

RGPD : Impact sur l'Email Marketing



En mai 2018 entrera en vigueur le fameux RGPD : le Règlement Européen sur la Protection des Données. Il vise avant tout à renforcer la protection des données personnelles des internautes. De nombreux articles en ont déjà parlé et beaucoup imaginent que cette réglementation touchera de plein fouet les acteurs de l'email marketing français et leurs utilisateurs.

Sarbacane Software propose une infographie* résumant les réels changements qui seront apportés par le RGPD, et son implication pratique dans le domaine de l'emailing.



[lire la suite]

LE NET EXPERT

- **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX → MISE EN CONFORMITÉ)**
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - **FORMATIONS / SENSIBILISATION :**
 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD ;**
- Accompagnement à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contenus, détournements de clients... ;
- **Expertises de systèmes de vote électronique ;**



Contactez-nous



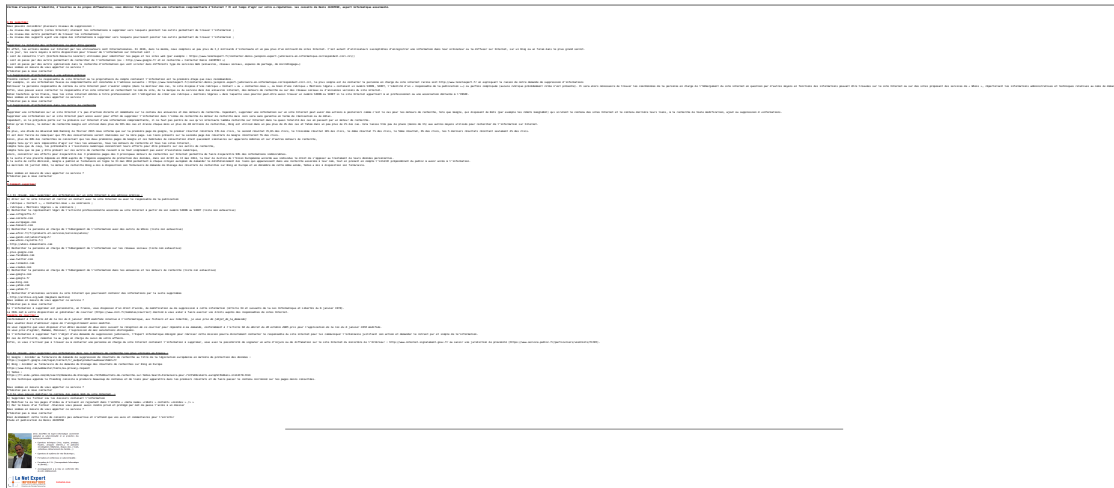
Réagissez à cet article

Source : Sarbacane : Tout comprendre sur le RGPD, le règlement européen qui va impacter toutes les entreprises en 2018 – Global Security Mag Online

et Sarbacane.com

Suppression d'un contenu web : comment procéder ? | Denis JACOPINI





LIENS SOURCES

Utilisation des moteurs de recherche en France

<http://www.journaldunet.com/ebusiness/le-net/1087481-parts-de-marche-des-moteurs-de-recherche-en-france/>

Taux de clic en fonction de la position dans les résultats

<http://www.mathiasp.fr/blog/seo/quel-est-le-taux-de-clic-en-fonction-des-positions-dans-google/544>

Comment retrouver l'auteur d'un e-mail ou d'un post ? | Denis JACOPINI



Denis JACOPINI



Comment
retrouver
l'auteur d'un e-
mail ou d'un
post ?

Victime d'usurpation d'identité, d'insultes ou de propos diffamatoires, vous désirez retrouver l'auteur d'un e-mail ou d'un post sur un forum ou sur un réseau social ? Les conseils de Denis JACOPINI, expert informatique assermenté.

1. RETROUVER L'AUTEUR D'UN EMAIL

1.1 Les envois d'e-mail

Tout comme un courrier postal sans système de sécurité tel le Recommandé avec Accusé de Réception, l'envoi d'un e-mail ne garanti pas sa réception par le destinataire désiré.

Il devient ainsi aisé de contester la réception d'un e-mail et quand bien même il a été prouvé qu'un email a été reçu et lu, rien ne peut attester qu'il a bien été consulté par la bonne personne. Pour parer à ses failles, il existe des solutions rarement utilisées d'envoi sécurisés par des tiers de confiance pouvant attester la récupération d'un e-mail par une personne identifiée et des procédés de cryptages/décryptages permettant de rendre consultable l'email par le détenteur d'une clé unique.

Sachez que la notion d'accusé de réception n'est pas universelle et dépendant de la compatibilité éventuelle être les logiciels de messagerie de l'expéditeur et du destinataire.

