

# Cyber-Sécurité : des menaces de plus en plus présentes, mais des collaborateurs pas assez formés | Le Net Expert Informatique



La Cyber-Sécurité de plus en plus menaçante, mais des collaborateurs pas assez formés

**Les entreprises ont encore trop souvent tendance à sous-estimer le #risque lié au manque de formation de leurs équipes (hors services informatiques) à la cybersécurité. La preuve...**

Une enquête réalisée par Intel Security montre que si les collaborateurs de la DSI restent les plus #exposés aux cyberattaques (26 % au niveau européen contre 33 % en France, ce taux étant le plus élevé), les équipes commerciales et les managers (top et middle management) le sont aujourd'hui de plus en plus. En France, 18 % des commerciaux, 17 % du middle management et 14 % des dirigeants sont des #cibles potentielles. Viennent ensuite les personnels d'accueil (5 % en France, taux identique à la moyenne européenne), et le service client (seulement 7 % en France, contre 15 % au niveau européen).

Or ces types de personnel restent tous #mal formés à la sécurité informatique. Le risque est particulièrement fort au niveau des équipes commerciales avec 78 % de professionnels non formés et 75 % des personnels d'accueil. Ces taux descendent un peu pour le top management (65 % de non formés) et pour les équipes du service client (68 %). Côté middle management, la moitié est formée (51 % en France, 46 % au niveau européen).

L'enquête souligne également qu'au-delà des attaques ciblant les personnes non averties via leurs navigateurs avec des liens corrompus, les #attaques de réseaux, les #attaques furtives, les #techniques évasives et les #attaques SSL constituent une menace croissante pour les entreprises. On en recense plus de 83 millions par trimestre. Pour les contrer, les professionnels informatiques français réévaluent la stratégie de sécurité en moyenne tous les huit mois, en ligne avec les pratiques des autres pays européens sondés. 21 % mettent par ailleurs à jour leur système de sécurité moins d'une fois par an (contre 30 % en moyenne au niveau européen). Et 72 % d'entre eux (et 74 % en moyenne en Europe) sont persuadés que leur système de sécurité pourra contrer ces nouvelles générations de cyberattaques.

Or, ils se trompent. Les #attaques DDoS par exemple. Conçues pour créer une panne de réseau et permettre aux hackers de détourner l'attention de l'entreprise, tandis qu'ils se faufilent dans son système et volent des données, elles ne sont pas vraiment prises au sérieux (malgré leur augmentation +165% et leur dangerosité), puisque seuls 20 % des professionnels informatiques français estiment qu'elles constituent la principale menace pour le réseau de leur entreprise.

Au final, il existe un profond décalage entre l'évolution des attaques et la perception qu'en ont les entreprises qui ne peuvent plus négliger la formation de leurs équipes non IT.

---

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

---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.itchannel.info/index.php/articles/157059/cyber-securite-menaces-plus-plus-presentes-mais-collaborateurs-pas-formes.html>

---

# GDPR compliance: Request for costing estimate

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



**GDPR compliance:  
Request for  
costing estimate**

You seem to express an interest in the GDPR (perhaps a little by obligation) and you want to tell us about a project. We thank you for your confidence. Intervening on Data Protection missions since 2012, after having identified different types of expectations, we have adapted our offers so that they best meet your needs. Thus, we can assist you in bringing your structure into compliance in several ways :

We can assist you to learn the essentials of European regulations relating to the Protection of Personal Data and the necessary to understand and start a compliance. Once the training is completed, you are independent but can always count on our support either in the form of personalized training, or in the form of personalized support:

At the end of this training, we will give you a certificate proving the implementation of a process to bring your establishment into compliance with the GDPR (General Data Protection Regulations). For information, we are referenced to the CNIL.

1. Are you looking for autonomy ?

2. Do you want to be accompanied for the implementation of compliance ?

We carry out for you the audit which will highlight the points to be improved. At the end of this stage you can, if you wish, achieve compliance or let us proceed with the improvements that you have validated;

At the end of this audit, we will give you a report proving the implementation of corrections as part of your process to bring your establishment into compliance with the GDPR (General Data Protection Regulations).

3. Do you want to entrust all of your compliance?

In a perfectly complementary way with your IT service provider and possibly with your legal department, we can take care of the entire process of bringing your establishment into compliance with the GDPR (General Data Protection Regulation) and the various regulations relating to the protection of Personal Data.

From the audit to the follow-up, you can count on our technical and educational expertise so that your establishment is supported externally. In order to send you a personalized proposal adapted both to the needs of your structure, in accordance with your strategy and your priorities, we would like you to answer these few questions : **We guarantee extreme confidentiality on the information communicated. Persons authorized to consult this information are subject to professional secrecy.**

Do not hesitate to communicate as many details as possible, this will allow us to better understand your expectations.

Your First Name / NAME (required)  
  
Your Organization / Company (required)

Your email address (required)

A telephone number (will not be used for commercial prospecting)

You can write us a message directly in the free text area. However, if you want us to establish precise costing for you, we will need the information below.

In order to better understand your request and establish a quote, please provide us with the information requested below and click on the "Send entered informations" button at the bottom of this page for us to receive it. You will receive an answer quickly.

