Sensibilisation au Phishing

Sensibilisation au Phishing

Vous feriez confiance à cet homme ? Sur Internet aussi, soyez vigilants: il arrive que des acheteurs ou vendeurs malhonnêtes essaient de vous arnaquer. Découvrez les bons réflexes sécurité avec PayPal. Acheter et vendre en ligne est simple et sécurisé avec PayPal, 7 millions de Français nous utilisent déjà.

Campagne Paypal France 2016

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Sensibilisation aux Arnaques à la Loterie

Sensibilisation aux Arnaques à la Loterie

Vous feriez confiance à cet homme ? Sur Internet aussi, soyez vigilants: il arrive que des acheteurs ou vendeurs malhonnêtes essaient de vous arnaquer. Découvrez les bons réflexes sécurité avec PayPal. Acheter et vendre en ligne est simple et sécurisé avec PayPal, 7 millions de Français nous utilisent déjà.

Campagne Paypal France 2016

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Euro 2016 et sécurité informatique, quelques conseils face à quelques risques…

Euro 2016 et sécurité informatique, quelques conseils face à quelques risques…

Euro 2016 – Les événements sportifs mondiaux ont toujours constitué un terrain de chasse idéal pour les cybercriminels. L'Euro 2016, qui débute le 10 juin prochain, ne devrait pas déroger à la règle.

Euro 2016 – Voici quelques éléments clés à retenir, amateur de football, de l'Euros 2016 ou non. Se méfier du spam et autre fausses « bonnes affaires » (places pour assister aux matchs à des prix défiant toute concurrence, par exemple). Ces mails peuvent contenir une pièce jointe infectée contenant un malware accédant au PC et interceptant les données bancaires des internautes lorsqu'ils font des achats en ligne. Ils peuvent également contenir un ransomware, qui verrouille et chiffre les données contenues dans le PC et invite les victimes à verser une rançon pour les récupérer.
Détecter les tentatives de phishing (vente de tickets à prix cassés voire gratuits, offres attractives de goodies en lien avec l'évènement,…) en vérifiant l'URL des pages auxquelles le mail propose de se connecter et en ne communiquant aucune information confidentielle (logins/mots de passe, identifiants bancaires, etc.) sans avoir préalablement vérifié l'identité de l'expéditeur.
Être prudent vis à vis du Wi-Fi public pour éviter tout risque de fuite de données, par exemple en désactivant l'option de connexion automatique aux réseaux Wi-Fi. Les données stockées sur les smartphones circulent en effet librement sur le routeur ou le point d'accès sans fil (et vice-versa), et sont ainsi facilement accessibles.
Redoubler de vigilance vis-à-vis des mails invitant à télécharger un fichier permettant d'accéder à la retransmission des matchs en temps réel. Il s'agit en réalité de logiciels malveillants qui, une fois exécutés, permettent d'accéder aux données personnelles stockées dans le PC (mots de passe, numéro de CB, etc.) ou utilisent ce dernier pour lancer des procédures automatiques comme l'envoi de mails massifs. (TrendMicro).
Auteur : Damien Bancal

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

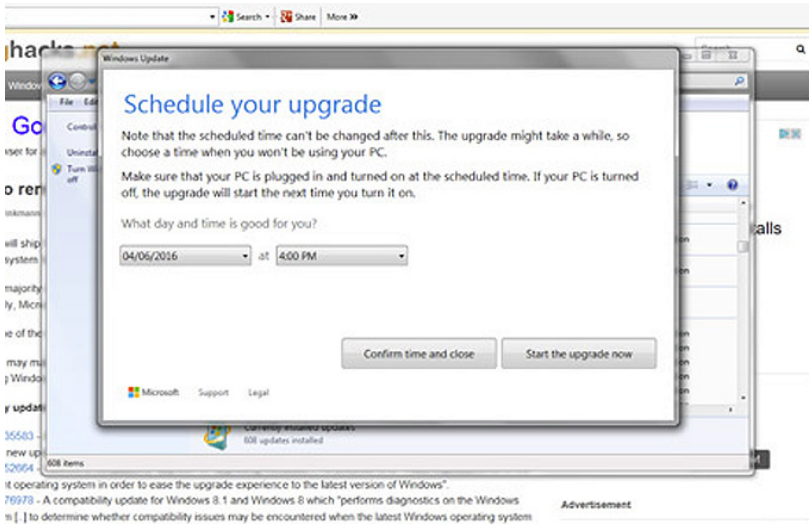
Original de l'article mis en page : Football : Euro 2016 et sécurité informatique – Data Security BreachData Security Breach

