

Peut-on être licencié pour ce qu'on y a écrit dans les réseaux sociaux ? | Denis JACOPINI

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<h2>Peut-on être licencié pour ce qu'on y a écrit dans les réseaux sociaux ?</h2>
---	---

Peut-on être licencié pour ce qu'on y a écrit dans les réseaux sociaux ?

Oui.

Dans une affaire concernant trois salariés licenciés pour avoir dénigré leur hiérarchie sur Facebook, un Conseil des prud'hommes a considéré que les propos publiés sur le mur d'un des salariés étaient publics car accessibles aux « amis d'amis ».

Ces propos ont perdu leur caractère privé du fait qu'ils étaient accessibles à des personnes non concernées par la discussion.

Soyez donc vigilant lorsque vous publiez des commentaires sur un réseau social !

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://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=D48813C492DFE134132210B5E195173E?id=199&back=true>

5 points à changer immédiatement sur votre profil LinkedIn | Denis JACOPINI



5 points à changer
immédiatement sur
votre profil LinkedIn

Difficile de sortir du lot dans la jungle du réseau social professionnel LinkedIn. Les cinq conseils de Camille Travers, consultante en recrutement web, pour se démarquer et éviter les grosses erreurs.

Trente secondes suffisent aux recruteurs en ligne pour scanner votre profil sur LinkedIn. Est-il suffisamment soigné ? Le réseau social professionnel réunit plus de 8 millions d'utilisateurs en France (300 millions dans le monde), et les chasseurs de tête y pullulent. Tout comme, peut-être, votre futur employeur. Camille Travers, consultante en recrutement sur le web et auteur de l'ouvrage « Du e-recrutement au recrutement 2.0 » (Editions Studyrama) livre 5 conseils pour que votre profil tape à l'oeil des recruteurs.

1) Pas de selfie ni de photos de vacances

Le selfie à la cote. Pas sur LinkedIn. « Gardez-le pour Facebook ou des réseaux sociaux moins professionnels », conseille Camille Travers. A bannir aussi : « les photos de vacances avec des lunettes de soleil et le bras de quelqu'un d'autre autour du cou. Choisissez une photo qui vous ressemble mais qui reste professionnelle. Sourire ? Pourquoi pas. Mais à condition que ce soit dans vos habitudes. Inutile de se forcer". Si aucune photo ne vous convient, continuez à chercher ou prenez en une nouvelle. "Avoir une photo, c'est essentiel. Cela permet d'être mieux référencé et les autres utilisateurs vous identifieront plus facilement, surtout si vous les avez déjà rencontrés."

2) Un intitulé créatif

« C'est la deuxième chose que voient les recruteurs. L'intitulé apparaît juste après la photo dans la barre de recherche. Il faut sortir de l'intitulé jargon d'entreprise et être plus original. Mieux vaut mettre en avant des projets, des compétences que l'intitulé d'un poste trop précis. Par exemple : « peut booster vos ventes" plutôt que « commercial ». Autre astuce : privilégier les mots-clés universels, mieux référencés. Cela multiplie les chances que le profil soit consulté. »

3) Bichonner son résumé

« La plupart des candidats délaissent le résumé par flemme ou par peur de se fermer des portes. Pourtant, c'est la partie plus personnelle. Celle où le candidat peut parler de l'avenir, de ses projets, de ses envies professionnelles. Inutile d'en faire des tartines, 5 lignes suffisent. Et surtout éviter d'en faire un mini CV, ramassé en une centaine de mots. Cela ne correspond pas du tout aux codes de LinkedIn et cela peut être rédhitoire pour un employeur à la recherche d'un salarié rompu aux nouvelles technologies et aux réseaux sociaux. »

4) Débroussailler ses expériences professionnelles

« Rien ne sert de faire un copier-coller du CV avec le déroulé des missions. Il vaut mieux en choisir quelques-unes et préciser les compétences maîtrisées grâce à ces expériences. Surtout, illustrez les par des exemples concrets comme des chiffres de ventes. Pas la peine non plus d'écrire un roman pour chaque expérience professionnelle. Il ne s'agit pas d'être exhaustif mais de donner envie aux recruteurs d'en savoir plus. D'ailleurs, plus les utilisateurs occupent une poste haut placé, plus les descriptions de leurs expériences sont courtes. »

