

En Afrique la communication digitale s'impose en entreprise

Le Net Expert Informatique



Décidément, la communication digitale rivalise avec les outils du marketing classique, et grignote désormais une part importante du « budget communication » des entreprises, associations, organisations et institutions gouvernementales.

Au fur et à mesure de l'accroissement de l'utilisation d'Internet en Afrique, les différentes formes d'entreprises et institutions se tournent de plus en plus vers des experts en communication digitale pour renforcer leur présence sur le web.

« le nombre des utilisateurs d'Internet en Afrique devrait être multiplié par 3.5 d'ici 2015 pour que le nombre d'internautes atteigne près de 600 millions » Indique l'UIT

Quelques chiffres clés sur le digitale en Afrique

Selon le rapport annuel publié par l'UIT (Union Internationale des Télécommunications), en fin de l'année 2014, seulement 42% de la population mondiale soit 3,025 milliards de personnes utilisent le réseau internet. Sur l'ensemble du continent africain, le taux de pénétration d'Internet est estimé à 16% en 2014 soit 167 millions d'internautes, contre 110 millions en 2010, une croissance considérée relativement importante en une période de 4 ans. Selon la même source, le nombre des utilisateurs d'Internet en Afrique devrait être multiplié par 3.5 d'ici 2015 pour que le nombre d'internautes atteigne près de 600 millions.

Pénétration Internet et Mobiles dans les pays d'Afrique

La même année Google a également réalisé une étude statistique portant sur le comportement des internautes dans le monde notamment les Africains qui sont de plus en plus présents sur Internet dans l'objectif d'acheter quelque chose ou simplement consulter des produits sur le web. Cette étude chiffrée indique que l'augmentation des achats en ligne est de 33% au Kenya, 37% en Afrique du Sud et 49% au Nigeria.

Ces chiffres illustrent en partie l'évolution du comportement des Africains vis-à-vis du réseau internet.

Ces estimations indiquent également un avenir prometteur pour la communication digitale sur ce continent. Les pays les plus matures en matière de marketing digital sont certainement ceux ayant les taux de pénétration d'Internet les plus élevés, à citer le Nigeria, l'Afrique du Sud, l'Égypte, le Maroc et la Tunisie.

Rôle des agences de communication digitale ou webmarketing

Une présence proactive sur Internet permet non seulement de maîtriser l'e-réputation mais aussi de booster les ventes et conquérir de nouveaux marchés. Les agences de communication digitale utilisent aujourd'hui des techniques très avancées pour cibler efficacement les internautes et aussi suivre l'audience des sites web.

En exemple, l'Inbound marketing (ou marketing entrant), par opposition au marketing classique, consiste à faire venir le client vers l'entreprise. Cette forme de webmarketing, mettant en œuvre divers leviers du marketing digital, prouve depuis quelques temps son pouvoir et son mérite d'être un moyen de communication pertinent. Chaque site internet devient donc son propre média en diffusant en ligne des contenus attractifs, de bonne lisibilité et visibilité.

Le marketing digital ou webmarketing, est assez vaste qu'il devient difficile à cerner

Ce nouveau mode de communication touche divers domaines, de la création des sites internet au management de l'e-réputation en passant par le référencement, la gestion des contenus web et la diffusion d'informations via les réseaux sociaux, sans oublier les bannières, outil de publicité classique sur Internet.

L'un des avantages du marketing digital est qu'il permet de communiquer directement avec les clients et de suivre efficacement leur comportement, contrairement au marketing traditionnel. Cette forme de marketing permet également un certain degré de précision pour le ciblage des internautes par centres d'intérêt, âge, sexe ou encore par zones géographiques.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.info-afrique.com/5336-en-afrique-communication-digitale/>

Par Thierry Barbaut avec l'Agence 360

Le Bundestag se montre incapable de surmonter une cyber-attaque | Le Net Expert Informatique



Le Bundestag
se montre
incapable de
surmonter une
cyber-attaque

Depuis quelques semaines le parlement allemand est victime d'attaques informatiques à répétition. Un phénomène qui inquiète certains députés.

