

# Comment empêcher Android de sauvegarder automatiquement nos données personnelles ?

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

x

x

x

x

x

x

x

**Comment empêcher Android de sauvegarder automatiquement nos données personnelles ?**

Nos smartphones et tablettes Android sauvegardent certaines de nos données personnelles sur les serveurs de Google sans forcément nous demander notre avis. Un système qui peut s'avérer aussi pratique pour certains qu'il peut être dérangerant pour d'autres. Encore faut-il savoir quelles sont les données sauvegardées par Google et celles qui ne le sont pas. Nous allons donc aujourd'hui nous pencher sur la question.



N'avez-vous jamais remarqué que lorsque vous entrez vos identifiants Google dans un nouvel appareil Android, ce dernier retrouvait automatiquement certaines de vos informations personnelles, notamment vos contacts. Pourtant, vous n'avez jamais rien fait pour, et pour cause puisque cette option est activée par défaut. Ce qui signifie que vous pouvez également la désactiver. La plupart des utilisateurs la conservent néanmoins activée pour des raisons de praticité.

Il faut dire que cette sauvegarde automatique peut s'avérer utile lorsque vous changez de smartphone, lorsque vous disposez de plusieurs appareils Android ou si par malheur, vous vous faisiez voler votre téléphone. Mais certains ne veulent pas que leur vie privée se retrouve sur le cloud de Google. Ce tutoriel est pour eux mais avant de passer à la pratique, un peu de théorie.

## Les données automatiquement sauvegardées par Google

Au sein de son OS, Google a intégré un outil du nom d'Android Backup Service qui sauvegarde certaines données liées aux services que vous utilisez. Ces données sont les suivantes :

- **Contacts** qui sont sauvegardés au sein de Google Contacts. Vous pouvez ainsi les retrouver sur tous vos appareils et même sur votre PC en vous connectant simplement à votre compte.
- **Emails** qui sont sauvegardés au sein de Gmail
- **Documents**, ce qui vous permet d'ailleurs d'éditer vos documents sauvegardés dans le cloud à partir de n'importe lequel de vos appareils
- **Calendriers**
- **Chrome** : vos favoris et votre historique de navigation sont synchronisés avec votre compte. Idem pour vos mots de passe si vous avez activé la fonction Smart Lock
- **Hangouts** : vos conversations sont sauvegardées
- **Google Play Store** : les applications que vous avez téléchargées sont automatiquement sauvegardées. Vous pouvez ensuite les retrouver dans l'onglet « Mes applications » de la boutique. C'est très pratique lorsque vous changez de smartphone car vous n'avez pas besoin de les rechercher une par une, en outre, les applications achetées sont également sauvegardées
- Vos **photos** et vidéos, à condition d'utiliser l'application Google Photos et d'avoir activé la sauvegarde automatique de vos médias
- Certaines **données d'applications**

## Comment empêcher Google de sauvegarder vos données

Vous n'êtes pas ravis à l'idée que Google en sache autant sur vous et vous souhaiteriez que certaines de vos données ne soient pas sauvegardées ? Et bien rassurez-vous, c'est possible et en quelques clics. Il vous suffit pour cela de :

- Vous rendre dans le menu **Paramètres > Personnel > Comptes de votre smartphone**
- Sélectionner votre compte Google
- Décocher toutes les données que vous ne voulez pas que Google sauvegarde



Et pour aller plus loin, n'hésitez pas à jeter un œil à notre tutoriel comment préserver sa vie privée sur Android.

## Les données non sauvegardées par Google

Les données listées ci-dessous ne sont pas sauvegardées par Google. Pour éviter de les perdre en changeant de smartphone, il faudra donc utiliser une application tierce mais nous y viendrons après.

- Les SMS, il est néanmoins possible de sauvegarder ses SMS sur Android en utilisant une application
- Google Authenticator : pour des raisons de sécurité, les données d'authentification Google en deux étapes ne sont pas sauvegardées
- Réglages : les paramètres personnalisés de votre smartphone ne sont pas sauvegardés
- Bluetooth : Android ne synchronise pas les périphériques Bluetooth appairés vers votre smartphone

## Comment sauvegarder toutes ses données personnelles

Bien que Google ne le permette pas par défaut, il est tout à fait possible de sauvegarder toutes les données de votre smartphone Android à l'aide de notre précédent tutoriel. Certaines de vos données iront directement sur votre support externe, d'autres seront sauvegardées en ligne afin de pouvoir ensuite être réintégrées à votre nouveau smartphone si votre but est de sauvegarder vos données pour les retrouver sur un nouvel appareil.

