



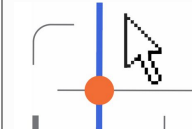


Combien de temps une crèche peut-elle conserver des informations sur les enfants et leurs familles ? | Denis JACOPINI

| | | | | | |
|---|--|--|--|---|---|
| Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer | | | | | |
|  LE NET EXPERT AUDITS & EXPERTISES |  LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES |  LE NET EXPERT RGPD CYBER MISES EN CONFORMITE |  LE NET EXPERT SPY DETECTION Services de détection de logiciels espions |  LE NET EXPERT FORMATIONS |  LE NET EXPERT ARNAQUES & PIRATAGES |
|  Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité vous informe... | | <h2>Combien de temps une crèche peut-elle conserver des informations sur les enfants et leurs familles ?</h2> | | | |
| <p>Les crèches et les autres structures d'accueil de jeunes enfants sont amenées à enregistrer dans leur logiciel de gestion des informations personnelles sur les enfants accueillis et sur leurs parents.</p> <p>La durée de conservation de ces informations ne doit pas dépasser la durée nécessaire aux finalités pour lesquelles ces informations sont collectées et traitées.</p> <p>Dans le cas de l'accueil de jeunes enfants, la CNIL recommande que ces informations soient effacées au plus tard trois ans après leur départ. Au-delà de ce délai, elles ne peuvent être conservées que de manière anonymisée, dans un but statistique par exemple.</p> | | | | | |

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



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

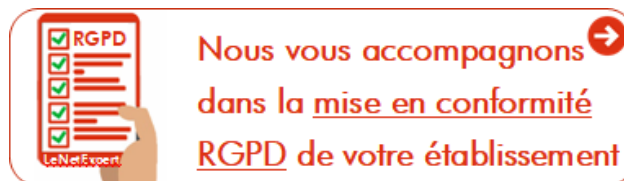
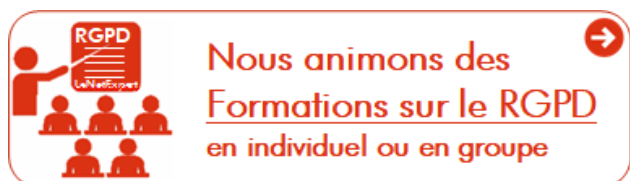
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

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

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



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

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

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles

en 6 étapes

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

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

Source :
<http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=193E337DAA685A15B25C9E90E19E80BF?name=Combien+de+temps+une+cr%C3%A8che+peut-elle+conserver+des+informations+sur+les+enfants+et+leurs+familles+%3F&id=483>

L'employé comme pion dans la lutte pour la cyber-sécurité | Denis JACOPINI

| | |
|---|---|
|  | L'employé comme pion dans la lutte pour la cyber-sécurité |
|---|---|

Les études ne le démentiront pas, les employés apparaissent comme l’une des causes principales, volontairement ou non, des fuites de données et des atteintes aux dispositifs de sécurité IT au sein des entreprises. Par conséquent, outre les protections adéquates contre les attaques par des hackers externes, les entreprises ont tout intérêt à passer les dispositifs de sécurité internes de leur organisation au peigne fin. La résistance de la chaîne est en effet celle de son maillon le plus faible..

L’employé en tant que hacker

Il ressort du rapport de la RAND intitulé « Markets for Cybercrime Tools and Stolen Data » que l’élément humain reste un point faible. Parfois, des actes de malveillance entrent en jeu, comme par exemple l’employé mécontent ou envieux qui disperse ou subtilise les informations confidentielles d’une entreprise. En janvier, Morgan Stanley licenciait un travailleur, qui avait prétendument subtilisé des données personnelles (en ce compris des numéros de compte) concernant près de 900 de ses clients et les avait brièvement publiées sur Internet. Néanmoins, le plus souvent, les cyber-incidents connus par une entreprise peuvent être imputés à des actes de négligence, ce dont les criminels tirent volontiers profit. Selon le rapport de la RAND, lesdites campagnes de « phishing » et « spear-phishing » augmenteront substantiellement et sont en même temps de plus en plus sophistiquées. Un exemple connu de spear-phishing concerne la fuite de données – entretemps devenue tristement célèbre – de la chaîne de magasins américaine Target. Les enquêteurs avaient découvert que les hackers avaient obtenu l’accès aux systèmes informatiques de Target au moyen d’un e-mail de spear-phishing adressé à un employé de l’un des fournisseurs externes de Target.

