Attention au whaling, ce phishing qui cible les équipes dirigeantes

	**Attention au whaling, ce phishing qui cible les équipes dirigeantes**

Selon l'entreprise de sécurité Mimecast, les e-mails conçus pour les attaques de phishing de type whaling, qui ciblent de « gros poissons », sont difficiles à détecter.

Selon l'entreprise de sécurité Mimecast, les e-mails conçus pour les attaques de phishing de type whaling, qui ciblent de « gros poissons », sont difficiles à détecter.
Si vous travaillez dans la finance ou la comptabilité et si vous recevez un email de votre patron vous demandant de transférer des fonds vers un compte externe, mieux vaut réfléchir à deux fois avant d'obtempérer. Selon le cabinet de sécurité Mimecast, ces attaques de phishing très élaborées, dites whaling attacks, qui ciblent des cadres ou des directeurs d'entreprises, mais aussi des personnalités du monde politique ou des personnes célèbres, sont en hausse. Pour camoufler la provenance de e-mails, les pirates utilisent des noms de domaine usurpés ou très proche de domaines familiers du destinataire. Tout est fait pour ce dernier croit que les messages proviennent bien de son directeur financier ou du directeur général.

Le nom de domaine est usurpé dans 70% des attaques

55 % des 442 professionnels IT interrogés par Mimecast ce mois-ci ont déclaré que leur entreprise avait constaté une augmentation du volume de ces « chasses à la baleine » au cours des trois derniers mois, comme l'a déclaré le cabinet de sécurité. Les entreprises visées sont localisées aux États-Unis, au Royaume-Uni, en Afrique du Sud et en Australie. « L'usurpation de nom de domaine est la stratégie la plus courante, puisqu'elle est utilisée dans 70 % des attaques », a précisé le cabinet de sécurité. La majorité des faux messages sont signés du CEO, mais près de 35 % des entreprises ont vu passer des emails signés par le directeur financier. « Les messages conçus pour des attaques de whaling peuvent être plus difficiles à détecter, car ils ne contiennent pas de lien hypertexte ou de pièce jointe malveillante, et comptent uniquement sur l'ingénierie sociale pour tromper leurs cibles », explique Orlando Scott-Cowley, un stratège de la cybersécurité chez Mimecast. « Souvent, des sites comme Facebook, LinkedIn et Twitter fournissent aux attaquants les détails dont ils ont besoin pour préparer ces attaques », a encore déclaré Mimecast.

Informer est la première chose à faire

Alors, que faire ? Mimecast a quelques suggestions. D'abord informer les dirigeants, les équipes de management et de la comptabilité sur ce risque. Ensuite, réaliser des tests sur l'entreprise en montant de fausses attaques de whaling pour évaluer la vulnérabilité des employés. Une autre solution consiste à marquer les emails provenant de l'extérieur du réseau de l'entreprise, ou encore à créer des alertes pour signaler des noms de domaine qui ressemblent étroitement à celui de votre entreprise. « Les barrières pour bloquer l'entrée de ces attaques sont à niveau dangereusement bas », a déclaré Orlando Scott-Cowley. « Étant donné que la pêche est très bonne pour les cybercriminels, il est probable que le volume et la fréquence de ce type d'attaques augmentent », a mis en garde Mimecast.

Réagissez à cet article

Les super cartes bancaires

débarquent

Les super cartes bancaires débarquent

Pour lutter contre la fraude, les banques misent sur la technologie. Demain, on paiera avec une carte à code éphémère ou un smartphone à reconnaissance faciale.

Cette révolution est à portée de main. Dans quelques mois, tout devrait changer… dans votre portefeuille. Votre carte bancaire va s'offrir une deuxième jeunesse. Un relooking qui porte un nom barbare : «cryptogramme dynamique». Ce qui, en français, signifie que les trois petits chiffres, situés au verso de votre carte, changeront au bout de quelques minutes.
Les plus grands fabricants de cartes bancaires au monde, Gemalto et Oberthur, ont lancé ces derniers mois la commercialisation de cette technologie. BNP Paribas, la Banque postale, la Société générale… La quasi-totalité des établissements financiers français sont en train de la tester auprès de leurs clients.