---

Microsoft supprimerait carrément la possibilité de refuser Windows 10

Microsoft supprimerait carrément la possibilité de refuser Windows 10

Selon une capture d'écran diffusée par The Register, Microsoft changerait à nouveau de méthode pour imposer la mise à jour vers Windows 10. Cette fois littéralement.



Le site britannique The Register publie ainsi la capture d'écran réalisée par un lecteur, qui montre qu'en lieu et place de la popup, Windows 7 lui a affiché une fenêtre qui impose de programmer une mise à jour vers Windows 10, avec un réglage de la date et de l'heure de l'opération. Il y a deux boutons sur la fenêtre ; le premier qui permet de confirmer la date et l'heure saisis ; le deuxième qui permet de demander une mise à jour immédiate.
Il n'y a aucun autre bouton pour refuser la mise à jour, ni de bouton « X » pour fermer la fenêtre (ce que Microsoft prenait de toute façon pour un accord).

COMMENT FAIRE ?

Les utilisateurs qui souhaitent refuser la mise à jour pourront toujours mettre une date de programmation très lointaine. Notez qu'au pire, en cas de mise à jour involontaire, il est possible de revenir vers Windows 7 ou Windows 8 en refusant d'accepter les conditions d'utilisation de Windows 10, présentées lors du premier lancement du système d'exploitation.
Le refus entraîne en effet une annulation de l'installation de Windows 10 puisque, même s'il peut forcer l'installation des fichiers du système, Microsoft ne peut pas encore obliger l'utilisateur à accepter son contrat.
La mise à jour vers Windows 10 reste gratuite jusqu'au 29 juillet 2016. Il faudra ensuite payer une licence. Notez que si vous avez déjà effectué la mise à jour et que vous devez réinstaller votre système, la gratuité de Windows 10 ne vaudra que si vous réinstallez l'OS sur le même ordinateur, reconnu par ses principaux composants. En cas de changement de carte mère ou de processeur par exemple, il devrait être imposé d'acheter la licence de Windows 10, auquel vous vous serez habitué…
Auteur : Guillaume Champeau

Réagissez à cet article

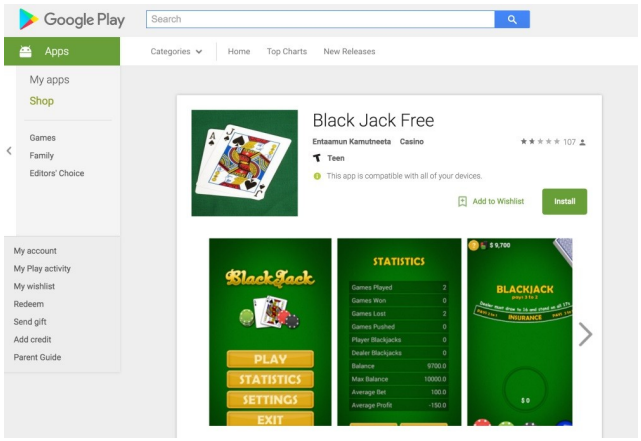
Original de l’article mis en page : Microsoft supprimerait carrément la possibilité de refuser Windows 10 – Tech – Numerama

---

Alerte : Un Trojan détecté sur Google Play

Alerte : Un Trojan détecté sur Google Play

Lookout, spécialiste dans la sécurité mobile a détecté « Black Jack Free », un jeu gratuit sur Google Play qui appartient à la famille du Trojan Acecard.



