Publier un selfie devant la pyramide du Louvre, est-ce du vol ?

Publier un selfie devant la pyramide du Louvre, est-ce du vol ?

Oui, selon les sénateurs, qui ont réservé cette publication aux particuliers sur des sites strictement non commerciaux pour protéger les droits des créateurs.

Avez-vous le droit de photographier la pyramide du Louvre, et d'en publier l'image sur les réseaux sociaux ? Avez-vous le droit de vous prendre en photo devant la tour Eiffel illuminée en arrière-plan, et de diffuser le cliché ? C'était tout l'enjeu de la « liberté de panorama » qui était soumise à la discussion parlementaire dans le cadre du vote de la loi numérique. Et comme les députés avant eux, les sénateurs ont répondu non. Sauf à demander son avis à l'ayant-droit de l'oeuvre, il sera possible de diffuser des photos de bâtiments ou de sculptures protégées par le droit d'auteur, mais en les réservant aux seuls particuliers et à l'exclusion de tout usage à caractère directement ou indirectement commercial. Excluant de ce champ les associations, les sénateurs ont plongé Wikimedia (l'association qui a pour objet la diffusion de connaissance, via Wikipedia entre autres) dans un cauchemar sans fin : le site internet ne pourra désormais plus illustrer ses articles avec des photos des œuvres dont il parle.

Protéger la démarche artistique

L'objectif de cet amendement est d'empêcher un quidam de tirer un bénéfice financier de l'utilisation d'une photo d'une œuvre (même si c'est lui qui l'a prise) sans en avoir demandé l'autorisation aux ayants-droit de leur créateur, de manière à protéger la création. L'amendement concerne « les reproductions et représentations d'oeuvres architecturales et de sculptures, placées en permanence sur la voie publique », comme par exemple les illuminations de la tour Eiffel ou encore la pyramide du Louvre.

Mais les partisans d'une liberté totale de panorama pointent les restrictions considérables qu'apporte cet amendement. En effet, de tels clichés devenant interdits pour « tout usage à caractère directement ou indirectement commercial », ils seront désormais interdits de séjour sur les réseaux sociaux comme Facebook, Twitter ou Instagram. Il ne restera plus qu'à patienter jusqu'à ce que les œuvres tombent dans le domaine public (70 ans après la mort de l'artiste) pour partager entre amis un selfie touristique, ou bien créer un site internet personnel ne laissant aucune place à la publicité. Le nain de jardin d'Amélie Poulain, photographié devant les monuments du monde entier pour les besoins d'un film – commercial –, ne connaîtrait plus aujourd'hui le même fabuleux destin…. [Lire la suite]

Réagissez à cet article

Source : *Liberté de panorama : publier un selfie devant la pyramide du Louvre, est-ce du vol ?*

Un casseur de 17 ans retrouvé

par la police grâce à YouTube

	**Un casseur de 17 ans retrouvé par la police grâce à YouTube**

Un jeune homme de 17 ans qui a participé au saccage du magasin Go Sport de Nantes en cachant son visage sous une capuche, a été appréhendé par la police. Il avait raconté les faits sur YouTube.

Tout ce que vous direz sur Internet pourra être retenu contre vous et heureusement, les imbéciles n'en ont pas toujours conscience. France 3 Pays-de-la-Loire rapporte ainsi que la police nantaise consulte les vidéos amateurs qui circulent notamment sur YouTube, dans lesquelles des casseurs sont visibles, voire celles dans lesquelles ils se vantent de leurs propres délits (ce qui arrive plus souvent qu'on ne l'imagine).
C'est ainsi que les policiers ont pu appréhender un jeune lycéen de 17 ans, qui s'était vanté sur une vidéo d'avoir « fait Go Sport la dernière fois » et d'avoir « eu des chaussures gratuites » en se servant dans la vitrine cassée de la boutique située à deux pas de la tour de Bretagne, au cœur de la métropole de Nantes. Le magasin de sport avait été vandalisé le 5 avril dernier et la vidéo avait été tournée après une nouvelle manifestation du 9 avril… [Lire la suite]

Réagissez à cet article

Source : *Un casseur de 17 ans retrouvé par la police grâce à YouTube*

Une faille du Login de Facebook corrigée

Une faille du Login de Facebook corrigée

Les pirates se faisaient passer pour les titulaires des comptes en exploitant une faille du Login de Facebook.

