

**Victime d'une fraude sur
votre carte de paiement ?
L'état met à votre
disposition une nouvelle
plateforme : Percev@l**

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



**Victime d'une
fraude sur votre
carte de paiement
? L'état met à
votre disposition
une nouvelle
plateforme :
Percev@l**

Depuis quelques jours, un nouveau téléservice est disponible sur service-public.fr. Il permet aux victimes de fraude à leur carte de paiement de se signaler auprès des autorités.

Un tel service était nécessaire et attendu depuis longtemps. En effet, la fraude aux cartes de paiement a lieu essentiellement sur Internet aujourd'hui (à plus de 70% selon les statistiques publiées par l'Observatoire de la sécurité des moyens de paiement). Cela veut dire que le lieu où se commet réellement l'infraction n'a en général aucun rapport avec l'endroit où se trouve la victime. De surcroît, c'est le cumul des informations provenant des nombreuses victimes qui permettra d'identifier les fraudeurs et leur mode opératoire et facilitera la coopération internationale (plus facile si on peut identifier un préjudice conséquent lié aux mêmes auteurs).

Lorsqu'on constate un paiement frauduleux avec son numéro de carte bancaire (en consultant son relevé de compte en ligne, ou encore en étant prévenu par sa banque ou son prestataire de paiement), les opérations suivantes peuvent maintenant être réalisées par les victimes:

- Mettre sa carte en opposition en contact son organisme de paiement (en général par un simple appel téléphonique)
- Réaliser son signalement sur le téléservice Percev@l (on le retrouve simplement sur le site service-public.fr en cherchant Percev@l ou « fraude carte bancaire »)
- Transmettre le récépissé fourni par Percev@l à sa banque pour faciliter les opérations de remboursement

[lire la suite]

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 cyberarnaques 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'arnaques 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'arnaques 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://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



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](https://www.fnac.fr)

Source : *Percev@l – plateforme de signalement des fraudes aux cartes de paiement – est ouverte! – Investigation & transformation numériques*

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

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



La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

Il n'est pas possible pour l'employeur d'utiliser les résultats de la géolocalisation si ce n'est pas déclaré à la CNIL (Commission nationale de l'informatique et des libertés) et sans que le sache le salarié, encore moins si l'entreprise possède déjà un moyen de contrôler la durée de travail. Si un salarié a une liberté de son temps de travail, c'est surtout le résultat qui compte.

Réagissez à cet article

Quelques articles sélectionnés par nos Experts :

Quels sont les droits et devoirs des salariés en matière de sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

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)

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

Besoin d'une formation pour apprendre à vous mettre en conformité avec le RGPD ?

Contactez-nous



Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a 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 (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services. ».

Source : *Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord*

Comment se prémunir du phishing | Denis JACOPINI

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

x

x

x

x

x

x

x

Comment se prémunir du phishing

Le phishing, francisé sous le nom de „hameçonnage », est une méthode de fraude qui sévit sur le Web depuis 2005. Cette dernière permet de soutirer des données sensibles en exploitant les failles informatiques pour piéger les internautes.

[popup show= »ALL »]

Un phénomène actuel omniprésent

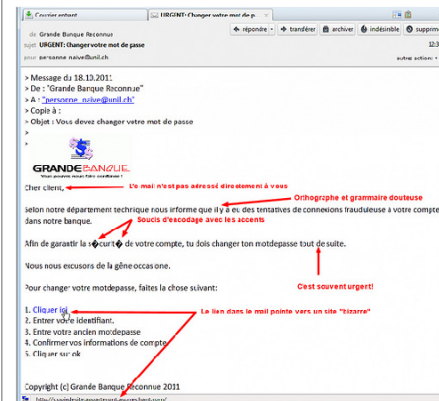
L'actualité ne cesse d'en rapporter les méfaits : l'attaque de TV5 Monde, la création d'un phishing Google qui ressemble comme deux gouttes d'eau au célèbre moteur de recherche et l'élaboration d'une opération phishing pour s'évader d'une prison sont autant de phénomènes d'actualité qui démontrent que ce genre de fraude est de plus en plus perfectionné. Il est d'ailleurs estimé qu'un Internaute sur 10 se laisserait prendre au piège, c'est ce que révèle un article de Metronews. Afin de contrer ce phénomène, l'association Phishing-Initiative a été créée dans le but de protéger les internautes et de freiner les tentatives de phishing, toujours plus nombreuses.