Les conséquences de tels actes de malveillance ou de négligence sont souvent tout sauf anecdotiques. Dans l’exemple de Target, le préjudice se chiffre actuellement à plus de 162 millions de dollars. L’attaque faite sur la marque et la perte de parts de marché constituent à cet égard des dommages importants. Les employeurs se sentent souvent impuissants dans ce genre de situation et observent les bras ballants la manière dont une cyber-attaque cause un préjudice grave à leur entreprise. Cependant, cela ne devrait pas être le cas. Ci-dessous, nous esquissons certains outils ou méthodes pouvant aider à mobiliser vos propres employés, en tant que frères d’armes privilégiés dans la lutte pour la cyber-sécurité.

L’employé en tant que pion contre les hackers

La prévention est et reste le meilleur remède. Les mesures suivantes – spécifiquement en lien avec les activités des employés – fonctionnent en tout cas comme mesures préventives :

– Des dispositifs de sécurité adéquats

Outre la sécurisation effective des données et de l’infrastructure de l’entreprise, il est recommandé de couler les règles d’entreprises concernant la protection des données, la sécurité des systèmes, l’utilisation d’appareils propres (ordinateurs portables, smartphones, tablettes) au sein du réseau de l’entreprise, le travail à distance et d’autres encore, dans ce que l’on appelle des « policies ».

– Des formations périodiques et adaptées pour les employés

Afin de pouvoir mettre en oeuvre les protocoles de sécurité mentionnés ci-dessus de manière effective, les employés au sein de l’entreprise devraient au moins être au courant de leur existence, ainsi que de leur contenu (ainsi que de toute modification), ce que l’on obtient en donnant des formations périodiques et adaptées. Un employé qui de manière durable est bien informé sur ses responsabilités en termes de cyber-sécurité au sein de l’entreprise, et qui sait comment traiter des informations sensibles et confidentielles concernant l’entreprise ou les personnes, constituera une cible moins évidente pour les hackers externes et sera plus attentif. Une telle approche met également l’accent sur l’intérêt que l’entreprise porte à la sécurité de ses propres systèmes et données.

– Un screening adéquat des nouveaux employés

Lors du recrutement et de la sélection de nouveaux employés, l’employeur scrute de plus en plus souvent le profil d’un candidat sur les réseaux sociaux (Facebook, Twitter etc.). Attention cependant : l’employeur peut consulter ces données, mais ne peut les traiter sans respecter les règles légales sur la protection des données personnelles. En outre, il existe également une interdiction de discrimination : le fait de vérifier des informations qui sont publiées par un candidat sur un réseau social ne peut mener à une sélection inéquitable.

– Prévoyez un dispositif d’alerte adéquat

Afin de révéler certains sujets, que l’employé ne peut faire remonter via la voie hiérarchique habituelle et pour lesquels il n’existe pas de procédure ou organe organisé par la loi, l’on peut prévoir un dispositif d’alerte (« whistleblowing ») au sein de l’entreprise. Ce dispositif doit être établi conformément à la législation sur la vie privée et aux recommandations de la Commission de la protection de la vie privée sur le sujet.

– Surveillance de l’utilisation d’Internet et des e-mails par les employés

Une autre mesure de prévention importante réside dans l’installation d’un système au moyen duquel le contrôle de l’utilisation d’Internet et des e-mails par les employés peut être effectué par l’employeur. En effet, une entreprise qui est victime d’une cyberattaque et suppose que l’un de ses membres du personnel en est responsable, ne peut pas rechercher l’employé coupable à la légère. L’employeur doit, à cet égard, respecter la législation sur la vie privée, en ce compris la CCT n° 81, qui met en balance le droit à la vie privée de l’employé et le droit de surveillance de l’employeur.