Les Bitdefender Labs ont révélé une vulnérabilité lors de l'authentification en ligne sur des sites Web tiers via Facebook. Un manque de mesure de sécurité lors de la validation permet aux pirates d'usurper l'identité des internautes et d'accéder, sans mot de passe, à leurs comptes en ligne.
Les *social logins* sont une alternative à l'authentification traditionnelle et un mode apprécié par les utilisateurs pour leur côté pratique : ils permettent aux utilisateurs de se connecter à leurs comptes Web sans saisir leur nom d'utilisateur ni leur mot de passe. La plupart des sites offrent des social logins via Facebook, LinkedIn, Twitter ou Google Plus.
Les chercheurs des Bitdefender Labs ont trouvé un moyen d'usurper l'identité de l'utilisateur et d'avoir accès à ses comptes Web en utilisant le plug-in Facebook Login.
« Il s'agit d'une vulnérabilité grave qui permet aux pirates de créer un compte avec une adresse e-mail ne leur appartenant pas et de changer l'adresse e-mail liée au compte d'un site par une autre adresse non vérifiée », prévient Ionut Cernica, chercheur spécialiste des vulnérabilités chez Bitdefender. *« Cela signifie qu'un pirate peut effectuer des paiements en ligne au nom de l'utilisateur, arrêter son moteur antivirus pour infecter ses périphériques, propager des malwares à ses contacts et bien plus encore. »*
Pour que l'attaque réussisse, l'adresse e-mail de la victime ne doit pas déjà être enregistrée sur Facebook. La plupart des internautes ont plus d'une adresse e-mail publiée sur différents sites Web, accessibles à tout le monde. Il est donc assez simple pour le pirate d'obtenir une de ces adresses et de créer un compte Facebook avec cette dernière.
Pour vérifier l'identité d'un utilisateur sans exposer ses identifiants d'authentification, Facebook Login utilise le protocole OAuth. Grâce à OAuth, Facebook est autorisé à partager certaines informations de l'utilisateur avec le site Web tiers… [Lire la suite]

Réagissez à cet article

Source : *Une faille du Login de Facebook corrigée – Data Security BreachData Security Breach*

Que risquent les enfants sur les réseaux sociaux ?

Que risquent les enfants sur les réseaux sociaux ?

Avoir des profils dans les réseaux sociaux peut représenter de nombreux dangers pour les enfants.
Denis JACOPINI, expert Informatique assermenté spécialisé en cybercriminalité a souhaité couvrir le sujet et a collecté quelques informations bien utiles pour comprendre le phhénomène.

Quels sont les risques d'une trop grande exposition sur les réseaux sociaux?

Attardons nous rapidement sur quelques analyses bien inquiétantes :
• 38% des 9-12 ans ont un profil sur un réseau social, alors que la plupart de ces réseaux ne sont autorisés qu'à partir de 13 ans !
• 77% des 13-16 ans sont présents !
• 1/4 ont un profil public ;
• 1/5 y communique son adresse, son numéro de téléphone…
• Seulement 55% des jeunes discutent avec leurs parents de ce qu'ils font sur Facebook ;
• 92% des jeunes de 8 – 17 ans utilisent leur vraie identité sur Facebook et livrent des informations personnelles ;
• 25% des jeunes de 8 – 17 ans disent avoir déjà été victimes d'insultes ou rumeurs sur Facebook ;
• 36% ont déjà été choqués par certains contenus.

1°/ Les jeunes, trop peu sensibilisés, ont tendance à communiquer bien trop d'éléments (photos, éléments de leur vie). L'effet immédiat est que les cybercriminels auront tous les éléments dont ils auront besoin pour pouvoir usurper leur identité.

2°/ Sur Internet, tout peut être copié collé (et altéré dans le processus), il n'y a aucune garantie de confidentialité dans les échanges électroniques via les réseaux sociaux. Des photos prises lors de soirées ou dénudées peuvent facilement se retrouver à la vue de tout le monde, tout comme un message insultant, écrit dans un moment d'énervement. Les jeunes n'hésitent pas à « taguer » des amis sur les photos de groupe, sans se rendre compte que cette action impacte directement la vue privée des amis tagués.

3°/ Autre risque bien réel, s'exposer sur les réseaux sociaux augmente le risque de contact avec un pédophile cherchant avant tout à rencontrer des enfants ou des ados naïfs, crédules ou confiants.

4°/ Autre faits inquiétants, 25% des jeunes de 8 – 17 ans disent avoir déjà été victimes d'insultes ou rumeurs sur Facebook. Les cyberviolences, souvent initiée à l'école est souvent poursuivies sur les réseaux sociaux sont très courantes. Une publication d'albums de photos de vacances ou d'une soirée entre amis peut vite déraper et se transformer en détournement obscène en ligne avec un impact sur la vie réelle. Intimidations, insultes, piratage de compte, commentaires humiliants, création de groupes de discussion pour moquer la victime – la violence des rapports entre jeunes peut pousser la victime jusqu'au suicide.
Le phénomène d'entraînement peut conduire les plus influençables à imiter des comportements violents et à se lancer dans des campagnes d'insultes contre le bouc émissaire désigné par le leader du groupe.

5°/ Enfin, risque souvent méconnu, les cybercriminels rivalisent d'ingéniosité pour concevoir des messages séduisants qui invitent à « Liker » un post viral avec un lien corrompu, des applications contenant des virus, des campagnes de phishing pour soutirer les informations de connexion, etc.