Comment reconnaître un mail frauduleux ?

Comment repérer le vrai du faux ? Voici quelques méthodes qui permettent de voir si vous avez à faire à une tentative de phishing par e-mail :

- Votre e-mail semble provenir de votre banque et a l'air d'en être une copie originale, avec son logo et ses couleurs. Commencez par lire le message, si vous trouvez des erreurs d'orthographe ou des erreurs d'affichage, vous saurez qu'il ne s'agit alors que d'une pâle copie.
- Un message vous invite à vous rendre sur une page externe. Méfiance ! Avant de cliquer sur le lien, passez la souris sur le lien sans cliquer dessus. En bas à droite, vous découvrirez une URL « bizarre », qui n'a rien à voir avec l'entreprise.
- Le mail est trop insistant (dans le pire des cas, vous prédit une catastrophe) et vous demande expressément de donner vos codes bancaires et informations personnelles.

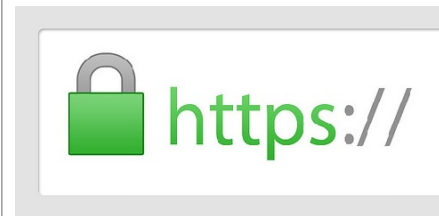
En voici un exemple type :



Flicker – phishing_exemple hameconnage pardownloadsource.fr, CC BY 2.0, Certains Droits Réservés

Comment effectuer un paiement en ligne sécurisé ?

• Comment éviter la fraude et payer en toute sécurité quand vous faites vos achats en ligne ? Comment savoir s'il ne s'agit pas d'une tentative de phishing ? Vérifiez toujours lors de votre paiement que le site est sécurisé : l'URL débute par « https » et est accompagnée d'un petit cadenas, de cette façon :



Flicker – https par Sean MacEntee, CC BY 2.0, Certains Droits Réservés Et si vous ne souhaitez pas livrer vos coordonnées bancaires lors d'un achat en ligne, il existe des modes de paiements alternatifs qui ne nécessitent pas vos données bancaires. Plus sûrs, ils ne sont toutefois pas infaillibles :

- PayPal, que l'on ne présente plus, permet de la même manière d'acheter ou de vendre en ligne sans livrer le moindre code bancaire grâce à un compte virtuel qu'il est possible de remplir selon vos besoins. Si des systèmes tels que PayPal sont régulièrement confrontés à des tentatives de phishing (vigilance donc !), le fraudeur ne peut cependant remonter à votre compte en banque, ce qui vous offre une sécurité supplémentaire.
- La carte virtuelle prépayée autorise un paiement en ligne sécurisé puisqu'en aucun cas vous ne livrez vos coordonnées bancaires sur Internet. Pour comprendre comment cela fonctionne, vous pouvez vous fier aux instructions de Paysafecard.
- Concernant le m-paiement, soit le paiement par mobile, Apple Pay utilise les concepts de jetons de paiement et l'identification biométrique pour une protection optimale. Mais, malgré la technologie développée par Apple, des hackers ont réussi à mener une vaste fraude bancaire en volant des données bancaires et en les installant sur de nouveaux Iphone.

Quel que soit votre moyen de paiement en ligne, restez vigilants !