<b>YOUR ACTIVITY</b>	
Details about your activity :	
Are you subject to professional secrecy?	Yes@No@I don't know
Does your activity depend on regulations?	Yes@No@I don't know
If "Yes", which one or which ones?	
<b>YOUR COMPUTER SYSTEM</b>	
Can you describe the composition of your computer system. We would like, in the form of an enumeration, to know the equipment which has any access to personal data with for each device ALL the software (s) used and their function (s) .	
Examples :	
- 1 WEB server with website to publicize my activity;	
- 1 desktop computer with billing software to bill my clients;	
- 2 laptops including:	
> 1 with email software to correspond with clients and prospects + word processing for correspondence + billing software to bill my clients ...	
> 1 with email software to correspond with customers and prospects + accounting software to do the accounting for my company ;	
- 1 smartphone with email software to correspond with customers and prospects.	
Do you have one or more websites?	Yes@No@I don't know
What is (are) this (those) website (s)?	
Do you have data in the Cloud?	Yes@No@I don't know
Which cloud providers do you use?	
<b>YOUR PERSONAL DATA PROCESSING</b>	
If you have already established it, could you provide us with the list of processing of personal data (even if it is incomplete)?	
<b>SIZING YOUR BUSINESS</b>	
Number of employees in your structure :	<input type="text"/>
How many of these employees use computer equipment ?	<input type="text"/>
Number of departments or departments ** in your structure (example: Commercial service, technical service ...) :	<input type="text"/>
Please list the services or departments ** of your structure:	
<b>SERVICE PROVIDERS &amp; SUBCONTRACTORS</b>	
Do you work with sub-contractors?	Yes@No@I don't know
Please list these subcontractors :	
Do you work with service providers who work on your premises or in your agencies (even remotely) ?	Yes@No@I don't know
Please list these providers :	
How many IT companies do you work with ?	<input type="text"/>
Please list these IT companies indicating the products or services for which they operate and possibly their country of establishment :	
<b>YOUR SITUATION TOWARDS THE GDPR</b>	
Does your establishment exchange data with foreign countries ?	Yes@No@I don't know
If "Yes", with which country(ies)?	
Have you already been made aware of the GDPR ?	Yes@No@I don't know
Have people using IT equipment already been made aware of the GDPR ?	Yes@No@I don't know
If you or your employees have not been made aware of the GDPR, would you like to undergo training ?	Yes@No@I don't know
<b>YOUR WORKPLACE</b>	
The analysis of the data processing conditions in your professional premises or your professional premises is part of the compliance process.	
Do you have several offices, agencies etc. legally dependent on your establishment ?	Yes@No
If "Yes", how much ?	<input type="text"/>
In which city (ies) (and country if not in France) do you or your employees work ?	
<b>TYPE OF SUPPORT DESIRED</b>	
We can support you in different ways.	
A) We can teach you to become autonomous (training) :	
B) We can support you at the start and then help you become independent (support, audit + training) :	
C) We can choose to entrust us with the entire process of compliance (support) :	
D) We can accompany you in a personalized way (thank you to detail your expectations).	
IP barodatee est également collectée.	
What type of support do you want from us (A / B / C / D + details) ?	
<b>END OF QUESTIONNAIRE</b>	
If you wish, you can send us additional information such as:	
- Emergency of your project;	
- Any additional information that you deem useful to allow us to better understand your project.	

Les informations recueillies sont enregistrées dans la messagerie électronique et le système informatique de LenetExpert pour les traitements correspondant à la gestion de vos demandes et la proposition de services correspondant à votre demande. Le lieu de traitement de stockage et de sauvegarde se situe en France et auprès d'établissements respectant le bouclier de protection des données UE-Etats-Unis (en anglais : EU-US Privacy Shield). Elles sont conservées 3 ans après notre dernier échange et sont destinées aux services internes. Une démarche de mise en conformité a été entamée en interne depuis 2019 et jusqu'à ce jour par des formations régulières, l'identification des traitements, la réalisation d'un registre des traitements, une analyse de risques sur nos traitements manipulant des données sensibles ou des « données à caractère hautement personnel » pour lesquels leur violation pourrait avoir de graves conséquences dans la vie quotidienne des personnes concernées et un suivi semestriel. Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 dit RGPD (Règlement Général sur la Protection des Données), à la loi n°78-17 dite «Informatique et Libertés» du 6 janvier 1978 et à la Loi n° 2018-493 du 30 juin 2018 relative à la protection des données personnelles, vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier en contactant Le Net Expert, Monsieur le Délégué à la Protection des Données - 1 les Magnolias - 84300 CAVAILLOM par Remandé avec accusé de réception. Enfin, sur le fondement des articles 131-13, 222-17, 222-18, 222-18-1, 322-12, 322-13, R-621-1, R-621-2, R-623-1, R-624-3, R-624-4, R-631-1 et R634-1 du code Pénal et l'article 29 de la loi du 29 juillet 1881 sur la liberté de la presse, votre adresse Sauf indication contraire ou information publique, nous nous engageons à la plus totale discrétion et la plus grande confidentialité concernant les informations que vous nous communiquez.

\*\* = for example, commercial service, technical service, educational service, administrative and financial service ...

or send an email to [rgpd\[at\]lenetexpert.fr](mailto:rgpd[at]lenetexpert.fr)

Denis JACOPINI is our Expert who will accompany you in your compliance with the GDPR.



Let me introduce myself: Denis JACOPINI. I am an expert in sworn IT and specialized in GDPR (protection of Personal Data) and in cybercrime. Consultant since 1996 and trainer since 1998, I have experience since 2012 in compliance with the regulations relating to the Protection of Personal Data. First technical training, CNIL Correspondent (CIL: Data Protection Correspondent) then recently Data Protection Officer (DPO n° 15845), as a compliance practitioner and trainer, I support you in all your procedures for compliance with the GDPR.

« My goal is to provide all my experience to bring your establishment into compliance with the GDPR. »

---

# La cybercriminalité, un vrai risque pour les chefs d'entreprises | Denis JACOPINI



La cybercriminalité, un vrai risque  
pour les chefs d'entreprises

**Alors que le numérique fait désormais partie intégrante de nos vies personnelles et professionnelles, la sécurité est trop rarement prise en compte dans nos usages. Les nouvelles technologies, omniprésentes, sont pourtant porteuses de nouveaux risques pesant lourdement sur les entreprises.**

Par exemple, les données les plus sensibles (fichiers clients, contrats, projets en cours...) peuvent être dérobées par des attaquants informatiques ou récupérées en cas de perte ou vol d'un ordiphone (smartphone), d'une tablette, d'un ordinateur portable. La sécurité informatique est aussi une priorité pour la bonne marche des systèmes industriels (création et fourniture d'électricité, distribution d'eau...). Une attaque informatique sur un système de commande industriel peut causer la perte de contrôle, l'arrêt ou la dégradation des installations.

