

Nouvelles formations sur les déclarations à la CNIL et en cybercriminalité | Denis JACOPINI

x	Nouvelles formations sur les déclarations à la CNIL et en cybercriminalité
---	--

Pour information, Denis JACOPINI propose depuis quelques mois deux nouveaux sujets de formation à destination des chefs d'entreprise, de leurs salariés mais aussi des administrations et de leurs agents :

- **La cybercriminalité, un vrai risque pour les chefs d'entreprises- Mettre son entreprise en conformité avec la CNIL, secrets et mode d'emploi**
- **Cybercriminalité, sécurité informatique et CNIL, bonnes pratiques et cadre juridique**
- **La cybercriminalité, un vrai risque pour administrations**

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

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Etapes à suivre si vous comptez rendre votre ordinateur professionnel à votre employeur



Etapes à suivre
si vous comptez
rendre votre
ordinateur
professionnel à
votre employeur

Quelles étapes faut-il suivre avant d'effacer nos données personnelles présentes sur notre futur ancien ordinateur de fonction (sauvegarder des fichiers importants et personnelles (contacts importants, copier des fichiers et tout ce qui nous concerne (photo, pdf, CV etc..)) sur un disque dur ou un système de Cloud etc..) ?

L'ordinateur professionnel qui vous a été mis à disposition était probablement en état de marche. A moins d'avoir des circonstances ou des consignes particulières, vous devrez donc rendre cet appareil au moins dans l'état initial.

1. En premier lieu, pensez à identifier les données à sauvegarder dont il vous sera nécessaire de conserver copie. Attention aux données professionnelles frappées de confidentialité ou d'une clause de non concurrence, tel que les fichiers clients. On pourrait bien vous reprocher d'en avoir conservé une copie et de l'utiliser contre votre ancien employeur.
2. Identifiez les données ayant un caractère confidentiel et qui nécessiteront une sauvegarde dans un format protégé par un procédé tel que le cryptage ou le hashage.
3. Identifiez les données devant être conservées pendant un grand nombre d'années tels que des justificatifs d'assurance, de sinistre...
4. Identifiez les données que vous ne devez absolument pas perdre car non reproductibles (contrats, photos de mariage, des enfants, petits enfants...)
5. Identifiez les données que vous souhaitez rendre accessibles sur plusieurs plateformes (ordinateurs, téléphones, tablettes) que ça soit au bureau à la maison, en déplacement ou en vacances.

Ensuite, en fonction des logiciels permettant d'accéder à vos données, identifiez les fonctions de « Sauvegarder », « Enregistrer sous » ou d' « Export ». Vous pourrez alors choisir le support adapté.

Enfin, en fonction des critères de sécurité choisis, vous pourrez sauvegarder sur des supports adaptés soit :

- à la confidentialité (tout support numérique en utilisant un logiciel de cryptage ou de hashage tel de Truecrypt, Veracrypt, ou AxCrypt...);
- à l'intégrité (multiplier le nombre de sauvegardes en réalisant plusieurs exemplaires de vos données à n'absolument pas perdre);
- à la longévité en utilisant des supports avec une durée de vie adaptée à vos attentes. Sachez qu'à ce jour, il est difficile de garantir la lecture d'une informations numérique au delà de plusieurs dizaines d'années (en raison de l'altération des supports avec le temps, mais aussi de l'évolution des versions, des formations et des logiciels). Qui peut vous garantir de pouvoir visualiser vos photos numériques dans cinquante ans ?
- à la disponibilité sur plusieurs plateformes et sur plusieurs lieux, comme le proposent les solutions cloud qui sont éclos il y a quelques dizaines d'années seulement;
- à la quantité (car vous devez rapidement stocker pour ensuite trier et choisir un support adapté) en choisissant par exemple un disque dur USB externe auto-alimenté (si le port USB de votre ordinateur l'autorise), ce support est actuellement celui ayant le meilleur rapport capacité / prix avec une bonne rapidité d'écriture.

Les risques

Les clés USB sont des outils permettant de conserver une copie facilement accessible et aisément transportable. 100% des clés USB tomberont un jour ou l'autre en panne. Pensez-y pour ne pas leur confier les documents de votre vie.

Idem pour les disques durs. 100% des disques durs tomberont un jour en panne. Cependant, contrairement aux clés USB ou aux cartes mémoire, les disques durs (mécaniques et non SSD) permettront plus facilement de récupérer leur contenu en cas de panne.

