

« Bloctel », la nouvelle « liste rouge » contre les spams téléphoniques | Denis JACOPINI

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



Denis JACOPINI



« Bloctel », la nouvelle « liste rouge » contre les spams téléphoniques

Invitation par SMS à télécharger une vidéo, demande de rappel d'un correspondant inconnu, démarchage pour une cuisine, des fenêtres en PVC ou des panneaux solaires... Tout possesseur d'un téléphone mobile a déjà dû faire face à ces nombreuses sollicitations, plus ou moins intrusives.

Message
Aujourd'hui 13:22



Info message vocal. Vous avez une notification vocale disponible. Cliquez pour l'écouter : <http://allo-mms.com/>

Depuis le 1er juin, les particuliers qui le désirent peuvent inscrire gratuitement leurs numéros (fixe et portable) sur la liste d'opposition au démarchage téléphonique « Bloctel » (bloctel.gouv.fr), mise en place par l'Etat.

Elle va remplacer la liste « Pacitel » créée en 2011, à l'initiative du gouvernement, par la Fédération française des télécoms. Cette dernière regroupe les principaux opérateurs (hors Free). Contrairement à Pacitel, l'ensemble des entreprises de démarchage auront obligation de se conformer à cette nouvelle liste Bloctel, sous peine d'amende allant jusqu'à 75 000 euros. Ils devront chaque mois retirer de leurs bases de données les numéros de téléphone inscrits sur la liste.

LA MAJORITÉ DES DÉMARCHAGES SE FAIT DEPUIS L'ÉTRANGER

Martine Pinville, secrétaire d'Etat en charge du commerce, qui a pris la succession de Carole Delga, à l'origine de l'entrée en vigueur de ce système, se dit « confiante » dans le succès de cette plate-forme. Mais elle précise que si un démarchage abusif est constaté, « il faudra à ce moment-là relever le numéro de téléphone et, si possible, le nom de la société qui a appelé, afin de nous le signaler sur Bloctel ou à la DGCCRF. Nous ferons les poursuites nécessaires ». Difficile toutefois d'identifier un numéro bien souvent masqué. L'autre écueil réside dans le fait que la majorité des démarchages se fait depuis l'étranger... [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

Source : « Bloctel », la nouvelle « liste rouge » contre les spams téléphoniques

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					
x	x	x	x	x	x
x	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*

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

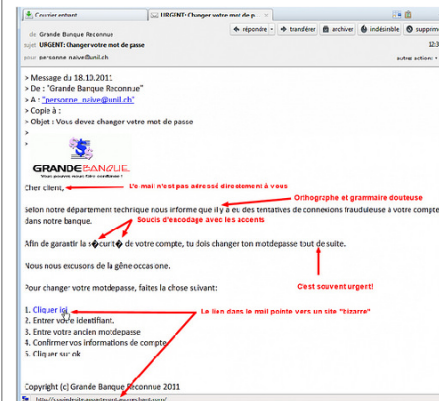
L'actualité ne cesse d'en rapporter les méfaits : l'attaque de TV5 Monde, la création d'un phishing Google qui ressemble comme deux gouttes d'eau au célèbre moteur de recherche et l'élaboration d'une opération phishing pour s'évader d'une prison sont autant de phénomènes d'actualité qui démontrent que 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.

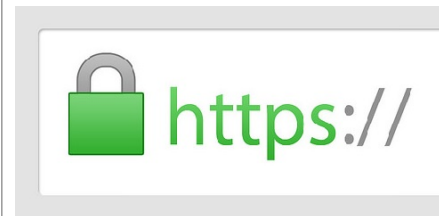
En voici un exemple type :