Ces incidents s'accompagnent souvent de sévères répercussions en termes de sécurité, de pertes économiques et financières et de dégradation de l'image de l'entreprise. Ces dangers peuvent néanmoins être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses et faciles à mettre en oeuvre dans 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

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 protection juridique du chef d'entreprise.

Contactez-nous

---

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : Denis JACOPINI

---

# Mettre son entreprise en conformité avec la CNIL, secrets et mode d'emploi

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



Denis JACOPINI



Mettre son entreprise en conformité avec la CNIL, secrets et mode d'emploi

---

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

---

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

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

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



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

Contactez-nous

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

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

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



Quelques articles sélectionnés par nos Experts :

[Comment se mettre en conformité avec le RGPD](#)

[Accompagnement à la mise en conformité avec le RGPD de votre établissement](#)

[Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles](#)

[Comment devenir DPO Délégué à la Protection des Données](#)

[Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL](#)

[Mise en conformité RGPD : Mode d'emploi](#)

[Règlement \(UE\) 2016/679 du Parlement européen et du Conseil du 27 avril 2016](#)

[DIRECTIVE \(UE\) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016](#)

[Comprendre le Règlement Européen sur les données personnelles en 6 étapes](#)

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

Réagissez à cet article

Source : Denis JACOPINI

# Les entreprises ne sont pas prêtes pour la nouvelle



# législation européenne sur la protection des données | Denis JACOPINI

 <p><b>Le Net Expert</b> <b>INFORMATIQUE</b> Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<p>Les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données</p>
---	---

Varonis a mené une enquête en mars auprès des informaticiens professionnels participant au CeBIT, le plus grand salon IT d'Allemagne, afin de recueillir leur opinion sur la nouvelle réglementation régissant la protection des données qui doit entrer en vigueur cette année ou l'année prochaine. Le constat est sans appel : les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données. Les professionnels interrogés par Varonis ne pensent pas que leurs entreprises soient en mesure de respecter les délais imposés par l'UE pour la notification des violations de données.

Il ressort de cette enquête que 80 % des personnes interrogées pensent qu'une banque sera très probablement la première entreprise à être frappée par l'amende maximale de 100 millions d'euros pour non-respect de la réglementation européenne sur la protection des données. À la question concernant le pays le plus probable de cette banque, les répondants indiquent l'Allemagne (30 %), les États-Unis (28 %) et 22 % mentionnent un autre pays européen. 48 % seulement des personnes interrogées pensent que leur entreprise pourrait signaler une violation dans le délai obligatoire de 72 heures.

Seuls 31 % disposent d'un plan leur permettant de se conformer à la nouvelle législation et seulement un tiers des personnes enquêtées a mis en place les processus et la technologie nécessaires pour empêcher leur entreprise de se voir infliger une amende importante dans le cadre de cette loi. 71 % des répondants sont incapables de dire ce que les entreprises doivent faire pour se conformer à la nouvelle réglementation.

Seuls 22 % des répondants savaient que l'amende maximale prévue par la nouvelle législation est de 100 millions d'euros, 41 % pensaient qu'elle ne serait que de 10 millions d'euros et 32 % l'estimaient à 1 million d'euros, avec un nombre réduit de personnes interrogées croyant qu'elle pouvait s'élever à un milliard d'euros. Un tiers a déclaré que la réglementation européenne sur la protection des données entrera en vigueur en 2015, 28 % ont indiqué que tel serait le cas en 2016, 7 % estiment que la loi ne verra jamais le jour et 32 % des personnes interrogées ont dit ne pas savoir quand la loi entrerait en vigueur.

« Nous pouvons attendre une refonte majeure de la loi européenne sur la protection des données au cours des prochains 12 à 24 mois », déclare David Gibson, vice-président du marketing de Varonis. « Les amendes devraient s'élever à 2 % du revenu annuel avec un plafond de 100 millions d'euros ou de dollars pour la non-protection des données personnelles des citoyens européens. Il pourrait également y avoir un nombre important de plaintes individuelles en plus des amendes et les sommes mises en jeu pourraient donc représenter des coûts substantiels, même pour les grandes entreprises. La nouvelle loi marquera aussi le passage d'un environnement autoréglementé à un régime d'application obligatoire qui aura une incidence sur toute entreprise stockant des informations d'identification personnelle concernant les citoyens européens (y compris sur les sociétés américaines menant des activités dans l'UE). Les entreprises doivent être préparées à protéger les données de leurs clients et prouver qu'elles le font avec le soin approprié, rendre compte de toute violation et supprimer les données à la demande des citoyens de l'UE. »

« Compte tenu de la vaste portée de la nouvelle réglementation et de l'importance accrue des amendes, cette enquête révèle des inquiétudes très importantes quant aux efforts que les entreprises sont prêtes à fournir pour se conformer aux conditions de la réglementation et gérer les scénarios de violation de données », indique Mark Deem, partenaire de Cooley LLP au Royaume-Uni. « En fait, l'échelle des amendes potentielles sera plus proche de celles infligées pour corruption ou violation antitrust, ou dans le secteur des services financiers. La conformité en matière de protection des données sera tout aussi importante que la conformité aux réglementations de la FCA. Même si la législation n'entre pas en vigueur avant 2017, un travail considérable doit être accompli par ceux qui souhaitent offrir des biens et des services aux habitants de l'UE et s'assurer qu'ils se trouvent dans la meilleure situation possible pour respecter la loi. »