Les supports de type lecteurs ZIP, lecteur JAZ, lecteurs magnéto-optiques, lecteurs de bandes etc. sont de plus en plus rares. Conserver des données importantes sur de tels supports peut s'avérer dangereux. En effet, imaginez un instant jour ou vous souhaitez y accéder mais que vous n'avez plus le lecteur pour les consulter et que le lecteur ne se vend même plus. Ne laissez pas la vies de vos données numériques entre les mains du bon coin...

Voilà, en fonction de tous ces critères et à partir de ces conseils, il ne vous reste plus qu'à sauvegarder vos données importantes avant de les effacer de l'appareil que vous allez rendre.

Comparatif

Disque dur : Quelques Go à quelques To – Bon marché Rapide mais fragile

Clé USB : Quelques Go – Rapide, léger mais quasiment impossible de récupérer des données en cas de panne.

Cloud : Quelques Mo à quelques To – Accessible de n'importe où mais aussi par tous ceux qui ont le mot de passe (risqué) – Dépend du fonctionnement et de la rapidité d'Internet – Les services de cloud gratuits peuvent s'arrêter du jour au lendemain et vous perdrez tout.

Disques optiques (CD, DVD, Magnéto Optique) : Bonne tenue dans le temps si conservés dans de bonnes conditions mais utilisables (pérennité des lecteurs de disques) jusqu'à quand ?

Supports spéciaux (ZIP/Jazz/OIC/DAT/DLT/DD5/SDLT) : Supports fragiles, lecteurs trop rares pour garantir une lecture au delà de 5 ans.

Denis JACOPINI anime des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux CyberRisques.

Il est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire et a été pendant a une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

<https://www.letnetexpert.fr/contact>

<https://twitter.com/lenetexpert>

<https://www.linkedin.com/in/lenetexpert>



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

- Expertises techniques (virus, espion, piratages, fraudes, attaques Internet...) et judiciaires (investigation téléphones, disques durs, e-mails, contenus, dédouanement de clients...);
- Expertises de systèmes de vote électronique;
- Formations et conférences en cybercriminalité;
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Supprimer vos données personnelles avant de donner ou recycler un ordi – FrancoisCharron.com

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

GUIDE D'HYGIÈNE INFORMATIQUE



AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION



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

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

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

LISTE DES GUIDES DISPONIBLES

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

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

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

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

Votre responsabilité engagée en cas de piratage de vos données | Denis JACOPINI



Votre
responsabilité
engagée en
cas de piratage de
vos données

Si vous vous faites pirater votre ordinateur ou votre téléphone, votre responsabilité pourrait bien être engagée vis-à-vis des données que ce support numérique renferme.

Imaginez que vous disposiez de différents appareils numériques informatiques renfermant une multitude de données, dont des données d'amis, de prospects, de clients, de fournisseurs (tout ce qu'il y a de plus normal), et tout à coup, à cause d'un malware (maliciel selon D. JACOPINI), un pirate informatique en prend possession de ces données, les utilise ou pire, les diffuse sur la toile. Que risquez-vous ?

En tant que particulier victime, pas grand chose, sauf s'il est prouvé que votre négligence est volontaire et l'intention de nuire retenue.

Par contre, en tant que professionnel, en plus d'être victime de piratage (intrusion clandestine par un fichier, un virus, un cryptovirus, un bot, un spyware), et d'avoir à assumer les conséquences techniques d'un tel acte illicite pourtant pénalement sanctionné notamment au travers de la loi goffrain du 5 janvier 1988 (première loi française réprimant les actes de criminalité informatique et de piratage), vous risquez bien de vous rendre une seconde cible vis à vis de la loi Informatique et Libertés du 6 janvier 1978.

En effet, les entreprises, les sociétés, tous ceux exerçant une activité professionnelle réglementée ou non, les associations, les institutions, administrations et les collectivités, sont tenues de respecter la loi Informatique et Libertés du 6 janvier 1978 et notamment la sécurité des données selon les termes de son Article n°34 :

Le responsable de traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

De plus, les sanctions jusqu'alors limitées à 5 ans d'emprisonnement et 300 000 euros d'amendes vont à partir du 25 mai 2018, par la mise en application du RGPD (Règlement Général sur la Protection des Données) être portées à 20 millions d'euros et 4% du chiffre d'affaire mondial.

Partons d'un cas concret.

La société Cochabonairails voit son système informatique piraté. Des investigations sont menées et le pirate informatique arrêté.

Vis à vis de la loi Goffrain du 5 janvier 1988, le voyou risque jusqu'à 2 ans de prison et 20 000 euros d'amende. Or ce dernier, après avoir découvert que la société Cochabonairails n'était pas en règle avec la CNIL la dénonça auprès de cette dernière.

Le responsable de traitement, abominablement le chef d'entreprise risquera, lui, 5 ans de prison et 300 000 euros d'amende, une peine bien supérieure à son voleur.