5) Renvoyer vers ses réalisations

« LinkedIn permet aussi de renvoyer vers d'autres pages. Des blogs, des vidéos YouTube de ses réalisations ou des présentations PowerPoint... Tous ces éléments prouvent l'étendue des compétences de l'utilisateur, améliorent la visibilité du profil. Si le candidat est choisi pour passer un entretien d'embauche, cela permet d'engager la conversation sur des réalisations concrètes. » A noter aussi : une fois tous ces changements effectués, la mission LinkedIn n'est pas encore accomplie. « Un profil visible, c'est un profil en activité. Il faut prendre le temps de mettre à jour votre page, de suivre et de commenter les publications, les changements de postes de vos contacts, voire de publier vous même des articles sur ce réseau. Cela demande du temps mais cela accroît considérablement votre visibilité », conclut Camille Travers.

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://tempsreel.nouvelobs.com/bien-bien/20150618.OBS1104/5-points-a-changer-immédiatement-sur-votre-profil-linkedin.html>

Propos recueillis par Angèle Guicharnaud

Quelques conseils pour surfer un peu plus tranquille sur Internet



Quelques conseils de bon sens pour se protéger au mieux des attaques liées à l'utilisation d'Internet.

Des mises à jour régulières et automatiques

L'un des meilleurs moyens de se prémunir des risques de piratage, est de **maintenir son matériel informatique et ses logiciels à jour** avec les derniers correctifs de sécurité et les dernières mises à jour.

Par ce biais, le risque d'intrusion est minimisé. Il est donc très important de **configurer son ordinateur** pour que le système d'exploitation se mette **régulièrement et automatiquement à jour**.

Une bonne configuration matérielle et des logiciels adaptés

Les **niveaux de sécurité** de l'ordinateur doivent être **réglés au plus haut** pour minimiser les risques d'intrusions. Les **paramètres des navigateurs** et des **logiciels de messageries** électroniques peuvent aussi être configurés avec des niveaux de sécurité élevés.

L'utilisation d'un **anti-virus à jour** et d'un **pare-feu (firewall)** assureront un niveau de protection minimum pour surfer sur la toile. Le **firewall** permet de filtrer les données échangées entre votre ordinateur et le réseau. Il peut être réglé de manière à bloquer ou autoriser certaines connexions.

Utiliser un bon mot de passe

Les mots de passe sont une **protection incontournable** pour sécuriser l'ordinateur et ses données ainsi que tous les accès au service sur Internet.

Mais encore faut-il en choisir un bon. Un bon mot de passe doit être difficile à deviner par une personne tierce et facile à retenir pour l'utilisateur.

Lire nos conseils pour choisir un bon mot de passe .

Se méfier des courriers électroniques non-sollicités et leurs pièces jointes

A la réception d'un mail dont l'**expéditeur est inconnu**, un seul mot d'ordre : **prudence** !

Les courriers électroniques peuvent être accompagnés de **liens menant vers des sites frauduleux** (voir l'article sur le **phishing**) ou de **pièces jointes piégées**. Un **simple clic sur une image suffit pour installer à votre insu un logiciel ou code malveillant** (cheval de Troie) sur votre ordinateur. La pièce jointe piégée peut être : une page html, une image JPG, GIF, un document word, open office, un PDF ou autre.

Pour se protéger de ce type d'attaque, la règle est simple : **ne jamais ouvrir une pièce jointe dont l'expéditeur est soit inconnu, soit d'une confiance relative**.

En cas de doute, une recherche sur internet permet de trouver les arnaques répertoriées.

Que faire si j'ai déjà cliqué sur la pièce jointe?

Déconnectez-vous d'internet et **passez votre ordinateur à l'analyse anti-virus** (à jour) pour détecter l'installation éventuelle d'un logiciel malveillant.

Pour tout renseignement ou pour signaler une tentative d'escroquerie :



Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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



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

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



[Contactez-nous](#)

Réagissez à cet article

Comment réagir lorsque vous êtes victime de harcèlement en ligne ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LENETEXPERT.fr</p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
 <p>Denis JACOPINI vous informe L'CI</p>		<p>Comment réagir lorsque vous êtes victime de harcèlement en ligne ?</p>			

Selon un rapport européen, près de 10 % de la population européenne a subi ou subira un harcèlement*. Voici quelques conseils si vous êtes victime de ces violences sur internet et les médias sociaux.

Qui sont les cyber-harceleurs ?