Qui va payer ?
Objectif affiché : mieux lutter contre la fraude à la carte bancaire. Un fléau dont la finance aimerait bien se débarrasser. Pas question de laisser les arnaques et les fraudes nuire à l'engouement des Français pour ce mode de paiement. Imaginez, le 5 décembre dernier, la France a battu un record : 42 millions de transactions par carte bancaire en un week-end. Soit 12 % de plus que lors du premier samedi de décembre 2014 !
Un effet logique du boom du commerce en ligne. Pourtant, les banques se laissent encore quelques mois pour un développement à grande échelle de cette carte bancaire plus sécurisée. Car un petit détail reste encore à trancher. Ce bout de plastique bourré de technologies coûte plus cher à produire que la carte à puce classique. Qui va payer ? La banque, les commerçants ou le client ? Les réponses du milieu bancaire restent floues. Les banques trancheront ces prochains mois. Mais elles n'ont plus vraiment le temps de tergiverser. Des start-up dénommées FinTech (technologie financière) commencent déjà à les bousculer, notamment en utilisant le smartphone pour lancer de nouveaux modes de paiement. Et comme d'autres secteurs l'ont appris à leurs dépens, l'immobilisme face aux nouvelles technologies ne paye pas.
«2016 sera l'année des nouveaux modes de paiements», pronostique donc un cadre de banque. Nombre d'établissements ont, dans les cartons, de nouveaux produits qui n'attendent plus qu'une autorisation de la Cnil (Commission nationale de l'informatique et des libertés) pour passer des simples tests à la commercialisation. C'est le cas des technologies de biométrie utilisant des éléments du corps (empreinte digitale, vocale, etc.). Les bons vieux codes bancaires bientôt périmés ?

Un cryptogramme valable 20 minutes
Même largeur, agilité, finesse, robustesse, touché… A priori, rien ne la distingue de sa prédécesseur. A un détail près : la carte bancaire de nouvelle génération est équipée d'un écran. Tout petit. Pas de quoi regarder un film en haute définition. Non, mais tout de même assez large pour afficher, en noir et blanc, les trois chiffres du fameux cryptogramme visuel. Ce code de sécurité réclamé à chaque achat sur la Toile devient «dynamique». «Cette carte est équipée d'une horloge interne. Le code de sécurité sur l'écran change toutes les vingt minutes», explique Frédérique Richert, marketing manageur chez Gemalto, le leadeur mondial de la carte à puce, qui commercialise depuis quelques semaines cette nouvelle technologie. «Cette carte lutte mieux contre la fraude», ajoute-t-elle.

Réduire le coût des fraudes
A priori, rien ne change pour l'utilisateur. Pour effectuer un achat en ligne, il doit toujours remplir les mêmes formulaires en indiquant son nom, son numéro de carte bancaire, la date de validité et le cryptogramme. La différence, c'est que ces coordonnées ont une durée de vie limitée. Si un pirate informatique les vole, il ne peut alors les utiliser que pendant une vingtaine de minutes. Un laps de temps, a priori, trop court pour multiplier les achats sur le Web ou revendre ces informations à d'autres escrocs.
La plupart des grands réseaux bancaires sont en train de tester auprès de leurs clients cette nouvelle technologie. Ainsi, BPCE a équipé depuis plusieurs semaines un millier de clients. BPCE utilise la technologie d'Oberthur, concurrent de Gemalto. Avec un avantage, celui de réduire le coût des fraudes. Car les banques assument une partie du coût de l'arnaque : indemnisation du client pour les achats réalisés frauduleusement, coût du changement du support, etc. «Nous regardons à la fois l'effet de cette nouvelle technologie sur le coût lié à la fraude mais aussi sur la confiance des utilisateurs dans le paiement en ligne, dans l'usage des cartes bancaires», explique Nicolas Chatillon, directeur du développement fonctions transverses du groupe BPCE. Un point stratégique. Car un possesseur de carte bancaire en confiance, c'est un consommateur qui dépense !