Le Bundestag est vulnérable. Depuis le début du mois de mai, les services informatiques du parlement allemand sont la cible de cyber-attaques répétées. Les députés ne sont plus en mesure de sécuriser leurs communications. Des données ont été piratées, sans qu'il soit possible d'en connaître la nature. Impossible pour l'heure de savoir si des documents confidentiels ont été volés. «Et ce n'est pas terminé», a déclaré un porte-parole, selon des propos rapportés par les médias allemands, comme Der Spiegel ou Die Zeit, qui ont notamment révélé l'affaire. Le «cheval de Troie» utilisé par les hackers n'a pas encore été neutralisé. Selon le quotidien Süddeutsche Zeitung, le BSI, chargé de la sécurité fédérale informatique, aurait même demandé une aide extérieure pour en venir à bout.

L'exaspération et l'inquiétude commencent à se répandre au Bundestag, principalement dans les rangs de l'opposition. Les députés Verts et Die Linke semblent davantage touchés par l'attaque. Mais la cible exacte des hackers reste encore inconnue. «L'incertitude demeure sur l'intensité de l'attaque et son ampleur», a expliqué le député Vert Konstantin von Notz, spécialiste des questions informatiques. «Il n'y avait encore jamais une telle attaque pendant plusieurs jours», a déploré la vice-présidente Petra Pau (Die linke). «Il y a une attente évidente pour que la protection des communications soient rétablies», a observé le responsable SPD Lars Klingbeil. Le Bundestag envisage la possibilité de devoir réinstaller totalement l'infrastructure du réseau, pour purger la menace. Toute l'activité informatique du Bundestag en serait interrompue. L'opération pourrait avoir lieu au moment des vacances parlementaires, en juillet.

20 tentatives d'intrusion par jour en 2014

Qui se cache derrière l'assaut? Pour l'instant, la seule piste connue mène vers Europe de l'Est, où sont situés des serveurs qui auraient infiltré au moins deux ordinateurs du Bundestag. Mais l'enquête de la Sécurité intérieure est toujours en cours. Toutefois, à écouter les experts, la complexité de l'attaque témoigne d'une capacité technologique dont seuls des services secrets peuvent disposer.

Il ne s'agit pas de la première attaque informatique dont est victime l'administration allemande, loin de là. Selon le BSI, les services internes du gouvernement auraient subi en moyenne 20 tentatives d'intrusion par jour l'année dernière. Des services de renseignement étrangers seraient à l'origine d'au moins une attaque quotidienne. Pour renforcer la sécurité informatique de l'Allemagne et notamment de ses entreprises, le gouvernement élabore un nouveau projet de loi. «Avec cette loi, une amélioration significative de la sécurité des communications informatiques devra être atteinte», promet le texte en préparation. Le Bundestag sera amené à en débattre.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.lefigaro.fr/international/2015/05/22/01003-20150522ARTFIG00173-le-bundestag-se-montre-incapable-de-surmonter-une-cyber-attaque.php>

L'employeur face au droit d'accès du salarié à ses

données informatiques | Le Net Expert Informatique

L'employeur face au droit d'accès du
salarié à ses données informatiques

Pour Isabelle Renard, docteur ingénieur et avocate au barreau de Paris, la loi Informatique et libertés encadre encore de manière floue les relations employeurs/employés, notamment dans le cadre de l'accès au salarié à ses traces « informatiques ». Elle recommande aux entreprises d'encadrer de façon explicite et précise dans leur charte informatique les modalités de ce droit d'accès, pour éviter les demandes abusives de la part de leurs employés.

La loi Informatique et libertés prévoit que toute personne dont les données personnelles sont traitées peut demander au responsable de traitement d'accéder à celles-ci, dans des conditions qui sont précisées par l'article 39 du texte.

