

# Recommandations de la CNIL sur les mot de passe (Délibération n° 2017-012 du 19 janvier 2017)

*Le mot de passe reste le moyen d'authentification le plus répandu. Alors que les compromissions de bases entières de mots de passe se multiplient, la CNIL a adopté une nouvelle recommandation sur les mots de passe. Elle fixe les mesures minimales à mettre en œuvre.*

✕	<b>Recommandations de la CNIL sur les mot de passe (Délibération n° 2017-012 du 19 janvier 2017)</b>
---	--

---

Le mot de passe reste le moyen d'authentification le plus répandu. Alors que les compromissions de bases de données de mots de passe se multiplient, la CNIL a adopté une nouvelle recommandation sur les mots de passe. Elle fixe les mesures minimales à mettre en œuvre.

Basée sur la gestion d'un secret, l'authentification par identifiant et mot de passe est un moyen simple et peu coûteux à déployer pour contrôler un accès. Toutefois, cette méthode d'authentification présente un niveau de sécurité faible. Les dernières années, de nombreuses attaques informatiques ont entravé la confidentialité de bases de données entières de comptes et des mots de passe associés. Ces fuites de données ont notamment contribué à éroder les connaissances des entreprises et sociétés de mots de passe. Les risques de compromission des comptes associés à cette méthode d'authentification se sont fortement accrus et nécessitent une vigilance particulière.

Les risques liés à la gestion des mots de passe sont multiples et passent notamment par :

1. La complexité de ces mots de passe ;
2. L'absence de leur mise à jour ;
3. La conservation de ces mots de passe ;
4. La faiblesse des modalités de renouvellement de mot de passe en cas d'oubli (cas des questions « secrètes »).

Les précones recommandées se trouvent au cœur de ce guide de mot de passe.

Il s'agit de définir des mots de passe sécurisés et de les renouveler régulièrement. Le risque de réussite d'une attaque informatique qui consisterait à tester successivement de nombreux mots de passe (attaque dite en force brute). On considère que la longueur du mot de passe suffit pour résister aux attaques courantes à partir de 12 caractères. Lorsque la taille du mot de passe dépasse, des mesures complémentaires doivent être prévues.

**PHRASE-PASSE : UN OUTIL POUR ACCOMPAGNER LES UTILISATEURS**

Pour aider les utilisateurs à choisir un mot de passe robuste et à mieux l'utiliser, la CNIL a développé un outil pour générer un mot de passe à partir d'une phrase. Le code de cet outil est disponible sous la forme d'une extension logicielle en JavaScript, afin que vous puissiez l'intégrer dans vos applications.

**Les exigences de la CNIL**

**L'authentification par mot de passe : longueur, complexité, mesures complémentaires**

Les recommandations de la CNIL ont été actualisées et complétées. Des mesures complémentaires mises en place pour faciliter le processus d'authentification : ainsi, si une authentification est basée sur un mot de passe, il est recommandé de compléter l'authentification par un autre facteur de sécurité. Des mesures complémentaires à la taille d'un mot de passe (restriction, durée, collecte d'autres données, support dédié en propre par l'utilisateur) permettant de réduire la longueur et la complexité du mot de passe, car ces mesures permettent d'assurer un niveau de sécurité équivalent au mot de passe seul.

Exemple d'utilisation	Longueur minimale	Complexité du mot de passe	Mesures complémentaires
Mot de passe simple	FORUM, BLOG	12	<ul style="list-style-type: none"> <li>• majuscules</li> <li>• minuscules</li> <li>• chiffres</li> <li>• caractères spéciaux</li> </ul> Connecter l'utilisateur sur un bon mot de passe
Avec restriction d'accès (cas simple)	SITE DE E-COMMERCE, COMPTE D'ENTREPRISE, MESSAGERIE	8	<ul style="list-style-type: none"> <li>• au moins 3 des 4 types suivants :               <ul style="list-style-type: none"> <li>• majuscules</li> <li>• minuscules</li> <li>• chiffres</li> <li>• caractères spéciaux</li> </ul> </li> </ul> Blocage des tentatives multiples : <ul style="list-style-type: none"> <li>• temporisation d'accès au compte après plusieurs échecs</li> <li>• « verrouillage » de compte après 10 échecs</li> </ul>
Avec information complémentaire	BANQUE EN LIGNE	5	<ul style="list-style-type: none"> <li>• chiffres et/ou lettres</li> </ul> Informations complémentaires communiquées en propre d'une taille d'au moins 7 caractères (ex : identifiant dédié au service) de <ul style="list-style-type: none"> <li>• Identification de l'adresse IP, adresse MAC</li> </ul>
Avec matériel dédié par la personne	CARTE BANCAIRE OU TELEPHONE	4	Matériel dédié en propre par la personne (ex : carte SIM, carte bancaire, certificat) <ul style="list-style-type: none"> <li>• Blocage au bout de 3 tentatives échouées</li> </ul>

**Dans tous les cas,**

- le mot de passe ne doit pas être communiqué à l'utilisateur en clair par courrier électronique.
- ces exigences sont des règles minimales. Le contrôle d'accès peut devoir répondre sur des règles plus robustes selon les risques auxquels le système est exposé.