Un tel système de contrôle ne peut (i) être institué sans que l’employeur en ait informé le conseil d’entreprise et les employés individuellement sur tous les aspects du contrôle ; (ii) seulement être implémenté qu’en raison d’une finalité légitime, telle que par exemple la sécurité et le bon fonctionnement technique du système de réseau IT de l’entreprise. En outre, l’employeur ne peut effectuer qu’un contrôle graduel et progressif. En premier lieu, seuls les contrôles généralisés et anonymes (au moyen d’échantillons) sont autorisés sans que les données puissent être individualisées et donc sans pouvoir cibler un employé en particulier. Ce n’est que lorsque l’employeur suspecte qu’un abus par un employé a eu lieu qu’il peut procéder à l’individualisation des données personnelles afin de pouvoir rechercher le « coupable ».

Conclusion

En résumé, l’on peut dire qu’au vu des atteintes à la réputation et autres conséquences financières des cyber-incidents sur les entreprises, il vaut mieux prévenir que guérir. La mise en application des mesures décrites ci-dessus constitue en tout cas un pas dans la bonne direction.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d’entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire..

Source : <http://datanews.levif.be/ict/actualite/l-employe-comme-pion-dans-la-lutte-pour-la-cyber-securite/article-opinion-373053.html>

La sensibilisation des utilisateurs est la principale clé pour se protéger des pirates informatiques. Il n'est pas trop tard !



La sensibilisation des utilisateurs est la principale clé pour se protéger des pirates informatiques. Il n'est pas trop tard !

La sensibilisation des utilisateurs est la clé pour se protéger des pirates informatiques

L'avis de Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité (arnaques, virus, phishing...) en Direct sur LCI le 23 mai 2016 dans l'émission « Ca nous Concerne » de Valérie Expert.

En mai 2016, Denis JACOPINI nous sensibilisait encore et déjà aux **cyber risques**.

Nos formations / nos sensibilisations
Toutes nos vidéos

LE NET EXPERT ET DENIS JACOPINI FONT DÉSORMAIS PARTIE
DES PRESTATAIRES DE CONFIANCE DE LA PLATEFORME



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

Besoin d'un Expert ? contactez-nous

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

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



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



[Contactez-nous](#)

Réagissez à cet article

10 habitudes à prendre pour vous protéger des escroqueries sur le net | Denis JACOPINI



10 habitudes à
prendre pour
vous protéger
des
escroqueries
sur le net

Tout comme dans la réalité, il existe sur Internet des fraudeurs et des escrocs. Pourtant, une question vous revient sans cesse : comment se protéger des arnaques sur internet ? N'allez pas croire qu'un bon antivirus vous mettra à l'abri de n'importe quelle attaque venue du Web. Désormais, il vaut mieux prévenir que guérir (comme le dit le vieil adage). C'est pourquoi j'ai trouvé bon de vous proposer 10 habitudes à prendre pour vous protéger des escroqueries sur le net...

1°/ Si l'adresse d'un service Web qui gère des données personnelles ne commence pas par HTTPS, méfiez-vous ! Cela signifie que les données transmises sur cette adresse Web ne sont pas sûres.

2°/ Recevez-vous régulièrement des mails où on vous demande le mot de passe d'un service ? Marquez-le tout de suite comme SPAM car AUCUN service ne vous le demandera !

3°/ Si vous voulez vous connecter à vos comptes bancaires depuis Internet, vérifiez que l'option du clavier virtuel numérique de saisie du mot de passe est mis en avant. C'est un outil visuel dans lequel vous pouvez entrer le mot de passe avec les clics de souris. Toutes les bonnes banques le proposent. Vous vous protégez ainsi des keyloggers.

4°/ Si vous soupçonnez un lien trompeur, copiez l'adresse à laquelle il se lie et collez-la dans votre barre d'adresse. Ainsi, vous pouvez vérifier la direction que ce lien prend.