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

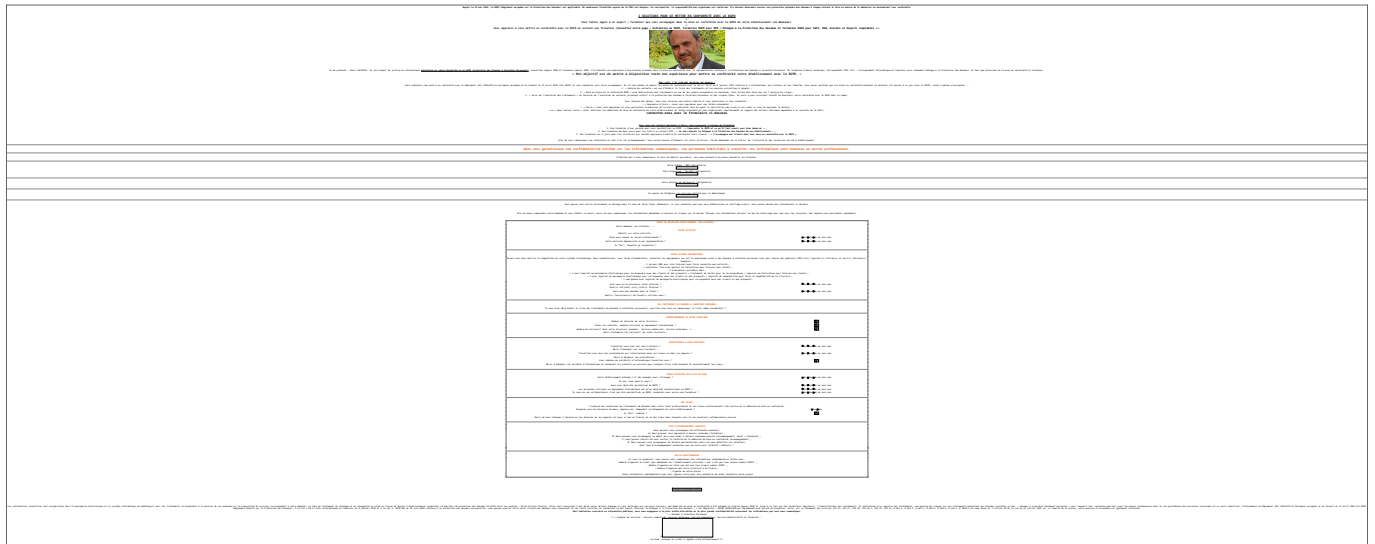
Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



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 ?

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 body of the document, which would contain the detailed content of each section listed in the table of contents.

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>

Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants

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



Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants

Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

2 SOLUTIONS POUR SE METTRE EN CONFORMITÉ AVEC LE RGPD

Vous apprenez à vous mettre en conformité avec le RGPD en suivant une formation (ci-dessous) ;

Vous faites appel à un expert / formateur qui vous accompagne dans votre mise en conformité avec le RGPD de votre établissement (Consultez notre page « Services d'accompagnement à la mise en conformité avec le RGPD »).



Je me présente : Denis JACOPINI. Je suis Expert de Justice en informatique spécialisé en cybersécurité et en RGPD (protection des Données à Caractère Personnel), consultant depuis 1996 et formateur depuis 1998. J'ai 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 aisé d'expliquer le côté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

Pour cela, j'ai créé 3 niveaux de formation.

1. Une formation d'une journée pour les indépendants, TPE et les PME « Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer ». Cette formation a pour objectif de vous faire découvrir l'essentiel de ce règlement Européen, de vous apprendre les principes du RGPD permettant à la fois de comprendre l'intérêt de la démarche de mise en conformité RGPD et de réaliser les premières actions ;
2. Une formation de deux jours pour les DPO « Je veux devenir le Délégué à la Protection des Données de mon établissement ». Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement ;
3. Une formation sur 4 jours pour les consultants « J'accompagne mes clients dans leur mise en conformité avec le RGPD ». Vous êtes une société d'informatique, un cabinet d'avocat, un cabinet d'expertise comptable et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation est composée de 2 jours de théorie et 2 jours de pratique dont 1 dans l'établissement de votre choix (le votre ou celui d'un client). Suivez la formation qui vous apportera la plus grande autonomie avec le RGPD de tout notre catalogue.

et des services sur mesure.

1. Vous souhaitez tout faire -> Nous vous apprendrons à mettre votre établissement en conformité, la plupart du temps, le contenu de ces formations est personnalisé et adapté à vos besoins spécifiques ;
 2. Vous ne savez pas par où commencer -> Nous ferons l'état des lieux, mettrons en place le registre puis nous vous apprendrons à maintenir la conformité des traitements ;
 3. Vous ne souhaitez rien faire -> Nous nous occuperons de tout.
- Plus d'information sur nos services d'accompagnement à la mise en conformité avec le RGPD ici

Formation pour TPE/PME « Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer » : 1 jour

Découvrez l'essentiel du RGPD, apprenez les principes du RGPD permettant à la fois de comprendre l'intérêt de la démarche de mise en conformité RGPD et de réaliser les premières actions.
Consultez les dates de nos prochaines formations
« Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »

Formation pour DPO « Je veux devenir le Délégué à la Protection des Données de mon établissement » : 2 jours

(Découvrez et comprenez la démarche de mise en conformité)
Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement.
Consultez les dates de nos prochaines formations
« Je veux devenir le Délégué à la Protection des Données de mon établissement »

Formation pour consultants « J'accompagne mes clients dans leur mise en conformité avec le RGPD » : 3 jours + 1 jour dans votre établissement