Un(e) internaute peut être harcelé(e) pour son appartenance à une religion, sa couleur de peau, ses opinions politiques, son comportement, ses choix de vie ... Le harceleur peut revêtir l'aspect d'un « troll » (inconnu, anonyme) mais également faire partie de l'entourage de la victime (simple connaissance, ex-conjoint, camarade de classe, collègue, voisin, famille ...).

A quoi ressemble une situation de cyber-harcèlement ?

- Happy slapping : lynchage en groupe puis publication de la vidéo sur un site
- Propagation de rumeurs par téléphone, sur internet.
- Création d'un groupe, d'une page ou d'un faux profil à l'encontre de la personne.
- Publication de photographies sexuellement explicites ou humiliante
- Messages menaçants, insulte via messagerie privée
- Commande de biens/services pour la victime en utilisant ses données personnelles
- ...

Comment réagir ?

Ne surtout pas répondre ni se venger

Vous avez la possibilité de bloquer l'accès de cette personne à vos publications, de la signaler auprès de la communauté ou d'alerter le réseau social sur un comportement qui contrevient à sa charte d'utilisation.

Verrouiller l'ensemble de vos comptes sociaux

Il est très important de limiter au maximum l'audience de vos comptes sociaux. Des options de confidentialité existent pour « ne plus me trouver », « ne pas afficher/partager ma liste d'amis ». Il est également possible de « bannir » les amis indésirables. Sur Facebook, une option vous permet d'être avertis si un autre utilisateur mentionne votre nom sur une photo (tag).

Les paramètres conseillés sur Facebook :

PARAMÉTRAGE POSSIBLE	CHEMIN D'ACCÈS
Limiter la visibilité de vos photos	Ce type d'option ne fonctionne que photo par photo
Limiter la visibilité de vos informations de profil	Informations générales : page du profil > encart gauche > sélectionner « amis » ou « moi uniquement »
Cacher votre liste d'amis	Page du profil > onglet « amis » > « gérer section » > « modifier la confidentialité » > « liste d'amis » ou « moi uniquement »
Cacher vos mentions « j'aime »	Page du profil > Mentions j'aime (encart gauche) > « modifier la confidentialité » > « moi uniquement »
Être prévenu si quelqu'un vous « tague »	Paramètre > journal et identification > Paramètres d'identification et de journal > « examiner les identifications »
Limiter la visibilité de vos publications	Journal > sélectionner la publication > « moi uniquement » / ou « supprimer »
Examiner votre historique	Page du profil > « afficher l'historique personnel » > supprimer au cas par cas

• Capture écran des propos / propos tenus

Ces preuves servent à justifier votre identité, l'identité de l'agresseur, la nature du cyber-harcèlement, la récurrence des messages, les éventuels complices. Sachez qu'il est possible de faire appel à un huissier pour réaliser ces captures. Fiche pratique : comment réaliser une copie d'écran ?

• Portez plainte auprès de la Gendarmerie/Police si le harcèlement est très grave

Vous avez la possibilité de porter plainte auprès du commissariat de Police, de Gendarmerie ou du procureur du tribunal de grande instance le plus proche de votre domicile.

• En parler auprès d'une personne de confiance

La violence des termes employés par l'escroc et le risque d'exposition de votre vie privée peuvent être vécus comme un traumatisme. Il est conseillé d'en parler avec une personne de confiance.

Si quelqu'un d'autre est harcelé ?

Le fait de « partager » implique votre responsabilité devant la loi. Ne faites jamais suivre de photos, de vidéos ou de messages insultants y compris pour dénoncer l'auteur du harcèlement. Un simple acte de signalement ou un rôle de conseil auprès de la victime est bien plus efficace ! **Le chiffre : 61% des victimes indiquent qu'elles n'ont reçu aucun soutien quel qu'il soit de la part d'organismes ou d'une personne de leur réseau personnel.** * Source: rapport européen sur le cyber-harcèlement (2013)

Si vous êtes victime et avez moins de 18 ans ...

Composez le 3020. Il est ouvert du lundi au vendredi de 9h à 18h (sauf les jours fériés). Le numéro vert est géré par la plateforme nonaharcelement.education.gouv.fr qui propose de nombreuses ressources pour les victimes, témoins, parents et professionnels (écoles, collèges, lycées). **Si le harcèlement a lieu sur internet**, vous pouvez également composer le 0800 200 000 ou vous rendre sur netecoute.fr. La plateforme propose une assistance gratuite, anonyme, confidentielle par courriel, téléphone, chat en ligne, Skype. Une fonction « être rappelé par un conseiller » est également disponible. La réponse en ligne est ouverte du lundi au vendredi de 9h à 19h. **Un dépôt de plainte est envisagé ?** Renseignez vous sur le dépôt de plainte d'un mineur. Celui-ci doit se faire en présence d'un ou de plusieurs parents ou d'un représentant légal. N'hésitez pas à contacter les télé-conseillers du fil santé jeune au 0800 235 236.