N'oubliez pas non plus de jeter un œil à notre sélection d'applications pour sauvegarder ses données personnelles. Certaines nécessiteront que votre téléphone soit rooté, d'autres non, et elles vous permettront de sauvegarder toutes vos applications et pas seulement les données.

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 : <http://www.phonandroid.com/comment-empecher-android-sauvegarde-r-automatiquement-donnees-personnelles.html>

---

# Denis JACOPINI sur LCI : Les techniques des cybercriminels pour pirater votre CB

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



Denis JACOPINI sur LCI : Les techniques des cybercriminels pour pirater votre CB

---

**Denis Jacopini, expert informatique assermenté spécialisé en cybercriminalité, explique que quoi que l'on fasse, les fraudeurs auront une longueur d'avance. Néanmoins, il y a des failles dans le système, et en particulier au niveau du cryptogramme visuel.**

En direct sur LCI avec Serge Maître Maître, président de l'AFUB (Association Française des Usagers des Banques) et Nicolas CHATILLON, Directeur du développement-fonctions transverses du groupe BPCE et Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité débattent le 7 mars 2016 sur les techniques des cybercriminels pour vous pirater votre CB.



<http://lci.tf1.fr/france/societe/cartes-bancaires-les-fraudeurs-ont-toujours-une-longueur-d-avance-8722056.html>

Une liste non exhaustive avec 10 techniques de cybercriminels pour vous pirater votre carte bancaire :  
<http://www.lenetexpert.fr/10-techniques-de-cybercriminels-pour-vous-pirater-votre-carte-bancaire/>

---

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 cyberarnaqes dont chacun peut être victime.

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

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

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

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

---

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

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

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

Commandez sur Fnac.fr

---

[https://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 : *Cartes bancaires* : « Les fraudeurs ont toujours une longueur d'avance » – Société – MYTF1News

---

# **Le phishing, ça c'était avant : place aux fraudes au paiement par autorisation dans lesquelles on vous fait dire OK par téléphone**

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





Le phishing, ça  
c'était avant :  
place aux fraudes  
au paiement par  
autorisation dans  
lesquelles on vous  
fait dire OK par  
téléphone

---

Interviewé par Atlantico, Denis JACOPINI nous parle d'une nouvelle forme de Phishing. Le APP (Authorised Push Payment Fraud – fraude au paiement par autorisation) serait une des techniques de fraude en forte croissance au Royaume Uni, et combinerait des techniques sophistiquées, au travers de SMS et d'appels, pour soutirer de l'argent aux victimes.

Le APP (Authorised Push Payment Fraud – fraude au paiement par autorisation) serait une des techniques de fraude en forte croissance au Royaume Uni, et combinerait des techniques sophistiquées, au travers de SMS et d'appels, pour soutirer de l'argent aux victimes. 19 370 cas auraient été répertoriés au Royaume Uni au cours de ces 6 derniers mois selon le daily mail. Quelles sont les techniques ici employées ? La France est-elle touchée ?

Denis Jacopini : Cette technique de fraude utilise de nombreux ingrédients de base :

- L'ingénierie sociale (pratique utilisant des techniques de manipulation psychologique afin d'aider ou nuire à autrui)
- L'usurpation (d'identité);
- Le passage en mode émotionnel par la peur ;
- L'interlocuteur est votre sauveur et est là pour vous aider.

Dans le cas précis, nous avons aussi :

- L'usurpation du nom de la banque ;
- L'usurpation du numéro de téléphone de la banque ;
- Le passage en mode émotionnel de la victime basé sur la peur du piratage mais heureusement elle est en ligne avec un sauveur (baisse de la prudence, confiance aveugle...);
- La création d'une ambiance téléphonique de centre d'appel ;
- Un excellent comédien qui joue le rôle de l'employé de banque ;
- Une excellente connaissance des procédures internes des banques dont la banque usurpée.

En France, ce type d'arnaque n'est pas encore médiatisé. En effet, les banques n'aiment pas tellement communiquer sur leurs failles car :

- Ce n'est pas bon pour leur image ;
- Elles sont ensuite obligées de dépenser beaucoup pour corriger ;
- Elles préfèrent investir lorsque la fraude commence à leur coûter plus cher que les mesures de sécurité à mettre en place (gestion du risque).