S'il est de bon augure de se méfier des jeux d'argents, il faut les craindre d'autant plus lorsqu'ils sont sur internet. L'application Black Jack Free qui était en fait un Trojan a été téléchargée plus de 5000 fois avant d'être retirée du Google Play Store quatre jours plus tard. A première vue, il n'y avait rien à craindre de ce jeu de cartes qui permettait de jouer gratuitement tout en utilisant de l'argent fictif. Sauf que, dans l'arrière boutique l'application dérobait des données, mais aussi de l'argent sur les comptes en banque des utilisateurs. «Black Jack Free n'était pas directement le problème. Mais il installait une deuxième application, Play Store Update qui repérait les applications actives sur internet et imitait les pages d'accueil» explique Arnaud Simon, responsable technique Europe du sud chez Lookout.
Par ce stratagème, l'application superposait des fenêtres sur les applications bancaires, ou sur les réseaux sociaux comme Facebook ou Skype par exemple. Ensuite, les utilisateurs entraient leurs codes et identifiants sans se douter que des pirates les récupéraient. Play Store Update pouvait aussi intercepter des SMS, les envoyer vers un serveur malicieux, transférer des appels, verrouiller l'écran et effacer les données d'un terminal.

Un risque plus ou moins écarté

Il est donc fortement conseillé aux utilisateurs ayant téléchargé Black Jack Free de supprimer l'application de leurs terminaux Android et de se débarrasser de Play Store Update également. Ensuite, pour éviter les mauvaises surprises, Lookout invite les personnes concernées à modifier leurs codes d'accès.
A noter que « l'application était disponible sur Google Play car les pirates disposaient d'un accès potentiel à de nombreux terminaux. Mais les hackers ne se sont pas contentés de diffuser Black Jack Free sur cette seule et unique plateforme, elle est disponible ailleurs sur le web», ajoute Arnaud Simon. Comprendre que le Trojan court toujours et que la méfiance reste de mise.
Article original de Victor Mayet

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Un Trojan détecté sur Google Play*

Alerte Arnaques ! Des pirates informatiques se font passer pour des stars

	Alerte Arnaques ! Des pirates informatiques se font passer pour des stars

Des pirates informatiques se font passer pour les animateurs vedettes de NRJ, Virgin Radio et autres stars de la FM pour soutirer des informations bancaires.

Des pirates informatiques se font passer pour les animateurs vedettes de NRJ, Virgin Radio et autres stars de la FM pour soutirer des informations bancaires.
Nous connaissions la Fraude au Président, l'arnaque aux faux virements via des informations bancaires soutirées à des entreprises par ruse. Un piège qui fonctionne, malheureusement aussi, sur les locataires de logements sociaux. Les escrocs se font passer pour le bailleur afin de faire modifier les données concernant les virements des loyers.
Aujourd'hui, je viens d'apprendre une nouvelle ruse. Des escrocs se font passer pour les stars de la radio (Manu de NRJ, Camille Combal de Virgin Radio…) en téléphonant et en promettant de l'argent à leurs interlocuteurs. « Un homme dans un soi-disant bureau d'antenne de radio vous dit que vous venez de gagner 2000€ et de doubler vôtre salaire, souligne l'un des témoins de ZATAZ.COM. Il y a beaucoup de bruit derrière. Comme dans un studio de radio ».

Ils visent vos informations bancaires

Une fois l'interlocuteur appâté, l'appel est transféré à une standardiste « On vous demande un numéro de compte bancaire, souligne un autre lecteur de ZATAZ. Ce qui m'a mis la puce à l'oreille est que le soi-disant animateur fusionne plusieurs jeux du 6/9 de NJR et de Virgin Radio. Pour mettre la personne en confiance, on vous ovationne et félicite pour votre prix. »
La question est de savoir maintenant comment les escrocs peuvent avoir le numéro de téléphone portable et l'identité complète (Nom, prénom) des personnes appelées.
Bref, prudence ! Si vous ne vous inscrivez pas à un jeu officiel, il n'y a pas de raison que ce dernier vous téléphone !… [Lire la suite]

Merci à Damien Bancal auteur de cet article

M

Réagissez à cet article

Source : *ZATAZ Informations bancaires : des pirates se font passer pour Manu, Camille Combal – ZATAZ*

Forte hausse des applications Android malveillantes

Forte hausse des applications Android malveillantes

Les applications Android malveillantes et les ransomwares dominent le paysage des menaces au 1er trimestre 2016.