Est-ce bien normal ?

Non, mais pourquoi ? c'est comme ça et ça peut être le cas de toutes les entreprises, administrations et administrations françaises en cas de piratage de leurs ordinateurs, téléphones, boîtes e-mail.

Autre cas concret

Monsieur Roudbou-Maitout voit son téléphone portable mal protégé et exposé aux virus et aux pirates. Un jour il apprend par un ami que les contacts de son téléphone se sont fait pirater. Il se déplace à la Police ou à la Gendarmerie, dépose une plainte mais le voleur n'est jamais retrouvé. Qui est responsable de cette fuite d'informations ?

La première chose à savoir, c'est si ce téléphone est professionnel ou personnel. S'il est professionnel, réfère vous au cas concret précédent. Si par contre le téléphone portable est personnel, vis à vis de la loi Informatique et Libertés, les particuliers ne sont pour l'instant pas concernés par l'obligation de sécurisation des données.


Ainsi, si la faute volontaire du propriétaire de l'appareil n'est pas retenue, le seul responsable de cette fuite de données sera et restera l'auteur du piratage.

Denis JACOPINI est Expert Informatique et aussi formateur en Protection des données personnelles (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 de 62042 04).

Nous pouvons vous assister des actions de sensibilisation ou de formation à la Protection des données Personnelles, au risque informatique, à l'hygiène informatique et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

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

Denis JACOPINI



Denis JACOPINI est Expert Informatique spécialisé dans la sécurité et la protection des données personnelles.

- Expertises techniques (logs, réseaux, logiciels, hardware, logiciels, réseaux, etc.) et analyses forensiques (logiciels, données, etc.)
- Expertises de systèmes de vote électronique
- Formations et conférences en cybersécurité
- Fondateur de l'IAI (Commissariat Informatique et Internet)
- Accompagnement à la mise en conformité DGS et en cybersécurité

Le Net Expert
INFORMATIQUE
SÉCURITÉ

Réagissez à cet article
Original de l'article mis en page : Informatique et Libertés : suis-je concerné ? | CNIL

Cybercriminalité – Retour sur les principales attaques informatiques en France et dans le monde | Denis JACOPINI



Cybercriminalité – Retour sur les principales attaques informatiques en France et dans le monde qui ont fait la une

Selon la commission européenne, la cybercriminalité englobe 3 catégories d'activité criminelles :

1) Les atteintes directes à des systèmes informatiques (ou Système de traitement automatisé de données, ou encore S.T.A.D.) en perturbant leur fonctionnement, tels que les attaques par déni de services (appelé aussi denial of service attack ou aussi DOS) destinées à faire tomber un serveur (comprenez rendre inaccessible ou mettre en panne un serveur) à distance.

2) Réaliser des actes illicites en utilisant les outils numériques (escroqueries, vols de données bancaires ou personnelles, espionnage industriel, atteinte à la propriété intellectuelle, sabotage, accès frauduleux, fraudes, usurpation d'identité, phishing, création de PC zombies, contamination d'autres postes informatiques ou d'autres serveurs...)

3) Modifier le contenu d'un espace numérique pour y déposer ou diffuser des contenus illicites (pédopornographie, racisme, xénophobie).

Les cyberdélinquants n'ont d'autre objectif que de gagner beaucoup d'argent. Virus, spams, et autres botnets drainent plusieurs centaines de millions de dollars chaque année à travers le monde.

Sans nous étaler sur les 144 milliards de courriers électroniques qui transitent dans le monde chaque jour dont 70% ne sont que du spam, les 10 millions de français victimes d'actes cybercriminels et 75% de ces actes de cybercriminalité qui sont de grande envergure (Norton 2013) qui concernent les 3,2 milliards d'internautes dans le monde en 2014 (dont la moitié pour l'Asie), vous trouverez ci-dessous, par ordre anté-chronologique, quelques principaux actes cybercriminels recensés par notre Expert, Denis JACOPINI.