En conclusion, après l'envoi d'un e-mail qui n'utilise pas de procédé de traçabilité, il n'y a pas d'outil permet de confirmer la lecture de l'e-mail par une personne précise. Les outils de traçabilité standards communément rencontrés dans les solutions d'e-mailing, utilisent généralement une petite image spécifique, invisible stockée sur un serveur qui, une fois affichée sur le logiciel de messagerie du destinataire, horodate et mémorise l'adresse IP de l'accès et les paramètres du destinataire ayant affiché l'image.

1.2 La réception d'emails

Lorsque le destinataire d'un e-mail prend connaissance de son message, il est mis en forme par son logiciel de messagerie électronique. Les e-mails peuvent être reçus au format « texte » ou au format « html » avec des mises en forme esthétiquement intéressantes et peuvent contenir ou non une ou plusieurs pièces jointes.

Cependant, chaque e-mail reçu répond à un format spécifique

Un courrier électronique est composé de deux parties : les entêtes et le corps du message, séparés par une ligne vide. Les entêtes stockent les informations contextuelles : qui envoie le message, à qui, avec quel objet, ou encore à quelle date. Le corps du message est quant à lui encodé sous forme de texte, ou de parties multiples (par exemple un texte et des images).

Exemple d'entête d'un message ayant comme seul texte affiché pour le destinataire :

Objet : Bonjour !

Message :

Bonjour David,

Tiens-moi au courant pour la réunion.

Thomas

L'entête contiendra :

Received: from 31.121.118.45 (EHLO serveur.fr)

by mta1007.mail.ukl.yahoo.com with SMTP; Fri, 21 Sep 2012 21:31:16 +0000

Received: by serveur.fr (Postfix, from userid 106)

id 3DF2F15A0CD; Fri, 21 Sep 2012 23:31:16 +0200 (CEST)

From: "Thomas"

To: david@yahoo.fr

Subject: Bonjour !

Date: Fri, 21 Sep 2012 23:31:16 +0200

MIME-Version: 1.0

Content-Transfer-Encoding: 8bit

Content-Type: text/plain; charset=iso-8859-1

X-Mailer: Mozilla Thunderbird

Message-Id:

Bonjour David,

Tiens-moi au courant pour la réunion.

Thomas

L'analyse de l'entête nous permet d'avoir la date et l'heure d'envoi (attention aux indications de fuseau horaire), l'adresse IP et le nom de domaine du serveur expéditeur, l'ID de l'e-mail sur le serveur expéditeur

Remarque :

Un échange d'e-mails (minimum envoi + réponse) permettra plus facilement d'apporter la preuve de que le destinataire a bien reçu le message électronique puisqu'il y répond...

A la suite d'une usurpation d'identité, d'une arnaque, d'un dénigrement, d'injures, de médisance ou de propos diffamatoires, vous pouvez souhaiter retrouver l'expéditeur d'un e-mail :

A) Constat éventuel par Procès Verbal d'Huissier de l'e-mail ;

B) Analyse des éventuels échanges d'e-mails

C) Analyse par un Expert Informatique de l'entête de l'email afin d'extraire la date, l'heure, l'adresse IP et le nom de domaine du serveur d'expédition de l'e-mail ;

D) Rechercher le propriétaire d'une adresse IP avec l'outil www.ripe.net ou <http://network-tools.com> ;

E) Plages d'adresses IP attribuées par opérateurs sur la page <http://www.nirsoft.net/countryip/fr.html> ;

F) Contact éventuel des fournisseur d'accès à Internet pour retrouver l'abonné à Internet à partir de l'adresse IP (ordonnance d'un Juge).

2. RETROUVER L'AUTEUR D'UN POST SUR UN FORUM

A la suite d'une arnaque, d'un dénigrement, d'injures, de médisance ou de propos diffamatoires, vous pouvez chercher des traces de l'auteur dans des forums ou réseaux sociaux. Vous aurez alors des traces de ses posts, souvent bien insuffisants pour remonter jusqu'à l'auteur malveillant.

Pourtant, quelques pistes peuvent être exploitées :

A) Constat éventuel par Procès Verbal d'Huissier du post avec horodatage.

B) L'auteur peut utiliser des éléments permettant de retrouver son identité (par exemple, son pseudo est peut-être utilisé sur plusieurs sites et l'identification peut être tentée par recoupement d'informations...)

C) Rechercher d'autres traces du pseudo dans d'autres sites (Social Mention, Samepoint, Mention.net, Alerti, Youseemii.fr, Webmii, Sprout social, eCaim.com, zen-reputation) ;

D) L'analyse de données Exif permet d'avoir des renseignements supplémentaires (par exemple : ExifViewer) ;

E) Si une demande de retrait par voie amiable des informations par l'auteur n'aboutit pas, vous avez la possibilité de signaler un acte d'injure ou de diffamation sur le site Internet du ministère de l'Intérieur : <http://www.internet-signalement.gouv.fr> ou saisir une juridiction de proximité (<https://www.service-public.fr/particuliers/vosdroits/F1785>) ;

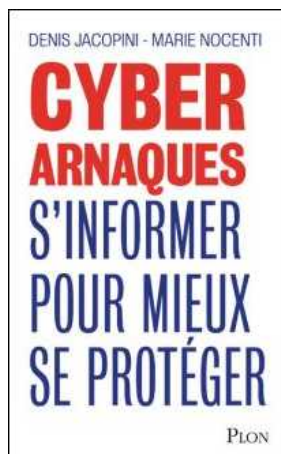
F) Comme pour un contenu dans un moteur de recherche, on peut essayer d'utiliser le Flooding pour envoyer le post dans des pages de résultat lointaines.