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 cyberarnaques 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'arnaques 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'arnaques 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://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



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](https://www.fnac.fr)

Source : <https://www.globalsecuritymag.fr/Cybercriminalite-se-premunir-du,20150429,52544.html>

Accompagnement à la mise en conformité avec le RGPD de votre établissement

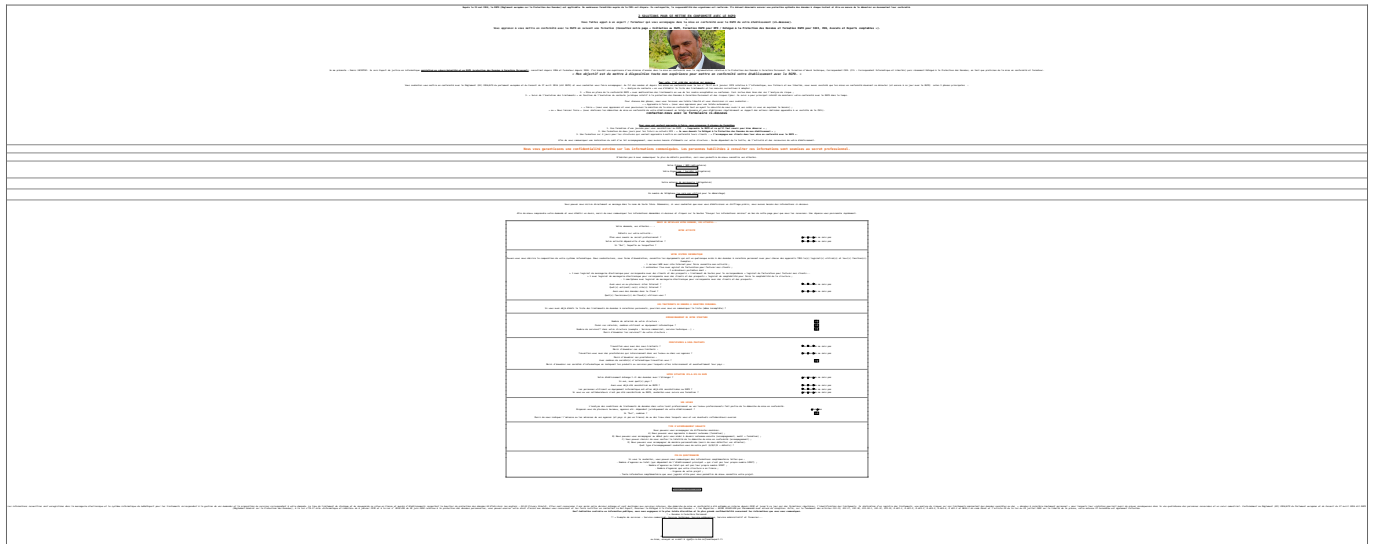
Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



Depuis 2012, nous accompagnons des établissements dans leur mise en conformité avec la réglementation sur les Données à Caractère Personnel.



Accompagnement à la mise en conformité avec le RGPD de votre établissement



Source : Denis JACOPINI

Céder au chantage finance et renforce l'infrastructure des attaques DDoS | Denis JACOPINI