La société Proofpoint a publie son Rapport trimestriel sur les menaces, qui analyse les menaces, les tendances et les transformations observées au sein de notre clientèle et sur le marché de la sécurité dans son ensemble au cours des trois derniers mois. Chaque jour, plus d'un milliard de courriels sont analysés, des centaines de millions de publications sur les réseaux sociaux et plus de 150 millions d'échantillons de malwares afin de protéger les utilisateurs, les données et les marques contre les menaces avancées. On apprend, entre autres, que 98 % des applications mobiles malveillantes examinées au 1er trimestre 2016 ont ciblé des appareils Android. Cela demeure vrai en dépit de la découverte médiatisée d'un cheval de Troie pour iOS et de la présence persistante d'applications iOS ou officieuses dangereuses. Les applications Android malveillantes sont de plus en plus nombreuses.

75 % des attaques de phishing véhiculées par des e-mails imposteurs comportent une adresse «répondre à » usurpée afin de faire croire aux destinataires que l'expéditeur est une personne représentant une autorité. Ce type de menaces est de plus en plus mature et spécialisé, et c'est l'un des principaux ciblant les entreprises aujourd'hui, qui leur auraient coûté 2,6 milliards de dollars au cours des deux dernièresannées selon les estimations.

Applications Android malveillantes

Les ransomwares se sont hissés aux premiers rangs des malwares privilégiés par les cybercriminels. Au 1er trimestre, 24 % des attaques par e-mail reposant sur des pièces jointes contenaient le nouveau ransomware Locky. Seul le malware Dridex a été plus fréquent.

L'e-mail reste le principal vecteur de menaces : le volume de messages malveillants a fortement augmenté au 1er trimestre 2016, de 66 % par rapport au 4ème trimestre 2015 et de plus de 800 % comparé au 1er trimestre 2015. Dridex représente 74 % des pièces jointes malveillantes.

Chaque grande marque analysée a augmenté ses publications sur les réseaux sociaux d'au moins 30 %. L'accroissement du volume des contenus générés par les marques et leurs fans va de pair une accentuation des risques. Les entreprises sont constamment confrontées au défi de protéger la réputation de leurs marques et d'empêcher le spam, la pornographie et un langage grossier de polluer leur message.

Les failles de Java et Flash Player continuent de rapporter gros aux cybercriminels. Angler est le kit d'exploitation de vulnérabilités le plus utilisé, représentant 60 % du trafic total imputable à ce type d'outil. Les kits Neutrino et RIG sont également en progression, respectivement de 86 % et 136 %. (ProofPoint)… [Lire la suite]

Article de Damien BANCAL

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Forte hausse des applications Android malveillantes – Data Security BreachData Security Breach*

Sensibilisation aux arnaques aux petites annonces

Sensibilisation aux arnaques aux petites annonces

Vous feriez confiance à cet homme ? Sur Internet aussi, soyez vigilants: il arrive que des acheteurs ou vendeurs malhonnêtes essaient de vous arnaquer. Découvrez les bons réflexes sécurité avec PayPal. Acheter et vendre en ligne est simple et sécurisé avec PayPal, 7 millions de Français nous utilisent déjà.

Campagne Paypal France 2016

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

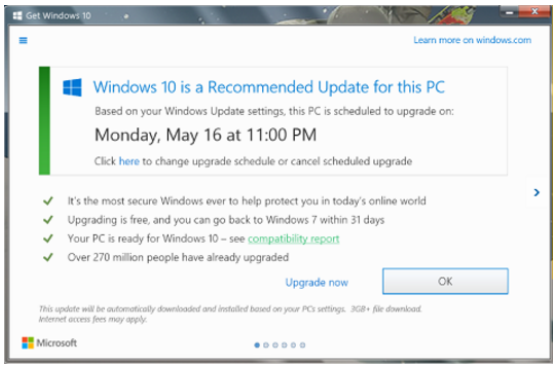
Réagissez à cet article

Vous ne voulez pas installer Windows 10, comment Microsoft vous-y oblige ?