Bien évidemment cette liste de conseils pas exhaustive et n'attend que vos avis et commentaires pour l'enrichir

Réagissez à cet article

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)

Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaqes dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaqes Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaqes Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

<https://www.youtube.com/watch?v=lDw3kI7ra2s>

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur [Fnac.fr](https://www.fnac.fr)

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur [amazon.fr](https://www.amazon.fr)



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Etude et publication de Denis JACOPINI

LIENS SOURCES

Utilisation des moteurs de recherche en France

<http://www.journaldunet.com/ebusiness/le-net/1087481-parts-de-marche-des-moteurs-de-recherche-en-france/>

Taux de clic en fonction de la position dans les résultats

<http://www.mathiasp.fr/blog/seo/quel-est-le-taux-de-clic-en-fonction-des-positions-dans-google/544>

Comment supprimer une informations gênante sur Internet ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Denis JACOPINI VOUS INFORME		Comment supprimer une information gênante sur Internet ?			

Victime d'usurpation d'identité, d'insultes ou de propos diffamatoires, vous désirez faire disparaître une information compromettante d'Internet ? Il est temps d'agir sur votre e-réputation. Les conseils de Denis JACOPINI, expert informatique assermenté.

1.0. Supprimer

Nous pouvons considérer plusieurs niveaux de suppression :
– Au niveau des supports (sites Internet) stockant les informations à supprimer vers lesquels pointent les outils permettant de trouver l'information ;
– Au niveau des outils permettant de trouver les informations ;
– Au niveau des supports ayant une copie des informations à supprimer vers lesquels pourraient pointer les outils permettant de trouver l'information ;

Supprimer la totalité des informations ne peut être garanti

En effet, les actions menées sur Internet par les utilisateurs sont Internationales. En 2016, dans le monde, nous comptons un peu plus de 3,3 milliards d'internaute et un peu plus d'un milliard de sites Internet. C'est autant d'utilisateurs susceptibles d'enregistrer une information dans leur ordinateur ou la diffuser sur Internet, sur un blog ou un forum dans le plus grand secret.

A ce jour, les seuls moyens à notre disposition pour trouver de l'information sur Internet sont :

- soit de connaître l'URL (Uniform Resource Locator) utilisées pour identifier les pages et les sites web (par exemple : <https://www.lenetexpert.fr/contacter-denis-jacopini-expert-judiciaire-en-informatique-correspondant-cnil-cil/>)
- soit on passe par des outils permettant de rechercher de l'information (ex : <http://www.google.fr> et on recherche « Contacter Denis JACOPINI »)
- soit on passe par des outils spécialisés dans la recherche d'information qui vont scruter dans différents type de services Web (annuaires, réseaux sociaux, espaces de partage, de microblogage...)

Nous sommes en mesure de vous apporter ce service ?

N'hésitez pas à nous contacter

1.1 Suppression d'informations à une adresse précise

Prendre contact avec le responsable du site Internet ou le propriétaire du compte contenant l'information est la première étape que nous recommandons.

Par exemple, si une information fautive ou compromettante est constatée à l'adresse suivante : <https://www.lenetexpert.fr/contacter-denis-jacopini-expert-judiciaire-en-informatique-correspondant-cnil-cil/>, le plus simple est de contacter la personne en charge du site internet racine soit <http://www.lenetexpert.fr> en expliquant la raison de notre demande de suppression d'informations

Retrouver la personne responsable du contenu du site Internet peut s'avérer simple (dans le meilleur des cas, le site dispose d'une rubrique « Contact » ou « contactez-nous », ou bien d'une rubrique « Mentions légale » contenant un numéro SIREN, SIRET, l'identité d'un « responsable de la publication »...) ou parfois compliquée (aucune rubrique précédemment citée n'est présente). Il sera alors nécessaire de trouver les coordonnées de la personne en charge de l'hébergement du site internet en question par d'autres moyens en fonctions des informations pouvant être trouvées sur le site Internet ou sur des sites proposant des services de « Whois », répertoriant les informations administratives et techniques relatives au noms de domaines.

Enfin, vous pouvez aussi contacter le responsable d'un site internet en recherchant le nom du site, de la marque ou du service dans des annuaires internet, des moteurs de recherche ou sur des réseaux sociaux ou d'anciennes versions du site internet.