**Ces nouvelles techniques de fraude marquent elles une réelle professionnalisation de cette forme de criminalité ?**

Denis Jacopini : Cette forme de criminalité existe depuis très longtemps et n'a pas attendu l'informatique et Internet pour se développer et se professionnaliser. Prétexter un gros risque et usurper l'identité des pompiers, des policiers, du plombier en utilisant leur costume, leur jargon, leur outils pour vous rassurer et reviennent ensuite pour mieux vous arnaquer ou vous cambrioler existe depuis que les escrocs existent.

Plus récemment, Gilbert Chikli Pionnier de l'arnaque au faux président, utilisait des techniques de manipulation psychologique et se servait de sa parfaite connaissance des procédures internes aux très grandes entreprises et sa maîtrise du langage juridique ou financier en fonction de l'identité de la personne usurpé pour obtenir de ses victimes des virements définitifs pour des sommes détournées de plusieurs dizaines de millions d'euros.

Chaque fois que des techniques d'arnaque ou d'escroquerie sont déjouées, décortiquées et dévoilées au grand jour, il y a des millions d'escrocs du dimanche vont analyser l'arnaque pour la reproduire et l'utiliser pour eux. Une fois que l'arnaque commence à être connue et de plus en plus de gens sont sensibilisés, les escrocs professionnels et utilisant leur génie à des fins illicites modifient leurs techniques pour toujours utiliser des moyens basés sur les ingrédients de base + des failles inexploitées utilisant ou non la technologie.

Comme les banques ont mis en place des mesures de sécurité utilisant l'internet, le SMS, le téléphone, les escrocs utilisent ces mêmes technologies en recherchant le moyen d'exploiter les failles qui ne seront jamais suffisamment protégées : Les failles du cerveau humain.

**Quels sont les réflexes à avoir pour éviter tout problème de ce type ?**

Denis Jacopini : Le seul moyen que nous avons pour nous protéger est d'une part la prudence ultime en plus de la sensibilisation. Selon moi, les médias devraient signaler ce type d'arnaque afin de sensibiliser le plus grand nombre. Cependant, cette solution ne plait pas aux banques qui considèrent inutile de répandre la peur car cela risquerait d'écorcher de manière irréversible la confiance que nous avons mis des années à avoir envers les moyens de paiement électronique sur Internet.

A notre niveau, si j'ai un conseil à vous donner pour éviter tout problème de ce type, si vous vous trouvez dans une situation anormale qui vous est présenté par un interlocuteur, contactez directement l'établissement à l'origine de l'appel à partir des coordonnées dont vous disposez, et allez jusqu'au bout de la vérification AVANT de réaliser des opérations financières irréversibles et partagez le plus possible les cas d'arnaques.

Quand on sait à quoi ressemble le loup, on ne le fait pas rentrer dans sa bergerie. Par contre, s'il met un nouveau costume, le piège fonctionnera tant que ce nouveau costume ne sera pas connu du plus grand nombre. (d'où l'utilité de mon livre CYBERARNQUES ☐

<https://www.amazon.fr/Cyberarnques-Denis-JACOPINI/dp/2259264220>

---

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 cyberarnaqes dont chacun peut être victime.

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

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

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

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

---

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

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

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

Commandez sur Fnac.fr

---

[https://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 : *Le phishing, ça c'était avant : place aux fraudes au paiement par autorisation dans lesquelles on vous fait dire OK par téléphone* | [Atlantico.fr](https://atlantico.fr)

---

# 3 points à retenir pour vos élections par Vote électronique

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
x	x	x	x	x	x
x	<b>3 points à retenir pour vos élections par Vote électronique</b>				

x





les décrets d'application de la Loi Travail continuent d'arriver en ce dernier mois de l'année 2016. L'objet de ce document concerne le vote électronique (1). En tant que représentants du personnel, ou vos voyez délégué de personnel ou membre de comité d'entreprise, vous vous demandez quelles sont les conditions à réunir pour recourir à ce type de dispositif. Vous souhaitez savoir quel sont les apports de la Loi Travail sur le vote électronique : quel accord mettre en place et quelles garanties pour le système adopté ? Voici les 3 points essentiels à connaître à propos du vote électronique :

Avant la loi Travail, le vote électronique n'était possible que sous réserve d'accord préalable par un accord collectif. Mais est-ce toujours le cas ? Pour quelles élections peut-on recourir au vote électronique ? Quelles sont les garanties de régularité de ce vote ?

