

# Pourquoi le vol de données personnelles devient-il de plus en plus commun ? | Denis JACOPINI

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



Pourquoi le vol de données personnelles devient-il de plus en plus commun ?

Des pirates informatiques Russes viennent de réaliser « le casse du siècle » en récoltant 1,2 milliard de comptes utilisateurs (identifiants et mots de passe associés) et plus de 500 millions d'adresses e-mail, provenant de 4200 000 site Internet d'entreprises de toute taille. NetIQ, fournisseur de solutions de #sécurité informatique, ne s'étonne pas de la multiplication de ce type de hack. Geoff Webb, Senior Director, Solution Strategy chez NetIQ, explique pourquoi le vol de données personnelles devient de plus en plus commun :

« Dans ce type de cas, la faute ne repose pas uniquement sur les hackers. Il faut aussi prendre en compte le comportement des entreprises et celui des utilisateurs finaux face à la sécurisation des accès.

Commençons par les hackers. De nos jours, il n'est pas nécessaire d'avoir un groupe sophistiqué et étendu de pirates informatiques expérimentés pour perpétrer les plus gros cyber-crimes. Aujourd'hui une simple recherche Internet permet à quiconque de rapidement trouver toutes les informations nécessaires pour pénétrer les systèmes informatiques vulnérables. Les pirates informatiques ont même cartographié toutes les vulnérabilités de la toile, et le tout est disponible en ligne. De plus, avec l'avènement du cloud, les hackers ont une porte d'entrée supplémentaire pour accéder aux données des entreprises. On entend régulièrement parler dans nos médias de la sécurité, ou plutôt du manque de sécurité lié au cloud.

Continuons avec les entreprises. Le cloud n'est pas le cœur du problème. Le problème de fond est que les entreprises ne mettent pas assez l'accent sur la sécurité des accès, que ça soit au niveau des accès cloud, aux applications d'entreprise, ou aux applications Web. Tant que les entreprises n'auront pas assimilé le caractère critique de la protection des mots de passe, ce type de hack continuera de se multiplier.

Enfin, il faut s'intéresser au comportement des utilisateurs finaux, qui ne facilitent pas la tâche des entreprises en matière de sécurité des mots de passe. En effet, de nombreuses études l'ont révélé récemment, par souci de facilité, les mots de passe utilisés sont souvent très (trop) simples. Les utilisateurs utilisent les mêmes mots de passe pour accéder à leurs comptes bancaires, messagerie électronique qu'elle soit personnelle ou professionnelle, et compte Facebook, par exemple. Ce comportement est une aubaine pour les cybercriminels. En laissant aux utilisateurs finaux le choix de leurs mots de passe, nous confions tout simplement une étape cruciale dans le processus de sécurisation des données à ceux qui sont les moins qualifiés et surtout les moins préoccupés par la sécurité informatique. Vous comme moi, nous n'avons pas envie d'avoir à nous souvenir de mots de passe compliqués et différents pour chaque compte que nous devons utiliser au quotidien. C'est donc bien notre propre comportement en tant qu'utilisateur qui constitue le plus gros risque.

On ne peut empêcher un hacker d'agir, mais on peut le stopper aux portes de l'entreprise en ayant des solutions de sécurité globale prenant en compte toutes les potentielles portes d'entrée. C'est pourquoi il est impératif que des solutions de gestion des identités et des accès soient intégrées dans les projets de sécurité des entreprises, au même titre que peut l'être la sécurisation des réseaux, ou des terminaux. »

---

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](#)



## Références

: <http://www.globalsecuritymag.fr/1-2-milliard-de-mots-de-passe,20140806,46775.html>

---

**Denis JACOPINI sur Europe 1  
parle de son livre «  
CYBERARNAQUES S'informer pour  
mieux se protéger » dans  
l'émission « Bonjour la  
France » avec Daphné BURKI  
et Ariel WIZMAN**

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



**Denis JACOPINI sur Europe 1  
parle de son livre «  
CYBERARNAQUES S'informer  
pour mieux se protéger »  
dans l'émission « Bonjour  
la France » avec Daphné  
BURKI et Ariel WIZMAN**

**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.**

Denis JACOPINI en parle ce jeudi 14 avril 2018 en direct sur Europe 1 dans l'émission « Bonjour la France » avec Daphné BURKI et Ariel Wizman



<http://www.europe1.fr/emissions/bonjour-la-france>



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](http://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*