Vous pouvez directement contacter Denis JACOPINI [ici](#)

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](#)

30/09/2015 : Les sites Web du gouvernement thaïlandais
attaqués

[Consulter](#)

12/09/2015 : Cyberattaque contre le site officiel de la
Commission électorale centrale (CEC) de Russie

[Consulter](#)

05/08/2015 : La SNCB victime d'un piratage

[Consulter](#)

25/07/2015 : Le Pentagone visé par une cyber-attaque russe

Consulter

28/07/2015 : Les e-mails de hauts gradés de l'armée américaine piratés

Consulter

18/07/2015 : Piratage du site de rencontres adultères Ashley Madison

Consulter

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](#)

06/07/2015 : Hacking Team, société d'espionnage informatique hacké

Consulter

19/05/2015 : Un hacker a modifié en vol la puissance d'un réacteur

[Consulter](#)

14/05/2015 : Un ordinateur de Merkel touché par la cyberattaque contre le Bundestag

[Consulter](#)

14/05/2015 : Des hôtels suisses victimes d'un piratage informatique

[Consulter](#)

12/05/2015 : Kaspersky annonce être victime d'une Cyberattaque

[Consulter](#)

05/05/2015 : Arnaque aux faux virement : Vol de 15 millions d'euros à Intermarché

[Consulter](#)

29/04/2015 : Des pirates informatiques volent 5 millions de dollars à Ryanair

[Consulter](#)

10/04/2015 : Lufthansa victime d'une cyberattaque

[Consulter](#)

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](#)

05/05/2015 : Les états -Unis (Office of Personal Management) victime de piratage. Plus de 4 millions de données personnelles de personnels fédéraux piratées;
Consulter

09/04/2015 : Arte victime d'une attaque informatique
Consulter

08/04/2015 : La chaîne TV5 Monde victime d'un piratage de grande ampleur par des individus se réclamant du groupe Etat Islamique | Le Net Expert Informatique
Consulter

02/2015 : Thales aurait été la cible d'une cyberattaque

Consulter

02/01/2015 : Les données de deux millions d'abonnés du site de TF1 ont été piratées. Les hackers détiennent les RIB et autres informations sensibles de ces internautes.

Consulter

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](#)

26/12/2014 : PlayStation et Xbox victimes d'une panne après une cyber-attaque. Les joueurs de Xbox (ci-dessus) et de Playstation ne peuvent actuellement plus connecter leur console aux services en ligne en raison d'un piratage.

Consulter

21/12/2014 : Des documents internes de Korea Hydro & Nuclear Power Co. (KHNP), notamment des plans de réacteurs nucléaires sud-coréens, ont été dérobés et publiés de nouveau vers 1h30

ce dimanche sur Internet, pour la quatrième fois depuis le 15 décembre.

Consulter

19/12/2014 : Le régulateur mondial d'internet, l'Icann, a annoncé que des pirates informatiques avaient réussi à pénétrer dans ses ordinateurs.

Consulter

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](#)

18/12/2014 : Une usine métallurgique allemande a subi une cyberattaque qui a provoqué des dégâts matériels conséquents, a révélé jeudi la publication d'un rapport gouvernemental allemand, cité par le site ITworld.

Consulter

18/12/2014 : L'ICANN (Le régulateur mondial d'Internet)

victime d'un piratage informatique

Consulter

21/10/2014 : Staples a annoncé mener une enquête concernant un possible piratage de cartes de paiement, le numéro deux mondial des articles de bureau allongeant ainsi potentiellement la liste des entreprises américaines visées par une cyber-attaque.

Consulter

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](#)

14/10/2014 : Le service de stockage de documents a pris les devants et réinitialisé les comptes utilisant les informations volées. Il affirme ne pas avoir subi d'intrusion sur ses serveurs.

Consulter

02/10/2014 : JP Morgan Chase a indiqué que 76 millions de foyers et 7 millions de PME parmi ses clients avaient été piratés lors d'une attaque informatique dans le courant du mois d'août.

Consulter

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](#)

08/09/2014 : Home Depot : finalement 56 millions de cartes bancaires piratées

Consulter

16/06/2014 : Payer une rançon ou voir les données de centaines de milliers de ses clients publiées sur Internet. C'est le choix auquel devait faire face jusqu'à lundi 16 juin au soir l'entreprise de livraisons de pizzas Domino's Pizza.

Consulter

21/05/2014 : Victime d'une attaque, eBay demande à ses utilisateurs de changer de mot de passe

Les vols de données se suivent et se ressemblent (Target, Orange...). Le spécialiste de l'e-commerce, eBay, vient de communiquer sur une attaque informatique qui aurait visé ses bases de données.

[Consulter](#)

20/05/2014 : Malware BlackShades : 100 arrestations dont 29 en France

A l'origine de l'infection de plus de 500.000 ordinateurs, le logiciel espion BlackShades a donné lieu à une opération de police internationale. En France, 29 personnes ont été placées en garde à vue, en majorité des adolescents ayant avoué avoir exploité le malware.

[Consulter](#)

15/04/2014 : Les deux premiers sites internet reconnaissant avoir subi une attaque liée à la Faille Heartbleed

Au Royaume Uni, le site parental Mumsnet a été attaqué via la vulnérabilité Heartbleed.