**Les élections concernées par le vote électronique**  
 Il est possible de recourir au vote électronique pour deux élections visées dans le décret du 5 décembre 2016 :

- Les délégués du personnel ;
- Les représentants du personnel au comité d'entreprise.

Sachez qu'il est d'ailleurs possible de combiner vote électronique et vote sous enveloppe, à condition que l'acte qui autorise le recours au vote électronique n'exclue pas cette possibilité (2).

**Les modalités du vote électronique**  
 La mise en place de vote électronique est soumise à quelques formalités préalables. Ce recours doit être prévu dans un accord de groupe ou un accord d'entreprise (3).  
 De surcroît, à défaut d'accord collectif, l'employeur peut décider unilatéralement de recourir au vote électronique (2). C'est la nouveauté inscrite dans ce décret d'application de la loi Travail.  
 Sachez aussi que le protocole d'accord prélectoral, qui doit être signé entre l'employeur et les organisations syndicales représentatives, doit mentionner l'accord collectif ou la décision de l'employeur de recourir au vote électronique.

**Quel est le contenu du protocole d'accord prélectoral ?**  
 Lors de la négociation de ce protocole, il faudra tenir compte des contraintes techniques posées par ce vote particulier. En effet, comme tout dispositif électronique, des garanties doivent être prises pour assurer la régularité du vote et sa confidentialité.

À ce titre, le code de travail établit un cahier des charges à respecter :

- Des fichiers distincts dans l'urne : il doit y avoir deux fichiers qui doivent être bien séparés. Le premier « Fichier des électeurs » doit permettre l'authentification des électeurs. Le second fichier nommé « Contenu de l'urne électronique » détaillera lui les clés de chiffrement et de déchiffrement, ainsi que le contenu de l'urne. Ce fichier n'est consultable que par les personnes en charge de la gestion et de la maintenance du système de vote (3).
- Le système de vote doit pouvoir être scellé pendant toute la durée du scrutin (4).
- une expertise indépendante doit être réalisée avant la mise en service de l'employeur.
- une assistance technique doit être mise en place par l'employeur pour veiller au bon fonctionnement du système et intervenir en cas de besoin (6). Des tests doivent être effectués sur le matériel avant le déroulement du vote.

**Les garanties prévues pour la régularité du vote**  
 Le vote électronique doit présenter certaines garanties indispensables à sa régularité :

- le respect du cahier des charges prévu par la loi ;
- le maintien dans l'accord collectif ou la décision unilatérale de l'employeur de recourir au vote électronique.

Par ailleurs, chaque salarié doit avoir accès à ce cahier des charges selon le décret du 5 décembre 2016 (2). Il peut être mis à leur disposition via l'intranet de l'entreprise ou consultable dans les locaux de l'entreprise.

**L'expertise préalable par un expert indépendant.**  
 Tout le système et le matériel de vote doit avoir été examiné par un expert rémunéré par l'employeur.  
 Il assure de l'existence de la décision unilatérale de l'employeur ou de l'accord collectif autorisant le recours au vote électronique.  
 Il doit s'assurer également des modalités garantissant la confidentialité et la sécurité de dispositif : l'existence des deux fichiers séparés concernant les électeurs et le contenu de l'urne, l'exclusivité de l'accès aux données électroniques par les gestionnaires du système, le caractère hermétique et scellé du matériel.  
 Il rédigera un rapport sur ces points. Ce dernier doit être tenu à la disposition de la CNIL (7).

**La déclaration à la CNIL.**  
 Comme tout dispositif électronique et de stockage informatique de données, le vote électronique doit faire l'objet d'une déclaration auprès de la Commission nationale de l'Informatique et des Libertés (8).  
 À ce titre, la CNIL a fait une recommandation relative à la sécurité des systèmes de vote électronique.  
 Lire la recommandation de la CNIL

Les organisations syndicales représentatives de salariés doivent être informées de l'accomplissement de cette formalité déclarative auprès de la CNIL.

**Les résultats de vote.**  
 Si l'acte qui autorise le recours au vote électronique n'a pas exclu le vote sous enveloppe à bulletin secret, sachez qu'il ne sera pas possible d'obtenir des premiers résultats pendant le scrutin. En effet, le récent décret précise bien qu'aucun résultat partiel n'est accessible pendant le déroulement du vote. L'ouverture des enveloppes ne pourra être faite qu'après la clôture du vote électronique (9).