Aux termes de ces dispositions, chacun peut obtenir l'ensemble des renseignements qui caractérisent le traitement dont ses données font l'objet : quelles sont les données traitées, dans quel but, à qui sont-elles transmises, le responsable s'appuie-t-il sur ces informations pour prendre des décisions personnelles à l'égard de la personne concernée ?

Le responsable du traitement des data est tenu de répondre à ces interrogations, sauf si celles-ci procèdent d'un abus manifeste, par leur nombre ou leur répétition trop systématique.

Ces dispositions sont entièrement applicables aux relations entre salariés et employeurs qui, avec les nouvelles technologies, sont en possession de données personnelles de plus en plus nombreuses concernant leurs employés : données de connexion Internet, gestion centralisée des compétences, données des badgeuses, géolocalisation, enregistrements vidéos et vocaux...

UNE FICHE PRATIQUE DE LA CNIL

Les données des employés doivent être collectées licitement, ce qui suppose que les employeurs aient déclaré à la Commission nationale de l'informatique et des libertés (Cnil) les traitements afférents, selon la procédure applicable (déclaration simplifiée, normale, ou demande d'autorisation), selon qu'il existe – ou non – un correspondant informatique et libertés dans l'entreprise. En cas de non déclaration ou de déclaration partielle par l'employeur d'un fichier, les données recueillies ne peuvent pas être opposées au salarié pour fonder une procédure disciplinaire. Ce principe posé par le Cour de cassation est rappelé de façon constante par la jurisprudence.

Mais ce n'est pas tout. Encore faut-il que l'employeur soit en mesure de répondre aux demandes d'accès à leurs données exercées par les salariés. La Cnil, dans la fiche pratique numéro 3 de son guide « pour les employeurs et les salariés », donne une liste des informations auxquelles le salarié a le droit d'accéder, sur simple demande :

- recrutement
- historique de carrière
- rémunération
- évaluation des compétences professionnelles (entretiens d'évaluation, notations)
- dossier disciplinaire

De façon générale, le salarié doit pouvoir accéder à l'ensemble des données de gestion de ressources humaines le concernant, dès lors que celles-ci ont servi de base à une décision à son égard. Ce critère manque singulièrement de clarté, et semble ne concerner que les données de ressources humaines.

S'agissant des traces informatiques, la Cnil ne met aucune condition à leur droit d'accès par le salarié. Par exemple, pour les données de géolocalisation, elle a prononcé une sanction de 10 000 euros à l'encontre de la société Nord Picardie, qui a refusé de transmettre à un employé une copie de ses données de géolocalisation, dont il avait besoin pour prouver qu'un accident de la circulation dont il avait été victime avait un caractère professionnel. De la même façon, l'employeur est tenu de mettre à disposition d'un salarié en faisant la demande ses données de vidéosurveillance, ses écoutes téléphoniques ou ses données de navigation web.

UNE CHARTE INFORMATIQUE EXPLICITE

Confrontés à de telles requêtes l'employeur, même de bonne foi, a parfois du mal à savoir comment se positionner, surtout lorsque lesdites requêtes sont exercées par certains salariés uniquement par principe, pour obliger l'employeur à se plier à une exigence qu'ils estiment être de droit, et alors même que la fourniture de ces informations hors contexte peut se heurter à de réelles difficultés pratiques. Ne reste alors à l'employeur qu'à sortir le joker de la demande « manifestation abusive », et pour cela, il faut caractériser l'abus, ce qui n'est pas simple.

Le « droit d'accès » prévu de façon générale par la loi Informatique et libertés reste un sujet mal encadré dans les relations employeurs/employés, surtout s'agissant de l'accès au salarié à ses traces « informatiques », dont il est en tout état de cause informé de la collecte dès lors que celle-ci est clairement mentionnée dans la charte informatique. Le point n'est pas plus traité dans le projet de règlement européen sur la protection des données personnelles.