A la suite d'une exposition trop massive sur les réseaux sociaux, est-ce qu'un nouveau type de criminalité est né ?
Je répondrais à celà qu'un nouveau terrain de jeu est né !
Un espace rempli de prédateurs ou les jeunes sont des proies potentielles.

Comment optimiser la sécurité sur les réseaux sociaux?
Limitez la navigation et les échanges dans un périmètre adapté à l'âge et aux besoins du jeune. Si besoin, bloquez les réseaux sociaux jusqu'à ce qu'il soit en mesure de comprendre l'impact de ses interactions en ligne.
Discutez régulièrement avec votre enfant ou ado de ce qu'il fait sur Internet : quels sites il aime consulter, avec qui il tchatte, ce qu'il ou elle a découvert de nouveau. Expliquez-lui la différence entre de vrais amis et des connaissances numériques.
Apprenez aux enfants l'importance de la protection des informations personnelles, que ce soit les leurs ou celles de leurs amis. Informer le monde que l'on est seul ce week-end n'est peut être pas l'action la plus prudente, tout comme « taguer » ses amis sur une photo peu valorisante.
Vérifiez que les paramètres de protection de vie privée sont activés sur toutes les plates-formes utilisées par l'enfant. Expliquez que les traces numériques resteront dans le temps et qu'ils seront un jour ou l'autre confrontés à leurs actions en ligne. Soulignez l'importance de mesurer ses propos et de ne pas participer aux chasses à l'homme digitales.
Expliquez au jeune que si jamais il (ou elle) est victime d'harcèlement, ou bien s'il voit ses camarades s'acharner contre quelqu'un, il doit avertir le plus rapidement un adulte, parents ou professeur. Souvent les enfants n'osent pas avouer, par honte ou bien parce qu'ils sont manipulés par les harceleurs.
Pour plus d'informations, consultez le site du Ministère de l'Éducation Nationale Agir Contre le Harcèlement à L'École (http://www.agircontreleharcelementalecole.gouv.fr).

Réagissez à cet article

Sources :

Denis JACOPINI

http://www.e-enfance.org/actualite/enfants-et-reseaux-sociaux-prudence-_151.html

http://www.e-enfance.org/enfants-danger-reseaux-sociaux.php

http://www.witigo.eu/controle-parental/dangers-reseaux-sociaux

---

Un canular sur Periscope fait

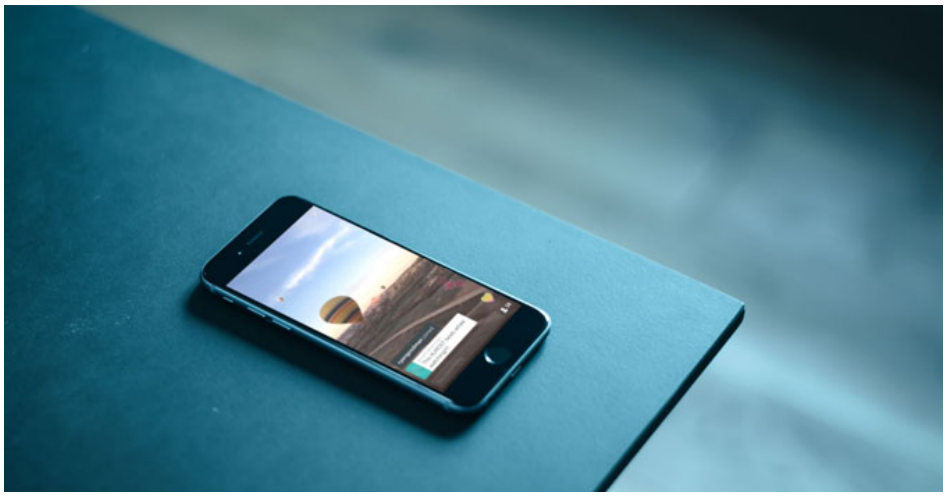
passer par la case prison ferme

	**Un canular sur Periscope fait passer par la case prison ferme**

Le tribunal correctionnel de Meaux a rendu son verdict dans l'affaire du canular sur Periscope. Les trois prévenus écopent d'une peine d'emprisonnement avec sursis, dont deux mois ferme pour l'un d'entre eux.

Les blagues les plus courtes sont les meilleures, surtout lorsqu'elles ne provoquent pas inutilement l'intervention des secours. Telle pourrait être la conclusion de ce fait divers un peu idiot, qui s'est heureusement avéré n'être qu'un canular qui a dérapé. Appréhendés en début de semaine pour une farce sur Periscope qui a déclenché le déploiement d'importants moyens d'intervention pour rien, trois hommes ont été condamnés mercredi par la justice.

