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 rédhibitoire pour un employeur à la recherche d'un salarié rompu aux nouvelles technologies et aux réseaux sociaux. »

4) Déboussailler 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.

Source : http://tempsreel.nouvelobs.com/bien-bien/20150618.OBS1104/5-points-a-changer-immediatement-sur-votre-profil-linkedin.html
Propos recueillis par Angèle Guicharnaud

Quelques conseils pour surfer un peu plus tranquille sur Internet

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.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Conseils de prévention sur Internet / Cybercrime / Dossiers / Actualités – Police nationale – Ministère de l’Intérieur

---

Comment réagir lorsque vous êtes victime de harcèlement en ligne ?

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 paramétrages 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 nonauharcelement.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, confidentiel 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 surle 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"]

Original de l’article mis en page : Réagir en cas de harcèlement en ligne | CNIL

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

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

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

---

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.

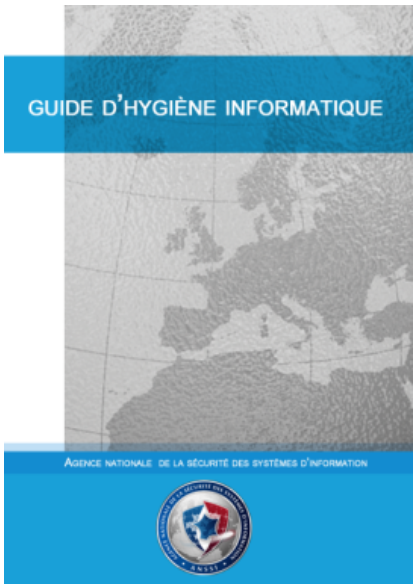
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation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

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

Contactez-nous

Réagissez à cet article

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



Les guides des bonnes pratiques de l’Anssi en matière de sécurité informatique

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

---

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

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*

A quoi ressemble une situation de cyber-harcèlement ?

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.

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

[lire la suite]

[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 : *Réagir en cas de harcèlement en ligne | CNIL*

Harcèlement en ligne : Qui sont les cyber-harceleurs ?

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 internaute peut être harcelé 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 …)…[lire la suite]

[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 : *Réagir en cas de harcèlement en ligne | CNIL*

Et si Google, Facebook ou Amazon payaient les internautes pour utiliser leurs données personnelles ?

Et si Google, Facebook ou Amazon payaient les internautes pour utiliser leurs données personnelles ? L'idée n'est pas nouvelle, mais elle a officiellement été reprise par Gavin Newsom, le nouveau gouverneur de la Californie. « Les consommateurs devraient avoir le droit de partager la richesse créée à partir de leurs données », a fait valoir l'élu démocrate, mardi 12 février, lors d'un discours devant les parlementaires locaux.

M. Newsom propose de créer un *« dividende sur les données »*. Les contours de la future loi restent à définir, tout comme son calendrier. Mais le gouverneur promet « *quelque chose d'audacieux ».* Son projet pourrait se heurter à l'opposition des grands groupes Internet, qui disposent toujours d'importants appuis politiques à Sacramento, la capitale de la Californie. Le puissant lobby Internet Association se dit d'ailleurs déjà sur ses gardes…[lire la suite]

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

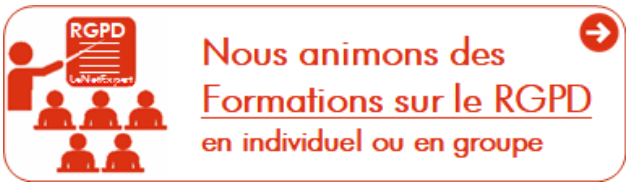
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

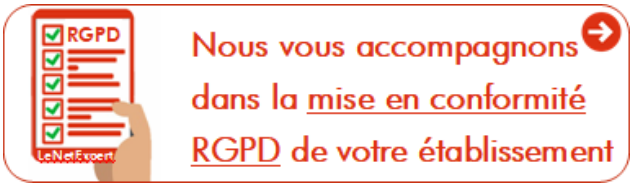
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
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
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)

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

Source : *Et si Google, Facebook ou Amazon payaient les internautes pour utiliser leurs données personnelles ?*