Varonis propose 7 conseils pour garantir la conformité des données non structurées et permettre aux entreprises de se préparer à la réglementation européenne sur la protection des données :

1. Minimiser la collecte des données : la proposition de loi de l'UE comporte de fortes exigences en ce qui concerne la limitation des données recueillies auprès des consommateurs.
2. Favoriser le signalement des violations de données : la notification des atteintes à la protection des données constitue une nouvelle exigence que les entreprises européennes devront respecter.
3. Conserver les données avec attention : les règles de minimisation de la nouvelle loi concernent non seulement l'étendue des données collectées, mais aussi leur durée de rétention. En d'autres termes, une entreprise ne doit pas stocker les données plus longtemps que nécessaire aux fins prévues.
4. Nouvelle définition des identifiants personnels : l'UE a étendu la définition des identifiants personnels et ce changement s'avère important parce que les lois de l'UE portent sur la protection de ces identifiants.
5. Employez un langage clair : il faudra à une entreprise le consentement préalable et explicite des consommateurs lors de la collecte des données.
6. Bouton d'effacement : le « droit d'effacement » signifie qu'en cas de retrait du consentement accordé par les consommateurs, les sociétés devront supprimer les données concernées.
7. Le Cloud computing n'échappe pas à cette nouvelle loi de l'UE, car celle-ci suit les données.

#### Méthodologie de l'enquête

Les 145 personnes interrogées constituent un échantillon représentatif des participants du plus grand salon informatique d'Allemagne qui a compté 221 000 visiteurs en mars 2015. Parmi les répondants, 16 % sont issus de banques allemandes, 3 % de banques américaines, 3 % de banques européennes, 45 % d'entreprises allemandes hors du secteur financier, 26 % d'entreprises européennes hors du secteur financier et 7 % d'entreprises américaines.

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

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.infodsi.com/articles/157046/entreprises-sont-pas-pretes-nouvelle-legislation-europeenne-protection-donnees.html>

# Guide du Cloud Computing et des Datacenters à l'attention des collectivités locales | Denis JACOPINI



# Guide du Cloud Computing et des Datacenters à l'attention des collectivités locales

## A l'attention des collectivités locales

Les concepts de Cloud Computing et de Datacenters suscitent un fort intérêt de la part des collectivités locales, mais soulèvent également de nombreuses questions.

La Direction Générale des Entreprises, la Caisse des Dépôts et le Commissariat Général à l'Égalité des territoires proposent un guide pratique pour orienter les collectivités locales dans leurs réflexions.

- Comment répondre aux nouveaux besoins et disposer rapidement de nouvelles ressources informatiques ?
- Comment gérer et administrer facilement les ressources nécessaires à l'ensemble des services ?
- Comment assurer la disponibilité en continu de ces services ?
- Comment garantir l'interopérabilité des plateformes et la pérennité des solutions technologiques ?
- Comment gérer les problématiques de confidentialité et de sécurité des données ?
- Comment maîtriser les coûts de construction et d'exploitation des solutions ?
- Quels changements ces solutions imposent-elles dans le fonctionnement des Dsi et des services numériques ?
- Comment contractualiser avec les fournisseurs de services et maîtriser la relation client – fournisseur ?
- Quelles sont les contraintes liées à la construction et à la maintenance d'un Datacenter ?
- Comment mesurer la rentabilité d'un Datacenter ?
- Quelle est la pérennité des investissements dans les Datacenters locaux ou Datacenters de proximité implantés sur le territoire ?
- Quelle stratégie adopter pour mutualiser les projets et conserver la maîtrise des coûts ?

Ce guide a ainsi pour mission d'apporter un éclairage sur les différents concepts et de proposer aux collectivités un ensemble de solutions et de moyens pour réussir leurs projets.

Il s'adresse à la fois aux élus locaux, aux responsables du développement économique des territoires, aux responsables informatiques, aux opérationnels au sein des collectivités, associations et structures de mutualisation, ainsi qu'à tous les acteurs publics et privés de ces écosystèmes.

---

Nous organisons régulièrement, en collectivité ou auprès des CNFPT des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité 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

---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.entreprises.gouv.fr/secteurs-professionnels/guide-du-cloud-computing-et-des-datacenters>

---

# Comment bien choisir ses mots de passe ?

✖	Comment bien choisir ses mots de passe ?
---	--

---

Les mots de passe sont une protection incontournable pour sécuriser l'ordinateur et ses données ainsi que tous les accès aux services sur Internet. Mais encore faut-il en choisir un bon. Un bon mot de passe doit être difficile à deviner par une personne tierce et facile à retenir pour l'utilisateur.

### Qu'est ce qu'un bon mot de passe ?

Un bon de passe est constitué d'au moins **12 caractères** dont :

- des lettres majuscules
- des lettres minuscules
- des chiffres
- des caractères spéciaux

Un mot de passe est d'autant plus faible qu'il est court. L'utilisation d'un alphabet réduit ou de mot issu du dictionnaire le rend très vulnérable.

Les mots du dictionnaire ne doivent pas être utilisés.

Aussi à proscrire, les mots en relation avec soi, qui seront facilement devinables : nom du chien, dates de naissances...

Réseaux sociaux, adresses mail, accès au banque en ligne, au Trésor public, factures en ligne.

Les accès sécurisés se sont multipliés sur internet.

Au risque de voir tous ses comptes faire l'objet d'utilisation frauduleuse, il est impératif de **ne pas utiliser le même mot de passe** pour des accès différents.

Alors, choisir un mot de passe pour chaque utilisation peut vite devenir un vrai casse-tête.

### Comment choisir et retenir un bon mot de passe ?

Pour créer un bon mot de passe, il existe plusieurs méthodes :

#### La méthode phonétique

Cette méthode consiste à utiliser les sons de chaque syllabe pour créer une phrase facilement mémorisable.