Notez toutefois qu'en France, tous les sites internet édités à titre professionnel ont l'obligation de créer une rubrique « mentions légales » dans laquelle vous pourrez peut-être aussi trouver un numéro SIREN ou SIRET si le site Internet appartient à un professionnel ou une association déclarée à l'INSEE.

Nous sommes en mesure de vous apporter ce service ?

N'hésitez pas à nous contacter

1.2 Suppression d'informations dans les outils de recherche

Supprimer une information sur un site Internet n'a pas d'action directe et immédiate sur le contenu des annuaires et des moteurs de recherche. Cependant, supprimer une information sur un site Internet peut avoir des actions à posteriori comme c'est le cas pour les moteurs de recherche, tels que Google, qui disposent de Bots (par exemple les robots GoogleBot) qui scrutent le contenu des sites Internet et le contenu derrière leurs liens, à la recherche de toute modification, ajout ou suppression d'informations.

Supprimer une information sur un site Internet peut ainsi avoir pour effet de supprimer l'information dans l'index de recherche du moteur de recherche mais ceci sera sans garantie en terme de réalisation ou de délai.

Cependant, si le préjudice porte sur la présence sur Internet d'une information compromettante, il ne faut pas perdre de vue qu'un internaute lambda recherche sur Internet dans la quasi totalité des cas en passant par un moteur de recherche.

Notez qu'en France, le moteur de recherche Google est utilisé dans plus de 93% des cas et draine chaque mois un plus de 40 millions de recherches, Bing est utilisé dans un peu plus de 4% des cas et Yahoo dans un peu plus de 2% des cas. Cela laisse très peu de place (moins de 1%) aux autres moyens utilisés pour rechercher de l'information sur Internet.

De plus, une étude de Advanced Web Ranking de février 2015 nous informe que sur la première page de google, le premier résultat récoltera 33% des clics, le second résultat 15,6% des clics, le troisième résultat 10% des clics, le 4ème résultat 7% des clics, le 5ème résultat, 6% des clics, les 5 derniers résultats récoltant seulement 4% des clics.

Il est donc facile de remarquer que 75% des consultations seront réalisées sur la 1ère page. Les liens présents sur la seconde page des résultats de Google récolteront 5% des clics.

Ainsi, plus de 80% des recherches ne concernant que les deux premières pages de Google et ces habitudes de consultation étant quasiment similaires sur appareils mobiles et sur d'autres moteurs de recherche,

compte tenu qu'il sera impossible d'agir sur tous les annuaires, tous les moteurs de recherche et tous les sites Internet,

compte tenu que le coup, les prétendants à l'existence numérique concentrent leurs efforts pour être présents sur ces outils de recherche,

compte tenu que ne pas y être présent sur ces outils de recherche revient à ne tout simplement pas avoir d'existence numérique,

alors, concentrer ses efforts pour disparaître des 3 premières pages des 3 principaux moteurs de recherches sur Internet permettra de faire disparaître 98% des informations indésirables.

À la suite d'une plainte déposée en 2010 auprès de l'Agence espagnole de protection des données, dans son Arrêt du 13 mai 2014, la Cour de Justice de l'Union Européenne accorde aux individus le droit de s'opposer au traitement de leurs données personnelles.

À la suite de cette décision, Google a publié un formulaire en ligne le 31 mai 2014 permettant à chaque citoyen européen de demander le déréférencement des liens qui apparaissent dans une recherche associée à leur nom, tout en prenant en compte l'intérêt prépondérant du public à avoir accès à l'information.

Le mercredi 16 juillet 2014, le moteur de recherche Bing a mis à disposition son formulaire de demande de blocage des résultats de recherches sur Bing en Europe et en décembre de cette même année, Yahoo a mis à disposition son formulaire.

Nous sommes en mesure de vous apporter ce service ?

N'hésitez pas à nous contacter

2. Comment supprimer

2.1 En résumé, pour supprimer une information sur un site Internet à une adresse précise :

A) Aller sur le site Internet et rentrer en contact avec le site Internet ou avec le responsable de la publication

– rubrique « Contact », « Contactez-nous » ou similaire ;

– rubrique « Mentions légales » ou similaire ;

B) Rechercher le représentant légal de l'activité professionnelle associée au site Internet à partir de son numéro SIREN ou SIRET (liste non exhaustive)

– www.infogreffe.fr

– www.societe.com

– www.europages.com

– www.hoovers.com

C) Rechercher la personne en charge de l'hébergement de l'information avec des outils de Whois (liste non exhaustive)

– www.afnic.fr/fr/produits-et-services/services/whois/

– www.gandi.net/whois?lang=fr

– www.whois-raynette.fr/

– <http://http://whois.domaintools.com>

D) Rechercher la personne en charge de l'hébergement de l'information sur les réseaux sociaux (liste non exhaustive)

– plus.google.com

– www.facebook.com

– www.twitter.com

– www.linkedin.com

– www.viadeo.com

E) Rechercher la personne en charge de l'hébergement de l'information dans les annuaires et les moteurs de recherche (liste non exhaustive)

– www.google.com

– www.google.fr

– www.bing.com

– www.yahoo.com

– www.yahoo.fr

F) Rechercher d'anciennes versions du site Internet qui pourraient contenir des informations par la suite supprimées

– http://archive.org/web (Wayback machine)

Nous sommes en mesure de vous apporter ce service ?