---

**Denis JACOPINI sur Europe 1  
parle de son livre «  
CYBERARNAQUES S'informer pour  
mieux se protéger » ce jeudi  
12 avril 2018 en direct dans  
l'émission « Bonjour la  
France » avec Daphné BURKI  
et Ariel WIZMAN**

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



**Denis JACOPINI sur Europe 1  
parle de son livre «  
CYBERARNAQUES S'informer  
pour mieux se protéger » ce  
jeudi 12 avril 2018 en  
direct dans l'émission «  
Bonjour la France » avec  
Daphné BURKI et Ariel  
WIZMAN**

**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.** Denis JACOPIN en parle ce jeudi 14 avril 2018 en direct sur Europe 1 dans l'émission « Bonjour la France » avec Daphné BURKI et Ariel Wizman   
<http://www.europe1.fr/emissions/bonjour-la-france>



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](http://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*

---

# Sécurisez votre MAC avec Security Growler | Denis JACOPINI

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



Sécurisez votre  
MAC avec  
Security Growler

**Security Growler est un soft pour OSX qui se loge dans la barre de menu et qui vous alertera via le Centre de Notifications en cas d'événements suspects liés à la sécurité de votre Mac.**

Security Growler vous alerte lorsqu'il y a des tentatives de connexions SSH (ou des connexions réussies)...



Lorsque des connexions TCP entrantes ou sortantes ont lieu... (FTP, SMB, AFP, MySQL, PostgreSQL, partage iTunes, VNC)



Lorsqu'une commande utilisant « sudo » est lancée...



Lorsqu'un scan de ports déboule sans crier gare...



...etc., etc.

Security Growler permet de ne plus être en aveugle sur sa propre machine et d'être averti du moindre truc louche. Indispensable donc ! De plus, Security Growler est très économique : il consommera moins de 0,01% de votre CPU et jamais plus de 15 Mb de RAM. Et si vous utilisez Prowl, vous pourrez faire suivre les alertes sur votre iPhone / iPad. À télécharger [ici](#).

---

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 : Security Growler – Soyez aware sur la sécurité de votre Mac – Korben

---

# Votre employeur doit-il vous

# informer de la géolocalisation des véhicules professionnels ? | Denis JACOPINI

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



Votre employeur doit-il vous informer de la #géolocalisation des véhicules professionnels ?

---

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

---

**Avant d'installer un dispositif de géolocalisation dans les véhicules mis à disposition de ses employés, votre employeur doit d'abord consulter les représentants du personnel.**

De plus, il doit informer individuellement chaque employé utilisant ces véhicules de :

- L'identité du responsable du dispositif.
- L'objectif de la géolocalisation (sécurité d'un employé, suivi de facturation, etc. ).
- Les destinataires des informations issues de la géolocalisation (services des ressources humaines, service logistique, service de sécurité etc. ).
- Son droit d'opposition s'il a un motif légitime.
- Son droit d'accès et de rectification des informations le concernant enregistrées dans le système.

A la question « Votre employeur doit-il vous informer de la géolocalisation des véhicules professionnels ? »

La réponse est donc OUI

**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

---

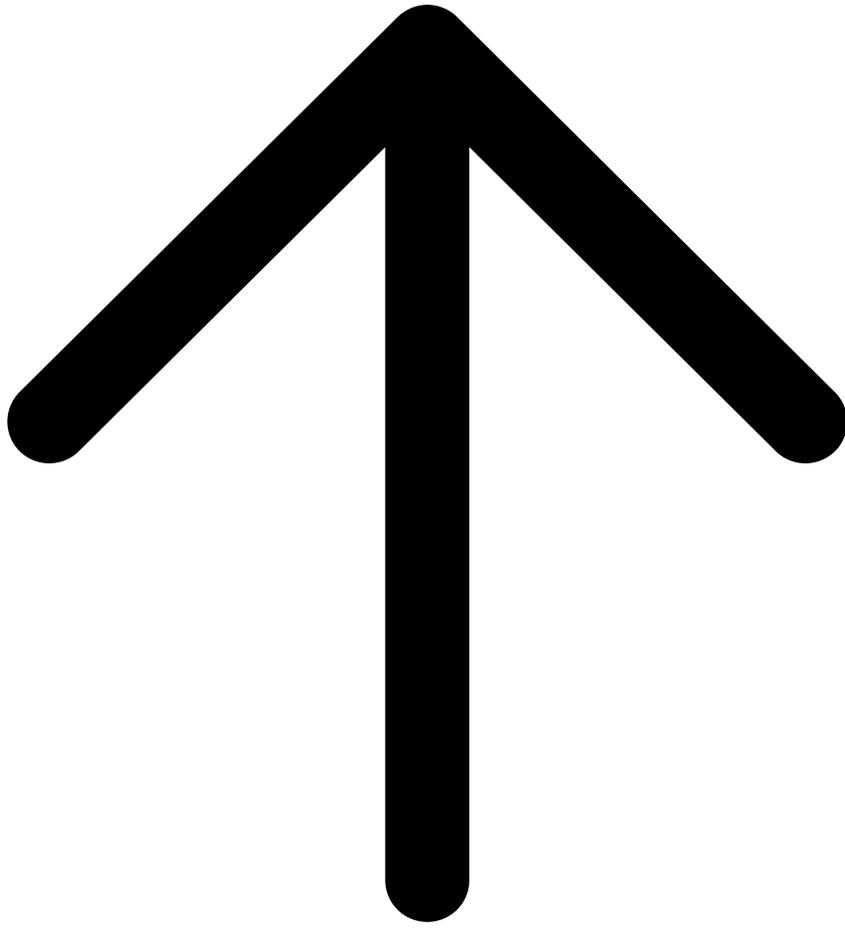
Source :  
<https://cnil.epticahosting.com/selfcnil/site/template.do?id=333&back=true>