	Vous ne voulez pas installer Windows 10, comment Microsoft vous-y oblige ?

« Mon ordinateur m'a demandé si je voulais passer à Windows 10. J'ai cliqué sur le bouton X pour fermer la fenêtre car je ne voulais pas, et une heure après, Windows 10 est en train de s'installer. » Ce type de commentaire s'est multiplié sur les réseaux sociaux ces derniers jours. De nombreux internautes se sont plaints de voir leurs ordinateurs installer automatiquement la mise à jour vers Windows 10, alors qu'ils pensaient l'avoir refusée. Tous avaient cliqué sur la croix rouge permettant de fermer la fenêtre proposant ce téléchargement.

En général, ce bouton sert à fermer une pop-up sans avoir à donner de réponse à sa proposition. Mais depuis quelques jours, le fait de cliquer dessus a l'effet inverse : cela installe Windows 10. Une « *tromperie* », selon de nombreux utilisateurs du célèbre système d'exploitation de Microsoft.



Si l'utilisateur ferme cette fenêtre, alors Windows 10 s'installera automatiquement sur son ordinateur. Microsoft

L'entreprise, de son côté, assume et explique sur son site le fonctionnement de cette fenêtre. En fait, celle-ci fait plus que proposer une mise à jour : elle indique que la mise à jour est déjà programmée et précise la date. L'utilisateur est alors invité à cliquer sur le gros bouton « OK ». Il a aussi la possibilité, inscrite en petits caractères, de modifier la date ou d'annuler la programmation de mise à jour. Mais s'il décide simplement de fermer la fenêtre, alors Microsoft part du principe que l'utilisateur accepte la mise à jour, comme s'il avait cliqué sur « OK ».

Les utilisateurs forcés. Normal ?

Cette manœuvre de Microsoft est considérée par beaucoup comme une manière de leur forcer la main, alors que l'entreprise a annoncé sa volonté d'équiper un milliard de machines de Windows 10 en trois ans. D'autant qu'une date clé se rapproche dangereusement : à partir du 30 juillet, la mise à jour, jusqu'ici gratuite pour les utilisateurs de Windows 7 et 8, deviendra payante. Il sera alors bien plus compliqué de convaincre les sceptiques de s'y convertir.

Source : *L'étrange méthode de Microsoft pour imposer le téléchargement de Windows 10*

Réagissez à cet article

Blogueurs, attention aux promesses des Publicités …

Blogueurs, attention aux promesses des Publicités …

Publicité malveillante – Elles se nomment Elena, Yoana, Elise… elles sont toutes éditrices indépendantes et recherchent des espaces publicitaires sur votre blog. Attention, piège à la Publicité malveillante pour casinos.

Des courriers et autres sollicitations commerciales sont légions dans le monde des blogueurs. Achats d'espaces publicitaires, d'articles ou de liens sponsorisés sont des demandes constantes dès qu'un site fonctionne et attire les internautes. Je vais cependant vous mettre en garde contre des promesses venues du ciel 2.0. « ***Bonjour, je me présente, je m'appelle Yoana et je suis une éditrice indépendante. Je suis intéressée par l'achat d'un espace publicitaire sur votre site http://www.zataz.com . Je souhaite acheter la publication pour un de nos articles, qui contiendra un ou plusieurs liens internes.***«
L'espace entre l'url est important à prendre en compte, je vais vous expliquer pourquoi. Les espaces situés entre le début et la fin de l'adresse Internet sont générés par un logiciel qui automatise les courriels. Bilan, Elena, Yoana, Elise… ne savent pas qui vous êtes. Elles (ou ils), il s'agit aussi très certainement de la même personne officiant d'Italie et d'Israel, espèrent une réponse de votre part. Ne mordez pas à son hameçon. « ***Je peux payer via Paypal sous 24/48h*** » stipulent les interlocutrices.