Le tribunal correctionnel de Meaux a en effet rendu son jugement dans « l'affaire » de ce canular qui a simulé la torture et le meurtre d'un faux pédophile, le tout filmé via Periscope, une application pour smartphone qui permet à chacun de retransmettre en direct ce qu'il voit. Les conclusions des juges, rapportées par Le Parisien, incluent de la prison ferme et de la prison avec sursis.



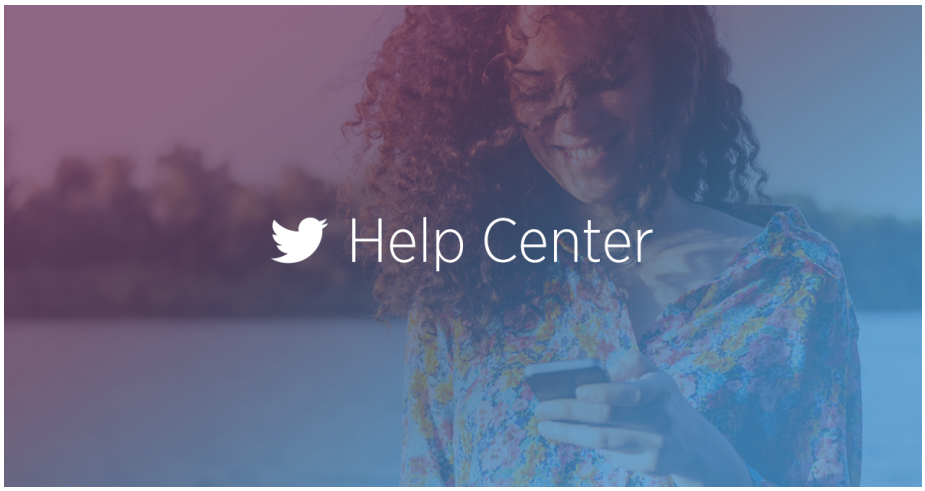
Le personnage central de cette affaire a été condamné à dix mois de prison, dont deux qu'il devra effectivement passer derrière les barreaux. Il s'agit de la peine la plus lourde, puisque les deux comparses s'en tirent avec six mois de prison avec sursis. Le fait qu'il ait déjà un casier judiciaire bien garni, avec 12 condamnations incluant des fausses alertes à la bombe, a peut-être pesé dans la balance. D'autant qu'il doit encore être jugé pour une autre affaire, ajoutent nos confrères.

Le jugement a également permis d'évaluer le coût total de l'opération : 32 000 euros. Il faut dire que les moyens déployés alors étaient conséquents : des dizaines d'hommes mobilisés (policiers, plongeurs, pompiers), des véhicules (dont un hélicoptère équipé d'une caméra thermique et deux bateaux dotés de sonars)… [Lire la suite]

Réagissez à cet article

Source : *Prison ferme pour le sinistre canular sur Periscope – Politique – Numerama*

Retrouvez l’historique de vos tweets depuis le tout premier envoyé



Retrouvez l’historique de vos tweets depuis le tout premier envoyé

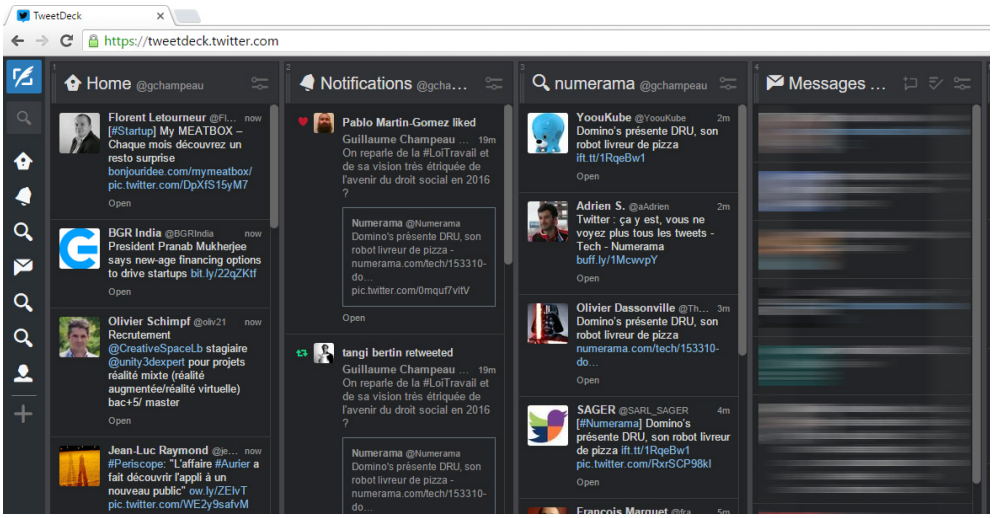
Télécharger votre archive Twitter vous permet de parcourir les éléments publiés sur Twitter depuis votre tout premier Tweet.