Au Canada, l'administration fiscale CRA a admit publiquement avoir été victimes de la faille de sécurité découverte dans l'outil de chiffrement OpenSSL. (900 numéros d'assurance sociale volés) .

[Consulter](#)

12/02/2014 : Une attaque par déni de service (DDoS) a frappé de multiples serveurs aux Etats-Unis et en Europe en début de semaine. Il s'agit de [l'attaque informatique de ce type la](#)

plus grande recensée à ce jour.

Consulter

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](#)

31/01/2014 : La messagerie de Yahoo! victime d'une attaque informatique massive

Des cybercriminels se sont introduits dans des comptes email, à la recherche de données personnelles. Les utilisateurs impactés sont invités à modifier leur mot de passe.

Consulter

27/11/2013 : La chaîne américaine de grande distribution Target a été victime de pirates informatiques qui se sont procuré les coordonnées bancaires de plus de 40 millions de ses clients entre le 27 novembre et le 15 décembre. Ce piratage tombe mal en pleine période des fêtes et ses conséquences sont potentiellement désastreuses pour les

clients ainsi que pour la marque.

Consulter

28/04/2013 : L'auteur présumé de la cyberattaque contre Spamhaus arrêté

Un Néerlandais de 35 ans a été interpellé en Espagne. Il est soupçonné d'être à l'origine d'une cyberattaque fin mars contre une entreprise basée en Suisse, Spamhaus, qui fournit aux messageries des listes permettant de bloquer les mails indésirables – les fameux spams.

Consulter

15/02/2013 : Facebook a subi une attaque informatique « sophistiquée »

Le réseau social Facebook a annoncé avoir subi, le mois dernier, une attaque informatique « sophistiquée », qui n'aurait toutefois pas compromis les données de ses utilisateurs.

« Nous avons remédié au problème dans tous les appareils infectés, nous avons informé la police et commencé une vaste enquête qui se poursuit à ce jour », a ajouté le réseau.

Consulter

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](#)

02/02/2013 : Twitter touché par des attaques informatiques
Le réseau social Twitter a annoncé, vendredi 2 février, que certains de ses utilisateurs avaient été victimes d'attaques informatiques similaires à celles portées contre des sociétés et des médias américains.

Consulter

28/12/2012 : Le groupe pétrolier d'Arabie Saoudite Aramco a révélé avoir fait l'objet d'une attaque informatique de grande ampleur au milieu du mois d'août. Ce sont ainsi 30.000 postes de travail de l'entreprise qui ont été infectés par un virus informatique, provenant de l'extérieur.

Consulter

21/08/2012 : Le nouveau virus Shamoon illustre une fois de plus la progression des attaques visant de 'nouvelles'

cibles. Le virus Shamoon (ou Disttrack) semble écraser des fichiers dans les PC Windows, puis les 'master boot records'. Il en résulte que ces fichiers ne peuvent être récupérés. Or le PC ne peut être redémarré sans qu'ils soient réinstallés.

Consulter

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

29/05/2012 : Flame, le virus le plus puissant de l'histoire du cyber-espionnage ?

Découvert au Proche-Orient, ce malware circulerait depuis plus de cinq ans et viserait, comme Stuxnet, des entreprises sensibles et des sites académiques. Une nouvelle arme pour la cyber-guerre ?

Consulter

27/04/2011 : Sony s'est fait pirater en mai 2011 12700 numéros de cartes de crédit non américaines issues d'une vieille base de données.

Consulter

07/03/2011 : Bercy et plus précisément **la direction du Trésor victime d'une vaste opération de piratage** informatique

Au total, plus de cent cinquante ordinateurs du ministère ont été infiltrés et de nombreux documents piratés. La méthode des espions est classique : à partir d'une adresse e-mail piratée, le « hacker » prend le contrôle de l'ordinateur de sa cible grâce à un cheval de Troie, en l'occurrence une pièce jointe. Chacun de ses correspondants au sein de l'administration peut à son tour être infiltré.

Ingénierie sociale a encore frappé. Crédulité ou excès de confiance ?

Consulter

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

21/11/2010 : Quand le piratage informatique s'en prend au Nucléaire

Les experts sont maintenant convaincus que le virus Stuxnet a été conçu pour s'attaquer aux centrifugeuses de Natanz utilisées par Téhéran pour enrichir l'uranium.

Consulter

Pour combattre cela, les états organisent 3 branches : Cyberdéfense (atteinte à la sécurité nationale), Cybersécurité (anticipation des risques numériques) et Cybercriminalité qui est la délinquance transposée dans le monde numérique.