Faute d'attendre une amélioration des textes ou un positionnement de la Cnil, nous pensons que la meilleure façon pour les employeurs de se prévaloir de demandes abusives est d'encadrer de façon explicite et précise dans les chartes informatiques les modalités du droit d'accès, pour chaque type de trace « numérique », au lieu des dispositions génériques et floues qu'on y voit actuellement.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.usine-digitale.fr/article/l-employeur-face-au-droit-d-acces-du-salarie-a-ses-donnees-informatiques.N330908>

Par Isabelle Renard, docteur ingénieur et avocate au barreau de Paris

Contrôle de la CNIL aujourd'hui à France Télévisions | Le Net Expert Informatique

Contrôle de la CNIL aujourd'hui à France Télévisions

L'Express l'a révélé ce jeudi matin: le siège de France Télévisions a été fouillé mercredi par la Commission nationale de l'informatique et des libertés. Le groupe audiovisuel est soupçonné d'avoir opéré un fichage illégal de ses salariés.

France Télévisions a subi mercredi un contrôle de la Commission nationale de l'informatique et des libertés (Cnil) pour vérifier l'existence de fichiers contenant notamment des données sur les opinions politiques et l'orientation sexuelle de ses salariés, a révélé L'Express ce jeudi matin.

Dénoncé par une lettre anonyme, France Télévisions ficherait ses employés

Ce contrôle avait pour but de vérifier si, oui ou non, France Télévisions a illégalement fiché ses employés. D'après une lettre anonyme envoyée à la Cnil, le groupe audiovisuel aurait recueilli des données personnelles sur leurs opinions politiques, leur orientation sexuelle ou leur casier judiciaire.

Selon le procès-verbal de cette perquisition, les six agents de la CNIL dépêchés sur place ont effectué des recherches au sein des boîtes mails de la direction des ressources humaines du groupe audiovisuel public. D'après plusieurs sources syndicales, les enquêteurs n'auraient a priori pas trouvé « d'éléments probants » en fin de matinée, mais ils ont réalisé des copies de plusieurs fichiers internes. L'instruction, elle, « est toujours en cours ».

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

http://www.lexpress.fr/actualite/medias/soupons-de-fichage-illegal-de-salaries-france-televisions-perquisitionne-par-la-cnil_1681974.html

87% des actes cybercriminels commis en France sont du fait de hackers made in France | Le Net Expert Informatique

87% des actes cybercriminels commis en France sont du fait de hackers made in France

Une étude révèle que 87% des actes cybercriminels commis en France sont du fait de hackers made in France. Russes, Africains, Chinois ou Coréens seraient moins offensifs qu'on ne le pense.

La dernière étude de ThreatMetrix va secouer les idées reçues sur la cybercriminalité en France. Selon ce rapport, qui porte sur le 1er trimestre 2015, « la plus grande cyber-menace ayant pesé sur les entreprises françaises durant cette période aurait pour origine l'hexagone ».

L'étude précise que 87% des attaques sont commises depuis la France. Pour les auteurs du rapport, il ne s'agit pas de pointer la performance de la cyberdélinquance made in France, mais de noter que désormais, les attaques menées dans chaque pays sont pilotées dans leur frontière. Ce constat est « en rupture avec les tendances dominantes où la grande majorité des cyberattaques avaient pour origine la Russie, l'Asie ou l'Afrique. »

Ainsi, la France n'est donc pas une exception, mais elle exprime une véritable tendance. En Grande-Bretagne, 75% des actes cybercriminels proviennent d'Irlande ou d'Angleterre, 81% en Allemagne, 54% aux Pays-Bas, 94% en Italie et 85% en Russie.

Sur les attaques, ThreatMetrix a constaté que l'usurpation d'identité (spoofing) est devenue la plus courante. Lors des fêtes de Noël, le cabinet a dénombré 11.4 millions de tentatives de transactions frauduleuses.

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

Contactez-nous

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

Source : <http://bfmbusiness.bfmtv.com/entreprise/les-hackers-francais-sont-les-rois-du-cybercrime-en-france-888210.html>
Par Pascal Samama

Les opérateurs télécoms nous espionnent-ils ? | Le Net Expert Informatique

Les opérateurs télécoms nous espionnent-ils ?