Pour télécharger et visualiser votre archive Twitter :
Accédez à vos paramètres de compte en cliquant sur l’icône Profil en haut à droite de la page et en sélectionnant Paramètres dans le menu déroulant.
Cliquez sur Demander votre archive.
Une fois votre téléchargement prêt, nous enverrons un email contenant un lien de téléchargement à l’adresse confirmée associée à votre compte Twitter.
Quand vous recevez cet email, cliquez sur le bouton Télécharger maintenant pour vous connecter à votre compte Twitter et télécharger le fichier .zip de votre archive Twitter.
Dézippez le fichier et cliquez sur index.html pour voir l’archive dans le navigateur de votre choix.
Remarque : Il nous faudra peut-être plusieurs jours pour préparer le téléchargement de votre archive Twitter.
… [Lire la suite]

Réagissez à cet article

Source : *Télécharger votre archive Twitter | Centre d'assistance Twitter*

Tweetdeck désactivé sous Windows le 15 avril



Tweetdeck désactivé sous Windows le 15 avril

Twitter conserve TweetDeck, mais seule la version Web sera fonctionnelle après le 15 avril.

Bonne nouvelle : Twitter n'a pas oublié Tweetdeck. Mauvaise nouvelle : seule la version Web va continuer à exister. Alors que nous nous demandions récemment si Twitter n'avait pas en projet d'abandonner son client alternatif, le réseau social a assuré vendredi dans un billet de blog qu'il « continuera à améliorer TweetDeck à l'avenir », au détriment du client Windows.

À partir du 15 avril prochain, il ne sera plus possible de se connecter sur la version Windows de TweetDeck, qui n'était déjà plus proposée en téléchargement depuis de nombreux mois. Les utilisateurs devront obligatoirement se retourner vers la version web.

TweetDeck, version web

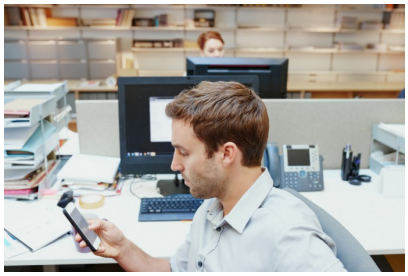
Celle-ci étant strictement identique dans ses fonctionnalités, ça ne devrait pas poser de problèmes à la majorité des utilisateurs. Les hardcore users regretteront toutefois la disparition des notifications en pop-up qui s'affichent actuellement sous Windows lorsque l'on reçoit un DM (message privé) ou qu'un nouveau message apparaît avec un tag suivi. Celles-ci ne peuvent pas être affichées dans les navigateurs HTML.

Espérons au moins que désormais, comme semble le promettre Twitter, la version Web de Tweetdeck bénéficie d'un développement plus suivi des nouvelles fonctionnalités apportées aux clients grand public et mobiles… [Lire la suite]

Réagissez à cet article

Source : *Twitter désactivera Tweetdeck sous Windows le 15*

Comment motiver vos salariés par l’e-réputation ?



Comment motiver vos salariés par l’e-réputation ?

La marque employeur n'est pas un concept tout nouveau mais il serait bien dommageable de la négliger pour autant. Avec l'apparition et la démocratisation des réseaux sociaux, il est nécessaire aujourd'hui d'envisager une numérisation de cette marque employeur si l'on ne veut pas se laisser dépasser et garder la main sur son « e-réputation ».

Parmi les canaux de communication autour de la marque employeur, il y a ceux que l'entreprise peut directement maîtriser (le site web, le profil LinkedIn, etc.) et ceux sur lesquels elle n'a pas la main (les comptes personnels des collaborateurs sur les réseaux sociaux). Or, les avis des collaborateurs sont considérés comme plus fiables que la communication officielle. Il est plus naturel de faire confiance à des témoignages individuels qui seront, à tort ou à raison, considérés comme plus authentiques.
En dépit de ce constat, beaucoup d'entreprises tardent à « numériser » leur marque employeur et subissent leur e-réputation plus qu'ils ne la construisent. Seules 28 % des entreprises (enquête StepStone) donnent une place centrale à la communication numérique au cœur de leur stratégie. Pourtant, beaucoup ont conscience de l'importance de celle-ci sur le recrutement puisque 79 % des employeurs prévoient de s'investir dans cette direction.
Pour commencer, il serait judicieux d'identifier, en interne, les collaborateurs engagés et volontaires et de les inviter à participer à la communication numérique sur la marque employeur. Il convient aussi d'encourager, former et conseiller les moins sensibilisés à la question.