(C'est le moment où jamais de vendre des services autour du RGPD)
Enfin, si votre objectif est avant tout de développer l'activité de mise en conformité avec le RGPD afin de vendre cette prestation auprès de vos clients, cette formation est faite sur mesure pour vous en vous apportant l'ensemble des mesures et des cas qu'il est nécessaire de maîtriser pour que vos clients soient mis sur le chemin de la mise en conformité. Vous êtes une société d'informatique, un cabinet d'avocat, un cabinet d'expertise comptable, un consultant et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation se passe sur 3 jours en groupe plus une journée supplémentaire en individuel pour superviser la mise en place du RGPD dans votre établissement ou chez un de vos clients (frais liés au déplacement dans cet établissement en sus). Suivez la formation qui vous apportera la plus grande autonomie dans la mise en conformité de tout notre catalogue.
Consultez les dates de nos prochaines formations
« J'accompagne mes clients dans leur mise en conformité avec le RGPD »

Formation RGPD « Mise en conformité RGPD sur mesure » (pour TPE/PME)

(Pour ceux qui souhaitent une formation ou un accompagnement personnalisé dans la mise en conformité RGPD)

Que vous soyez bientôt ou déjà désigné « Délégué à la Protection des Données » ou « DPO » dans votre établissement, si vous souhaitez que nous établissions une formation personnalisée dans son contenu ou dans son organisation, nous nous ferons un plaisir d'étudier votre demande et d'élaborer une proposition adaptée à vos besoins.

Accompagnement à la mise en conformité RGPD de mon établissement

(Mettez en place une démarche de mise en conformité RGPD)
Vous souhaitez vous mettre en conformité avec le Règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 (dit RGPD) et vous souhaitez vous faire accompagner. Au fil des années et depuis les mises en conformité avec la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nous avons constaté que les mises en conformité devaient se dérouler (et encore à ce jour avec le RGPD) selon 3 phases principales :

1. « Analyse du contexte » en vue d'établir la liste des traitements et les mesures correctives à adopter ;
2. « Mise en place de la conformité RGPD » avec amélioration des traitements en vue de les rendre acceptables ou conformes. Ceci inclue dans bien des cas l'analyse de risque ;
3. « Suivi de l'évolution des traitements » en fonction de l'évolution du contexte juridique relatif à la protection des Données à Caractère Personnel et des risques Cyber. Ce suivi a pour principal intérêt de maintenir votre conformité avec le RGPD dans le temps.

Pour chacune des phases, nous vous laissons une totale liberté et vous choisissez si vous souhaitez :

- « Apprendre à faire » (nous vous apprenons pour une totale autonomie) ;
- « Faire » ;
- ou « Nous laisser faire ».

Afin de vous communiquer une indication du coût d'un tel accompagnement, nous aurons besoin d'éléments sur votre structure : Durée dépendant de la taille, de l'activité et des ressources de votre établissement.

N'hésitez pas à contacter notre équipe.

Intéressé pour assister à une de nos sessions de formation en France, choisissez la ville qui vous intéresse. Vous souhaitez que nous nous déplaçons au sein de votre établissement pour une formation ou pour un accompagnement individuel, indiquez le dans les commentaires.

Votre Prénom / NOM (obligatoire)

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (pour faciliter l'organisation)

Vous souhaitez avoir des informations sur :

- la formation « Comprendre le RGPD » : 1 jour
- la formation « Je veux devenir Délégué à la Protection des Données » : 2 jours
- la formation « Je mets en conformité mon établissement » : 3+1 jours
- la formation « Mise en conformité RGPD sur mesure »
- un accompagnement personnalisé au RGPD

Vous souhaitez réserver une ou plusieurs places à la formation :

Formation pour TPE/PME : « Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour DPO : « Je veux devenir le Délégué à la Protection des Données de mon établissement »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour consultants : « J'accompagne mes clients dans leur mise en conformité avec le RGPD »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Autre ville ou sujets souhaités en individuel (indiquez ci-dessous)

Votre message avec vos préférences de date ou vos commentaires

Envoyer

Nos formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre accepté. Si la formation était annulée (nombre de participants insuffisants ou en cas de force majeure), votre accepté sera remboursé en intégralité dans les 5 jours (Les chèques seront encaissés à partir du jour de la formation). En cas d'annulation de votre part moins de 48 heures avant la formation, l'accepté pourra ne pas être remboursé car destiné à régler les frais de réservation de salle et d'organisation, eux même non remboursables.