Réagissez à cet article

Source : *Les super cartes bancaires débarquent*

Hyatt : encore une chaine d’hôtels prise pour cible par un logiciel malveillant

Hyatt : encore une chaine d’hôtels prise pour cible par un logiciel malveillant

---

La chaine d'hôtels Hyatt vient d'annoncer avoir découvert un logiciel malveillant dans son système de paiement. Il est désormais éradiqué, mais l'étendue des dégâts n'est pas connue. Hyatt n'est que le dernier d'une longue liste d'hôtels dont la sécurité a été mise à mal.

Alors que l'histoire de la porte dérobée dans les pare-feu de Juniper n'est pas encore terminée, une nouvelle affaire de sécurité informatique remonte à la surface. La chaine d'hôtels Hyatt vient en effet d'annoncer officiellement qu'elle a « identifié un logiciel malveillant sur les ordinateurs qui gèrent les systèmes de paiements ».

Le groupe ne donne pas d'informations supplémentaires sur les tenants et aboutissants de cette histoire, pas plus que sur le nombre de clients potentiellement touchés ou sur les données dérobées. Il est simplement demandé aux clients de scruter attentivement leurs relevés bancaires afin de vérifier qu'aucune transaction suspecte n'a été effectuée.

Bien évidemment, Hyatt ajoute avoir pris des mesures pour renforcer sa sécurité informatique (notamment avec l'aide d'une société spécialisée dans ce domaine) et indique que, désormais, ses « clients peuvent utiliser en toute confiance des cartes de paiement dans les hôtels Hyatt dans le monde entier ».
Mais il faut également rappeler que cette brèche dans la sécurité d'un hôtel n'est que la dernière d'une longue série pour 2015. En effet, il y a tout juste un mois, c'était la chaine Hilton qui annonçait avoir découvert un logiciel malveillant dans certains terminaux de paiements. Sur son blog, Krebs dresse une triste liste d'hôtels ayant fait face à une importante brèche dans leur sécurité informatique en 2015 : Starwood, Mandarin Oriental, White Lodgging et Trump Collection.

Réagissez à cet article

Source : *Hyatt : encore une chaine d’hôtels prise pour cible par un logiciel malveillant*

Google propose d’utiliser son téléphone en guise de mot de passe

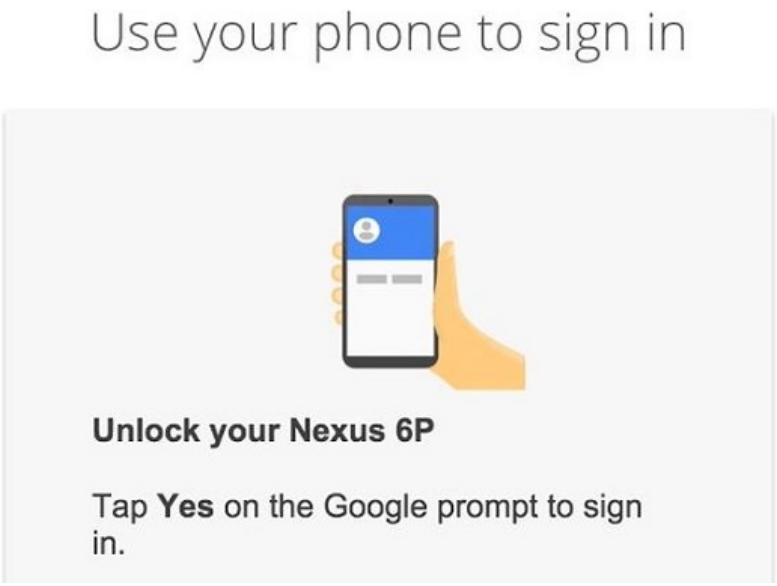
Google propose d’utiliser son téléphone en guise de mot de passe

---

Saisir sur votre ordinateur un long mot de passe pour accéder à votre compte Google pourrait devenir une chose du passé pour peu que vous ayez en poche votre téléphone mobile.