(1) Décret n°2016-1536 du 5 décembre 2016 relatif au vote par vote électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise  
 (2) Article R2234-8 et R2234-9 du Code de travail  
 (3) Article R2234-8 du Code de travail  
 (4) Article R2234-7 du Code de travail  
 (5) Article R2234-8 du Code de travail  
 (6) Article R2234-9 du Code de travail  
 (7) Article R2234-12 et R2234-8 du Code de travail  
 (8) Article R2234-14 et R2234-10 du Code de travail  
 (9) Article R2234-19 et R2234-15 du Code de travail

## Réagissez à cet article

### A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles

3 points à retenir pour vos élections par Vote électronique

Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique

Modalités de recours au vote électronique pour les Entreprises  
 L'Expert Informatique obligatoire pour valider les systèmes de vote électronique

Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

---

**Vous souhaitez organiser des élections  
par voie électronique ?  
Cliquez ici pour une demande de chiffrage  
d'Expertise**



---

Vos expertises seront réalisées par **Denis JACOPINI** :

- Expert en Informatique **assermenté et indépendant** ;
- **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
- ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
- qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solutions de vote électronique ;
- et possède une expérience dans l'analyse de nombreux

systemes de vote de prestataires differents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

---

Contactez-nous

---

Article original de Juritravail : Vote électronique : les 3 points à retenir !

---

# Un guide pour aider les entreprises face à Facebook ou Twitter | Denis JACOPINI

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



Un guide pour  
aider les  
entreprises face  
à #Facebook ou  
#Twitter

## **Le Medef a édité un guide pour informer les entreprises des risques liés aux #réseaux sociaux et des mesures à prendre.**

Facebook, Twitter, LinkedIn, Viadeo: les réseaux sociaux n'ont plus secret pour des millions de Français. Les entreprises, elles, ne sont pas forcément à l'aise avec la question. Ces outils, qui sont souvent à la limite des sphères privées et publiques, induisent de nouveaux risques pour les sociétés: se faire dénigrer sur la Toile, se faire usurper son identité, ou voir des salariés, par des conversations sur les réseaux professionnels livrer, sans s'en rendre compte, des informations confidentielles. Pour aider les chefs d'entreprise, le Medef vient d'éditer un guide sur le sujet, intitulé «réseaux sociaux et entreprises, quels enjeux juridiques». Le petit livret est très didactique puisque le premier chapitre consiste à expliquer... ce qu'est un réseau social.

«On s'est rendu compte que les entreprises avaient en la matière des pratiques très différentes. Certaines encouragent leurs salariés à communiquer sur les réseaux sociaux, mais sans fixer aucun cadre. Dans d'autres, la communication est beaucoup plus contrôlée. Certaines ont déjà mené des actions de sensibilisation auprès de leurs salariés, dont une avec une pièce de théâtre», explique-t-on au Medef, où un groupe de travail avait été constitué pour rédiger le guide. D'après une étude du cabinet Proskauer, la manière forte est aussi de mise. 29% des 120 grandes entreprises internationales interrogées ont bloqué l'accès à Twitter, Facebook et autres réseaux sur le lieu de travail, et 27% en contrôlent l'utilisation. A vrai dire, ce sont les PME qui sont le plus «en retard»: elles n'ont souvent pas le temps de se pencher sur la question, ni les moyens de monter des cellules de veille. Le guide est donc là pour les sensibiliser.

Sur ces réseaux, les règles de droit classique – code du travail, code civil, code de la propriété intellectuelle etc... – s'appliquent. Mais il existe également des dispositifs spécifiques. Et tout cela s'entremêle. Le poids d'une charte sur l'utilisation des réseaux sociaux par les salariés ne sera pas le même si cette charte est inscrite dans le règlement intérieur, ou pas. Les salariés ont le droit de parler sur les réseaux de l'organisation et du fonctionnement de l'entreprise, à condition que leurs propos ne soient pas injurieux. L'entreprise elle-même doit évidemment respecter les règles de droit à l'image lorsqu'elle publie sur ces réseaux. Bref, un guide n'est pas de trop dans ce maquis!