Exemple : « j'ai acheté huit cd pour cent euros ce après-midi » donnera : ght8CD%E7am

#### La méthode des premières lettres

Utiliser les premières lettres d'une phrase en variant majuscules, minuscules et caractères spéciaux.

Exemple : « un tiens vaut mieux que deux tu l'auras » donnera : lTvmQ2tl@

#### Diversifier facilement les mots de passe

Opter pour une politique personnelle avec, par exemple, un préfixe pour chaque type d'activité. Comme BANQUE-MonMotDePassz pour la banque, IMP-MonMotDePasse pour les impôts.

Quelque chose de très facile à mémoriser qui complexifie votre mot de passe et, surtout, vous permet de le diversifier.

#### Diminuer les imprudences

Pour finir, il est utile de rappeler de **ne pas stocker ses mots de passe à proximité de son ordinateur** si il est accessible par d'autres personnes. L'écriture sur le post-it déposé sous le clavier est à proscrire par exemple, de même que le stockage dans un fichier de la machine.

En règle général, les logiciels proposent de **retenir les mots de passe**, c'est très **tentant mais imprudent**. Si votre ordinateur fait l'objet d'un piratage ou d'une panne, les mots de passe seront accessibles par le pirate ou perdus.

#### Que faire en cas de piratage ?

Il est recommandé de préserver les traces liées à l'activité du compte.

Ces éléments seront nécessaires en cas de dépôt de plainte au commissariat de Police ou à la Gendarmerie.

Exemple

#### Compte email piraté

Vos contacts ont reçu des messages suspects envoyés de votre adresse.

Contactez-les pour qu'ils conservent ces messages.

Ils contiennent des informations précieuses pour l'enquêteur qui traitera votre dépôt de plainte.

Récupérez l'accès à votre compte afin de changer le mot de passe et re-sécurisez l'accès à votre compte.

#### Changer de mots de passe régulièrement

Cette dernière règle est contraignante mais assurera un niveau supérieur de sécurité pour vos activités sur Internet.

Un **bon mot de passe doit être renouvelé plusieurs fois par an** et toujours en utilisant les méthodes décrites ci-dessus.

---

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs aux **risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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



Réagissez à cet article

Original de l'article mis en page : Comment choisir ses mots de passe ? / Cybercrime / Dossiers / Actualités – Police nationale – Ministère de l'Intérieur

---

# Pourquoi, malgré le danger connu, cliquons nous sur des e-mails d'expéditeurs

# inconnus ?



Pourquoi, malgré le danger connu, cliquons nous sur des e-mails d'expéditeurs inconnus ?

---

Selon une enquête de la FAU (University of Erlangen-Nuremberg), près de la moitié des utilisateurs cliqueraient sur des liens d'expéditeurs inconnus (environ 56% d'utilisateurs de boîte mails et 40% d'utilisateurs de Facebook), tout en étant parfaitement conscient des risques de virus ou d'autres infections.

Le site d'information Français Pure Player Atlantico a interrogé à ce sujet Denis JACOPINI, Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles

**Atlantico :**  
Pourquoi donc, selon vous, le font-ils malgré tout ? Qu'est-ce qui rend un mail d'un inconnu si attirant, quitte à nous faire baisser notre garde ?

**Denis JACOPINI :**  
Ça vous est très probablement déjà arrivé de recevoir un e-mail provenant d'un expéditeur anonyme ou inconnu. Avez-vous résisté à cliquer pour en savoir plus ? Quels dangers se cachent derrière ces sollicitations inhabituelles ? Comment les pirates informatiques peuvent se servir de nos comportements incontrôlables ?

Aujourd'hui encore, on peut comparer le courrier électronique au courrier postal. Cependant, si l'utilisation du courrier postal est en constante diminution (-22% entre 2009 et 2014), l'usage des messages électroniques par logiciel de messagerie ou par messagerie instantanée a lui par contre largement augmenté. Parmi les messages reçus, il y a très probablement des réponses attendues, des informations souhaitées, des messages de personnes ou d'organismes connus nous envoyant une information ou souhaitant de nos nouvelles et quelques autres messages que nous recevons avec plaisir de personnes connues et puis il y a tout le reste, les messages non attendus, non désirés qui s'appellent des spams.

En 2015, malgré les filtres mis en place par les fournisseurs de systèmes de messagerie, il y avait tout de même encore un peu plus de 50% de messages non désirés.

Parmi ces pourriels (poubelle « e-mail ») se cachent de nombreux messages ayant des objectifs malveillants à votre égard. Les risques les plus répandus sont les incitations au téléchargement d'une pièce jointe, au clic sur un lien renvoyant vers un site Internet piégé ou vous proposer d'échanger dans le but de faire « copain copain » et ensuite vous arnaquer.

La solution : ne pas cliquer sur un e-mail ou un message provenant d'un inconnu, de la même manière qu'on apprend aux enfants de ne pas parler à un inconnu. Pourtant, des millions de personnes en France se font piéger chaque année. Pourquoi ?

A mon avis, les techniques d'ingénierie sociale sont à la base de ces correspondances. L'ingénierie sociale est une pratique qui exploite les failles humaines et sociales. L'attaquant va utiliser de nombreuses techniques dans le but d'abuser de la confiance, de l'ignorance ou de la crédulité des personnes ciblées.

Imaginez, vous recevez un message ressemblant à ça :

« Objet : changements dans le document 01.08.16  
Expéditeur : Prénom et Nom d'une personne inconnue  
Bonjour,  
Nous avons fait tous les changements nécessaires dans le document.  
Malheureusement, je ne comprends pas la cause pour la quelle vous ne recevez pas les fichiers jointes.  
J'ai essayé de remettre les fichiers jointes dans le e-mail. »

Dans cet exemple, on ne connaît pas la personne, on ne connaît pas le contenu du document, mais la personne sous-entend un nouvel envoi qui peut laisser penser à une ultime tentative. Le document donne l'impression d'être important, le ton est professionnel, il n'y pas trop de faute d'orthographe. Difficile de résister au clic pour savoir ce qui se cache dans ce mystérieux document.