Quelles sanctions encourues par l'auteur de ces violences en ligne ?

L'auteur de tels actes est susceptible de voir sa responsabilité engagée sur le fondement du Droit civil, du Droit de la presse ou du Code pénal.

Quelques exemples de sanctions :

- Une injure ou une diffamation publique peut être punie d'une amende de 12.000€ (art. 32 de la Loi du 29 juillet 1881).
- Pour le droit à l'image, la peine maximum encourue est d'un an de prison et de 45.000 € d'amende (art. 226-1, 226-2 du Code pénal).
- L'usurpation d'identité peut être punie d'un an d'emprisonnement et de 15.000€ d'amende (art. 226-4-1 du Code pénal).

Quels sont les recours auprès de la CNIL ?

La qualification et la sanction de telles infractions relève de la seule compétence des juridictions judiciaires. En parallèle de telles démarches, vous pouvez demander la suppression de ces informations à chaque site ou réseau social d'origine, en faisant valoir votre droit d'opposition, pour des motifs légitimes, sur le fondement de l'article 38 de la loi du 6 janvier 1978 modifiée dite « Informatique et Liberté ». Le responsable du site dispose d'un délai légal de deux mois pour répondre à votre demande. La majorité des sites propose un bouton « signaler un abus ou un contenu gênant ». Si aucun lien n'est proposé, contactez directement par courriel ou par courrier le responsable du site en suivant la procédure expliquée sur notre site. Par ailleurs, si ces informations apparaissent dans les résultats de recherche à la saisie de vos prénom et nom, vous avez la possibilité d'effectuer une demande de déréférencement auprès de Google en remplissant le formulaire. En cas d'absence de réponse ou de refus, vous pourrez revenir vers la CNIL en joignant une copie de votre demande effectuée auprès du moteur de recherche incluant le numéro de requête Google. Pour plus d'informations, consulter la fiche.

Source : CNIL

[block id="24761" title="Pied de page HAUT"]

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

[Les meilleurs conseils pour choisir vos mots de passe](#)

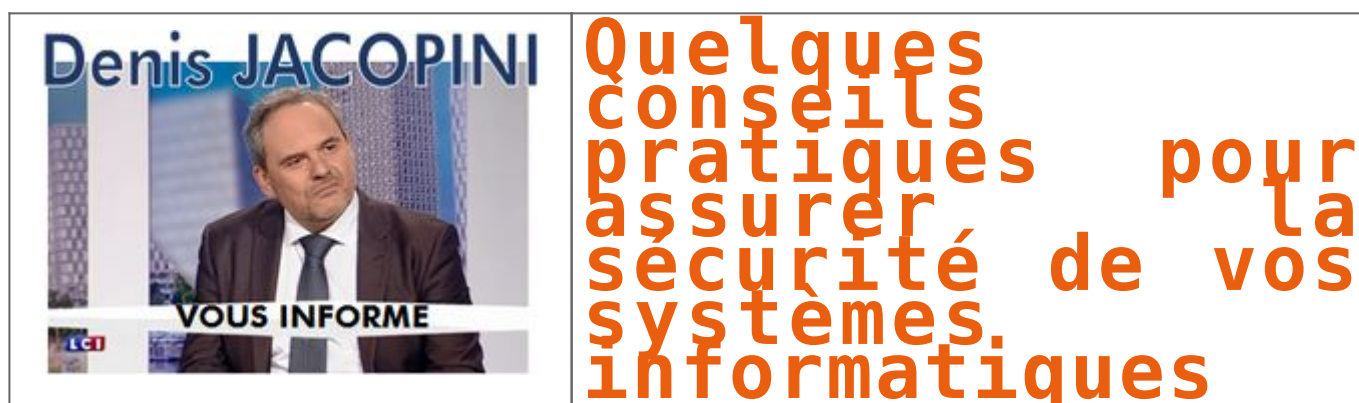
[Victime d'un piratage informatique, quelles sont les bonnes pratiques ?](#)

[Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?](#)

[Attaques informatiques : comment les repérer ?](#)

[block id="24760" title="Pied de page BAS"]

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques





Original de l'article mis en page : Conseils aux usagers |
Gouvernement.fr

Victime d'une arnaque sur Internet ? Faites-nous part de votre témoignage

	<p>Victime d'une arnaque sur Internet ? Faites-nous part de votre témoignage</p>
---	--

Vous êtes victime d'une arnaque ou d'un piratage sur Internet ? Votre témoignage nous permettra peut-être de vous aider.