N'hésitez pas à nous contacter

Si l'information à supprimer est personnelle, en France, vous disposez d'un droit d'accès, de modification ou de suppression à cette information (Article 34 et suivants de la Loi Informatique et Libertés du 6 janvier 1978).

La CNIL met à votre disposition un générateur de courrier (<https://www.cnil.fr/modeles/courrier>) destiné à vous aider à faire exercer vos droits auprès des responsables de sites Internet.

Exemple de courrier :

Conformément à l'article 40 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, je vous prie de [objet_de_la_demande]

Vous voudrez bien m'adresser copie de l'enregistrement ainsi modifié.

Je vous rappelle que vous disposez d'un délai maximal de deux mois suivant la réception de ce courrier pour répondre à ma demande, conformément à l'article 94 du décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée.

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

Si l'information à supprimer fait l'objet d'une demande de suppression judiciaire, l'Expert informatique désigné pour réaliser cette mission pourra directement contacter le responsable du site internet pour lui communiquer l'ordonnance justifiant son action et demander le retrait pur et simple de l'information.

En cas de difficulté, remontez la au juge en charge du suivi de votre affaire.

Enfin, si vous n'arrivez pas à trouver ou à contacter une personne en charge du site Internet contenant l'information à supprimer, vous avez la possibilité de signaler un acte d'injure ou de diffamation sur le site Internet du ministère de l'Intérieur : <http://www.internet-signalement.gouv.fr> ou saisir une juridiction de proximité (<https://www.service-public.fr/particuliers/vosdroits/F1785>).

2.2 En résumé, pour supprimer une information dans les 3 moteurs de recherche les plus utilisés en France :

A) Google : Accéder au formulaire de demande de suppression de résultats de recherche au titre de la législation européenne en matière de protection des données :

https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=fr

B) Bing : Accéder au formulaire de de demande de blocage des résultats de recherches sur Bing en Europe

<https://www.bing.com/webmaster/tools/eu-privacy-request>

C) Yahoo :

<https://fr.aide.yahoo.com/kb/search/Demande-de-blocage-de-r%C3%A9sultats-de-recherche-sur-Yahoo-Search-Formulaire-pour-r%C3%A9sidents-europ%C3%A9ens-sln24378.html>

D) Une technique appelée le Flooding consiste à produire beaucoup de contenus et de liens pour apparaître dans les premiers résultats et de faire passer le contenu incriminé sur les pages moins consultées.

Nous sommes en mesure de vous apporter ce service ?

N'hésitez pas à nous contacter

2.3 Si vous pouvez modifier le contenu des pages Web du site Internet :

A) Supprimez les fichier sou les dossiers contenant l'information

B) Modifiez la ou les pages d'index ou d'accueil en rajoutant dans l'entête « meta name= »robots » content= »noindex » /> »

C) Par le biais d'un fichier .htaccess vous pouvez aussi rendre privé et protégé par mot de passe l'accès à un dossier

Nous sommes en mesure de vous apporter ce service ?

N'hésitez pas à nous contacter

Bien évidemment cette liste de conseils pas exhaustive et n'attend que vos avis et commentaires pour l'enrichir

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



DÉSIGNATION
N° DPO-15945

Numéro de formateur

93 84 03041 84



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041

84) .

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)



Etude et publication de Denis JACOPINI

LIENS SOURCES


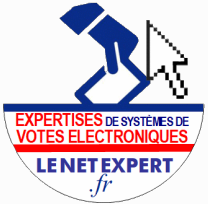





Utilisation des moteurs de recherche en France

<http://www.journaldunet.com/ebusiness/le-net/1087481-parts-de-marche-des-moteurs-de-recherche-en-france/>

Taux de clic en fonction de la position dans les résultats

<http://www.mathiasp.fr/blog/seo/quel-est-le-taux-de-clic-en-fonction-des-positions-dans-google/544>

Comment bâtir et préserver son e-réputation ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT RGPD CYBER MISES EN CONFORMITE	 LE NET EXPERT SPY DETECTION Services de detection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
		Comment bâtir et préserver son e-réputation ?			

A l'heure où les médias ne détiennent plus le monopole de l'information, il serait dangereux de penser qu'on arrive à bâtir, maîtriser et préserver sa réputation sans tenir compte d'Internet qui accélère, modifie, invente, et déstabilise les acquis. Etre capable de préserver son e-réputation nécessite donc de modifier ses repères, faire preuve d'humilité, contrôler ses tribus et ses communautés, adapter ses messages, et redoubler de vigilance. Car, si bâtir une bonne réputation demande du temps et de l'investissement, son anéantissement peut s'effectuer en quelques jours.