Lien pour télécharger le guide

---

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

<http://www.lefigaro.fr/conjoncture/2014/09/11/20002-20140911ARTFIG00296-un-guide-pour-aider-les-entreprises-face-a-facebook->



# Conseils pour assurer la sécurité numérique des nomades | Denis JACOPINI

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

x

x

x

x

x

x

x

**Conseils pour assurer la sécurité numérique des nomades**

Même lorsqu'il s'aventure dans le vaste cybermonde, le collaborateur nomade doit avoir accès aux ressources internes de l'entreprise. Il représente alors un danger. Comment se protéger ? Quelques conseils de Gérard Peliks, expert et enseignant en sécurité de l'information.

#### **#Identification et authentification fortes de l'utilisateur**

Ce n'est pas l'outil qui doit être tracé, mais l'individu qui s'en sert. « Il s'agit d'identifier et d'authentifier, avec la plus grande attention, l'ayant-droit aux ressources de l'organisation », indique Gérard Peliks, expert et enseignant en sécurité de l'information. Première étape : l'identifiant ou login. Seconde phase : l'authentifiant, autrement dit la preuve de l'identité de l'utilisateur. « Le plus fiable est la combinaison de deux paramètres : ce que l'on a (par exemple une calculatrice, un token usb...) et ce que l'on sait (un code pin). En attendant les solutions de biométrie multimodale... », précise Gérard Peliks.

#### **#Intégrité et confidentialité des transactions**

Les échanges entre l'organisation et le collaborateur nomade doivent être sécurisés dans leur confidentialité et leur intégrité. « Il s'agit de créer un tunnel chiffrant dont les deux extrémités sont mutuellement identifiées », souligne Gérard Peliks. Les virtual private networks (VPN) ou réseaux privés virtuels (RPV) garantissent la confidentialité des données transmises, donc vulnérables, sur Internet. La signature électronique peut en garantir l'intégrité. Ce qu'on appelle le protocole de « tunnellation » ou d'encapsulation consiste à chiffrer les transmissions entre le poste nomade et l'Intranet de l'organisation.

#### **#Chiffrement des données sur disque**

En cas de perte ou de vol d'un PC, ou d'un téléphone portable, la confidentialité des informations contenues n'est plus assurée, si elles sont stockées en clair. « On ne perd pas seulement l'objet, mais des données, avec tout ce que cela peut entraîner comme risque d'image, de réputation et même de conséquences juridiques », pointe Gérard Peliks. Tout l'enjeu est donc de rendre illisibles les informations contenues dans l'appareil, si on ne possède pas les clefs pour les déchiffrer. « Le chiffrement de fichiers, de partitions, voire même de l'intégralité du disque, permet de sécuriser les contenus sensibles », explique-t-il.

#### **#Destruction des fichiers**

Quand il s'agit d'éliminer un fichier, la touche « delete » et le vidage de la corbeille ne détruisent rien mais se contentent de cacher le document. Et des outils de récupération permettent de pister les anciennes données. Pour effacer définitivement, ou « massicoter » les contenus, il convient d'utiliser des méthodes de suppression sécurisée. « En utilisant des utilitaires de destruction, on s'assure que les fichiers sont réellement passés à la « déchiqueteuse », préservant ainsi leur confidentialité », indique Gérard Peliks.

#### **#Sensibilisation des collaborateurs**

Dans un contexte de dématérialisation généralisée, tous les collaborateurs sont potentiellement amenés à travailler un jour en mode nomade, ou avec des collègues en télétravail. D'où l'importance de sensibiliser l'ensemble des collaborateurs de l'organisation aux processus de sécurité. « Dès le début de la collaboration, mais aussi tout au long de la vie du collaborateur dans l'organisation, les règles de sécurité et de confidentialité doivent être rappelées », insiste Gérard Peliks. En plus de faire signer une charte sur l'utilisation du réseau, l'organisation doit communiquer sur les conséquences juridiques de tout manquement au règlement intérieur.