Devant une explosion de cas d'arnaques et de piratages par Internet et des pouvoirs publics débordés par ce phénomène, nous avons souhaité apporter notre pierre à l'édifice.

Vous souhaitez nous faire part de votre témoignage, contactez-nous.

Vous devez nous communiquer les informations suivantes (tout message incomplet et correctement rédigé ne sera pas traité) :

- une présentation de vous (qui vous êtes, ce que vous faites dans la vie et quel type d'utilisateur informatique vous êtes) ;
- un déroulé chronologique et précis des faits (qui vous a contacté, comment et quand et les différents échanges qui se sont succédé, sans oublier l'ensemble des détails même s'ils vous semblent inutiles, date heure, prénom nom du ou des interlocuteurs, numéro, adresse e-mail, éventuellement numéros de téléphone ;
- Ce que vous attendez comme aide (je souhaite que vous m'aidiez en faisant la chose suivante :)
 - Vos nom, prénom et coordonnées (ces informations resteront strictement confidentielles).

Contactez moi

Conservez précieusement toutes traces d'échanges avec l'auteur des actes malveillants. Ils me seront peut-être utiles.



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

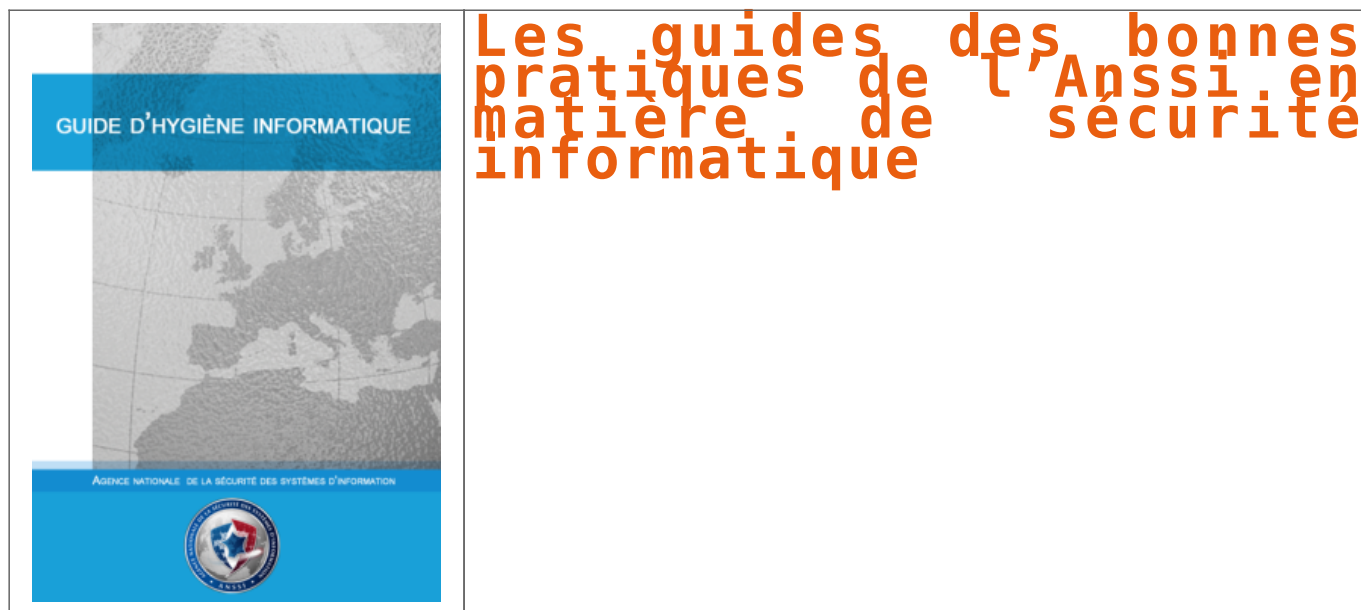
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation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



[Contactez-nous](#)

Réagissez à cet article

Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique | Denis JACOPINI



Vous voulez éviter que le parc informatique soit utilisé pour affaiblir votre organisation ? L'un des guides publiés par l'ANSSI vous aidera à vous protéger.