Des organismes sont créés ou réorganisés et des hommes embauchés :

O.C.L.C.T.I.C. : Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

D.C.R.I. : Direction centrale du Renseignement intérieur qui depuis début Mai 2014 d'appelle :

D.G.S.I. : Direction Générale de la Sécurité Intérieure

Gendarmerie Nationale

A.N.S.S.I : Agence Nationale de la Sécurité des Systèmes d'Information (créé en juillet 2009)

Cyberdouanes

B.E.F.T.I. : Brigade d'enquête sur les Fraudes aux Technologies de l'Information

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité | Denis JACOPINI



Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité

La sensibilisation et l'éducation des utilisateurs jouent un grand rôle dans la réduction des risques.

Il importe donc pour les entreprises d'encourager leurs collaborateurs à se comporter de manière cohérente, en respectant des processus et procédures communiqués clairement, dont la conception et la surveillance sont centralisées et qui couvrent la totalité des équipements en usage. Cela n'évitera peut-être pas toute tentative d'attaque mais renforcera certainement la sécurité de l'entreprise.

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

formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI et

<http://www.globalsecuritymag.fr/Les-entreprises-revoient-leur,20150826,55304.html>

Mise en conformité RGPD : Accompagnement personnalisé par des Experts

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

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
---	---	---	---	--	--



RGPD

LeNetExpert

Mise en conformité RGPD : Accompagnement personnalisé par des Experts

Alors que les entreprises sont de plus en plus sensibilisées aux risques de failles, de mise hors service de leurs systèmes (attaques DDOS) et de destruction de leurs données (via des ransomwares), elles ne pensent pas forcément que leurs outils de communication unifiée sont également concernés par les règles de protection.

- **Le chiffrement** : toutes les données, qu'elles soient stockées ou en transmission, doivent être protégées, les premières avec au minimum un chiffrement AES 128 bits et les secondes en ajoutant au moins le protocole TLS. Point important : il faut bien évidemment que les messages de tous les interlocuteurs, externes compris, soient cryptés.
- **Le pare-feu** : attention à ne pas tomber dans le piège d'une solution qui expose des applications, des serveurs ou des équipements hors du pare-feu. De plus, il faut s'assurer que les solutions gèrent correctement le parcours des données au travers des serveurs d'authentification déjà en place.
 - **Les mises à jour** : puisque les mises à jour de firmwares et autres logicielles corrigent essentiellement des vulnérabilités ou apportent des dispositifs de sécurité plus robustes, il est primordial qu'elles se fassent de manière automatique pour s'assurer que le SI est protégé le plus tôt possible. Une des approches consiste à passer par une solution en Cloud, automatiquement mise à jour par le fournisseur lui-même **mais à manier avec précaution car si vous avez déjà opté pour le Cloud, avez-vous la certitude que seuls les utilisateurs autorisés accèdent à cet espace de stockage externalisé ? Qui peut bien se connecter pendant que vous dormez ?**
- **La sécurité physique** : où se situent les données que stocke la solution de communication ? Il est essentiel d'avoir la garantie que le datacenter du fournisseur soit protégé 24/7 et qu'il soit régulièrement audité et protégé contre les intrusions physiques.
- **Changer les paramètres par défaut** : Changer tous les identifiants et mots de passe de ceux proposés par défaut pour quelque chose de plus complexe est une règle d'or en matière de cybersécurité.

« Parmi les nombreuses cyberattaques survenues en 2016, la plus célèbre fut celle lancée par le botnet Mirai qui ciblait les webcams. Or, si cette attaque a autant réussi, c'est parce que les mots de passe administrateurs par défaut de ces équipements étaient toujours actifs », dit-il.
- **Sécuriser le réseau, jusqu'aux utilisateurs** : Un segment non sécurisé du réseau est une porte d'entrée par laquelle peuvent passer les cyber-attaques pour atteindre tout le SI d'une entreprise. Les méthodes pour sécuriser le réseau comprennent l'application de restrictions d'accès, le blocage au niveau du pare-feu de certaines pièces attachées et le test régulier des failles de sécurité connues. Mais Gustavo Villardi prévient qu'il ne s'agit là que de résoudre une partie du problème. « Selon une étude récente menée par Verizon sur les failles de sécurité, l'erreur humaine continue d'être la cause principale des cyber-attaques. Les collaborateurs sont le maillon faible et les entreprises se doivent de former leur personnel pour qu'ils restent protégés en ligne et depuis quelque appareil que ce soit », témoigne-t-il.
- **L'usage à domicile** : les collaborateurs en télétravail ne bénéficient pas de l'encadrement de la DSI pour sécuriser leur accès domestique. Il est donc nécessaire de leur indiquer comment sécuriser une box pour activer le chiffrement du Wifi et passer par un VPN.
- **Les mots de passe** : des bonnes pratiques doivent être appliquées pour que les mots de passe de chaque salarié soient impossibles à deviner ; cela comprend aussi bien de la complexité dans l'enchaînement des caractères que la fréquence de remplacement des mots de passe.
- **L'accès** : les collaborateurs devraient toujours éteindre un équipement lorsqu'ils ne s'en servent pas, afin d'éviter que quelqu'un ne se connecte sur les services restés ouverts
- **Le mode privé** : l'utilisation d'un système de visioconférence uniquement avec les paramètres du mode privé évite que quelque des personnes extérieures puissent se greffer sur une conférence.