Un autre exemple d'e-mail ou similaire souvent reçu :

« Objet : Commande – CD2533  
Expéditeur : Prénom et Nom d'une personne inconnue  
Madame, Monsieur,  
Nous vous remercions pour votre nouvelle « Commande – CD2533 ».  
Nous revenons vers vous au plus vite pour les délais  
Meilleures salutations,  
VEDISCOM SECURITE »

En fait, bien évidemment pour ce message aussi, la pièce jointe contient un virus et si le virus est récent et s'il est bien codé, il sera indétectable par tous les filtres chargés de la sécurité informatique de votre patrimoine immatériel. Auriez-vous cliqué ? Auriez-vous fais partie des dizaines ou centaines de milliers de personnes qui auraient pu se faire piéger ?

Un autre exemple : Vous recevez sur facebook un message venant à première vue d'un inconnu mais l'expéditeur a un prénom que vous connaissez (par exemple Marie, le prénom le plus porté en France en 2016). Serait-ce la « Marie » dont vous ne connaissez pas le nom de famille, rencontrée par hasard lors d'un forum ou d'une soirée qui vous aurait retrouvé sur Facebook ? Dans le doute vous l'acceptez comme amie pour en savoir plus et engager pourquoi pas la conversation. C'est un autre moyen utilisé par les pirates informatiques pour rentrer dans votre cercle d'amis et probablement tenter des actes illicites que je ne détaillerai pas ici.

Vous rappelez-vous avoir accepté une demande de mise en contact provenant d'un inconnu sur Facebook ? Peut-être que vous ne connaissez pas les risques, mais qu'est-ce qui vous a poussé à répondre à un inconnu ? La politesse ? La curiosité ?

A mon avis, le principal levier utilisé pour pousser les gens à cliquer sur les emails pour en voir l'objet, cliquer sur les pièces jointes pour en voir le contenu ou cliquer sur les liens pour découvrir la suite, est une des nombreuses failles humaine : la curiosité.

Cette curiosité peut nous faire faire des choses complètement irresponsables, car on connaît les dangers des pièces jointes ou des liens dans les e-mails. Malgré cela, si notre curiosité est éveillée, il sera difficile de résister au clic censé la satisfaire.

Il est clair que la curiosité positive est nécessaire, mais dans notre monde numérique où les escrocs et pirates oeuvrent en masse le plus souvent en toute discrétion et en toute impunité, la pollution des moyens de communication numériques grand public est telle que le niveau de prudence doit être augmenté au point de ne plus laisser de place au hasard. Le jeu vaut-il vraiment la chandelle face aux graves conséquences que peut engendrer un simple clic mal placé ?

---

Denis Jacopini anime des conférences et des formations et est régulièrement invité à des tables rondes en France et à l'étranger pour sensibiliser les décideurs et les utilisateurs aux CyberRisques (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°33 04 0303 94).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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

---

 Réagissez à cet article

Original de l'article mis en page : One in two users click on links from unknown senders > FAU.EU

# Déplacements professionnels. Attention au Wi-Fi de l'hôtel...

 Déplacements professionnels. Attention au Wi-Fi de l'hôtel...



De nos jours, qui réussit à se passer d'Internet plus d'une journée, en vacances, en déplacement, lors d'une conférence ou au travail ? Nos vies aujourd'hui digitalisées nous poussent à nous connecter quasi automatiquement au premier réseau Wi-Fi disponible, quitte à mettre la confidentialité de nos données en danger.

Cela devient d'actualité plus problématique lorsque nous voyageons : une étude Kaspersky Lab révélait récemment que 52% des personnes interrogées se connectent à des réseaux Wi-Fi gratuits non sécurisés dans des terminaux d'aéroports, des hôtels, des cafés ou des restaurants.

Dans la rubrique de sécurité, Tammy de Costant, Directeur général de Kaspersky Lab France et dirige du Nord analyse les vulnérabilités des réseaux Wi-Fi dans les hôtels, une mise d'ur pour des cybercriminels en quête de données personnelles ou d'informations confidentielles.

Depuis 10 ans, le cyber crime s'est largement professionnalisé pour devenir un véritable industrie, portée sur la rentabilité. Les cybercriminels sont en quête permanente de victimes qui leur assurent un maximum de gains pour un minimum d'investissements techniques.

De son côté, l'industrie hôtelière a pu et se transforme pour répondre aux nouvelles attentes digitales de ses clients. Alors que plus d'un quart d'entre eux annoncent qu'ils renonceraient de séjourner dans un hôtel ne proposant pas de Wi-Fi, la technologie n'est plus un luxe mais bien une question de survie pour les établissements hôteliers. Face aux ruptures liées à la numérisation, il a donc fallu remettre les modèles existants et s'équiper, parfois en tête, de nouvelles technologies mal maîtrisées. Il n'était donc pas surprenant de voir émerger rapidement des problèmes de sécurité, dans les hôtels bon marché comme dans les 5 étoiles.

Par Tammy de Costant, Directeur général de Kaspersky Lab France et Afrique de Nord

**Le paradoxe de Wi-Fi à l'hôtel : privé mais public**

Il a été très décrié dans les médias récemment, que les Wi-Fi hôteliers restent des points d'accès publics. Ils sont même parfois complètement ouverts. Le processus de connexion, qui nécessite le plus souvent de confirmer son identité et son numéro de chambre, limite l'accès au réseau mais ne chiffre pas les communications. Il ne garantit pas non plus leur confidentialité. Est-ce que cela signifie que nos informations sont à la portée de tous ? La réalité n'est pas aussi sombre, mais elles sont à la portée de ce qu'on appelle un pirate. Les cybercriminels sont en quête permanente de victimes qui leur assurent un maximum de gains pour un minimum d'investissements techniques.