Initialement destinés aux professionnels de la sécurité informatique, les guides et recommandations de l'ANSSI constituent des bases méthodologiques utiles à tous. Vous trouverez sans peine votre chemin en utilisant les mots-clés, qu'un glossaire vous permet d'affiner, ou le menu thématique.

LISTE DES GUIDES DISPONIBLES

- Guide pour une formation sur la cybersécurité des systèmes industriels
- Profils de protection pour les systèmes industriels
- Sécuriser l'administration des systèmes d'information
- Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du rgs
- Recommandations pour le déploiement sécurisé du navigateur mozilla firefox sous windows
- Cryptographie – les règles du rgs
- Recommandations de sécurité concernant l'analyse des flux https
- Partir en mission avec son téléphone sa tablette ou son ordinateur portable
- Recommandations de sécurité relatives à active directory
- Recommandations pour le déploiement sécurisé du navigateur microsoft internet explorer
- l'homologation de sécurité en neuf étapes simples,
- bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,
- recommandations pour le déploiement sécurisé du navigateur google chrome sous windows,
- usage sécurisé d'(open)ssh,
- la cybersécurité des systèmes industriels,
- sécuriser une architecture de téléphonie sur ip,
- mettre en œuvre une politique de restrictions logicielles sous windows,
- prérequis à la mise en œuvre d'un système de journalisation,
- vulnérabilités 0-day, prévention et bonnes pratiques,
- le guide des bonnes pratiques de configuration de bgp,
- sécuriser son ordiphone,
- sécuriser un site web,
- sécuriser un environnement d'exécution java sous windows,
- définition d'une politique de pare-feu,
- sécuriser les accès wi-fi,
- sécuriser vos dispositifs de vidéoprotection,
- guide d'hygiène informatique,
- la sécurité des technologies sans contact pour le contrôle des accès physiques,
- recommandations de sécurité relatives à ipsec,
- la télé-assistance sécurisée,
- sécurité des systèmes de virtualisation,
- sécurité des mots de passe,
- définition d'une architecture de passerelle d'interconnexion sécurisée,
- ebios – expression des besoins et identification des objectifs de sécurité,
- la défense en profondeur appliquée aux systèmes d'information,
- externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques,
- archivage électronique... comment le sécuriser ?
- pssi – guide d'élaboration de politiques de sécurité des systèmes d'information,
- tdbssi – guide d'élaboration de tableaux de bord de sécurité des systèmes d'information,
- guide relatif à la maturité ssi,
- gissip – guide d'intégration de la sécurité des systèmes d'information dans les projets

Expert Informatique 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 protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/>

Comment retirer des publications gênante sur les réseaux sociaux ? Les conseils de la CNIL

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES <i>fr</i></p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
 <p>Denis JACOPINI vous informe</p>	<p>Comment retirer des publications gênante sur les réseaux sociaux ? Les conseils de la CNIL</p>				

Sur les réseaux sociaux, vous pouvez être confronté à la diffusion d'informations personnelles publiée par d'autres internautes. Voici quelques liens utiles pour demander rapidement l'effacement de ces contenus

Une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable ». Sur une publication, vous pouvez être identifié :

- **directement** (exemple : nom, prénom, etc.)
- ou **indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à votre identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi votre voix ou votre image).

Votre identification peut être réalisée :

- **à partir d'une seule de vos données** (exemple : numéro de sécurité sociale, etc.)
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

Avant de demander la suppression du contenu, assurez-vous que le compte ou l'information n'appartient pas à un homonyme.

En cas de doute raisonnable, le réseau social peut être en mesure de vous demander tout document permettant de prouver que ce contenu vous concerne. En revanche, **il ne peut pas vous demander des pièces justificatives qui seraient abusives, non pertinentes et disproportionnées par rapport à votre demande.**

1. Signaler la publication à effacer

En fonction du réseau social, vous devez vous rendre sur la page appropriée qu'il a mis à votre disposition à cet effet.