L'e-réputation est déterminée par la circulation sur le Web d'informations, d'échanges, d'avis, de commentaires, d'articles, de rumeurs qui forgent une opinion commune. L'identité d'une marque telle qu'elle est diffusée à ses différents publics par tous les moyens de médiatisation, ajoutée à la perception que les internautes en ont, crée l'e-réputation. Avec plusieurs milliards de contenus diffusés et partagés chaque jour rien que sur Facebook, la réputation d'une marque ou d'une enseigne échappe totalement à son contrôle.

Si le site de l'enseigne est le premier vecteur de la création de l'e-réputation, elle se forge aussi via son personnel interne, des articles publiés sur les sites de médias importants, les informations diffusées sur les blogs d'influence, les forums, les réseaux sociaux, les libres commentaires sur les sites communautaires, mais aussi via des plateformes de vidéo et photos.

Rester accessible évite le dénigrement

La majeure partie des problèmes d'e-réputation vient du fait que l'enseigne ne donne pas la possibilité à un client mécontent d'entrer directement et rapidement en contact avec elle. Dépit et frustré, il se tourne alors vers des canaux simples d'accès tels que Twitter, des blogs ou des sites de consommateurs. Afin d'éviter ce genre de dérive, il faut afficher clairement toutes les informations de contacts et non pas un simple formulaire, et apporter rapidement des solutions au client insatisfait. Un portail Web de service client peut aider à fluidifier l'information.

Créer du contenu positif

Diffuser des messages qui inspirent la sympathie, valoriser les produits par des témoignages utilisateurs, donner la possibilité d'ajouter des avis, ou encore certifier les modes de paiement... autant de moyens servant à sensibiliser et fidéliser une communauté. En pratiquant une politique de marketing social, les consommateurs « heureux » prennent le pouvoir, défendent la marque, se diffusent entre eux les bons plans, les promotions, les nouveautés et donc contribuent à bâtir comme une trainée de poudre la e-réputation. Mais attention, dans ce cas, à ne pas perdre le contrôle de son image !

S'emparer du contenu négatif

Les clients mécontents redoublant d'imagination pour faire savoir à un plus grand nombre les problèmes rencontrés avec une marque, ou par pure volonté de nuire, n'hésitent pas à créer des blogs, voire même des sites structurés portant l'URL de l'enseigne suivi d'un terme de type « problèmes » : www.nomdelenseigne-problemes.com .

Acheter des noms de domaine négatifs permet de recenser en un clic la mauvaise réputation car au final vous offrez aux mécontents la possibilité de s'exprimer tout en maîtrisant les problématiques.

Plus simple, créez une page « Foire aux questions » ou « service clients » et engagez-vous à répondre aux critiques ou aux avis négatifs dans un délai raisonnable. Pour garder le client, un geste commercial peut montrer de la considération à son égard et faire basculer du négatif au positif.

Enfin, un démenti public contre une rumeur permet de retrouver une forme de crédibilité et d'afficher une grande transparence dans sa manière de fonctionner.

Pratiquer la technique de l'enfouissement

Trop, c'est trop ! Si de nombreux commentaires négatifs apparaissent sur les premières pages de Google ou autre moteur de recherche lorsqu'on tape votre nom, il est vraiment temps de réagir ! Il faut alors pratiquer la technique dite « de l'enfouissement » qui consiste à créer du contenu positif pour faire baisser dans le référencement tous les liens négatifs. Il est en effet assez rare qu'un internaute dépasse la page 3 ou 4 lorsqu'il souhaite se renseigner sur une marque.

Une politique suivie de Relations Presse aide aussi à diffuser du contenu porteur, à crédibiliser l'offre, à redorer son blason et à nettoyer la toile.

Si la liberté d'expression permet de faire, défaire et refaire des réputations, il faut se dire que c'est une grande richesse. Alors pourquoi se contenter d'être simplement populaire alors qu'il est possible aujourd'hui de devenir influent.

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- EXPERTISES

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



DÉSIGNATION
N° DPO-15945

Numéro de formateur

93 84 03041 84



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041

84) .

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)



Enfants et adolescents sur le web : comment éviter les dangers ?

	Enfants et adolescents sur le web : comment éviter les dangers ?
-----------------------------------------------------------------------------------	------------------------------------------------------------------

À notre époque, internet fait partie intégrante de notre vie. Bien que le web ait beaucoup de points positifs (éducation, facilité, rapidité, accessibilité des informations...), il a aussi des mauvais côtés irréversibles. Les plus vulnérables sont les enfants, qui sont parfois mal avertis des dangers... Alors, pour surfer en toute sécurité, suivez le guide !