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

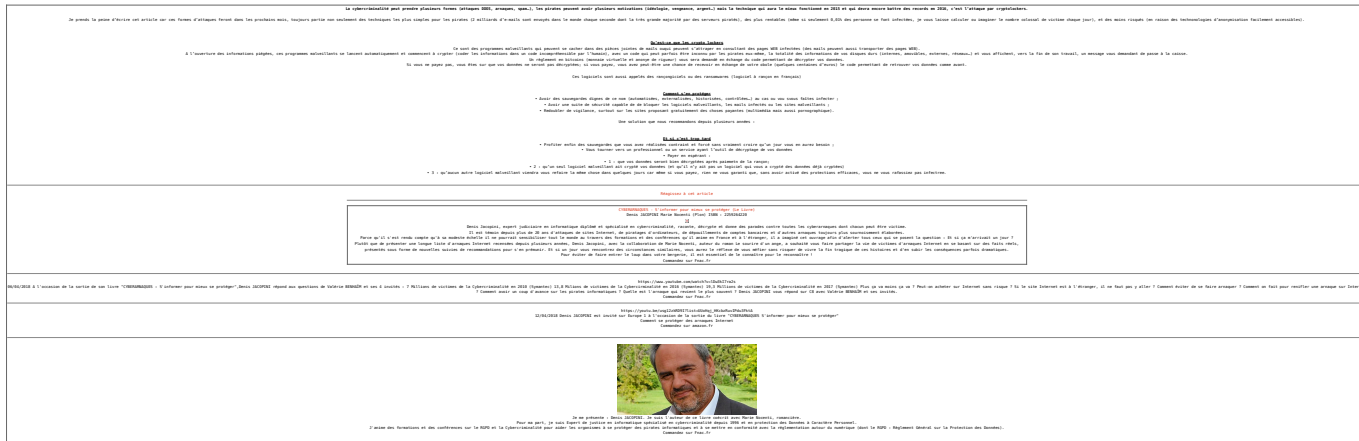


Denis JACOPINI



vous informe

Crypter données Les un nouveau métier ?



Source : Denis JACOPINI

Le dirigeant est responsable de ses déclarations à la CNIL | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Le dirigeant est responsable de ses #déclarations à la CNIL				

Nous attirons votre attention sur le fait que cette information est modifiée par la mise en place du RGPD (Règlement Général sur la Protection des données). Plus d'informations [ici](https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd) : <https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd> Nous l'avons toutefois laissée accessible non pas par nostalgie mais à titre d'information.

Nous attirons votre attention sur le fait que cette information est modifiée par la mise en place du RGPD (Règlement Général sur la Protection des données). Plus d'informations ici : <https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd> Nous l'avons toutefois laissée accessible non pas par nostalgie mais à titre d'information.

Quelles mesures les entreprises doivent-elles prendre pour être en règle avec la CNIL (commission nationale de l'informatique et des libertés), notamment pour le respect des données privées ?

Les entreprises doivent protéger les données personnelles, selon la loi Informatique et libertés ?

C'est une obligation légale des entreprises : elles doivent protéger les données personnelles de leurs salariés comme de leurs clients. Une donnée personnelle est toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement .

Certaines données peuvent sembler évidentes : nom, prénom, date de naissance, adresse postale, empreinte digitale. D'autres viennent moins spontanément à l'esprit : adresse IP, habitudes de consommation, entourage familial, plaque d'immatriculation.

L'entreprise se doit donc de sécuriser les informations personnelles qui transitent par son site Internet (ne serait-ce qu'à travers un formulaire de contact), par l'enregistrement des appels, la vidéosurveillance, l'annuaire interne, les contrôles d'accès aux locaux, etc.

Que doit faire l'entreprise pour être en conformité avec la loi ?

Informers les instances représentatives et mettre en œuvre une charte informatique ne suffit pas. Le site Internet de l'entreprise doit comporter des mentions légales, elle doit assurer la confidentialité des données, définir une durée de conservation des données, effectuer les déclarations préalables à la mise en place d'un dispositif de collecte auprès de la CNIL, respecter l'objectif de la collecte annoncé, etc.

Le dirigeant de l'entreprise est responsable et doit prendre les mesures nécessaires au traitement des données personnelles. Il est aussi fortement conseillé, dans les entreprises de taille importante, de mettre en place un CIL, un correspondant informatique et libertés, et de sensibiliser les utilisateurs et les salariés aux risques informatiques et à la loi informatique et libertés. Il peut aussi être utile de faire un inventaire des traitements des données à caractère personnel (site Internet, fichiers clients, prospects, fournisseurs, téléphonie, vidéo-surveillance, gestion de la paie, fichiers métiers).

Le coût de la mise en place de ces mesures varie en fonction de la taille de l'entreprise, donc du temps nécessaire à l'analyse des risques.

Quelles sanctions l'entreprise et son dirigeant risquent-ils ?