5°/ Si vous changez le mot de passe d'un service Web, par exemple Google, vérifiez que l'URL racine où vous vous situez est bien google.fr.

6°/ Utilisez toujours des mots de passe compliqués. Ajoutez au moins huit caractères avec des majuscules, des minuscules et des chiffres. C'est lourd à retenir, mais ça vous protégera contre les escroqueries sur le net !

7°/ Choisissez un mot de passe pour chaque site. Ne gardez jamais le même et variez.

8°/ Lorsqu'un service en ligne a été hacké par des pirates (une annonce est faite généralement), pensez à changer immédiatement votre mot de passe.

9°/ Vous avez reçu un email d'Apple avec une adresse @apple.com ? Vérifiez l'expéditeur, il se cache généralement quelque chose de louche là dedans !

10°/ Toujours garder votre navigateur et un antivirus à jour avec la dernière version. Toujours !

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.autourduweb.fr/10-habitudes-prendre-protéger-escroqueries-net/>

Mettre son établissement en conformité avec la CNIL, mode d'emploi | Denis JACOPINI



Mettre son établissement en conformité avec la CNIL, mode d'emploi

Se mettre en conformité avec la CNIL est une obligation depuis 1978.

Cependant, les préoccupations des établissements et organismes étant principalement orientées vers des réglementations sociales, fiscales et celles liées à leur métier, la réglementation numérique est longtemps restée délaissée.

En rapport direct avec l'explosion de la cybercriminalité en France, le non respect de la Loi Informatique et Libertés est de plus en plus montré du doigt et les établissements piratés ont de plus en plus leur image salie et leurs comptes bancaires siphonnés.

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés.

Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données.

UNE MISE EN CONFORMITÉ CNIL DOIT PASSER PAR UN AUDIT DE L'ENSEMBLE DE VOS SYSTÈMES DE TRAITEMENTS DE DONNÉES

Que se cache derrière cette loi ?

Quels sont les étapes indispensables et les pièges à éviter pour que cette mise en conformité ne se transforme pas en fausse déclaration ?

Plus d'information sur : www.cnil.lenetexpert.fr

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.aide.cnil.fr/selfcnil/site/template.do?id=572&back=true>

Petit manuel de contre-espionnage informatique | Denis JACOPINI

| | | | | | |
|---|---|--|--|--|--|
| Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer | | | | | |
|  <p>LE NET EXPERT AUDITS & EXPERTISES</p> |  <p>LE NET EXPERT EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES</p> |  <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITÉ</p> |  <p>LE NET EXPERT SPY DETECTION Services de détection de logiciels espions</p> |  <p>LE NET EXPERT FORMATIONS</p> |  <p>LE NET EXPERT ARNAQUES & PIRATAGES</p> |
|  <p>Partir en mission à l'étranger avec son téléphone mobile, son assistant personnel ou son ordinateur portable.</p> <p>PASSEPORT DE CONSEILS AUX VOYAGEURS</p> <p>Agence Nationale de la Sécurité des Systèmes d'Information</p> | | <h2>Petit manuel de #contre-espionnage informatique</h2> | | | |

Règle n°1 : ne jamais partir en voyage avec son ordinateur personnel, ni de travail, mais de ne voyager qu'avec un disque dur vierge de toute donnée. Règle n°2 : prenez connaissance de la législation locale. Règle n°3 : sauvegardez les données que vous emportez, "vous récupérerez ainsi vos informations à votre retour en cas de perte, de vol ou de saisie de vos équipements". Règle n°4 : évitez de partir avec vos données sensibles. "Privilégiez, si possible, la récupération de fichiers chiffrés sur votre lieu de mission en accédant :

- au réseau de votre organisme avec une liaison sécurisée, par exemple avec un client VPN mis en place par votre service informatique.