Qu'est-ce que le cyberharcèlement ?

Plusieurs formes de cyberharcèlement existent :

- intimidations, moqueries, insultes, menaces,
- propagation de rumeurs ou de documents personnels sans l'accord de la personne,
- discussion de groupe à l'encontre de quelqu'un.

Quelques conseils de prévention

Voici quelques conseils à l'usage des parents et des enfants, pour vous permettre d'utiliser internet **sans entacher votre e-réputation** :

- ne faire **aucune action** qui pourrait avoir de graves répercussions **sans en parler à un proche** (ami, parent, professeur...),
- installer l'ordinateur dans un espace de vie commun,
- ne pas dévoiler d'informations personnelles (mot de passe, coordonnées...), sur aucun site que ce soit (blog, réseaux sociaux ou autres),
- modifier les paramètres de confidentialité de certains sites et réseaux sociaux (pour protéger vos informations sensibles),
- éviter de contacter ou de répondre aux étrangers, en particulier s'ils sont plus âgés,
- en cas d'images violentes ou inadaptées, ne pas hésiter à se déconnecter et à en parler,
- si vous achetez sur internet, ne pas indiquer de coordonnées bancaires si le site n'est pas sécurisé,
 - ne pas publier de photos de ses proches sans leur autorisation;
 - choisir un mot de passe élaboré et le changer régulièrement,
- installer un **contrôle parental** sur tous vos appareils ainsi que sur la plupart des jeux vidéos (ce qui aura pour effet de limiter le temps de jeux ou empêchera vos enfants d'accéder à des contenus déconseillés pour leur âge).

Quels sont les recours possibles ?

En premier lieu, le plus important est de **rassembler les preuves** du cyberharcèlement. Vous pouvez demander au site web en question de **retirer les propos insultants** ou les documents incriminants.

Ensuite, selon la gravité des faits, il existe **plusieurs sanctions possibles** :

- **la sanction disciplinaire** : relative au chef d'établissement,
- **la sanction pénale** : Il n'y a pas de véritable sanction pénale, néanmoins il peut y en avoir dans les cas de droit à l'image, d'usurpation d'identité, diffusion d'images à caractère pornographique, ou d'injure et de diffamation publique,
- **la sanction civile** : il est possible de poursuivre des harceleurs en matière de responsabilité civile, ceux-ci seront alors condamnés à verser des dommages et intérêts...[lire la suite]

NOTRE MÉTIER :

- FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO
- EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES
- AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT
 - MISE EN CONFORMITE RGPD / FORMATION DPO

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, découvrez nos formations ;

EXPERTISES TECHNIQUES : Pour prouver un dysfonctionnement, dans le but de déposer plainte ou de vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Enfants et adolescents sur le web : comment éviter les dangers ?*

Comment faire disparaître ses données d'Internet ?

	Comment faire disparaître ses données d'Internet ?
-----------------------------------------------------------------------------------	----------------------------------------------------

Il est aujourd'hui difficile de limiter l'utilisation de nos données personnelles par les entreprises, mais une loi pourrait bientôt nous faciliter la tâche.

Un procédé complexe

Non, il n'existe pas de formulaire « *plainte* » ou « *comment disparaître de nos bases de données* » sur les sites qui utilisent nos données. Selon Daniela Parrot, responsable du service plaintes de la CNIL (la Commission nationale pour l'informatique et les libertés), il faut en premier lieu « *identifier l'entreprise* » qui possède les données qui vous posent problème. Pour cela, vérifier les mentions légales de leur site internet permet de savoir quelles données l'entreprise se permet d'utiliser à des fins commerciales. Il convient ensuite d'écrire un courrier à l'entreprise, d'évoquer un motif (commercial ou autre) et de pouvoir apporter une preuve (un scan par exemple) de ce courrier pour pouvoir déposer une plainte à la CNIL en cas d'absence de réponse. Il faut aussi ne pas oublier de joindre sa pièce d'identité.

Les entreprises bientôt limitées ?

Pour une meilleure harmonisation de la protection des données dans l'UE, le *Règlement général sur la protection des données* (le « *GDPR* ») sera applicable en mai 2018, après quatre années de négociations législatives au sein du parlement européen. Bien que la plupart des entreprises ont entamé des processus de régularisation, de nouvelles limitations vont les forcer à revoir leur politique. Seulement 10% des boîtes implantées dans l'Union Européenne seraient en mesure de faire face à ces mesures...[lire la suite]

NOTRE MÉTIER :

- FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO
- EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES
- AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT
- MISE EN CONFORMITE RGPD / FORMATION DPO

A Lire aussi :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Une agence de voyages victime d'une incroyable attaque informatique dans le Gard

	Une agence de voyages victime d'une incroyable attaque informatique dans le Gard
-----------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------

L'agence JCS, basée à Poulx (Gard), est spécialisée dans les séjours autour du thème de la tauromachie. Entre le 15 et le 20 juin derniers, elle a subi un véritable déferlement de messages d'insultes et de menaces, via les réseaux sociaux, sur sa page Facebook et sur son site internet.