**Sécurisation de l'authentification**

Quelle que soit la mesure mise en place, la fonction d'authentification doit être sûre :

- sa mise en œuvre logicielle est exempte de vulnérabilité connue.
- lorsque l'authentification se fait dans un navigateur, elle doit être contrôlée au moyen d'un certificat d'authentification de serveur et le canal de communication entre le serveur authentifié et le client doit être chiffré à l'aide d'une fonction de chiffrement sûre. La sécurité des clés privées doit être assurée.

**La conservation des mots de passe**

Le mot de passe ne doit jamais être stocké en clair. Il doit être transformé au moyen d'une fonction cryptographique non-réversible et sûre, intégrant l'utilisation d'un sel de hachage.

Le mot de passe ne doit être obtenu qu'au moment de la saisie de l'utilisateur et ne doit être transmis qu'à l'application de destination.

**Le renouvellement du mot de passe**

La responsabilité de l'utilisateur est de changer régulièrement son mot de passe. Dans ce cas, les règles relatives à la création de mots de passe s'appliquent.

Le responsable du traitement doit être en mesure de changer elle-même son mot de passe. Dans ce cas, les règles relatives à la création de mots de passe s'appliquent.

**Renouvellement des données**

La responsabilité de l'utilisateur est de changer régulièrement son mot de passe. Dans ce cas, les règles relatives à la création de mots de passe s'appliquent.

Le responsable du traitement doit être en mesure de changer elle-même son mot de passe. Dans ce cas, les règles relatives à la création de mots de passe s'appliquent.

**Que faire en cas de risque de compromission du mot de passe ?**

- en cas de compromission de données, le responsable du traitement doit être en mesure de changer elle-même son mot de passe.
- en cas de compromission de données, le responsable du traitement doit être en mesure de changer elle-même son mot de passe.
- en cas de compromission de données, le responsable du traitement doit être en mesure de changer elle-même son mot de passe.
- en cas de compromission de données, le responsable du traitement doit être en mesure de changer elle-même son mot de passe.

**Mises en œuvre**

Les professionnels sont invités à consulter la CNIL. Les difficultés de mise en œuvre peuvent poser l'application de cette recommandation. Cette recommandation pourra faire l'objet de révisions et de mises à jour.

Date d'adoption : 2017-02-10

Document n° 2017-022 du 10 janvier 2017 portant adoption d'une recommandation relative aux mots de passe

(lire la suite)

Vous aider à mieux protéger vos données personnelles (adresses, e-mails, cryptomonnaies) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par ses actions de formation, de sensibilisation de millions de citoyens dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec la réglementation européenne relative à la protection des données à caractère personnel (GDPR) et nous assistons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement. L'abonnement de la Services de Travail de l'Emploi et de la Formation Professionnelle N°39 53 33 84.

Pour d'informations sur : <https://www.lanouvelleprotectiondesdonneespersonnelles.com>


10

Retourner à cet article

# Arnaques par courriel (scam, phishing) : la CNIL peut-elle agir ? | Denis JACOPINI

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

✘	✘	✘	✘	✘	✘
---	---	---	---	---	---



## Arnaques par courriel (scam, phishing) : la CNIL peut-elle agir ?

**vous informe**

**LCI**

---

**Ces procédés ne sont pas liés à la protection des données personnelles : ce sont des tentatives d'escroquerie ou d'extorsion de fonds.**

Si vous en êtes victime, signalez-les sur le service PHAROS du ministère de l'Intérieur (<http://www.internet-signalment.gouv.fr>) et au service phishing-initiative (<http://www.phishing-initiative.com>) mis en place par plusieurs acteurs de l'internet.

Vous pouvez également joindre par téléphone le service Info Escroquerie de la police nationale au 0811 02 02 17 (coût d'un appel local).