Votre téléphone est-il sur écoute ? Depuis plusieurs semaines, une affaire secoue le milieu des télécoms suite à la révélation du journal arabophone Al Massae quant à l'utilisation d'un logiciel «d'espionnage des données personnelles» par un opérateur télécoms de la place. Il s'agit du LCS, un logiciel en principe prohibé en Europe et aux États-Unis, qui permet de surveiller l'activité des utilisateurs en dehors de tout cadre légal.

La question qui se pose aujourd'hui : les opérateurs télécoms ont-ils le droit d'utiliser les outils qu'ils ont pour contrôler et accéder aux informations et aux données des utilisateurs ? «Il s'agit d'un système permettant de retracer toutes les actions d'un utilisateur sur sa ligne téléphonique et d'effectuer les perquisitions numériques, explique Carlo Lando, un expert italien en sécurité des télécoms.

«En principe, les opérateurs téléphoniques doivent avoir des autorisations du tribunal pour utiliser cette technologie de système sur les réseaux, notamment pour les enquêtes», précise l'expert. Interpellé, le DG de l'Agence nationale de régulation des télécoms (ANRT), Azeddine Mountassir Billah, dit tout ignorer de cette affaire et refuse de la commenter.

En revanche, à la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), on apprend qu'une réunion aura lieu cette semaine, avec à l'ordre du jour, entre autres, cette affaire de «logiciel LCS». Le président du CNDP, Saïd Ihrai, a déclaré que la commission n'a pas encore été saisie sur ce type de «procédé prohibé» permettant de surveiller et de contrôler les données personnelles des utilisateurs.

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

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.leseco.ma/maroc/30623-donnees-personnelles-les-operateurs-telecoms-nous-espionnent-ils.html>

Par NAIMA CHERII

Alerte: Nouveaux courriels de phishing au nom d'Apple (iTunes) | Le Net Expert Informatique

✖	Alerte: Nouveaux courriels de phishing au nom d'Apple (iTunes)
---	--

Des fraudeurs envoient des courriels au nom d'Apple (iTunes) afin de s'emparer des données d'accès à votre compte.

Par ces courriels, les destinataires sont informés que leur compte n'a pas pu être validé et que celui-ci a été bloqué. Les escrocs demandent de suivre un lien et de fournir des données personnelles (nom d'utilisateur et mot de passe) sous prétexte de pouvoir réactiver leur compte.



Le SCOCI conseille :

1. Effacez le courriel !
2. Si vous soupçonnez quelqu'un d'être en possession de vos données d'accès à votre compte, veuillez immédiatement prendre contact avec le support d'Apple.
3. Soyez prudents avec tous les courriels qui vous demandent de cliquer sur un lien Internet pour contrôler vos données personnelles. En règle générale, ceci est l'œuvre de fraudeurs.
4. Contrôlez toujours l'adresse Internet (URL) sur laquelle vous êtes redirigés (cf. rectangle rouge sur l'image). De manière générale, si vous devez vous connecter à un compte en ligne, inscrivez l'URL vous même dans votre navigateur plutôt que de cliquer sur un lien qui vous est transmis par courriel.
5. Signalez ces cas au SCOCI par le biais de son formulaire d'annonce en ligne afin que nous puissions analyser ces courriels et faire fermer au plus vite les sites frauduleux.

En cas de doute sur une usurpation d'identité ou de doute sur une arnaque, n'hésitez pas à contacter Denis JACOPINI expert informatique assermenté.

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

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <https://www.cybercrime.admin.ch/kobik/fr/home/warmmeldungen/2015/2015-05-15.html>

Les «usines à clics» tournent

à plein régime aux Philippines | Le Net Expert Informatique



Les « usines à clics » tournent à plein régime aux Philippines

Les « usines à clics » aux Philippines produisent en masse de faux comptes pour les réseaux sociaux. De nombreuses célébrités, des personnalités politiques, de grandes entreprises et même de simples internautes en manque de fans, usent et abusent de cette contrefaçon numérique afin accroître leur popularité sur la Toile.