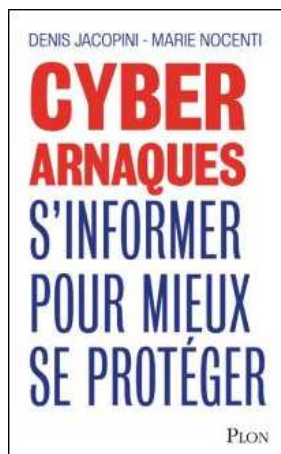
- sinon à une boîte de messagerie en ligne spécialement créée et dédiée au transfert de données chiffrées (via https) et en supprimant les informations de cette boîte après lecture".

Règle n°5 : emportez un filtre de protection écran pour votre ordinateur si vous comptez profiter des trajets pour travailler vos dossiers, afin d'éviter que des curieux lisent vos documents par-dessus votre épaule.

Règle n°6 : mettez un signe distinctif sur vos appareils (comme une pastille de couleur), "cela vous permet de pouvoir surveiller votre matériel et de vous assurer qu'il n'y a pas eu d'échange, notamment pendant le transport. Pensez à mettre un signe également sur la housse".

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

Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



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

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

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

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

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

Commandez sur Fnac.fr

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

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

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

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

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

Comment se protéger des arnaques Internet

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



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

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

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

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

Source :
<http://owni.fr/2010/05/24/petit-manuel-de-contre-espionnage-informatique>

La CGPME sensibilise les PME à la cybersécurité | Denis JACOPINI

| | |
|---|---|
|  | La CGPME sensibilise les PME à la cybersécurité |
|---|---|

La cybersécurité est un facteur de productivité, de compétitivité et donc de croissance pour les entreprises. Quelle que soit sa taille, une PME doit prendre conscience qu'elle peut être à tout moment confrontée à la cybercriminalité.

Qu'il s'agisse, par exemple, de malveillances visant à la destruction de données ou d'espionnage économique et industriel, les conséquences des attaques informatiques pour les entreprises, et plus particulièrement les TPE, sont généralement désastreuses et peuvent impacter leur pérennité. Pour la CGPME, chaque entreprise doit aujourd'hui se doter d'une politique de sécurisation des systèmes d'information inhérente à l'usage des nouvelles technologies. Si les contraintes financières des petites structures restent un frein à la construction d'une cybersécurité optimale, il existe des bonnes pratiques peu coûteuses et faciles à mettre en œuvre permettant de limiter une grande partie des risques liés à l'usage de l'informatique. Pour recenser ces usages, la Confédération, par le biais de sa Commission Economie Numérique, s'est rapprochée de l'ANSSI. Fruit d'un partenariat constructif, un guide des bonnes pratiques informatiques a été élaboré afin de sensibiliser les PME sur cette problématique tout en leur apportant les moyens opérationnels de préserver leurs systèmes d'information.

A vous désormais, chefs d'entreprises, de devenir les acteurs de votre propre sécurité !

François Asselin Président CGPME

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise. Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source : Guide des bonnes pratiques CGPME/ANSSI
http://www.lenetexpert.fr/wp-content/uploads/2015/03/guide_cgpme_bonnes_pratiques.pdf

RGPD Règlement européen sur la protection des données : ce qui change pour les professionnels



RGPD Règlement
européen sur la
protection des données
: ce qui change pour les
professionnels

Le nouveau règlement européen sur la protection des données personnelles est paru au journal officiel de l'Union européenne entrera en application le 25 mai 2018. L'adoption de ce texte doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique.

- Un cadre juridique unifié pour l'ensemble de l'UE
- Un renforcement des droits des personnes
- Une conformité basée sur la transparence et la responsabilisation
- Des responsabilités partagées et précisées
- Le cadre des transferts hors de l'Union mis à jour
- Des sanctions encadrées, graduées et renforcées
- Comment les autorités de protection se préparent-elles ?