L'usage des réseaux sociaux par les employés

En 2014, encore 20 % des salariés français n'étaient pas présents sur les réseaux sociaux selon l'étude Cegos sur l'impact du digital dans l'entreprise. Soit par manque d'intérêt, soit par crainte de divulguer leurs informations personnelles.
Si les 80 % restants eux, utilisent les réseaux sociaux, beaucoup en ont avant tout un usage personnel et peu y voient une utilité professionnelle. Parmi ceux qui ont décidé d'en faire un outil de travail cependant, on retrouve en grande majorité des cadres, des dirigeants et des managers. Les raisons d'utiliser les réseaux sociaux dans un but professionnel sont pourtant multiples :
• Entretenir et agrandir son réseau professionnel
• Exercer une veille professionnelle
• Rechercher un emploi / recruter de nouveaux collaborateurs
• Etc.
30 % des directeurs et managers s'en serviraient même pour « véhiculer une image positive de leur entreprise » !
Malgré cette tendance à communiquer sur leur entreprise, les salariés sont méfiants : 38 % craignent des répercussions de la part de leur employeur. Et pour cause, nous avons tous entendu parler de cas de licenciements, abusifs ou non, suite à des messages publiés par des usagers imprudents…
Paradoxalement, les salariés acceptent de plus en plus d'être en relation avec leur hiérarchie et leurs collègues sur les réseaux sociaux. 46 % d'entre eux seraient « amis » avec leur patron ou certains membres de la direction !

L'importance d'un accompagnement

Plus d'un salarié sur trois publierait des informations à propos de son entreprise sur les réseaux sociaux. Ces messages vont de simples appréciations sur les produits ou services proposés par l'entreprise à la diffusion d'informations confidentielles, en passant par des avis donnés sur la stratégie, le cadre de vie, l'ambiance, etc. Les salariés s'expriment de plus en plus au sujet de leur entreprise sur internet et cela peut être une force autant qu'une faiblesse pour la réputation de l'employeur.
Les conséquences sur l'e-réputation peuvent être importantes si des dispositifs d'accompagnement ne sont pas mis instaurés. Dans les faits, seuls 6 % des entreprises ont remis un guide de bonnes pratiques sur les réseaux sociaux et 9 % auraient organisé des réunions d'information sur le sujet.

Il serait pourtant temps d'y penser ! On identifie **3 conséquences majeures d'une mauvaise e-réputation** sur la marque employeur :
• Un problème de recrutement (une entreprise dont l'image est mauvaise sur Internet n'apparaît pas comme attractive)
• Une démotivation du personnel
• Une augmentation des coûts due à la création d'un poste spécifique de chargé de veille et e-réputation

Une bonne e-réputation apporte de bons candidats

Dans leur recherche d'emploi, les candidats se renseignent sur la réputation de l'entreprise avant de postuler. Ils se rendent sur les sites web et les comptes officiels des entreprises sur les réseaux sociaux en premier lieu.
L'une des premières conséquences d'une mauvaise réputation pour une entreprise est économique. Pour travailler dans une société à la réputation "peu séduisante", les candidats réclament un supplément salariat minimum de 5 %, selon une étude de LinkedIn sur la marque employeur, publiée en septembre dernier.
Par ailleurs, plus d'un tiers des candidats français refuseraient catégoriquement un poste dans une entreprise affligée d'une mauvaise réputation employeur, quel que soit le supplément salarial proposé.
60 % des salariés à plein temps affirment que la perception d'une entreprise qu'ils connaissent peut s'améliorer s'ils entendent ou lisent des commentaires positifs de la part de personnes travaillant dans leur secteur d'activité. De quoi confirmer que les collaborateurs sont bel et bien les meilleurs ambassadeurs de la marque employeur… [Lire la suite]

Réagissez à cet article

Source : *L'importance de l'e-réputation pour motiver vos salariés | Mieux*

La CNIL attaque Facebook. Que lui reproche t-elle ?

	La CNIL attaque Facebook. Que lui reproche t-elle ?

La Commission nationale informatique et liberté (CNIL), l'autorité chargée de la protection des données personnelles, a annoncé avoir mis en demeure Facebook, lundi 8 février, lui reprochant de nombreux manquements à la loi française sur la protection des données personnelles. Un long réquisitoire, contre la manière dont Facebook collecte et exploite les données de ses 30 millions d'utilisateurs français, que la CNIL a décidé de publier.

Que reproche-t-elle à Facebook ? La liste est longue.

UNE CHARGE CONTRE LA PUBLICITÉ CIBLÉE

La CNIL estime que Facebook combine les données personnelles de ses usagers pour proposer de la publicité ciblée sans aucune base légale. Pour la CNIL, aucun consentement direct n'est donné par l'internaute, contrairement à ce qu'exige la loi française. La question de la combinaison des données personnelles en vue de la publicité est bien évoquée dans les conditions d'utilisation du réseau social, ce texte qui définit ce que peut faire ce dernier avec les données. Pour la CNIL, c'est insuffisant : la combinaison de différentes données n'est pas strictement prévue par ce « contrat » entre l'usager et le réseau social, et nécessite donc une approbation distincte de l'internaute.