Au-delà des sanctions légales, c'est la réputation et la crédibilité de l'entreprise qui sont en jeu : son image et son patrimoine sont exposés.

Néanmoins, l'absence de mentions légales peut déboucher sur une amende de 6000 €, la surveillance permanente des zones réservées dans une entreprise ou la collecte de données sur la vitesse d'un véhicule, 5000 € ; le non respect des obligations de sécurisation des données personnelles peut aller jusqu'à 300 000 € d'amendes. Toutefois, la CNIL joue pour l'instant avant tout un rôle de prévention plus que de sanction.

Quid de la loi sur le renseignement qui oblige les opérateurs à mettre en place des dispositifs automatiques de collecte des données ?

Ce type de loi ne pose pas de problème dans une démocratie et remplit ses objectifs de sécurité. En revanche, la question se poserait de façon plus grave sous un autre régime.

ATTENTION !

Nous attirons votre attention particulièrement sur le fait que certains professionnels du monde informatique, de l'internet ou de la communication, concernés par un devoir d'information auprès de leurs clients, remplissent les déclarations à la CNIL de leurs clients pour leur simplifier les démarches.

Il faut savoir que la déclaration à la CNIL d'un système de traitement se compose d'abord d'un audit technique et logique de l'existant, tant au niveau organisationnel qu'au niveau technique jusqu'à la sécurité informatique mise en place.

Une déclaration incomplète ou ne correspondant pas à la réalité peut vite se transformer en FAUSSE DECLARATION.

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)

Réagissez à cet article

Source :
<http://www.tracescritesnews.fr/actualite/le-dirigeant-est-responsable-de-la-securite-informatique-de-l-entreprise-et-des-donnees-personnelles-56747>
par Pierre-Yves Ratti

Prospection par messagerie électronique : que risque une société qui ne respecte pas la loi ? | Denis JACOPINI

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



vous informe...

#Prospection par messagerie électronique : que risque une société qui ne respecte pas la loi ?

Une société commerciale ne peut envoyer de mails publicitaires sans l'accord préalable de la personne sollicitée.

Une société qui ne respecte pas cette règle risque des sanctions pénales et des amendes de 750 euros par message expédié.

De son côté, la CNIL peut prononcer des sanctions pouvant aller jusqu'à 300.000 Euros d'amende lorsque des messages sont adressés à des personnes physiques sans leur consentement.

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...)





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](#)



Source : <https://www.cnil.fr/fr/cnil-direct/question/372>

Quels sont les droits et devoirs des salariés en matière de sécurité informatique | Denis JACOPINI

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

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Quels sont les droits et devoirs des salariés, en matière de sécurité informatique				

Il n'est pas rare que des salariés soient surpris en train, au sein de leur entreprise, d'utiliser des outils de type Keylogger – permettant l'enregistrement des touches utilisées sur le clavier – et des logiciels visant à capter et à forcer les mots de passe de sessions de systèmes d'exploitation.

Or, dans la majorité des cas, aucune sanction n'est prise par les employeurs, y compris lorsque les auteurs des faits sont animés d'intentions malveillantes et non simplement ludiques.

Dans un raisonnement inspiré du droit du travail, l'employeur – arguant par exemple de ne pas disposer de charte de sécurité informatique spécifiant les comportements à respecter, ainsi que les sanctions applicables – estime qu'à défaut d'avoir porté par écrit à la connaissance de l'employé la réglementation en vigueur au sein de l'entreprise, celui-ci ne peut être légalement sanctionné.

Il est important de rappeler que le seul fait de collecter des données à caractère personnel par un moyen frauduleux est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (article 226-18 du Code pénal) et ce, quelles que soient les intentions du salarié. De même, le fait de s'introduire frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans de prison et de 30 000 euros d'amende (article 321-1 du même code). La loi est d'application directe et ne nécessite pas d'être citée dans une charte informatique pour en assurer le respect par les salariés. Les employeurs peuvent donc prendre immédiatement les sanctions afférentes à une telle faute.