Concrètement, il suffit à un criminel de se positionner physiquement entre l'utilisateur et le point de connexion pour récupérer toutes les données qui transitent par le réseau, qu'il s'agisse d'emails, de données bancaires ou encore de notes de route de passage qui lui donneront accès à tous les comptes de l'Internet. Une approche plus sophistiquée consiste à utiliser une connexion Wi-Fi non sécurisée pour piéger un utilisateur, en créant par exemple des fenêtres pop-up malveillantes qui invitent faussement l'utilisateur à mettre à jour un logiciel légitime comme Windows.

**Le mythe de la victime idéale**

En 2014, le groupe de cybercriminels Darkhotel avait utilisé une connexion Wi-Fi pour infiltrer un réseau d'hôtel de luxe et espionner quelques-uns de leurs clients les plus prestigieux. Un an plus tard, les activités de ce groupe étaient toujours en cours, continuant d'exploiter les données des dirigeants d'entreprises et dignitaires. Pour autant, les cybercriminels ne ciblent pas que des victimes à hauts profils. Beaucoup d'utilisateurs continuent de penser qu'ils ne courent aucun risque car les informations qu'ils partagent sur Internet ne méritent pas d'être piratées. C'est oublier que la rentabilité d'une attaque repose aussi sur le nombre de victimes. Parmi les 30 millions de clients pris en charge par l'hôtellerie française chaque année, seuls 20% sont des clients d'affaires. Les 80% de voyageurs de loisirs représentent donc une masse financière tout aussi importante pour des cybercriminels en quête de profits.

Dans certains cas, une faille Wi-Fi peut même espionner l'hôtel lui-même, en servant de porte d'entrée vers son réseau. Si l'on prend le cas d'une chaîne d'hôtellerie internationale qui disposerait d'un système de gestion centralisé et automatisé, une intrusion sur le réseau pourrait entraîner la vol à grande échelle d'informations confidentielles et bancaires sur les employés. Le fonctionnement de l'hôtel et ses clients.

**Hôtels indépendants vs. chaînes hôtelières : des contraintes différentes pour un même défi**

Pour une industrie aussi fragmentée que celle de l'hôtellerie, la sécurité est sans aucun doute un défi. Les hôtels indépendants ont une capacité d'accueil réduite et traitent donc moins de données. Le revers de la médaille est qu'ils disposent souvent d'une expertise informatique limitée et leur taille ne permet pas de réaliser les économies d'échelle qui rentabiliseraient un investissement important dans la sécurité informatique. Quant aux grands groupes, qui comptent des ressources humaines et financières plus importantes, ils sont mis à mal par l'échelle de leur écosystème, qui rend difficile l'harmonisation d'une politique de sécurité sur des centaines, voire des milliers de sites.

Il est important que tous les hôtels, quelle que soit leur taille ou leur catégorie, respectent quelques règles simples à commencer par l'isolation de chaque client sur le réseau. L'utilisation de technologies de chiffrement et l'installation de solutions de sécurité professionnelles. Enfin, le réseau Wi-Fi offert aux clients ne doit jamais être connecté au reste du système informatique de l'hôtel, afin d'éviter qu'une petite infection ne se transforme en épidémie généralisée. En respectant ces règles, la sécurité pourrait devenir un argument commercial au moins aussi efficace que le Wi-Fi.

Article original de Robert Nasson

Denis JACOPINI est Expert Informatique et aussi formateur en Cybercriminalité (Autorisation de la Direction du travail de l'Église et de la Formation Professionnelle n°03 84 03041 04).

Nous pouvons vous aider des actions de sensibilisation 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.limemexpert.fr/formation-en-cybercriminalite-et-en-protection-des-donnees-personnelles>

Denis JACOPINI

Original de l'article mis en page : Etude Kaspersky sur le Wi-Fi à l'hôtel... | InfoTravel.fr

# Sensibilisations et Formations à la Cybercriminalité et au RGPD (Protection des données personnelles) – Redirect

Parce que la Cybercriminalité et la Protection des données personnelles sont liés, nous couvrons ces sujets concomitamment (Intervention en France et étranger)

Nos formations sont personnalisées en fonction du type de publics présent (Dirigeants, cadres , informaticiens, responsable informatique, RSSI, utilisateurs).

Contactez-nous

## PROGRAMME

### **CYBERCRIMINALITÉ**

## **COMMENT PROTÉGER VOTRE ORGANISME DE LA CYBERCRIMINALITÉ**

### Présentation

La France a rattrapé son retard en matière d'équipement à Internet mais à en voir les dizaines de millions de français victimes chaque année, les bonnes pratiques ne semblent toujours pas intégrées dans vos habitudes.

Piratages, arnaques, demandes de rançons sont légions dans ce monde numérique et se protéger au moyen d'un antivirus ne suffit plus depuis bien longtemps.

Avons-nous raison d'avoir peur et comment se protéger ?

Cette formation couvrira les principaux risques et les principales solutions, pour la plupart gratuites, vous permettant de protéger votre informatique et de ne plus faire vous piéger.

### Objectifs

Découvrez les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant de naviguer sur Internet en toute sécurité.

Demande d'informations

### **CYBERCRIMINALITÉ**

## **LES ARNAQUES INTERNET A CONNAÎTRE POUR NE**

## **PLUS SE FAIRE AVOIR**

### Présentation

Que vous vous serviez d'Internet pour acheter, vendre, télécharger ou communiquer, un arnaqueur se cache peut-être derrière votre interlocuteur.

Quels sont les signes qui ne trompent pas ? Comment les détecter pour ne pas vous faire piéger ?