[lire l'intégralité de l'article source]

LE NET EXPERT

:

- **FORMATIONS / SENSIBILISATION (utilisateurs / chefs d'entreprises / DSI) :**
 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
 - MISE EN CONFORMITÉ RGPD / CNIL
 - ÉTAT DES LIEUX RGPD de vos traitements)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - 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 DDRTEFP (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).



- 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, contenus, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



Contactez-nous

Réagissez à cet article

Source : *Cybersécurité : les trois mesures à prendre pour protéger la communication unifiée – Global Security Mag Online*

Formations RGPD Protection des données personnelles et en Cybercriminalité

Parce que la Cybercriminalité et la Protection des données personnelles sont liés, nous couvrons ces sujets concomitamment.



NOS SERVICES :

- Formations **RGPD** (Règlement Général sur la Protection des Données) ;
- Formations en **Cybercriminalité** ;
- **Sensibilisations** à la cybercriminalité ;
- **État des lieux** RGPD ;

- **Mise en conformité** RGPD ;
 - **Analyses de risques** (PIA / DPIA) ;
- **Audits sécurité** ;

VOTRE PROFIL :

- **CLUB D'ENTREPRISES, ORDRES, FÉDÉRATIONS, CORPORATION**
: Quelles sont vos responsabilités, quels sont vos risques, quelles devraient être vos priorités ? Que ça soit en matière de Protection des Données Personnelles (RGPD) ou de cybercriminalité, faisons ensemble un état des lieux. Agir sur vos équipements ? Sensibiliser votre personnel ? Libre à vous ensuite d'agir en fonctions de nos recommandations sur les points qui vous sembleront prioritaires.
- **ÉTABLISSEMENTS / CENTRES DE FORMATION / ORGANISATEURS D'ÉVÉNEMENTS** : Que ça soit en protection des données personnelles ou en Cybercriminalité, permettez à vos stagiaires de découvrir les notions essentielles ;
- **CHEFS D'ENTREPRISE / ÉQUIPE INFORMATIQUE** : Nous vous formons dans vos locaux et réalisons en collaboration avec votre équipe informatique une analyse détaillée de vos installation à la recherche de failles et d'axes d'amélioration conformément aux règles de l'art ou de la réglementation en vigueur (RGPD).

LES SUJETS DE FORMATION :



Consultez notre catalogue

COMMENT PROTÉGER VOTRE ORGANISME DE LA CYBERCRIMINALITÉ

Durée : 2 jours ou 4 jours (2 jours tout public + 2 jours approfondissement pour techniciens/informaticiens)

VIRUS, DEMANDES DE RANÇONS, VOL DE DONNÉES... PROTÉGEZ-VOUS !

Durée : 1 jour

LES ARNAQUES INTERNET À CONNAÎTRE POUR NE PLUS SE FAIRE AVOIR

Durée : 1 jour

COMMENT BIEN UTILISER LE CLOUD

Durée : 1 jour

COMMENT PROTÉGER VOTRE IDENTITÉ ET VOTRE VIE PRIVÉE SUR INTERNET

Durée : 1 jour

DÉCOUVREZ 50 LOGICIELS GRATUITS À CONNAÎTRE ABSOLUMENT

Durée : 1 jour

RGPD CE QU'IL FAUT SAVOIR POUR NE PAS LE PAYER CHER

Durée : 1 jour

RGPD : ANALYSONS CE QUE VOUS AVEZ COMMENCÉ

Durée : 1 jour (il est recommandé d'avoir déjà mis en pratique une mise en conformité au moins 15 jours avant)

COMMENT BIEN UTILISER LES DONNÉES DANS LE CLOUD

Durée : 1 jour

À LA DÉCOUVERTE DU DARKNET (LE WEB CLANDESTIN)

Durée : 1 jour

DÉTECTER ET GÉRER LES CYBER-ATTAQUES

Durée : 2 jours

APPRENEZ À RÉALISER DES AUDITS SÉCURITÉ SUR VOTRE SYSTÈME INFORMATIQUE

Durée : 2 jours

APPRENEZ À RÉALISER DES TESTS D'INTRUSION SUR VOTRE SYSTÈME INFORMATIQUE

Durée : 2 jours

Remarque :

Un sujet peut être traité en quelques heures mais aussi en quelques jours.