Publicité malveillante
Mais que proposent donc ces « dames » ? Tout simplement… des articles et des liens renvoyant sur de faux blogs dédiés aux Casinos. L'idée est simple, plus il y aura de liens vers ces faux blogs, plus ils seront référencés. Plus ils seront référencés, plus les internautes auront envie de cliquer sur les autres adresses Internet proposées par ces faux blogs. Des urls qui dirigent tous vers des casinos illicites, interdits en France.
Elena, Yoana, Elise… ne vendent pas les liens directs vers ces casinos, mais pièges les blogueurs qui seraient tentés. Bref, ne sombrez pas aux sons de ses Calliopes car le prochain son que vous pourriez entendre risque d'être celui d'une convocation par le service central des courses et jeux de la Direction Centrale de la Police Judiciaire.

Fausse publicité mais vrai piège
*Les sommes varient pour cette publicité malveillante. Selon son emplacement de l'article, sa durée de mise en ligne. J'ai pu constater des propositions pécuniaires, qui m'étaient faites, pouvant aller de 200 à 1.500€. Autant dire que pour un blogueur, la manne financière est loin d'être négligeable. D'autant plus que Elena, Yoana, Elise… fournissent le texte, les photos, les liens. Malines, quelques jours après la diffusion de l'article en question, elles demandent une modification dans les urls, les ancres dédiées à certains mots du texte. Une manipulation permettant un référencement plus « musclé » dans les moteurs de recherche. « **C'était de l'argent facile**, me confiait il y a quelques temps Clément [prénom modifié], un blogueur. **Mon post était en ligne à 16h. J'ai reçu mon paiement à 20h. J'ai modifié l'article et les liens le lendemain. Une semaine plus tard je recevais un avertissement de l'ARJEL... et une convocation devant les policiers.***

L'ARJEL veille
*Ce qu'oublient de dire les mystérieuses sirènes, les sites qu'elles souhaitent mettre en avant dans la publicité malveillante commercialisée ne sont pas reconnues par l'ARJEL, l´Autorité de Régulation des Jeux en Ligne veille. En France, depuis le 12 mai 2010, l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ne permet plus aux blogueurs d'afficher n'importe quel site dédié aux casinos. Une loi qui s'applique à toute personne proposant, en France, une offre de jeux d'argent et de hasard en ligne. Bref, diffuser un article, des liens, vers des casinos et autres portails dédiés aux jeux de hasard non titulaires de l'agrément ARJEL, peut entraîner de sérieux ennuis aux blogueurs ne respectant pas la loi : « **Quiconque fait de la publicité, par quelque moyen que ce soit, en faveur d'un site de paris ou de jeux d'argent et de hasard non autorisé en vertu d'un droit exclusif ou de l'agrément prévu à l'article 21 est puni d'une amende de 100 000 €. Le tribunal peut porter le montant de l'amende au quadruple du montant des dépenses publicitaires consacrées à l'activité illégale. Ces peines sont également encourues par quiconque a, par quelque moyen que ce soit, diffusé au public, aux fins de promouvoir des sites de jeux en ligne ne disposant pas de l'agrément prévu à l'article 21, les cotes et rapports proposés par ces sites non autorisés.**«
Elena, Yoana, Elise… ne risquent rien, elles sont à l'étranger (Italie, Israël…). En France, 3 ans de prison et 90.000€ d'amende pour « **Quiconque aura offert ou proposé au public une offre en ligne de paris ou de jeux d'argent et de hasard sans être titulaire de l'agrément mentionné à l'article 21 ou d'un droit exclusif**« . Des peines portées à sept ans d'emprisonnement et à 200 000 € d'amende lorsque l'infraction est commise en bande organisée… [Lire la suite]*

Merci à Damien BANCAL l'auteur de cet article pour toutes ces précieuses informations.

Réagissez à cet article

Source : *ZATAZ Publicité malveillante : Piége à blogueur – ZATAZ*