---

Réagissez à cet article

---

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

Denis JACOPINI Marie Nocenti (Plon) ISBN :  
2259264220



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

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

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

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

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !  
Commandez sur Fnac.fr

---

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la

Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

[https://youtu.be/usg12zkRD9I?list=UUoHqj\\_HKcbzRuvIPdu3FktA](https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA)

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr

---



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

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


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

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

Source : *CNIL Besoin d'aide ? – Arnaques par courriel (scam, phishing) : la CNIL peut-elle agir ?*

---

# Combien de temps doivent être conservées les données utilisées pour le suivi du temps de travail ? | Denis JACOPINI

 <p><b>Le Net Expert</b> <b>INFORMATIQUE</b> Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<p>Combien de temps doivent être conservées les données utilisées pour le suivi du temps de travail ?</p>
---	---

Les éléments relatifs à l'identification des salariés et les données utilisées pour le suivi du temps de travail, y compris les données relatives aux motifs des absences, ne peuvent pas être conservés plus de 5 ans après le départ des employés.

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

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

S o u r c e

<http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=0245F4689A67B389E322EB9815FEF32B?name=Contr%C3%B4le+des+horaires+%3A+combien+de+temps+sont+conserv%C3%A9es+les+donn%C3%A9es+%3F&id=365>

# Quelles précautions prendre avant de fermer la messagerie professionnelle d'un employé ? | Denis JACOPINI

 <p>Denis JACOPINI</p> <p>vous informe</p> <p>LCI</p>	<p>Quelles précautions prendre avant de fermer la messagerie professionnelle d'un employé ?</p>
--	---

La CNIL recommande à l'employeur d'avertir l'employé de la date de fermeture de sa messagerie afin que ce dernier puisse faire le tri et transférer ses messages privés vers sa messagerie personnelle.

Une fois que l'employé a quitté l'organisme, l'employeur doit supprimer son adresse électronique nominative.

La CNIL invite les employeurs à définir, en concertation avec les représentants des personnels, des chartes d'utilisation des outils informatiques.



Réagissez à cet article

Source : *CNIL Besoin d'aide ? – Messagerie professionnelle : quelles précautions avant de fermer le compte d'un employé ?*

## Consommateurs, exercez vos droits auprès de la CNIL | Denis JACOPINI

 <p>Denis JACOPINI DENIS JACOPINI Expert Juriste Digital vous informe LCI</p>	<p>Consommateurs, exercez vos droits auprès de la CNIL</p>
--	--



Participer à un concours, demander une carte de fidélité, remplir un formulaire sur internet, ou simplement poster sur les réseaux sociaux, nous transmettons très souvent des données personnelles à des organismes.

Grâce à la loi Informatique et Libertés, vous bénéficiez de droits spécifiques que vous pouvez – dans la plupart des cas – faire valoir vous-mêmes.

**Droit d'accès**

**Droit de rectification**

**Droit d'opposition**

**Droit au déréférencement**



Réagissez à cet article

Source : *Exercer vos droits – CNIL – Commission nationale de l'informatique et des libertés*

---

# **RGPD dans les collectivités : Que faut-il mettre en oeuvre ?**

Denis JACOPINI est Expert en Cybercriminalité et en Protection des Données à Caractère Personnel.

Notre métier :

Animation de formations et de conférences

Cybercriminalité (virus, espions, piratages, fraudes, arnaques Internet)

Protection des Données à Caractère Personne (mise en conformité avec la CNIL et le RGPD)

Audits sécurité, Expertises techniques et judiciaires

Audit sécurité (ISO 27005) ;

ID Swatting

Recherche de preuves (Investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...)

Expertises de systèmes de vote électronique ;

---

# Formation pour DPO externe mutualisé et Délégués à la protection des données externalisé

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

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



Formation RGPD  
pour DPO externe  
mutualisé et  
Délégués à la  
protection des  
données  
externalisé

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 DPO externe ou Délégué à la protection des données externalisé : « J'accompagne mes clients dans leur mise en conformité avec le RGPD » : 3 jours + 1 jour d'accompagnement personnalisé (C'est le moment ou jamais de vendre des services « RGPD »)**

Si votre objectif est avant tout de développer l'activité de mise en conformité avec le RGPD afin de vendre cette prestation auprès de vos clients, cette formation est faite sur-mesure pour vous en vous apportant l'ensemble des mesures et des cas qu'il est nécessaire de maîtriser pour que vos clients soient mis sur le chemin de la mise en conformité. Vous êtes une société d'Informatique, un cabinet d'avocat, un cabinet d'expertise comptable, un consultant et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation se passe sur 3 jours en groupe plus une journée supplémentaire en individuel pour superviser la mise en place du RGPD dans votre établissement ou chez un de vos clients (frais liés au déplacement dans cet établissement en sus). Suivez LA formation qui vous apportera la plus grande autonomie dans la mise en conformité de tout notre catalogue.

Consultez les 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 coté pragmatique et 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 » 3+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 DPO : « **Je veux devenir le Délégué à la Protection des Données de mon établissement** »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.

Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.

N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

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

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.

Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.