LE FORMATEUR : Denis JACOPINI



Denis JACOPINI est Expert de Justice en informatique spécialisé en cybersécurité et en RGPD (protection des Données à Caractère Personnel). Il est diplômé en Cybersécurité, et, titulaire de l'expertise Judiciaire et est Certifié en Gestion des Risques des Systèmes d'Information. Il est formateur depuis 1998 et consultant depuis 1996, il a 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 dans la sécurité informatique, 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 lui est ainsi aisé d'expliquer le côté pragmatique de la démarche de mise en conformité avec le RGPD à tout public.

« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

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 : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes*

Les meilleurs conseils pour choisir vos mots de passe | Denis JACOPINI

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



Les meilleurs conseils pour choisir vos mots de passe

A l'occasion de la Journée du Mot de Passe, les meilleurs conseils aux utilisateurs pour éviter que leurs codes secrets ne soient découverts.



Le 5 mai était la Journée Mondiale du Mot de Passe. Une idée marketing lancée par des éditeurs de solution de sécurité informatique. Pour marquer cette date d'une pierre blanche, plusieurs éditeurs ont analysé les habitudes des utilisateurs. Avast Software par exemple propose des recommandations pour créer et protéger des mots de passe indéchiffrables.

Créer des mots de passe fiables et les modifier fréquemment

Une actualité ponctuée d'histoires comme celles de la faille d'Ashley Madison, le site de rencontres extra-conjugales, démontre que les gens n'utilisent pas correctement leurs mots de passe. Les utilisateurs ne créent pas de codes assez fiables et il est certain qu'ils ne les changent pas régulièrement – même face au risque de voir leurs données sensibles et leurs potentielles frasques exposées, ou leur mariage brisé. Les utilisateurs créent des mots de passe facilement déchiffrables souvent par manque d'information ou par paresse, en témoigne la liste des codes les plus souvent utilisés compilée par les chercheurs.

Dans le top 10 :

1. 123456
2. 123456789
3. password
4. 101
5. 12345678
6. 12345
7. Password1
8. qwerty
9. 1234
10. 111111

Cette liste comprend les mots de passe les plus simples, tels que 123456, password, et qwerty. D'autres se retrouvent plus bas dans la liste comme iloveyou (#19) ou trustno1 (#57) – une ironie pour un code figurant dans la liste des mots de passe les plus populaires. « Certains pensent qu'une Liste de mots de passe seuls qui fuite en ligne n'est pas un problème – cependant, environ 50 % de ces mots de passe étaient associés à une adresse mail, déclare le chercheur d'Avast Michal Salat. Nous savons que les gens utilisent les mêmes combinaisons de mails et de mots de passe pour différents comptes. C'est pourquoi si un hacker connaît le mot de passe de votre profil Ashley Madison, il connaîtra également celui de votre Facebook, Amazon, eBay, etc. »

Comment créer des mots de passe fiables ?

Il n'y a pas de meilleure occasion que le 5 mai pour commencer à changer ses habitudes et protéger ses codes. Voici quelques conseils pour garder un mot de passe fiable et sécurisé. Je vais être honnête avec vous, si vous ne prenez pas 5 minutes pour réfléchir à votre sécurité et à la bonne gestion de vos précieux, passez votre chemin !

Domus tutissimum cuique refugium atque receptaculum sit

- Créer des mots de passe longs et complexes. Il suffit de reprendre une phrase d'un livre que vous aimez. N'oubliez pas d'y placer quelques chiffres, majuscules et signes de ponctuations.
- Utiliser un mot de passe différent pour chaque compte. Lors de les conférences, je fais sortir les clés des participants. Une clé pour chaque porte (voiture, boîte aux lettres, maison, bureau...). En informatique, il faut la même règle pour ses mots de passe.
- Ne pas partager ses mots de passe. C'est peut-être une proposition idiote au premier abord, mais combien de fois, lors d'ateliers que je propose dans les écoles, j'entends le public m'expliquer avoir partagé avec son ami, son voisin... sa clé wifi !
- Changer ses mots de passe régulièrement. Pour mon cas, il change tous les 35 jours. Je ne suis pas à l'abris du vol d'une base de données dans les boutiques, sites... que j'utilise.
- Utiliser un gestionnaire de mot de passe pour mémoriser ses mots de passe ? Je suis totalement contre. Il en existe beaucoup. Mais faire confiance à un outil dont on ne maîtrise ni le code, ni la sécurité, me paraît dangereux. Beaucoup d'utilisateurs y trouvent un confort. L'ensemble de vos mots de passe sont regroupés dans une solution informatique qui chiffre les données. Un seul mot de passe est requis pour utiliser n'importe quel compte sauvegardé. Bref, vaut mieux ne pas perdre ce précieux cerbère !
- Verrouiller son matériel avec un mot de passe. Les systèmes existent. Utilisez les. Je croise bien trop d'ordinateur s'ouvrant d'une simple pression sur la touche « Entrée ».
- Activer la double-authentification ou l'authentification forte. Indispensable aide. Téléphone portable, sites Internet, Facebook, Twitter... La double authentification renforce l'accès à vos espaces. En cas de perte, vol, piratage de votre précieux. Sans la double authentification, impossible d'accéder à vos données.