En outre, la responsabilité de l'employeur peut se voir engagée par ce type d'agissements, sur la base de plusieurs fondements :

- la personne cible/victime des menées de son/ses collègues pourra, en cas de dommage, agir contre l'employeur, responsable de ses salariés. Il reviendra alors à la société de prouver que le mis en cause a agi « hors des fonctions auxquelles il était employé, sans autorisation et à des fins étrangères à ses attributions », ce qui est rarement admis en pratique.
- de par la jurisprudence « Sarenza c/ Jonathan » du 21 février 2013, le juge a précisé que la société devait supporter, à hauteur de 30%, son propre dommage, engendré par les lacunes dans la gestion des identifiants d'accès aux bases de données. Le juge a donc instauré l'obligation, pour l'employeur, de mettre en place des mesures de protection informatique efficaces, afin de prévenir l'installation de tout logiciel espion.
- Enfin, la plupart des logiciels utilisés à ces fins proviennent de téléchargements, susceptibles de contenir des virus. Les réseaux internes des entreprises sont régulièrement infectés par ce biais, ce qui facilite les intrusions informatiques et, partant, l'accès, l'utilisation, l'extraction, voire la destruction de données stratégiques pour l'entreprise.

Préconisations de la DGSJ

La DGSJ recommande à toute entreprise :

- En priorité, d'établir une charte de sécurité informatique qui permettra de sensibiliser les salariés aux enjeux numériques, tout en les responsabilisant.
- D'organiser régulièrement des conférences de sensibilisation à destination de l'ensemble des collaborateurs, qui insisteront sur leurs droits et obligations à l'ère du tout-numérique et dispenseront des mises à jour sur les évolutions technologiques en cours.
- De mettre en place des mesures de protection efficaces afin de prévenir l'utilisation potentielle de logiciels et matériels espions. L'existence de tels dispositifs de sécurité informatique permettra à l'employeur de dégager sa responsabilité juridique et d'optimiser le bon fonctionnement de son entreprise en augmentant le niveau de protection.

Vous avez besoin de recueillir des preuves, expertiser un système informatique, vérifier des contenus, Denis JACOPINI peut vous conseiller, vous accompagner et réaliser toutes les phases techniques nécessaires à la constitution d'un dossier juridique solide.

Contactez Denis JACOPINI

Réagissez à cet article

Quelques articles sélectionnés par nos Experts :

Quels sont les droits et devoirs des salariés en matière de sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

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)

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

Besoin d'une formation pour apprendre à vous mettre en conformité avec le RGPD ?

Contactez-nous



Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a 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 (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services. ».

Source

<http://www.ccirezo-normandie.fr/document/104108-flash-ingerence-economique-n-15-rappel-des-droits-et-devoirs-des-salaries-en-entrepr>

La cybersécurité pour les débutants – Un lexique informatique

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

×

×

×

×

×

×

×

La cybersécurité pour les
débutants – Un
lexique informatique

1. Introduction
2. Background
3. Methodology
4. Results
5. Discussion
6. Conclusion
7. References
8. Appendix
9. Glossary
10. Index

The following text is a placeholder for the main content of the document, which is currently blank.

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...)



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](#)



Original de l'article mis en page : Lexique – La préfecture de Police

Ne pas avertir son employeur de propos injurieux sur Facebook peut vite devenir une faute grave | Denis JACOPINI

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

x

x

x

x

x

x

x

Ne pas avertir son employeur de propos injurieux sur Facebook peut vite devenir une #faute grave

La cour d'appel de Lyon a confirmé le mois dernier le licenciement d'une salariée accusée d'avoir tenu sur Facebook des propos dégradants et injurieux à l'égard de ses collègues de travail. L'employeur n'a pourtant pas réussi à prouver que la personne mise en cause était bien l'auteur des messages délivrés sur un groupe spécialement créé à cet effet. Explications.