N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

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

Votre message avec vos préférences de date ou vos commentaires

Envoyer

Nos formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre 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)

---

Réagissez à cet article

---

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

---

# Pendant les vacances continuez à protéger vos données personnelles

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>		<b>Pendant les vacances, continuez à protéger vos données personnelles</b>			



**Pendant les vacances, continuez à protéger vos données personnelles**

---

Les utilisateurs sont de plus en plus concernés par le sort de leurs données. Potentiellement victimes, ils doivent prendre plus de temps pour consulter les pages de politique de confidentialité. Qu'en est-il de ces utilisateurs finaux ? Sont-ils acteurs de la sécurité en ligne de leurs données ? Il n'est pas inutile de rappeler certains points.

- **Les dangers du Wi-fi public**

Lorsque vous rejoignez un réseau Wi-Fi public ouvert à votre café préféré, vous pouvez obtenir plus qu'un expresso. Vous pourriez potentiellement être victime d'un vol d'informations. En outre, un pirate peut avoir créé un faux réseau Wi-Fi qui semble réel (avec un nom similaire par exemple). L'utilisation d'un VPN est donc fortement recommandée.

- **Les dangers des applications**

Les applications sur votre smartphone peuvent vous espionner. Soyez très prudent lorsque vous sélectionnez des applications. Jetez un œil aux fonctionnalités dictées par le développeur. Maximisez les paramètres de confidentialité autant que possible.

- **Les dangers des médias sociaux**

Évitez les quiz Facebook qui peuvent relever toutes vos données (Cambridge Analytica). Minimisez les informations que vous partagez sur les réseaux sociaux. N'acceptez pas les demandes de personnes que vous ne connaissez pas.

Tout le monde peut prétendre être quelqu'un d'autre en ligne – prenez des mesures supplémentaires pour assurer votre sécurité et celle de votre famille. En conclusion, n'hésitez pas à vous référer à des conseils, guides, vidéos de la part des professionnels du secteur et autres associations, sans oublier le site de la CNIL et ses guides qui fournissent de bons conseils et recommandations.

[Lire l'article complet sur [LaTrinune.fr](http://LaTrinune.fr)]



---

Réagissez à cet article

**Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :**

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

**Quel est notre métier ?**

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

**Quel sont nos principales activités ?**

▪ **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



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

*« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

*les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.*

*Denis JACOPINI »*

**Besoin d'un Expert ? contactez-nous**

---

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



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



[Contactez-nous](#)



Source : *Vous attendez tout du RGPD pour protéger vos données en ligne. Pas si vite !*

---

# Mise en conformité RGPD, privilégiez l'accompagnement sur mesure

Denis JACOPINI est Expert en Cybercriminalité et en Protection des Données à Caractère Personnel.

Notre métier :

Animation de formations et de conférences

Cybercriminalité (virus, espions, piratages, fraudes, arnaques Internet)

Protection des Données à Caractère Personne (mise en conformité avec la CNIL et le RGPD)

Audits sécurité, Expertises techniques et judiciaires

Audit sécurité (ISO 27005) ;

ID Swatting

Recherche de preuves (Investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;

Expertises de systèmes de vote électronique ;

---

# Victime d'un piratage informatique, quelles sont

# Les bonnes pratiques ?

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

x

x

x

x

x

x

x

**Victime d'un piratage informatique, quelles sont les bonnes pratiques ?**

**Les cas de piratages informatiques ne se comptent plus depuis bien longtemps. Cependant, si vous vous êtes retrouvés victimes, il est urgent de mettre en pratique des règles de base.**

Les 3 axes vers lesquels votre structure devra progresser seront :

- Technique, par une amélioration des mesures de sécurité en place ;
- Juridique, par une présentation, auprès des principaux acteurs de votre structure pour une meilleure acceptation, des principales mesures de mise en conformité avec les règles françaises et européennes relatives à la protection des données personnelles ;
- Humain, par une meilleure prise de conscience des dangers numériques, pour une évolution des comportements vers une utilisation plus responsable des outils numériques.

Face à vos besoins d'accompagnement, nos formateurs ont élaboré un parcours destinés aux équipes de direction de votre structure, à l'équipe informatique et aux utilisateurs susceptibles d'être piégés.

En vous accompagnant sur ces 3 axes et auprès de ces 3 profils, vous pourrez alors comprendre comment les pirates informatiques vous ont piégé, découvrir s'ils pourront encore vous piéger et surtout, le plus important, quelles changements mettre en place pour limiter les risques à l'avenir.

---

Réagissez à cet article

---

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

Denis JACOPINI Marie Nocenti (Plon) ISBN :  
2259264220



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

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

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

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

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

Commandez sur Fnac.fr

---

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site

Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

[https://youtu.be/usg12zkRD9I?list=UUoHqj\\_HKcbzRuvIPdu3FktA](https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA)

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr

---



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



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

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

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