Un journaliste du magazine en ligne New Republic a enquêté aux Philippines sur les « usines à clics », ces fabriques singulières qui créent à la chaîne de faux comptes « clef en main » et inondent les réseaux sociaux de recommandations bidons, de « j'aime » chimériques, de fans fictifs et de suiveurs imaginaires.

Le prix d'un faux profil n'excède pas 1€50, et n'importe quel internaute ou de grandes entreprises peuvent ainsi, en

quelques clics, gonfler artificiellement leur visibilité sur la Toile. Une activité frauduleuse en plein essor qui s'appuie sur un réseau d'intermédiaires peu scrupuleux, comme le démontrait récemment le magazine Envoyé Spécial sur France Télévisions, qui a surpris une start-up française spécialisée dans la revente d'abonnés virtuels, en pleine transaction.

Selon les conditions d'utilisation des réseaux sociaux, le commerce de faux profils en ligne est formellement interdit. Mais les autorités des Philippines considèrent que ces règlements n'ont aucune valeur juridique sur leur territoire. Pour elles, c'est donc un négoce illicite mais pas illégal.

Un fléau pour les géants d'Internet

Ce marché noir de la « web réputation » menace maintenant l'économie numérique mondiale, il serait nuisible aux activités des entreprises qui ont depuis longtemps investi dans les réseaux sociaux.

C'est un fléau, selon les géants du web, qui ne parviennent pas à endiguer le phénomène, particulièrement pour Facebook, Twitter et Google, dont les modèles économiques reposent exclusivement sur des offres publicitaires ciblées pour le commerce en ligne.

Les usines à clics fonctionnent comme de vraies entreprises, avec un personnel qualifié qui est composé principalement de jeunes informaticiens diplômés gagnant cinq fois le salaire d'une femme de ménage.

Les patrons, eux, profitent pleinement des infrastructures technologiques implantées dans le pays par de grandes compagnies américaines comme Microsoft. Un miracle économique

inattendu de la délocalisation, conclut ironiquement le journaliste de New Republic. Les « usines à clics » sont devenues en quelques années les principaux moteurs de la croissance aux Philippines.

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

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :
http://www.rfi.fr/asie-pacifique/20150506-philippines-usine-clics-commerce-fans-internet-reseaux-sociaux/?aef_campaign_date=2015-05-06&aef_campaign_ref=partage_user&ns_campaign=reseaux_sociaux&ns_linkname=editorial&ns_mchannel=social&ns_source=twitter

Facebook développe la reconnaissance faciale... de dos ! | Le Net Expert Informatique

Facebook développe la reconnaissance faciale... de dos !

Capture d'écran du film « Mon nom est personne » (1973) (Tonino Valerii)



Les méthodes les plus choquantes de Google | Le Net Expert Informatique

Les méthodes les plus choquantes de Google

Dans le cadre de son enquête sur d'éventuelles pratiques concurrentielles de Google, l'autorité américaine de la concurrence, la FTC, avait épinglé en 2012 des méthodes... illégales qui viennent d'être rendues publiques, par erreur.

L'information fait l'effet d'une bombe : la Federal Trade Commission américaine avait admis, dans un rapport tenu secret, que le géant de la recherche abusait de sa position dominante et discriminait ses concurrents. Ce rapport a été obtenu, par erreur, par le Wall Street Journal. Ce dernier avait demandé à la FTC une copie du rapport de 2012... mais cette dernière lui a transmis un rapport intermédiaire, visiblement non édulcoré comme sa dernière version. Ce qu'on peut y découvrir est renversant car, pour la première fois, une autorité met noir sur blanc ce que les nombreux concurrents de la firme de Mountain View crient haut et fort.

