroniques l'obligation de notifier les violations de données personnelles aux autorités nationales compétentes, et dans certains cas, aux personnes concernées.

Cette obligation de notification a été transposée en droit français à l'article 34 bis de la loi informatique et libertés. Les conditions de sa mise en œuvre ont été précisées par le décret n° 2012-436 du 30 mars 2012, ainsi que par le règlement européen n° 611/2013 du 24 juin 2013.

Dans quels cas l'article 34 bis s'applique-t-il ?
L'article 34 bis de la loi informatique et libertés s'applique lorsque plusieurs conditions sont réunies :
• condition 1 : il faut qu'un traitement de données à caractère personnel ait été mis en œuvre
• condition 2 : le traitement doit être mis en oeuvre par un fournisseur de services de communications électroniques
• condition 3 : dans le cadre de son activité de fourniture de services de communications électroniques (par exemple, lors de la fourniture de son service de téléphonie ou d'accès à d'internet)
• condition 4 : ce traitement a fait l'objet d'une violation. Selon l'article 34 bis, une violation est constituée par une destruction, une perte, une altération, une divulgation, ou un accès non autorisé à des données à caractère personnel. Elle peut se produire de manière accidentelle ou illicite, l'intention malveillante étant l'un des possibles cas de figure, mais pas le seul.

Sont, par exemple, constitutifs d'une violation :
• Une intrusion dans la base de données de gestion clientèle d'un fournisseur d'accès internet (FAI) ;
• Une faille dans la boutique en ligne d'un opérateur mobile permettant de récupérer les numéros de cartes de crédits des clients ayant commandé un nouveau téléphone associé à un forfait (car ce sont les données clients collectées en tant qu'opérateur) ;
• Un email confidentiel destiné à un client d'un FAI, diffusé par erreur à d'autres personnes ;
• La perte d'un contrat papier d'un nouveau client par un agent commercial d'un opérateur mobile dans une boutique.

Ne sont pas des violations de données personnelles au sens de l'article 34 bis :
• Toute violation ne concernant pas un traitement du FAI comme un virus informatique qui s'attaque aux PC des abonnés du FAI pour collecter des données personnelles ;
• Toute activité ne concernant pas la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public tel que le piratage du fichier des ressources humaines du FAI.

Qui doit notifier la CNIL et informer les personnes concernées par la violation ?
L'article 34 bis vise les « fournisseurs de services de communications électroniques accessibles au public ». Il s'agit des opérateurs devant être déclarés auprès de l'ARCEP (article L. 33-1 alinéa 1 du code des postes et des communications électroniques) (par exemple, les fournisseurs d'accès à internet ou de téléphonie fixe et mobile).
Les services de la société d'information, tels que les banques en ligne, les sites d'e-commerce ou les téléservices des administrations, ne sont pas concernés.

Quand et comment notifier la CNIL ?
Toute violation doit être notifiée à la CNIL, quelle que soit son niveau de gravité.
La notification doit être adressée à la CNIL dans les 24h de la constatation de la violation.
Si le fournisseur de services de communications électroniques ne peut fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, il est possible de procéder à une notification en deux temps :
Une notification initiale dans les 24 heures de la constatation de la violation ; puis
Une notification complémentaire dans le délai de 72 heures après la notification initiale.
Cette notification doit se faire par lettre remise contre signature ou via le formulaire de dépôt en ligne accessible sur le site de la CNIL, à l'aide du formulaire de notification prévu à cet effet [faire un lien vers le formulaire de notification].

Quand informer les personnes ?
L'information des personnes doit être effectuée sans retard injustifié après constat de la violation de données à caractère personnel (article 91-2 du décret).
Cependant, le fournisseur n'a pas l'obligation d'informer les personnes dans les cas suivants :
la violation n'est pas susceptible de porter atteinte aux données ou à la vie privée des personnes (un outil permettant d'évaluer le niveau de gravité d'une violation est disponible sur le site de la CNIL) ;
la violation est susceptible de porter atteinte aux données ou à la vie privée des personnes, mais le fournisseur a mis en place des mesures techniques de protection appropriées (article 91-3 du décret). Mises en place préalablement à la violation, ces mesures doivent avoir rendues les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès (voir ci-dessous).

Que sont des mesures de protection appropriées ?
Il s'agit de toute mesure technique efficace destinée à rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès. Par exemple, le fait de chiffrer les données permet de rendre les données incompréhensibles à des tiers dans la mesure où la clé de chiffrement n'a pas été compromise.
Si le fournisseur a mis en œuvre de telles mesures de protection, il doit en informer la CNIL au moment de la notification. En effet, pour que le fournisseur puisse être dispensé d'informer les personnes, la CNIL doit d'abord constater que les mesures sont appropriées et qu'elles ont été efficacement mises en œuvre.
La CNIL a deux mois pour se prononcer sur ces mesures. En cas de silence de la CNIL, elles sont considérées comme ne répondant pas aux exigences de l'article 34 de la loi informatique et libertés et le fournisseur doit avertir les personnes.

La CNIL peut-elle imposer au fournisseur d'informer les personnes ?
Oui, la CNIL peut imposer au fournisseur d'informer les personnes si elle constate que la violation porte atteinte aux données ou à la vie privée des personnes, que les mesures de protection mises ne place n'étaient pas appropriées ou que les personnes n'ont pas été ou ont été mal informé.

Comment informer les personnes ?
L'information des personnes doit être faite par tout moyen permettant d'apporter la preuve de l'accomplissement de cette formalité (par courrier électronique, par exemple). Cette information doit contenir les éléments suivants :
• le nom du fournisseur ;
• l'identité et les coordonnées du correspondant informatique et libertés ou d'un point de contact auprès duquel les personnes peuvent obtenir des informations supplémentaires ;
• le résumé de l'incident à l'origine de la violation ;
• la date estimée de l'incident ;
• la nature et la teneur des données concernées ;
• les conséquences vraisemblables de la violation pour la personne ;
• les circonstances de la violation ;
• les mesures prises pour remédier à la violation ;
• les mesures recommandées par le fournisseur pour atténuer les préjudices potentiels.
En outre, cette information doit être rédigée dans une langue claire et aisément compréhensible. Elle ne doit pas être utilisée comme un moyen de promouvoir ou d'annoncer de nouveaux services ou être associée à d'autres informations (être mentionnée sur la facture adressée aux personnes concernées, par exemple).

Quels sont les risques pris par le fournisseur qui ne notifierait pas ?
Le fournisseur encourt des sanctions pénales car le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la CNIL ou à l'intéressé est puni de cinq ans d'emprisonnement et de 300 000 € d'amende (article 226-17-1 du code pénal).
En outre, tout manquement à la loi informatique et libertés est passible de sanctions administratives, notamment financières pouvant aller jusqu'à 300 000 €.

En cas de violations, le fournisseur a-t-il d'autres obligations que la notification ?
Oui, il doit tenir à jour un inventaire des violations qui doit notamment contenir les modalités de la violation (ce qui s'est passé), l'effet de la violation (les conséquences) et les mesures prises pour remédier à la violation (les actions correctives mises en œuvre).
Ce recensement des violations peut être réalisé sous format papier ou numérique, et doit être conservé à la disposition de la CNIL.

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

Source : http://www.cnil.fr/linstitution/actualite/article/article/la-notification-des-violations-de-donnees-a-caractere-personnel