Travaillant en tant que sellière maroquinière depuis 2002 chez Hermès, Madame X est licenciée en décembre 2011 pour faute grave. C'est-à-dire sans préavis ni aucune indemnité. Il faut dire que les reproches formulés par son employeur sont relativement sérieux.

La salariée est en effet accusée d'avoir ouvert en octobre 2011 un groupe Facebook intitulé « Les potins d'Hermès », sur lequel étaient relatées des « situations tenant à la vie privée de certains collaborateurs nommément désignés », « sous forme de messages et anecdotes ». C'est suite à des remontées internes que la direction a eu vent de ces commentaires jugés « profondément dégradants et injurieux » à l'égard des employés concernés, ce qui a poussé les responsables de l'entreprise à chercher à remonter jusqu'à leur auteur.

Problème : l'administrateur de ce groupe dispose d'un compte Facebook au nom de « Jules César ». Autrement dit, il s'agit d'un beau pseudonyme... Après enquête, l'employeur affirme que l'adresse IP de l'auteur de ces messages correspond à celle du domicile de Madame X. Dans un premier temps, la salariée reconnaît avoir eu connaissance de ce groupe, tout en niant en être à l'origine. Mais dans un second temps, elle finit par admettre que le compte « Jules César » et le groupe « Les potins d'Hermès » ont bien été créés depuis son ordinateur, mais par sa sœur...

« Même dans le cas où les déclarations de votre soeur (par ailleurs très limitées quant à son hypothétique implication personnelle) [seraient] avérées, et dans la mesure où vous nous avez déclaré avoir eu connaissance de la création de la page et de son contenu dès sa mise en ligne, vous auriez dû à tout le moins nous alerter au sujet d'une telle initiative dont la teneur et la portée ne pouvaient rester sans conséquence vis-à-vis de l'entreprise et de ses collaborateurs » retient ainsi l'employeur dans sa lettre de licenciement.

Impossible d'identifier le créateur du groupe

Sauf que l'ex-salariée estime avoir été remerciée à tort. Elle a donc tout d'abord saisi le conseil des prud'hommes de Lyon, lequel a confirmé le licenciement pour faute grave en novembre 2013. Madame X a ensuite saisi la cour d'appel de Lyon, qui a justement rendu sa décision le 20 octobre dernier.

Les magistrats se sont intéressés en particulier aux adresses IP fournies par Hermès. Ils ont cependant constaté que la connexion ayant servi à créer le profil Jules César et à alimenter « la plupart » des messages litigieux correspondait en fait à « une adresse IP algérienne dont l'employeur n'a pu identifier le titulaire ». En clair, il était impossible de prouver en l'état qu'il s'agissait de Madame X ou même de sa sœur.

Mais cela n'a pas empêché la cour d'appel de considérer qu'il y avait malgré tout eu faute grave de la part de la salariée. Cette faute ? Savoir que le groupe « Les potins d'Hermès » existait et n'avoir rien signalé. La décision, que nous avons pu consulter, retient en ce sens que « la faute commise par Mme X en n'alertant pas sa direction sur la création de ce groupe de discussion alors qu'à partir de son propre ordinateur étaient mis en ligne des propos déshonorants pour ses collègues de travail (...) est d'une gravité suffisante pour rendre impossible le maintien de cette salariée dans l'entreprise pendant la durée limitée du préavis ».

La cour d'appel n'a donc pas donné suite aux demandes de l'ex-salariée, qui réclamait plus de 40 000 euros d'indemnités.

La décision de la cour d'appel de Lyon évoquée dans l'article ci-dessus

Réagissez à cet article

Quelques articles sélectionnés par nos Experts :

Quels sont les droits et devoirs des salariés en matière de sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

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)

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

Besoin d'une formation pour apprendre à vous mettre en conformité avec le RGPD ?

Contactez-nous



Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a 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 (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services. ».

Source

:
<http://www.nextinpact.com/news/91031-propos-injurieux-sur-face-book-ne-pas-avertir-son-employeur-peut-etre-faute-grave.htm>