Voici cinq points particulièrement percutants de ce rapport :

Favoriser ses propres services

Dans le cadre de son moteur de recherche, la firme de Mountain View a volontairement donné priorité à ses propres services en matière de voyage ou de shopping. Ainsi, Google aurait affiché en meilleure position les résultats de son comparateur de prix des billets d'avion alors même que d'autres concurrents proposaient plus d'alternatives... Pour y parvenir, Google aurait délibérément adapté les critères de classements pour améliorer la position de ses services. « Quand l'algorithme de Google constatait qu'un comparateur de prix était relevant pour le surfeur, il proposait la page Google Product Search. Pareil quand il constatait que l'internaute était intéressé par des sites locaux comme Yelp ou CitySearch, Google proposait plutôt Google Local. »

Déclasser les concurrents

Le rapport de la FTC souligne aussi que « Google a adopté une stratégie de rétrogradation et de suppression de liens vers des sites verticaux dans certaines catégories de produits hautement commerciales. »

Pomper les concurrents

Par ailleurs, Google a, d'après ce rapport, copié des informations provenant de sites concurrent pour améliorer l'efficacité de ses propres services. Il s'agit par exemple de commentaires issus des autres sites pour améliorer les classements de produits sur ses propres services. Parmi les sites évoqués, Yelp, TripAdvisor ou Amazon...

Minimiser ses parts de marché

Google -qui se plaint à soigner au maximum son image- n'aime pas avoir l'image du géant, de la pieuvre gigantesque du Net. Aussi, dans le rapport, on découvre que l'économiste en chef de Google s'était réjoui que les instituts d'audience sous-estiment la part de marché réelle de Google. Aux Etats-Unis, Comscore évaluait la part de marché de Google autour de 65% de la recherche. En réalité, selon le responsable du moteur de recherche, il s'agirait plutôt de parts comprises entre 69 et 84 %... (En Europe, c'est de facto encore bien plus).

La conclusion du rapport de l'autorité de la concurrence américaine est sans appel. On y lit clairement que « Google était dans une position unique lui permettant d'aider ou de casser n'importe quel business en ligne ». Une position qui, selon tous les faits énoncés dans le rapport secret de la FTC, aurait été mise à profit par Google pour asseoir sa domination. Les responsables de cette enquête soulevaient par ailleurs que « l'attitude de Google avait causé (et allait encore causer) de vrais dommages pour l'innovation et pour le consommateur dans le domaine de la recherche et de la publicité. »

On ignore les véritables raisons pour lesquelles la Federal Trade Commission n'a finalement pas poursuivi le mastodonte du Net. Certains évoquent que Google aurait accepté, à l'époque, de changer d'attitude pour empêcher toute pratique anticoncurrentielle. D'autres évoquent un embarras à l'égard de Barak Obama dont Google a été le deuxième plus gros contributeur financier de sa campagne électorale.

Du côté de Google, on nous transmet par e-mail une réaction toute faite de Kent Walker, General Counsel : « Après une enquête de 19 mois, 9 millions de pages de documents et des tas d'heures de témoignages, le staff de la FTC et les 5 commissaires de la FTC sont tombés d'accord pour dire qu'il n'y avait pas besoin de prendre une action sur la manière dont on trie et on affiche les résultats de recherche. Les spéculations sur un potentiel dommage pour le consommateur et les concurrents est totalement faux. Depuis la fin de l'enquête, voici 2 ans, l'accès à l'information a considérablement augmenté, laissant au consommateur plus de choix encore que par le passé. Et nos concurrents progressent. Yelp par exemple enregistre une croissance de 350% sur les 4 dernières années. Et sur la même période TripAdvisor a quasi doublé ses revenus... »

Malgré tout, ces révélations restent gênantes pour le géant du Net, également sous le coup de plusieurs affaires en Europe. La grande question c'est évidemment l'effet de ces révélations les procédures en cours de ce côté-ci de l'Atlantique.

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

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://m.trends.levif.be/economie/high-tech/numerik/les-methodes-les-plus-choquantes-de-google/article-normal-373435.html>

Par C C