Twitter : Signaler la divulgation d'informations privées

Instagram : Signaler une photo ou vidéo pour violation de vos droits de confidentialité sur Instagram

Facebook : Utiliser le lien » Signaler «

situé à côté de la publication, de la photo ou du commentaire

Snapchat : Signaler la publication ou Utiliser ce formulaire en ligne ou Utiliser le formulaire de droit à l'image

LinkedIn : Signaler le harcèlement d'un utilisateur ou un problème de sécurité

Youtube : Réclamer une atteinte à la vie privée

Dailymotion : Sous chaque vidéo figure un bouton » Signaler cette vidéo »

en cliquant dessus, vous aurez à remplir un formulaire.

2. Si le réseau social ne fait pas partie de cette liste

- Rendez-vous vous en bas de la page d'accueil du réseau social ;
- Identifiez une page « politique de confidentialité » ou « données personnelles » ou « vie privée » ;
- Dans cette page, recherchez les coordonnées du service ou le formulaire qui répondra à votre demande ;
- Envoyez si besoin un modèle à personnaliser qui comprend les références aux textes de loi et vous permet d'indiquer un motif.

Quelle réponse attendre du réseau social ?

Le réseau social doit procéder à l'effacement dans les meilleurs délais et au plus tard dans un délai d'un mois, qui peut être porté à trois mois. Dans ce dernier cas, l'organisme doit vous informer des raisons de cette prolongation dans le délai d'un mois.

En parallèle de cette démarche d'effacement – et si ce contenu est référencé dans les moteur de recherche – exercez votre droit au déréférencement de manière à ce que ce contenu ne soit plus associé à votre nom et prénom dans les résultats d'un moteur de recherche.

En cas de réponse insatisfaisante – ou d'absence de réponse sous un mois – de la part du réseau social ou du moteur de recherche, vous pouvez saisir la CNIL.

[block id="24761" title="Pied de page HAUT"]

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 ?

[block id="24760" title="Pied de page BAS"]

Source : *Publication gênante sur les réseaux sociaux : signalez pour supprimer ! | CNIL*







5 règles d'or pour les utilisateurs des réseaux sociaux | Denis JACOPINI



5 règles
d'or pour
les
utilisateurs
des réseaux
sociaux

Original de l'article mis en page : 5 règles d'or pour les utilisateurs des réseaux sociaux | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Comment naviguer incognito sur Facebook avec les règles de confidentialité actuelles | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
		<p>Comment naviguer incognito sur Facebook avec les règles de confidentialité actuelles</p>			

Fin novembre, le réseau social Facebook a annoncé son intention de changer ses conditions d'utilisations, principalement pour permettre un meilleur ciblage publicitaires. Et comme vous ne pourrez pas les refuser -considérant que ceux qui continuent à l'utiliser acceptent de fait la mise à jour- mieux vaut connaître les règles à appliquer pour maîtriser au mieux les nombreuses informations de votre profil.

Atlantico : Le réseau social Facebook a mis à jour ses règles de confidentialité au cours du mois de novembre. En quoi celles-ci sont-elles différentes ?

Emilie Ogez : En effet, courant novembre, Facebook a de nouveau modifié sa politique de confidentialité (pour le meilleur et pour le pire), qu'on peut aborder en trois points.

1. La mise en place de l'espace pédagogique « Privacy Basics » : Facebook a souhaité rassurer les utilisateurs en mettant en place une sorte de tutoriel qui les guide pas à pas sur la modification des paramètres.

Ces derniers sont divisés en 3 catégories :

- ce qu'on montre aux autres,
- comment les autres interagissent avec vous
- et ce que nous voyons.

C'est une bonne chose et ce sont de nouveaux efforts consentis par Facebook pour simplifier les paramètres de confidentialité.

2. La mise à jour des conditions d'utilisation, qui seront mises en application le 1er janvier 2015 : les conditions d'utilisation de Facebook ont été clarifiées et certains passages reformulés. La politique d'utilisation des données a particulièrement été revue. Et Facebook a décidé d'exploiter de nouvelles données personnelles ; en l'occurrence les localisations de ses utilisateurs. Ainsi, si vous décidez de partager votre position, vous pourrez voir les menus des restaurants à proximité ou le statut de vos amis aux alentours. Les informations relatives aux paiements sont également exploitées par le réseau social.