Google s'efforce depuis longtemps de retirer les différentes barrières s'opposant à un accès rapide aux données. Et il pourrait bien avoir un nouveau tour dans son sac : au lieu de saisir comme d'habitude un mot de passe depuis son PC, sa tablette ou un autre terminal, vous pourriez simplement utiliser votre téléphone pour vous authentifier.
L'utilisateur de Reddit, Rohit Paul, a été invité à tester la fonctionnalité, qui nécessite encore un peu de saisie de la part de l'internaute.

Adresse Gmail saisie sur un mobile pour se connecter sur PC



Comme relevé par Android Police, une fois le téléphone de Rohit Paul enrôlé comme terminal d'authentification, ce dernier n'a plus eu qu'à entrer son adresse Gmail sur son smartphone pour se connecter à Google depuis son ordinateur.
Si le processus ne s'avère pas aussi rapide pour tous, ceux dont le mot de passe Google compte de nombreux caractères pourraient en profiter en réduisant le temps de saisie nécessaire à l'authentification.
Naturellement, si vous perdez votre téléphone ou si vous ne souhaitez plus utiliser ce mode d'authentification, vous pouvez toujours vous connecter à votre compte Google de manière classique.
Google n'ayant pas annoncé officiellement cette nouvelle fonctionnalité, les détails techniques de la procédure d'accès restent inconnus. La firme de Mountain View n'est cependant pas la seule à vouloir s'affranchir des mots de passe et à développer des méthodes alternatives d'authentification. C'est par exemple le cas de Microsoft dans Windows 10 au travers d'une fonction comme Next Generation Credentials.

Réagissez à cet article

Source : *Google souhaite remplacer le mot de passe par votre téléphone*

Quelques explications sur le projet de règlement européen sur la Protection des Données Personnelles dans les tuyaux

	Quelques explications sur le projet de règlement européen sur la Protection des Données Personnelles dans les tuyaux

---

Le texte de la réforme du cadre juridique de l'UE sur la protection des données personnelles stipule, notamment, que les entreprises devront communiquer pro-activement sur les failles dont elles seraient victimes.

Le Parlement européen et le Conseil de l'Union européenne se sont mis d'accord au sujet de la future modification du cadre juridique de l'UE sur la protection des données personnelles. La Commission européenne a publié le contenu de la reforme qu'elle propose, aboutissement d'âpres débats entamés en 2012. La reforme concerne aussi bien le droit des citoyens que les futures règles en la matière pour les entreprises. En cas de feu vert du Parlement européen et du Conseil début 2016, les nouvelles règles entreront en vigueur deux ans plus tard.

Obligation d'informer sans délais sur les violations données

Du côté des individus, le texte vise à leur donner davantage le contrôle de leurs données personnelles. Le texte fait notamment état d'un droit d'être informé en cas d'accès non autorisé aux données personnelles. Ce droit signifie que les entreprises et organisations doivent notifier à l'autorité nationale de contrôle, dans les plus brefs délais et de façon proactive, les violations de données graves, afin que les utilisateurs puissent prendre les mesures appropriées. Les nouvelles règles permettront en théorie aux citoyens de disposer de plus d'informations sur la façon dont leurs données sont traitées.
La reforme prévoit en outre un droit à la portabilité des données personnelles d'un prestataire de services à un autre et contient également un droit à l'oubli «plus clair», permettant aux personnes qui le désirent de voir leurs données supprimées dès lors qu'aucun motif légitime ne justifie leur conservation. Un autre article de la reforme fait déjà couler beaucoup d'encre dans les médias généraliste. Il concerne l'interdiction aux moins de 16 ans de s'inscrire à des médias sociaux tels que Facebook ou Instagram.