La CNIL remarque que Facebook pourrait s'affranchir de ce consentement explicite en arguant, conformément à la loi, que l'affichage de publicité est fait dans l'intérêt de l'usager. Selon la CNIL, cet intérêt est trop faible et la collecte de données trop intrusive pour que Facebook se dispense d'un consentement.

DES DONNÉES COLLECTÉES TROP SENSIBLES

Dans certains cas, Facebook réclame des copies de documents permettant d'identifier l'utilisateur (afin, notamment, d'éviter qu'il se fasse passer pour quelqu'un d'autre). Parmi ces pièces, l'internaute peut soumettre un dossier médical : la CNIL estime que ce document est trop sensible et que le réseau social ne doit plus l'accepter.

Tout utilisateur de Facebook peut aussi renseigner, sur son profil, sa sympathie politique et ses préférences sexuelles. La CNIL juge que pour se conformer à la loi, Facebook devrait indiquer précisément ce qu'il compte faire de ces informations, compte tenu de leur sensibilité et de leur nature particulière que leur confère la loi française.

UN MANQUE DE TRANSPARENCE

La CNIL critique aussi vertement la manière dont Facebook explique à ses utilisateurs ce qui va être fait de leurs données personnelles. Pour la Commission, il faudrait que le réseau social les informe clairement dès le formulaire d'inscription à Facebook, conformément aux textes français, et non pas dans un texte séparé.

La CNIL juge aussi que les utilisateurs de Facebook ne sont pas suffisamment informés sur le fait que leurs données sont transférées aux USA.

UTILISATION ILLICITE DU SAFE HARBOR

Au sujet du transfert des données vers les Etats-Unis, la CNIL reproche aussi à Facebook de s'appuyer sur l'accord Safe Harbor. Ce dernier prévoyait que les données puissent librement être transférées, par des entreprisescomme Facebook, vers les Etats-Unis, au motif que ce pays apportait des garanties suffisantes en matière de protection des données. En octobre, la Cour de justice de l'Union européenne en a décidé autrement et l'a invalidé, au motif notamment que les Etats-Unis ne protégeaient pas suffisamment les données des Européens. La CNIL demande donc à Facebook de cesser de se baser sur cet accord pour transférer de l'autre côté de l'Atlantique les données de ses utilisateurs français.

PROBLÈMES DE COOKIES

Comme son homologue belge et la justice de Bruxelles avant elle, la CNIL reproche à Facebook son utilisation du cookie « datr ».

Lire aussi : La Belgique ordonne à Facebook de cesser de tracer les internautes non membres

Un cookie est un fichier qui peut être stocké sur l'ordinateur ou le téléphone d'un internaute lorsqu'il visite un site Web : il sert à mémoriser certaines informations (comme un mot de passe par exemple) ou à le reconnaître lorsqu'il visite à nouveau le même site. Facebook dépose le cookie « datr » y compris sur les appareils d'internautes qui n'ont pas de compte Facebook, lorsque ces derniers se rendent sur des pages Facebook accessibles à tous. De plus, le cookie mémorise toutes les visites de l'internaute sur les pages Web dotées par exemple du bouton « J'aime », soit la majeure partie des sites Web communément visités par les internautes français.

Facebook a fait valoir auprès la CNIL les mêmes arguments qu'il avait opposés aux autorités belges : ce cookie est destiné à reconnaître les utilisateurs « normaux » de Facebook – pour notamment empêcher le spam ou la création massive de compte – et aucun « pistage » des internautes non-inscrits à Facebook n'est effectué. Pour la CNIL, cette raison, valable, n'est pas suffisante : elle réclame à Facebook de mieux informer les utilisateurs de l'utilisation de ce cookie et des données qu'il mémorise.

La CNIL reproche aussi à Facebook de stocker trop longtemps les adresses IP – un numéro qui identifie la connexion utilisée par l'internaute pour se connecter à Internet – de ses utilisateurs.

La Commission, dans sa mise en demeure, fait de la loi de 1978 sur les données personnelles une lecture très littérale. Elle estime par exemple que Facebook y déroge en ne réclamant pas à ses utilisateurs, lorsqu'il s'inscrit, de mot de passe suffisamment compliqué. La Commission pointe qu'elle a pu s'inscrire sur le réseau social avec le mot de passe « 123456a », particulièrement faible car facile à deviner. Pour la Commission la loi impose à Facebook de prendre toutes les mesures pour protéger les données de ses membres, y compris, donc, en réclamant des mots de passe sûrs. Cette application pointilleuse devrait inquiéter de nombreuses entreprises du Web dont les pratiques sont similaires à celle du plus grand réseau social du monde.