Malgré un minimum de théorie à connaître, nous pouvons réaliser un mélange de ces thèmes afin de vous proposer un contenu personnalisé en fonction des thèmes et durées globales souhaités.

EN FORMAT CONFÉRENCE :

QUE NOUS RÉSERVE LA CYBERCRIMINALITÉ DANS LES 12 PROCHAINS MOIS ?

Conférence personnalisable en général sur 1h30 + 30min Questions / réponses) (Demandez le programme détaillé)

RGPD – CE QU’IL FAUT SAVOIR POUR NE PAS LE PAYER

Conférence personnalisable en général sur 1h30 + 30min Questions / réponses) (Demandez le programme détaillé)

FONCTIONNEMENT :

- Vous organisez des formations dans votre établissement ou dans des locaux adaptés : Nous pouvons animer de 1 à 6 jours de formation sur les sujets ci-dessus ;
- Vous organisez un forum ou un salon, nous pouvons préparer une conférence de 20 minutes à 1h30 ou participer à des tables rondes ;
- En faculté ou établissement scolaire, nos interventions seront de 3 à 35 heures.
- Pour une journée de formation, nos interventions sont prévues généralement prévues du mardi au jeudi (Lundi, Vendredi et Samedi sous conditions).
- Nos formations d’une journée sont prévues pour une durée de 7 heures par jour maximum.

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.



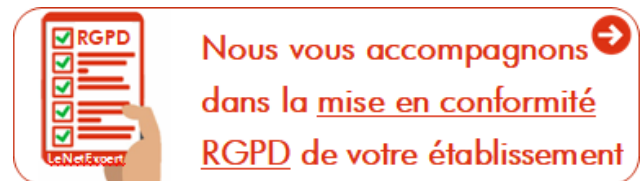
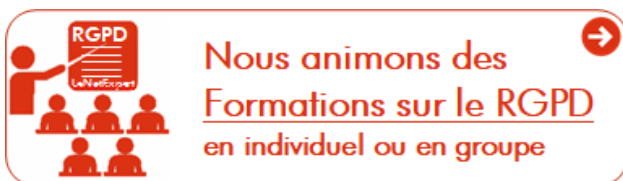
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

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"]

Formation RGPD pour devenir DPO de votre organisme – Prochaine formation les 17 18 et 19 septembre 2018 à Paris

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

 LE NET EXPERT AUDITS & EXPERTISES	 EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LE NET EXPERT fr	 LE NET EXPERT MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
--	---	--	--	---	---



Formation RGPD pour devenir DPO de votre organisme – Prochaine formation les 17 18 et 19 septembre 2018 à Paris

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.

**Formation pour DPD « Je veux devenir le Délégué à la Protection des Données de mon établissement » : 2 jours
(Mettez en place une démarche de mise en conformité RGPD)**

Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPD », 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 prochaines dates d'animation autour de chez vous ?



Je me présente : Denis JACOPINI. Je suis Expert de justice en informatique **spécialisé en cybercriminalité 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. »

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 » 3et 1 jours
- la formation « Mise en conformité RGPD sur mesure »
- un accompagnement personnalisé au RGPD

Vous souhaitez réserver une ou plusieurs place(s) 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 DPD : « **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 acompte. Si la formation était annulée (nombre de participants insuffisants ou en cas de force majeure), votre acompte 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'acompte pourra ne pas être remboursé car destiné à régler les frais de réservation de salle et d'organisation, eux même non remboursables.

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.



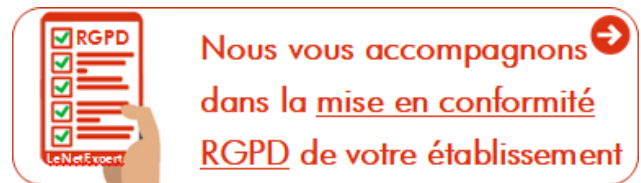
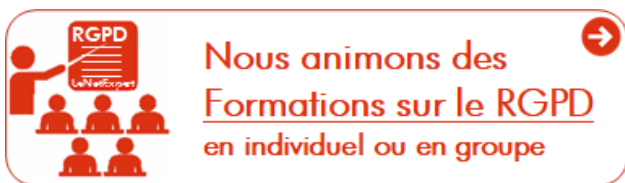
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

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