Les entreprises devront nommer un délégué aux données

Pour les entreprises, la Commission européenne propose des règles qui, selon elle, n'entravent pas le commerce, mais au contraire «créent des opportunités commerciales et encouragent l'innovation.» Un droit unique à l'échelle européenne devrait rendre moins coûteux l'exercice d'activités entrepreneuriales en Europe, précise le communiqué de l'UE. Lequel indique aussi que le règlement imposera que des garanties en matière de protection des données soient «intégrées aux produits et services dès la phase initiale de leur conception.»
La reforme exige également que les firmes européennes se dotent d'un délégué à la protection des données (une exigence à laquelle les PME seront exemptées dans le cas où le traitement des données n'est pas leur cœur de métier). Par ailleurs, le règlement établi que les entreprises établies hors d'Europe devront se conformer à la réglementation européenne pour pouvoir offrir leurs services dans l'Union. En cas de violations de ces règles, les sanctions pourront atteindre jusqu'à 4% de chiffre d'affaires de l'entreprise. Digital Europe, un groupe de lobbying représentant les intérêts de firmes US comme Google, Apple, IBM ou Microsoft, n'a pas attendu la fin des négociations pour monter au front. Faisant craindre à certains observateurs une édulcoration des règles de la réforme proposée. Mais cela n'a finalement pas été le cas.

Réagissez à cet article

Les entreprises doivent prendre au sérieux la protection des données

Les entreprises doivent prendre au sérieux la protection des données

L'intelligence économique est devenue un mode de gestion (Le management est la mise en ?uvre des moyens humains et matériels d'une entreprise pour (…)) et de gouvernance de l'entreprise. Cet ouvrage réfléchit sur la démarche que le chef d'entreprise peut entreprendre pour éclairer ses décisions, garder sa marge de manoeuvre de compétitivité et toutes ses possibilités de développement afin de sécuriser sa pérennité.

Traitement de l'information et renseignements

Un renseignement utile peut être obtenu de façon proactive, active, ou réactive.

Le cycle de renseignement pour l'entreprise doit s'intégrer au processus de veille stratégique sur les différents volets de l'intelligence économique : veille technologique, veille d'image, veille concurrentielle, etc.

L'intelligence économique distingue trois niveaux d'information utile au renseignement :

image: http://www.atlantico.fr/sites/atlantico.fr/files/u65387/2015/12/capture_2_0.jpg

L'intelligence économique ne cherche pas à obtenir l'information noire. Elle se limite à l'information que l'on peut obtenir par des moyens légaux (ex : pour se protéger des problèmes de réputation, d'escroquerie, de fraude, de cybercriminalité, de propriété intellectuelle, de savoir-faire, de brevets, etc.).

Il s'agit surtout de formaliser de façon pragmatique, ou de rendre systématique, une démarche proactive de veille dans ce domaine, notamment pour l'obtention de l'information « grise ».

Les PME sont souvent très en retrait sur la construction du savoir (ex : suivi des avancées des concurrents, organisation de la veille juridique, réglementaire, lobbying, etc.).

Sécurité et protection de l'information

Trop peu d'entreprises prennent au sérieux la protection des données. Il devient impératif de disposer d'un solide processus de sauvegarde, de prévention, d'action, et de réaction aux pannes et aux attaques informatiques. Notons ici que certaines entreprises sensibles aux problématiques de reprise après incident commencent à considérer les prestations d'externalisation applicatives (Cloud computing ou autres solutions) pour optimiser le niveau de sécurité des données.

Quantité et gouvernance des données

Les données sont la base de l'information, et comme le disent souvent les anglo-saxons: « data is the oil of the 21st century ». Savoir chercher et collecter l'information, la traiter et la diffuser (tout en protégeant la part de données sensibles qui doivent être protégées), constitue une tâche prioritaire de tous les acteurs économiques, et la définition même de l'intelligence économique.

image: http://www.atlantico.fr/sites/atlantico.fr/files/u65387/2015/12/capture_3_0.jpg

Le pouvoir c'est l'information, mais à condition qu'elle soit de qualité …

La direction et les organes sociaux doivent s'appuyer sur des informations de qualité (fiables, précises, actualisées)

Read more at http://www.atlantico.fr/decryptage/entreprises-doivent-prendre-au-serieux-protection-donnees-gouvernance-et-intelligence-economique-en-pme-georges-nurdin-daniel-2494228.html##Vrl3qqLdiB14upbK.99

Réagissez à cet article

Source : *Marketing/ Les entreprises doivent prendre au sérieux la protection des données*

La SACEM tente d’étendre ses taxes au Cloud

	La SACEM tente d’étendre ses taxes au Cloud

L'ennui avec le progrès, c'est qu'il se fiche comme d'une guigne des prés carrés, des rentes de situations et des petits arrangements entre amis. Parfois, ce progrès provoque l'effondrement plus ou moins rapide de juteuses pensions qu'on croyait établies pour toujours. C'est exactement ce à quoi est confronté la SACEM.