Où trouver le texte officiel du RGPD (Règlement européen sur 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

A Lire aussi :

Mise en conformité RGPD : Mode d'emploi

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

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

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

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

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

Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

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 ;



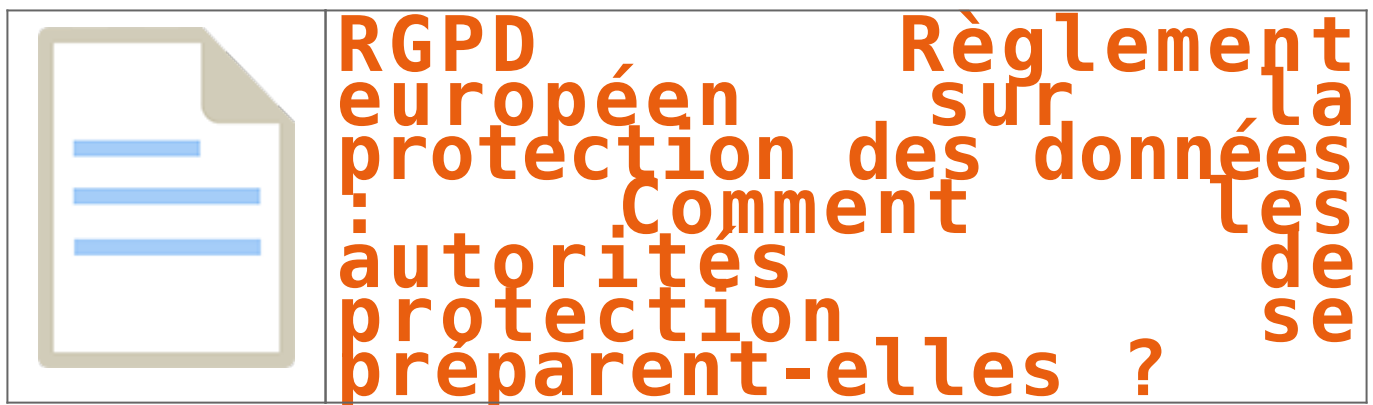
[Contactez-nous](#)



Réagissez à cet article

Source : *Règlement européen sur la protection des données : que faut-il savoir ? | Besoin d'aide | CNIL*

RGPD Règlement européen sur la protection des données : Comment les autorités de protection se préparent-elles ?



Le G29

Dans son plan d'action 2016, adopté en février 2016, le G29 a présenté ses priorités pour permettre l'application effective du règlement en avril 2018. Plusieurs groupes de travail se sont déjà mis en place pour décliner ce plan d'action.

Les 4 objectifs principaux :

1. Préparer la mise en place du Comité européen de la protection des données (CEPD), qui remplacera le G29 en 2018 ;
2. Préparer la mise en place du guichet unique et le mécanisme coopération et de cohérence entre les autorités ;
3. Proposer des lignes directrices ou des bonnes pratiques aux professionnels pour **les 4 sujets prioritaires identifiés** : le droit à la portabilité, la certification, le délégué à la protection des données (DPO), les traitements à risque d'ici la fin de 2016 ;
4. Promouvoir et diffuser le règlement afin que l'ensemble des acteurs se l'approprient.

Le G29 prévoit également la consultation régulière des parties prenantes dans une démarche itérative sur deux ans afin d'enrichir sa réflexion.

Il a organisé le 26 juillet 2016 à Bruxelles des ateliers collaboratifs. Cet espace de concertation multi-acteurs a réuni les représentants de la société civile, des fédérations professionnelles, des universitaires et des institutions européennes, autorités de protection des données autour des 4 sujets prioritaires qu'il a identifiés.

Les échanges et propositions de cette journée ont permis au G29 d'alimenter les différents groupes de travail qu'il a déjà mis en place autour de ces mêmes thèmes. L'objectif étant de décliner d'ici 2018 les principes du règlement en mesures opérationnelles correspondant aux besoins et attentes des principaux acteurs concernés par la mise en œuvre du règlement.

D'autres consultations seront organisées sur d'autres thématiques.

La CNIL

La CNIL est très impliquée dans chacun des groupes de travail mis en place par le G29, dont elle assure la Présidence jusqu'en février 2018. Elle a proposé une consultation en ligne des acteurs français **sur ces mêmes sujets**.

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

A Lire aussi :

Mise en conformité RGPD : Mode d'emploi

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

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

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

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

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

Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

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](#)

Réagissez à cet article

Source : *Règlement européen sur la protection des données : que faut-il savoir ? | Besoin d'aide | CNIL*

Qu'est ce qu'un cybercriminel ?