Par Hervé Sallafranque, France Bleu Gard Lozère



La capture d'écran du lancement de l'attaque informatique sur Facebook, réalisée par le responsable de l'agence – xxx

L'attaque des **anticorrida**, partie de France, s'est ensuite répandue à une très grande vitesse et l'agence a reçu des **messages venus du monde entier**. Son responsable a réussi à identifier la personne à l'origine de l'attaque : une dame basée dans les Alpes-Maritimes. Il a décidé de déposer plainte à la gendarmerie de Marguerittes ce samedi.

Des messages d'insultes venus des États-Unis, d'Australie, de Russie et du Brésil

« Le phénomène a été d'une ampleur énorme », explique le responsable de l'agence, Jean-Charles Roux. Parfois jusqu'à **1.200 messages d'insultes par jour** au plus fort de l'attaque, le week-end des 17 et 18 juin.

L'agence JCS est la seule en France à proposer ce genre de séjours. C'est sans doute pour cela qu'elle a été la cible des anticorrida, même si Jean-Charles Roux a du mal à comprendre un tel **déchaînement de haine**...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Une agence de voyages victime d'une incroyable attaque informatique dans le Gard*

Médecins : protéger votre e-réputation !



Médecins : protéger votre e-réputation !

Paris, le vendredi 16 juin 2017 – De plus en plus de sites Internet et moteurs de recherche proposent aux internautes de publier des avis ou de noter les médecins qu'ils ont consultés.

Plusieurs Conseils départementaux et de nombreux médecins ont fait part, ces derniers mois, au Conseil national de l'ordre des médecins (CNOM) de la recrudescence d'avis dépréciatifs publiés sur Internet par des patients et des difficultés rencontrées par les praticiens pour obtenir la suppression ou le déréférencement des contenus qui portent atteinte à leur réputation. Ceci alors que le médecin, lui, « est confronté à un devoir de réserve lorsqu'il s'agit d'un des patients qui l'a consulté alors même que sa réputation peut être injustement mise en cause » comme le rappelle l'Ordre qui publie une fiche-conseil à l'adresse de ces praticiens malmenés.

Celle-ci explique ainsi comment faire disparaître des commentaires désobligeants sur Google ou obtenir la suppression ou le déréférencement de données personnelles aux termes de la récente loi « pour une République numérique » et de l'article L.111-7-2 du code de la consommation qui « impose ainsi aux personnes physiques ou morales dont l'activité consiste à collecter, modérer ou diffuser des avis en ligne provenant de consommateurs » de « délivrer aux utilisateurs une information loyale, claire et transparente sur les modalités de publication et de traitement des avis mis en ligne ».

L'Ordre signale également avoir averti la CNIL, la DGCCRF et le Ministère de la santé de ces problèmes et avoir interrogé « les principaux assureurs pour savoir si dans le cadre de la protection juridique associée à l'assurance en responsabilité civile, l'assureur propose des solutions couvrant les atteintes à la e-réputation »...[lire la suite]

[Pour en savoir plus et protéger votre « e-réputation »](#)

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : JIM.fr – Médecins : protéger votre e-réputation !

Importance de l'e-réputation pour une entreprise ou une marque

Importance de l'e-réputation pour une entreprise ou une marque

Également connue sous le nom de « réputation numérique », « cyber-réputation » ou « web-réputation », l'e-réputation est la perception que les internautes se font d'une marque, d'une entreprise ou d'une personne en la recherchant sur Google.

Véritable facteur de différenciation, la notoriété numérique est un ingrédient crucial dans l'image publique qu'a une société ou une personne dans le monde réel. A l'ère du digital et des réseaux sociaux, l'e-réputation devient plus que jamais un enjeu capital.

Importance de l'e-réputation pour une entreprise ou une marque

Internet a conquis tous les secteurs et il n'existe pas une seule société qui n'ait pas de présence digitale (site web, comptes sur les réseaux sociaux, avis...). Les achats en ligne étant devenus une pratique extrêmement courante, les consommateurs ont de plus en plus tendance à vérifier l'opinion que les autres ont d'un produit avant de l'acheter. Selon une étude réalisée par l'IFOP pour Reputation VIP, sur internet, 85 % des consommateurs réalisent des achats et 80 % se renseignent avant d'acheter. Une mauvaise **réputation sur le web** peut désormais être synonyme de pertes colossales. En effet, toujours selon l'étude IFOP, 66% des consommateurs venus chercher un avis avant un achat diffèrent l'achat en cas de commentaires défavorables quand, dans 30% des cas, ils vont même jusqu'à renoncer à l'achat. Ainsi, 96% des internautes sont influencés par l'e-réputation d'une marque lors d'un achat...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Importance de l'e-réputation pour une entreprise ou une marque*