### Objectifs

Découvrez les mécanismes astucieux utilisés par les arnaqueurs d'Internet dans plus d'une vingtaine cas d'arnaques différents. Une fois expliqués, vous ne pourrez plus vous faire piéger.

[Demande d'informations](#)

## **PROTECTION DES DONNÉES**

### **RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES) – CE QU'IL FAUT SAVOIR POUR NE PAS LE PAYER CHER**

#### Présentation

Le Règlement Général sur la Protection de Données (RGPD) est entré en application le 25 mai 2018 et toutes les entreprises, administrations et associations ne se sont pas mises en conformité. Or, quelle que soit leur taille, elles sont toutes concernées et risqueront, en cas de manquement, des sanctions financières jusqu'alors inégalées.

Au delà de ces amendes pouvant attendre plusieurs millions d'euros, de nouvelles obligations de signalement de piratages informatiques risquent désormais aussi d'entacher votre réputation. Quelle valeur lui donnez vous ? Serez-vous prêt à

la perdre pour ne pas avoir fait les démarches dans les temps ?

Cette formation non seulement répondra la plupart des questions que vous vous posez, vous offrira des éléments concrets non seulement pour initier la mise en conformité de votre établissement mais surtout pour transformer ce qui peut vous sembler à ce jour être une contrainte en une véritable opportunité.

## Objectifs

Cette formation a pour objectif de vous apporter l'essentiel pour comprendre et démarrer votre mise en conformité avec le RGPD dans le but à la fois de répondre à la réglementation et de prévenir en cas de contrôle de la CNIL.

## Informations complémentaires

[Demande d'informations](#)

# **PROTECTION DES DONNÉES**

## **RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES) – ANALYSONS CE QUE VOUS AVEZ COMMENCÉ**

### Présentation

Après avoir suivi notre formation vous permettant de comprendre l'intérêt d'une telle réglementation et de savoir ce qu'il faut mettre en place pour bien démarrer, vous souhaitez aller plus loin dans la démarche de mise en conformité avec le RGPD.

Après un retour éclair sur les règles de base, nous ferons un point sur la démarche de mise en conformité que vous avez initiée ces derniers mois dans votre établissement. Nous détaillerons ensuite les démarches à réaliser en cas de

détection de données sensibles et d'analyse d'impact. Enfin, nous approfondirons des démarches périphériques essentielles pour répondre à vos obligations.

### Objectifs

Après avoir déjà découvert l'essentiel pour comprendre et démarrer votre mise en conformité avec le RGPD, cette formation aura pour objectif de vous perfectionner afin de devenir référent protection des données ou DPO (Data Protection Officer = Délégué à la Protection des Données).

[Demande d'informations](#)

## **CYBERSÉCURITÉ**

### **DÉTECTER ET GÉRER LES CYBER-ATTAQUES**

#### Présentation

Que vous ayez déjà été victime d'une cyber-attaque ou que vous souhaitiez l'anticiper, certaines procédures doivent absolument être respectées pour conserver un maximum de preuves et pouvoir les utiliser.

#### Objectifs

Que votre objectif soit de découvrir le mode opératoire pour savoir quelles sont les failles de votre système ou si vous avez été victime d'un acte ciblé avec l'intention de vous nuire, découvrez les procédures à suivre.

[Demande d'informations](#)

## **CYBERSÉCURITÉ**

# **APPRENEZ À RÉALISER DES AUDITS SÉCURITÉ SUR VOTRE SYSTÈME INFORMATIQUE**

### Présentation

Votre système informatique a très probablement de nombreuses vulnérabilités présentées aux pirates informatiques comme de nombreux moyens de nuire à votre système informatique.

Avant de procéder à un test d'intrusion, apprenez à réaliser l'indispensable audit sécurité de votre système informatique afin d'appliquer les mesures de sécurité de base présentes dans les référentiels internationalement utilisés.

### Objectifs

Vous apprendrez au cours de cette formation la manière dont doit être mené un audit sécurité sur un système informatique, quelques référentiels probablement adaptés à votre organisme et nous étudierons ensemble le niveau de sécurité informatique de votre établissement.

[Demande d'informations](#)

## **CYBERSÉCURITÉ**

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

### Présentation

Cette formation vous apporte l'essentiel de ce dont vous avez besoin pour adopter l'approche du Hacker pour mieux s'en protéger en élaborant vos tests de vulnérabilité, mettre en place une approche offensive de la sécurité informatique permettant d'aboutir à une meilleure sécurité et réaliser des

audits de sécurité (test d'intrusion) au sein de votre infrastructure.

La présentation des techniques d'attaques et des vulnérabilités potentielles sera effectuée sous un angle « pratique ».

## Objectifs

Cette formation vous apportera la compréhension technique et pratique des différentes formes d'attaques existantes, en mettant l'accent sur les vulnérabilités les plus critiques pour mieux vous protéger d'attaques potentielles.

## Demande d'informations

### **QUI EST LE FORMATEUR ?**

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

Il anime dans toute le France et à l'étranger des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles.

A ce titre, il intervient régulièrement sur différents médias et sur La Chaine d'Info LCI pour vulgariser les sujets d'actualité en rapport avec ces thèmes.

Spécialisé en protection des données personnelles, il accompagne les établissements dans leur mise en conformité CNIL en les accompagnant dans la mise en place d'un Correspondant Informatique et Libertés (CIL).

Enfin, il intervient en Master II dans un centre d'Enseignement et de Recherche en Informatique, en Master Lutte contre la Criminalité Financière et Organisée, au Centre National de la Fonction Publique Territoriale et anime le blog [LeNetExpert.fr](http://www.leNetExpert.fr) sur lequel il partage et publie de très nombreuses informations sur ses thèmes de prédilection.

Denis JACOPINI peut facilement être contacté sur :  
<http://www.leNetExpert.fr/contact>