Cette question a été posée à Denis JACOPINI par des étudiants. Ci-dessous une réponse succincte.

Avant de répondre à cette question, il est important de poser la définition de la cybercriminalité.

La définition qui selon moi définit le mieux la cybercriminalité est celle qui considère la cybercriminalité comme une **notion large qui regroupe toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau**. (Wikipedia)

Que ça soit dans le cas d'atteintes aux biens ou d'atteintes aux personnes, il est couramment décomposé 3 types d'infractions :

- **Les infractions spécifiques aux technologies de l'information et de la communication** : parmi ces infractions, on recense les atteintes aux systèmes de traitement automatisé de données, les traitements automatisés de données personnelles (comme la cession des informations personnelles), les infractions aux cartes bancaires, les chiffrements non autorisés ou non déclarés ou encore les interceptions.
- **Les infractions liées aux technologies de l'informations et de la communication** : cette catégorie regroupe la pédopornographie, l'incitation au terrorisme et à la haine raciale sur internet, les atteintes aux personnes, les atteintes aux biens.
- **Les infractions facilitées par les technologies de l'information et de la communication**, que sont les escroqueries en ligne, la contrefaçon ou tout autre violation de propriété intellectuelle.

Ainsi, un cybercriminel est une personne qui commet au moins une de ces 3 infractions.

Les principales motivations sont :

- Gagner de l'argent (ou ne pas en dépenser ce qui revient au même) en réalisant par exemple des actes de piratages d'oeuvres intellectuelles telles que des musiques ou des films. D'autres peuvent aussi prendre le risque de chercher à en tirer des bénéfices soit en les revendant ces oeuvres, en les mettant à disposition sur des sites internet mitraillant de publicités rémunérées leurs visiteurs ou permettant le téléchargement contre un appel vers un numéro surtaxe. D'autres vont réaliser des vols d'informations (Magasins TARGET en 2013), des blocages de systèmes informatiques (TVS Monde en 2015) ou des cryptages de fichiers en demandant à l'issue de l'opération une rançon en échange de tranquillité (Laboratoires Labio en 2015, Disney en 2017) ou de rétablir le système dans son état initial, une technique semblable à celles utilisées par la mafia (Pirates informatiques : des techniques très proches de la mafia – Gilles Fontaine) ;
- Terroriser la population en répandant des messages idéologiques (+ de 25000 sites Internet piratés diffusant un message pro islamiste à la suite des attentats de Charlie Hebdo) ou bien en coupant les ressources en électricité d'une population (Ukraine en 2015 et 2016) ;
- S'attaquer à un état dans un but politique (Attaque informatique de la centrale nucléaire de Bouchehr en Iran destinée à détruire des centrifugeuses d'enrichissement d'uranium en 2010) ou militaire (Attaque de la Georgie par la Russie en 2007) ou d'espionnage (Bercy en 2011) ;
- Dans un but de montrer ses capacités ou se lancer un défi (comme David Dennis en 1974). Débrouille-vous pour faire venir aux oreilles de hackers qu'un système informatique est inattaquable, vous verrez alors fleurir des volontaires masqués qui passeront leurs journées et leurs nuits à tenter de trouver la faille dans le but de prouver leur supériorité ;

Ainsi, selon moi, un cybercriminel est un individu qui commet avec ou sans intention une ou plusieurs infractions répréhensibles concernées par le champ couvert par la cybercriminalité, sans autorisation expresse du tiers concerné, quel que soit l'intention et l'objectif poursuivis.

LE NET EXPERT

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

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DORTEFP (Numéro formateur n°93 84 63041 84).

Denis JACOPINI est Expert Juridique 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 ;
- **Conformité** (et sensibilisation) à la **Cybercriminalité** (autorisation n°93 84 63041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- **Récupération de données** : téléphones, disques durs, e-mails, contenus, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;



Contactez-nous

Réagissez à cet article

Source : *Cybercrime – Wikipédia*