3. Le ciblage publicitaire plus fin : les annonceurs pourront désormais afficher des publicités adaptées aux habitudes des internautes à l'intérieur de Facebook mais aussi en dehors (sites web et des applications de tiers qui ont recours aux services Facebook). Prenons un exemple pour bien comprendre ce changement : « Imaginez que vous envisagez d'acheter un téléviseur et que vous commencez à faire des recherches sur le Web et dans des applications mobiles. Facebook pourrait alors vous montrer des publicités pour obtenir le meilleur prix ou vous faire connaître d'autres marques à considérer ». C'est une importante évolution mais Facebook reste prudent. Le site propose ainsi à l'utilisateur de savoir pourquoi il reçoit telle ou telle publicité mais aussi de les refuser.

Quelle est la marche à suivre pour assurer la maîtrise de ses données personnelles ?

1. Un bon début est de commencer par cliquer sur « Aperçu du profil en tant que » sous la photo de couverture de votre profil afin de voir comment certains de vos amis ou le « Public (ceux qui ne sont pas amis avec vous) vous voient.
2. Ensuite, passez à la phase « paramétrage » en suivant ces quelques conseils et selon vos souhaits (visibilité importante, limitée, etc.).

Les Photos

Lorsque vous publiez une photo sur Facebook, vous pouvez choisir à qui elle est accessible. Elle est peut être « publique » (et donc visible de tous, sur Facebook et en dehors de Facebook, dans les moteurs de recherche), accessible seulement aux « amis », à vous uniquement (« moi uniquement »), à certains amis (« personnalisé ») ou encore à une liste d'amis que vous aurez créée avant publication. Prenez le temps d'y réfléchir avant de poster ! Si toutefois, vous vous êtes trompés, rassurez-vous, il est encore possible de changer la visibilité de la photo (ainsi que celle des plus anciennes).

En cas d'identification sur une photo, vous avez deux possibilités : retirer la mention (ouvrez la photo, cliquez sur « Options » puis sur « Supprimer l'identification ») ou faire en sorte que la photo n'apparaisse pas dans le journal (en la masquant). Mais vous pouvez aussi décider d'examiner toutes les identifications avant qu'elles n'apparaissent sur Facebook.

Statuts

Comme pour les photos, il est possible de choisir à qui chacun de vos statuts est accessible. Certains contenus sont plus privés/intimes que d'autres. Mais c'est à chacun de définir ses propres « limites ». Sachez par ailleurs qu'il est possible de limiter l'accès à vos anciens statuts Facebook. Cliquez sur « Paramètres », puis « Confidentialité ». Vous trouverez alors une option « Limiter la visibilité des anciennes publications sur votre journal ». Lisez les instructions attentivement avant de vous lancer.

En ce qui concerne les identifications, la démarche est la même que pour les photos.

Infos personnelles

Il est possible de paramétrer très finement la visibilité de toutes les informations contenues dans son profil (famille et relations, lieux où on a habité, etc.). Par exemple, dans « Emploi et scolarité », pour chaque emploi occupé, vous pouvez très facilement choisir qui peut le voir (cliquez sur « Options » à côté du poste, puis sur « Modifier »).

Facebook propose aussi à ses utilisateurs qu'on ne puisse pas les retrouver au moyen d'un numéro de téléphone, d'une adresse e-mail ou encore via les moteurs de recherche (lien vers le profil). Pour activer ces options, allez dans les paramètres de confidentialité puis « Qui peut me trouver avec une recherche ? ».

Groupes / fan pages

Attention à ce que vous postez sur les Pages et dans les groupes de discussion. Les paramètres de confidentialité que nous avons évoqués ne concernent que votre profil. Les messages postés sur ces espaces Facebook peuvent être référencés par les moteurs de recherche.

Lorsque vous aimez une Page, elle apparaît sur votre profil. Mais si vous souhaitez que cela ne soit pas le cas, c'est possible. Rendez-vous sur votre profil personnel. Sous votre photo de couverture à droite, cliquez sur « Plus » puis sur « Mentions J'aime ». Une page regroupant tous vos favoris s'ouvre alors. En cliquant sur le crayon puis sur « Modifier la confidentialité », vous pourrez choisir qui voit vos mentions J'aime.

Pour les groupes, il est possible de les masquer.

Vous pouvez aussi souhaiter que cette section « Mentions J'aime » ne soit tout simplement pas visible du tout. Dans ce cas, sélectionner « Gérer les sections » dans le menu sous « Plus » et désélectionnez « Mentions J'aime ».

Même chose pour les groupes.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.atlantico.fr/decryptage/comment-naviguer-incognito-facebook-avec-regles-confidentialite-actuelles-1927087.html>