---

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 :  
<http://www.lesechos.fr/thema/02167451759-conseils-pour-assurer-la-securite-numerique-des-nomades-1121036.php>  
Par Julie Le Bolzer

---

**Comment se protéger sur Internet ? Denis JACOPINI vous répond sur Sud Radio à l'occasion de la présentation de son livre « CYBERARNAQUES : S'informer pour mieux se protéger »**

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



**Comment se protéger sur Internet ? Denis JACOPINI vous répond sur Sud Radio à l'occasion de la présentation de son livre « CYBERARNAQUES : S'informer pour mieux se protéger »**

Internet et les réseaux sociaux ont envahi notre quotidien, pour le meilleur mais aussi pour le pire... Qui n'a jamais reçu de propositions commerciales pour de célèbres marques de luxe à prix cassés, un email d'appel au secours d'un ami en vacances à l'autre bout du monde ayant besoin d'argent ou un mot des impôts informant qu'une somme substantielle reste à rembourser contre la communication de coordonnées bancaires ? La Toile est devenue en quelques années le champ d'action privilégié d'escrocs en tout genre à l'affût de notre manque de vigilance. Leur force ? Notre ignorance des dangers du Net et notre « naïveté » face aux offres trop alléchantes qui nous assaillent.

*« Puisse cet ouvrage avoir de nombreux lecteurs ! Il ne devrait pas plaire aux arnaqueurs, car il est un réquisitoire contre leur perfidie et, sans aucun doute, une entrave à leur chiffre d'affaire. »*

*Général d'armée (2S) Watin- Augouard*

Commandez CYBERARNAQUES



Plutôt qu'un inventaire, Denis Jacopini, avec la collaboration de Marie Nocenti, a choisi de vous faire partager le quotidien de victimes d'Internet en se fondant sur des faits vécus, présentés sous forme de saynètes qui vous feront vivre ces arnaques en temps réel. Il donne ensuite de précieux conseils permettant de s'en prémunir. Si vous êtes confronté un jour à des circonstances similaires, vous aurez le réflexe de vous en protéger et en éviterez les conséquences parfois dramatiques... et coûteuses.

Un livre indispensable pour « surfer » en toute tranquillité !

Denis Jacopini est expert judiciaire en informatique, diplômé en cybercriminalité et en droit, sécurité de l'information et informatique légale à l'université de droit et science politique de Montpellier.

Témoin depuis plus de vingt ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus soigneusement élaborées, il apprend aux professionnels à se protéger des pirates informatiques.

Marie Nocenti est romancière.

---

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 cyberarnaqes dont chacun peut être victime.

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

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

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

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

---

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

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

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

Commandez sur Fnac.fr

---

[https://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 : *Cyberarnaques S'informer pour mieux se protéger – broché – Denis Jacopini, MARIE NOCENTI – Achat Livre – Achat & prix | fnac*

---

# Le site Internet d'une entreprise peut-il être contrôlé à distance par la Cnil ? | Denis JACOPINI

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





## Le site Internet d'une entreprise peut-il être contrôlé à distance par la Cnil ?

La réponse de Benjamin Vialle, agent au service des contrôles, Commission nationale de l'informatique et des libertés.

Oui. Depuis la loi du 17 mars 2014 relative à la consommation, la Commission nationale de l'informatique et des libertés (Cnil) a la possibilité de procéder à des contrôles en ligne, sur internet.

Ils permettent de constater à distance, depuis un ordinateur connecté à internet, des manquements à la loi informatique et libertés. Ces constatations sont relevées dans un procès-verbal adressé aux organismes concernés et leur seront opposables.

**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 : <http://www.courrierdesmairies.fr/51195/le-site-de-la-mairie-peut-il-etre-controle-a-distance-par-la-cnil>

---

# Voici 320 millions de mots de passe ... à éviter pour votre cybersécurité !

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

✘

✘

✘

✘

✘

✘

✘

**Voici 320 millions de mots de passe ... à éviter, pour votre cybersécurité !**

Le spécialiste en sécurité informatique Troy Hunt a mis à disposition un nouvel outil recensant 320 millions de mots de passe corrompus. Une base de données impressionnante qui devrait limiter de futurs impairs.

Boîtes mail corrompues, comptes piratés... chaque jour les cas se multiplient : virus et hackers sont bien présents, et ce, partout sur la toile. Personne n'est à l'abri et sans le savoir, vous utilisez peut-être vous-même un mot de passe corrompu. L'expert en sécurité informatique Troy Hunt en a détecté 320 millions !

Sur son site *Have I been pwned ?*, il était déjà possible de savoir si un compte avait été compromis. En indiquant son adresse mail ou son nom d'utilisateur, sans révéler le mot de passe associé, vous pouvez savoir si votre compte a été piraté et fait l'objet d'une fuite de données.