La SACEM, c'est cette vénérable institution de ponctions culturelles qui utilisait jusqu'à présent le bras armé de l'État pour faire valoir des droits construits de toute pièce il y a un siècle et demi et qui arrivait encore assez facilement à prélever sa dime… Jusqu'à l'avènement du numérique : rapidement, la facilité de copie est devenue telle qu'il a rapidement été impossible de les tracer.

Parallèlement, l'effondrement des ventes de galettes de vinyle ou de polyacrylates a rendu la collecte des fameux droits beaucoup plus complexe. Moyennant une bonne couche de lobbying, on se souvient que les sociétés culturelles concernées (comprenant la SACEM mais aussi les majors musicales ou du cinéma) avaient réussi à pousser dans les tuyaux législatifs français des lois compensant assez largement ces changements drastiques de modes de revenus par une taxe française sur les supports numériques vierges, depuis les iPods jusqu'aux cartes mémoires en passant par les disques durs.

Cette taxe permit, on s'en doute, de largement renflouer les comptes de ces associations lucratives, et de placer presque instantanément les supports numériques français parmi les plus chers du monde. Commander un disque dur, un iPod ou une carte mémoire de l'autre côté de la frontière est rapidement devenu un sport national tant le différentiel devenait grotesque. Eh oui : la société civile s'adapte bien plus vite que les lois.

Quant aux progrès technologiques, ils continuent à un rythme tel qu'à peine les ponctions sur les supports numériques actés, ces derniers devinrent quasiment caduques. Rapidement, le consommateur déporte ses données dans le Cloud, et n'utilise plus, directement, de support numérique.
Autrement dit, le support numérique du consommateur est minimal, et ne comporte que la petite quantité de données qu'il écoute au moment où il veut. L'ensemble de ses bibliothèques numériques (films, musiques, vidéos, photos) est de plus en plus déporté dans un nuage numérique fourni par des entreprises spécialisées, allant de Google (GoogleDrive) à Microsoft (SkyDrive) en passant bien sûr par Apple (iCloud), Dropbox et autres solutions plus ou moins intégrées avec les outils numériques du moment.

Pour la SACEM, c'est une nouvelle catastrophe.
Comme le relate un récent article de NextInpact, David El Sayegh, le secrétaire général de la SACEM, a ainsi expliqué avec quelques trémolos dans la voix lors d'une table ronde organisée par la Commission de la Culture au Sénat toute la difficulté de la situation que rencontre sa société :
« on a décalage entre la législation française qui explique que la copie privée ne peut être invoquée que pour les particuliers qui ont la garde matérielle des produits et l'évolution technologique qui permet de réaliser des copies privées quand bien même vous n'avez pas la garde technique de ces matériels. »

Eh oui. *« si vous perdez votre iPad ou votre portable, c'est dommage de perdre toute votre discothèque »*, mais comme tout est dans ce fameux Cloud, pouf, vous pouvez tout récupérer.
Magie de la technologie moderne ? Peut-être, mais en tout cas, il y aurait comme des copies privées dans ce cloud que ce ne serait pas étonnant, insiste clairement notre bon secrétaire général. Ce qui voudrait dire (miam, miam et slurp) que ces copies seraient sujettes à redevance, pardi ! Et donc, « le Sénat, dans sa sagesse, doit absolument légiférer », sinon, c'est évidemment le début de la fin, la fermeture du robinet, et l'apocalypse de la création musicale, garantie sur facture.