De son côté TeamViewer rappelle aussi qu'il est déconseillé de fournir des informations personnelles identifiables : Utiliser plusieurs mots de passe forts peut impliquer quelques difficultés de mémorisation. Aussi, afin de s'en souvenir plus facilement, beaucoup d'utilisateurs emploient en guise de mot de passe des noms et des dates qui ont une signification personnelle. Les cyber-délinquants peuvent cependant exploiter des informations accessibles publiquement et des comptes de réseaux sociaux pour trouver ces informations et s'en servir pour deviner les mots de passe... [Lire la suite]

D'autres bons conseils pour gérer vos mots de passe sur disponibles le site de l'ANSSI ou de la CNIL.

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 : Générer un mot de passe indéchiffrable, possible ? –
Data Security BreachData Security Breach

Les PME face à la cybercriminalité – Quelques règles de bon sens... | Denis

JACOPINI

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



Les PME face à la
cybercriminalité –
Quelques règles de
bon sens...

Face à l'« industrialisation » de la cybercriminalité, aucune entreprise n'est à l'abri, pas même les plus petites. Il est désormais indispensable de s'y préparer pour éviter des déconvenues qui peuvent se révéler très coûteuses.

De plus en plus variées, les techniques des cybercriminels s'industrialisent.

Un montant impressionnant : 445 milliards de dollars, soit 327 milliards d'euros, c'est le coût annuel de la cybercriminalité et de l'espionnage économique au niveau mondial, selon le Center for Strategic and International Studies (CSIS). Et il n'a sans doute pas fini de croître. « La cybercriminalité ne cesse de se développer et les attaques sont de plus en plus variées et sophistiquées, touchant toutes les entreprises, quelle que soit leur taille », assure Paul-Henri Huckel, consultant au sein du cabinet de conseil en stratégie des systèmes d'information et de la cybersécurité Lexsi.

Virus bancaire permettant d'effectuer des virements frauduleux ; destruction de sites Web d'entreprises d'e-commerce ; vol de données revendues à un concurrent ; « ransomware », autrement dit cryptage de toutes les données d'une entreprise « libérables » après versement d'une rançon... Les techniques des cybercriminels s'industrialisent.

Le courrier électronique, maillon faible du système

« La première erreur est de penser que l'on est à l'abri, parce que l'on est petit », prévient Paul-Henri Huckel. Selon un rapport publié en avril 2014 par l'éditeur de logiciels Symantec, 30 % des attaques ciblées visent les PME. « Les dirigeants de petites entreprises ne sont pas suffisamment sensibilisés. Certaines sociétés n'ont même pas mis en place de système de sauvegarde de leurs données. Or, leur perte peut, dans certains cas, entraîner la fermeture de l'entreprise », remarque aussi Frédéric Desclos, responsable de l'Echangeur PME, espace de la chambre de commerce et d'industrie Paris Ile-de-France consacré à la sensibilisation et à la formation aux technologies de l'information des petites et moyennes entreprises.

Face à ce risque croissant de cyberattaque, sécuriser son système d'information est indispensable. Le courrier électronique est le maillon faible du système : selon Symantec, un message électronique sur 392 contiendrait une attaque de « phishing », ces faux courriers officiels destinés à détourner les coordonnées bancaires.

Les mots de passe doivent être modifiés au moins tous les six mois

« Il est indispensable de sensibiliser les salariés à cet aspect, ainsi qu'au caractère critique des mots de passe qui doivent être modifiés régulièrement, au moins tous les six mois », remarque Frédéric Desclos. Ce qui n'empêche pas, par ailleurs, de sécuriser au maximum son système d'information par le biais d'antivirus, d'anti-spam et de firewalls efficaces. « Un plan de sauvegarde des données est également indispensable », complète Paul-Henri Huckel. Une procédure qui n'est pas forcément coûteuse. Il suffit par exemple au dirigeant de l'entreprise de quitter chaque soir son bureau avec sa sauvegarde sous le bras...

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 : Jean-Marc Engelhard

<http://www.leparisien.fr/economie/les-pme-face-a-la-cybercriminalite-15-09-2014-4136531.php>