Depuis ce jeudi, le site propose désormais l'outil inverse : une collection de 320 millions de mots de passe consultables, déjà compromis, sans les identifiants associés. Car avec la multiplication des fuites de données, mieux vaut être armé. La CNIL conseille ainsi d'utiliser au moins 12 caractères et 4 types différents (minuscules, majuscules, chiffres et caractères spéciaux). Il faut également en changer régulièrement...[lire la suite]

---

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 : *Cyber-sécurité : voici 320 millions de mots de passe ... à éviter ! – LCI*

# Les 5 règles essentielles pour se protéger de la Cybercriminalité que les PME doivent absolument respecter

| Denis JACOPINI

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



Les 5 règles essentielles pour se protéger de la Cybercriminalité que les PME doivent absolument respecter

La protection des données numériques est rarement une priorité pour les dirigeants de PME alors même que les petites structures sont de plus en plus affectées par les problèmes de sécurité informatique et de cybercriminalité. Comment protéger votre entreprise ?



## Des PME de plus en plus touchées par la cybercriminalité

Les PME n'ont pas toujours conscience d'être devenues les cibles de prédilection des pirates informatiques, et pourtant celles-ci concentrent désormais **près de 80 % des attaques** en France ! Un chiffre en constante augmentation qui démontre un changement de stratégie de la part des «hackers» et «crackers» qui ciblent les petites structures du fait de leur sécurité souvent défectueuse.

Cette montée de la cybercriminalité concerne surtout le **vol de données numériques** (les fichiers clients, les coordonnées bancaires ou les contrats) qui sont ensuite revendues au plus offrant sur le marché noir. On note également des cas d'**espionnages économiques**, d'**escroqueries financières** ou de **sabotages des sites de commerce en ligne**.

Cibler une PME peut aussi être un moyen de s'attaquer à un plus gros poisson, dans le cadre d'une attaque de long terme. Puisqu'en infiltrant le réseau de cette petite structure, il devient plus facile de pénétrer par la suite dans celui d'un grand groupe dont elle est le sous-traitant.

Une problématique sérieuse d'autant que les entreprises victimes de cyberattaques font face à de sévères répercussions en termes de **pertes économiques** et d'**impact sur l'image de marque**. Ce risque peut néanmoins être réduit en appliquant quelques bonnes pratiques.

## Les règles essentielles pour bien protéger votre entreprise

1.  
**Sensibiliser les employés de l'entreprise**  
Il est recommandé d'organiser une campagne de sensibilisation pour informer les employés sur le danger bien réel de la cybercriminalité en insistant sur la nécessité de :
  - choisir des mots de passe d'au moins 12 ou 14 caractères mélangeant chiffres et lettres,
  - effectuer des sauvegardes fréquentes sur des supports externes ou une plateforme cloud,
  - adopter un usage prudent des messageries électroniques et des systèmes de paiement.
2.  
**Sécuriser l'ensemble des accès Internet**  
L'entreprise doit protéger tous les accès Internet (y compris les accès Wi-Fi) qui sont les principaux points d'entrée des pirates. De plus en plus de sociétés choisissent d'ailleurs d'installer un réseau privé virtuel (VPN) comprenant un seul et unique point d'échange sécurisé avec Internet.
3.  
**Uniformiser les logiciels et les maintenir à jour**  
Pour faire face aux nouvelles techniques d'attaques, il faut régulièrement mettre à jour les logiciels installés sur votre parc, dont les dernières versions doivent toujours être téléchargées sur les sites officiels des éditeurs. Une démarche qui peut être simplifiée en uniformisant le parc informatique avec un système d'exploitation et un logiciel de protection unique pour l'ensemble des appareils.
4.  
**Redoubler de vigilance avec les appareils mobiles**  
Il convient de faire preuve d'une vigilance particulière avec tous les appareils mobiles (smartphones et tablettes tactiles) qui sont généralement beaucoup moins sécurisés que les ordinateurs fixes, car chaque machine constitue une porte d'entrée potentielle pour les attaques informatiques.
5.  
**Adopter une politique de sécurité informatique**  
L'entreprise doit enfin mettre en place une politique de sécurité informatique précisant clairement les responsabilités de chacun et les procédures prévues en cas d'attaque, afin que les équipes ne soient pas prises au dépourvu et puissent reprendre l'activité le plus rapidement possible... [Lire la suite]

---

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 : *Cybercriminalité & PME : 5 règles pour se protéger | Microsoft pour les PME*