Le réseau social dispose désormais de trois mois pour pallier les manquements repérés par la CNIL, ou demander une extension de ce délai. À l'issue de cette période, la CNIL pourra, si elle estime que Facebook n'a pas suffisamment modifié ses pratiques, entamer une procédure de sanction. … [Lire la suite]

Réagissez à cet article

Source : *Données personnelles : le virulent réquisitoire de la CNIL contre Facebook*

La boîte à outils des gendarmes du Net pour lutter contre la Cybercriminalité

La boîte à outils des gendarmes du Net pour lutter contre la Cybercriminalité

Installé au sein du pôle judiciaire de la gendarmerie nationale à Cergy-Pontoise, le centre de lutte contre les criminalités numériques (C3N) utilise une palette d'outils pour patrouiller sur le web et détecter toutes sortes d'infractions en ligne.
Depuis un an, l'unité lutte de manière active contre la propagande djihadiste et l'apologie du terrorisme. Elle s'est dotée pour cela de nouveaux outils et a renforcé ses équipes.
« Nous sommes un peu la Bac du net. Notre travail consiste à patrouiller sur Internet pour détecter des infractions », explique le colonel de gendarmerie **Nicolas Duvinage**, chef du centre de lutte contre les criminalités numériques. Cette entité, baptisée le **C3N**, rassemble 35 militaires. Elle est installée au Pôle judiciaire de la gendarmerie nationale (**PJGN**), dont les nouveaux locaux se situent à Cergy-Pontoise (Val d'Oise).
Le C3N mène trois principales missions : il anime et coordonne le réseau **CyberGend,** déployé sur tout le territoire, effectue du renseignement criminel (pour réaliser une cartographie et une typologie des auteurs et des victimes et détecter les modes opératoires émergents) et réalise des enquêtes judiciaires pour détecter les fameuses infractions commises en ligne. Dans le cadre de cette mission, les gendarmes interviennent dans plusieurs cas : pour les atteintes aux stades (attaques informatiques), les atteintes aux biens (contrefaçon), et les atteintes aux personnes (porno-pédographie). *« Depuis janvier 2015, nous participons également de manière active à la lutte contre la propagande djihadiste et l'apologie du terrorisme. Nous nous inscrivons dans une activité plus pérenne dans ce domaine»,* confie le colonel Nicolas Duvinage, avant de poursuivre : *« Le but n'est pas simplement de fermer un site ou de retirer des tweets, mais d'identifier les auteurs des tweets et de les interpeller pour les juger ».*

OsintLab pour patrouiller sur Twitter
35 personnes pour patrouiller sur la toile cela fait peu… Les équipes se sont donc équipées d'une palette d'outils de surveillance automatique ou semi-automatique. Un investissement logiciel qui représente plusieurs centaines de milliers d'euros par an. Parmi ces outils, le logiciel **OsintLab** développé par **Thales**et acheté en 2015. Celui-ci permet de sillonner **Twitter** en s'appuyant sur des mots clefs. *« Cet outil nous a permis de mener plusieurs dizaines d'enquêtes judiciaires au travers desquelles nous avons pu identifier des personnes radicalisées »,* assure le colonel. Après avoir « logé » ces personnes, les équipes du C3N transfèrent le dossier à l'échelon spécialisé ou l'échelon territorial compétent, qui se chargera de réaliser l'interpellation.

Advestisearch pour identifier les primo-diffuseurs
Le C3N utilise également le logiciel **Advestisearch** d'**Hologram Industries**, qui permet de rechercher et d'identifier des contenus illégaux et illicites sous forme de texte, d'image ou de vidéo. *« Grâce à une image fournie en entrée, nous pouvons trouver en sortie des images similaires. Par exemple, lorsqu'une équipe de gendarmes récupère une vidéo de 10 secondes, l'outil nous permet de retrouver la vidéo complète. Cela nous permet aussi de détecter les primo-diffuseurs »,* détaille le colonel.

Et bientôt un *Scraper Deep Web* maison
Le C3N n'utilise pas uniquement des logiciels « sur étagère », mais développe également ses propres outils. L'unité s'attèle, par exemple, à mettre au point son propre *Scraper Deep Web*, un outil qui permet de collecter automatiquement des petits morceaux d'information sur des réseaux comme **TOR.** Une démarche qui rappelle le projet **Memex** mené par la **Darpa.** L'agence pour les projets de recherche avancés de défense américaine a, en effet, récemment créé un « *Google du Deep Web* » afin d'aider la police dans ses enquêtes en tout genre.

Le C3N s'emploie également à scruter les jeux en ligne. *« Les auteurs détournent de plus en plus les jeux en ligne comme **Clash of Clan**, **Call of Duty** ou encore **Oh My Dollz** »*, assure le spécialiste. *« Sur Clash of Clan, par exemple, nous avons identifié en 2015 plusieurs dizaines de cas d'apologie du terrorisme et de menaces d'attentats ».*
Outre les logiciels, le C3N mise également sur les compétences humaines. L'unité a récemment recruté plusieurs officiers commissaires, dont un docteur en informatique, un ingénieur en électronique et un universitaire spécialiste des systèmes d'information.

Réagissez à cet article

Source : *Cybercriminalité : la boîte à outils des gendarmes du Net*