Et c'est bien d'assujettir le Cloud à cette taxe de copie privée qu'il est question ici, puisque le brave secrétaire en appelle à l'amendement Rogemont qui proposait exactement ça : soit on ponctionnera le service en ligne, soit les espaces de stockages classiques, soit les offres de streaming en temps différé (typiquement, les « magnétoscopes » en ligne, proposés par les FAI). Décidément, rien n'échappe à la rage taxatoire des uns et des autres.
Il ne reste plus qu'à pondre une bonne petite loi, et l'affaire sera dans le sac : la SACEM, sauvée d'une pénurie inopinée de fonds, retrouvera vigueur et couleurs d'antan et pourra repartir à l'assaut des portefeuilles bien garnis des consommateurs.
Mais voilà : c'est bien joli, toutes ces décisions finement élaborées et frappées au coin du bon sens bien compris de la nomenklatura française, cependant, si on s'éloigne des intentions, toujours extrêmement claires et dont les effets sont tous parfaitement connus et même planifiés, et si on s'attarde un peu sur les résultats, toujours plus incertains, on découvre comme un petit écart.
Prenez par exemple notre magnifique HADOPI, que le monde, ébahi, ne comprend pas, ne nous envie pas et qui déclenche même souvent l'hilarité, en France comme ailleurs. Il en aura fallu, des aventures amusantes, pour en arriver à sa création. Il en aura fallu, du « pare-feu OpenOffice » et de fines manœuvres du Capitaine Anéfé pour aboutir à un appendice boursouflé incapable de faire, même vaguement, ce pourquoi il fut créé en premier lieu…

Or, au constat déjà catastrophique de la nullité de l'institution en terme de lutte contre le piratage, on doit maintenant ajouter un effet clairement négatif sur le cinéma français : on apprend en effet au détour d'une enquête de l'INSEE que la lutte contre le piratage menée par la Hototorité a « clairement favorisé » le cinéma américain au détriment des films français.

Apparemment, d'après l'étude, « l'introduction de la loi Hadopi est associée à une augmentation de la part de marché des films américains de 9%, mais sans augmentation de la demande totale pour les films en salle ». Pour HADOPI, c'est carton plein : les entrées en salle n'ont pas augmenté, mais les films américains ont été plus vus que les français, ce qui laisse furieusement à penser que les films français sont plus piratés. De là à conclure hardiment que leur valeur intrinsèque ne justifie pas le déplacement et l'achat d'une place en salle, et que le risque est moins grand de les pirater que pour les productions américaines, il n'y a qu'un tout petit pas facile à franchir.
Bref, vous avez bien lu : non seulement, la HADOPI ne parvient pas à endiguer, même un peu, le piratage qu'elle prétend combattre, non seulement cette création ubuesque nous coûte 8,5 millions d'euros par an (plus encore que les années précédentes suite à l'élargissement de son budget, sans doute pour la récompenser de ses performances), mais de surcroît, elle parvient même à saboter le marché sur lequel elle opère. C'est, on doit l'admettre, un échec de proportion épique.

À présent, il devient difficile de s'empêcher de mettre en regard ce résultat catastrophique de la HADOPI, instance d'ailleurs issue des belles législations de nos assemblées et de la fameuse « sagesse » à laquelle se réfère le secrétaire général de la SACEM, et ce que ce dernier propose de faire à nouveau concernant la copie privée et son avatar sur les clouds.
L'expérience permet d'éviter de répéter sans arrêt les mêmes bêtises. Inversement, Einstein notait judicieusement que la folie consistait à refaire toujours la même chose en espérant obtenir des résultats différents.
De l'expérience ou de la folie, que croyez-vous donc que notre législateur va choisir ?

Réagissez à cet article

Source : *La SACEM tente d'étendre ses taxes au Cloud | Contrepoints*

L'usurpation d'identité touche 200.000 Français

L'usurpation d'identité touche 200.000 Français

Ancien commissaire à la Direction de Surveillance du Territoire, Daniel Martin, spécialiste de la cybercriminalité, incite les internautes à être vigilants.

L'ex-flic est intarissable sur la cybercriminalité, phénomène qu'il a décrypté hier au CFA du bâtiment à Saint-Benoît. « J'ai vu l'évolution, surtout depuis vingt ans », insiste Daniel Martin. Rencontre.

C'est quoi la cybercriminalité ?
« C'est un terme générique qui suppose toute activité délictueuse qui met en œuvre les nouvelles techniques d'information et de communication. »

Pourquoi se développe-t-elle ?
« Avec les ordinateurs et la mondialisation, la notion de frontière et de territoire n'existe plus. En France, on compte 43 millions d'internautes et un sur trois est victime de la cybercriminalité. Le smartphone constitue l'objectif le plus important pour les pirates et il s'en est vendu 18 millions en France en 2014. »

Elle prend quelle forme ?
« Surtout l'usurpation d'identité qui touche 200.000 Français tous les ans. Il faut éviter de mettre tels quels dans la poubelle ses papiers de sécurité sociale, ses relevés bancaires… Ils peuvent être exploités. Attention aux réseaux sociaux. Quand je vois mon fils mettre quand et où il part en vacances, c'est faire le jeu des cambrioleurs. »

Les achats sur internet explosent…
« Attention aux prix trop alléchants, ce n'est pas normal. Et sur les sites de vente entre particuliers, vous pouvez envoyer la marchandise sans jamais avoir la compensation en retour. »

D'autres pièges à éviter ?
« On reçoit tous des messages d'amis réclamant une aide financière ou d'un organisme demandant nos coordonnées bancaires pour rembourser un trop perçu… »

Quoi faire ?
« Il faut être vigilant et prudent dans l'utilisation de son portable et de son ordinateur. Déjà, un mot de passe doit avoir de 8 à 12 caractères, être alphanumérique, avec des majuscules et des caractères spéciaux. »

Réagissez à cet article

Source : *L’usurpation d’identité touche 200.000 Français – 19/12/2015 – La Nouvelle République Vienne*

Droit de douane aboli pour 200 produits tech

Droit de douane aboli pour 200 produits tech

PC, TV, tablettes, consoles, GPS… autant de produits qui ne seront progressivement plus concernés par les droits de douane à partir de juillet 2016, suite à une décision de l'OMC.

C'est une décision qui vise à booster le commerce international. L'Organisation mondiale du commerce (OMC), réunie à Nairobi au Kenya, a décidé de lever les droits de douane sur 201 produits high-tech. Parmi eux : téléviseurs, consoles de jeux, ordinateurs, GPS, appareils photo… Dans le pire des cas, cette taxe peut atteindre 35 % du prix de vente du produit. Pour l'OMC, c'est incontestablement un frein au libre-échange.

Cette levée des taxes se fera par paliers. Le premier sera en juillet 2016, où 130 de ces produits informatiques seront concernés. C'est seulement en 2019 que la quasi-totalité des appareils (95 %) ne seront plus taxés. Et en 2024 que l'ensemble de ces 201 produits ne seront plus taxés. À l'échelle mondiale, ce marché, qui inclut également des outils professionnels comme des IRM, représenterait 10 % des échanges internationaux.

Selon Roberto Azevedo, le directeur général de l'OMC, ces « technologies de l'information » pèsent plus que le secteur automobile, du textile et de la sidérurgie réunis, soit quelque 1 300 milliards de dollars par an. En levant les taxes, l'OMC a estimé les retombées à 190 milliards de dollars dans le monde, et possiblement à la création de 60 000 emplois rien qu'aux États-Unis. Cinquante-trois pays ont signé cet accord, dont la Chine.

Réagissez à cet article

Source : *Droit de douane aboli pour 200 produits tech*

Préparez-vous à la dématérialisation fiscale pour le secteur public

Préparez-vous à la dématérialisation fiscale pour le secteur public

Depuis le 1er janvier 2012, la plateforme Chorus Factures permet aux fournisseurs de l'Etat de transmettre leurs factures au format PDF avec signature électronique ou via EDI (Echange de Données Informatisé)*. L'envoi de factures électroniques deviendra obligatoire entre 2017 et 2020 selon les typologies d'entreprises.

Suite à la directive européenne 2014/55/EU d'avril 2014, l'envoi de factures électroniques deviendra une obligation pour les fournisseurs du secteur public au sens large, à horizon 2017 pour les grands comptes, et d'ici 2020 pour les ETI, PME et TPE.

Depuis le 1er janvier 2012, en France, les fournisseurs qui le souhaitent ont déjà la possibilité d'envoyer aux ministères gouvernementaux des factures dématérialisées via le portail mis à disposition par l'Etat, Chorus factures.

Réagissez à cet article