---

# 3 nouvelles techniques de diffusion de phishing et virus identifiées | Denis JACOPINI

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





3 nouvelles  
techniques  
de  
diffusion  
de phishing  
et virus  
identifiées

Alors qu'auparavant le spam était essentiellement source de désagréments et de baisse de productivité, il sert également aujourd'hui à véhiculer des virus et des attaques par phishing très dangereuses.

L'e-mail reste la porte d'entrée préférée des hackers sur les réseaux d'entreprise. Ainsi, près de 90% des e-mails envoyés sur les adresses de messagerie professionnelles sont des spam. Alors qu'auparavant ces spam étaient essentiellement source de désagréments et de baisse de productivité, ils servent également aujourd'hui à véhiculer des virus et des attaques par phishing très dangereuses, qui gagnent continuellement en intensité et en intelligence.

Plusieurs finalités à ces attaques : voler des données (identifiants personnels, coordonnées bancaires, propriété intellectuelle, etc.), et de l'argent (via des trojan banking par exemple ou des cryptolocker et demandes de rançons) mais également infiltrer des réseaux pour mener des attaques ultérieures de plus grande envergure et développer des réseaux de botnets de plus en plus puissants pour diffuser encore plus de spam, virus et phishing.

### 3 nouvelles techniques identifiées

**> Des vagues qui utilisent des adresses IP non reconnues**

Les cybercriminels se servent de réseaux de botnets/spambots (réseaux de PC zombies) dont ils ont considérablement développé la puissance ces derniers mois. Grâce à ces réseaux, les cybercriminels sont en mesure d'envoyer régulièrement des vagues massives et intenses de spam – jusqu'à plusieurs millions de spam simultanément pour les plus gros réseaux. La force de ces campagnes de spam massives est qu'elles sont basées sur des réseaux de PC bénéficiant d'adresses IP non reconnues, que les outils de filtrage antispam classiques par signatures ou réputation ne sont pas en mesure d'identifier comme spam dans un premier temps.

L'utilisation d'adresses IP non blacklistées permet aux spam, et potentiellement aux virus et phishing de franchir les systèmes de filtrage – traditionnels basés sur les signatures ou réputation – qui ont besoin de temps pour identifier et blacklister ces nouvelles adresses. Pour les hackers, cela suppose toutefois de renouveler leurs réseaux de PC zombies non identifiés entre chaque attaque. On observe ainsi une période de 6 à 10 jours entre chaque très grosse vague de spam. Entre-temps les hackers se livrent surtout à de petites attaques pour infecter de nouveaux postes et ainsi faire croître leur réseau de PC zombies. Le seul moyen de bloquer efficacement ces vagues est d'utiliser le filtrage heuristique qui permet d'analyser le contenu des e-mails plutôt que de se baser uniquement sur son origine (réputation) ou sa propagation sur les réseaux et l'internet (signature).

**> Des virus à tout faire (polymorphes)**

Illustration de la nouvelle ère de l'industrialisation du hacking, les virus sont également de plus en plus intelligents. Alors qu'auparavant chaque virus était programmé pour une action précise, les virus actuels sont commandés à distance. Après avoir pénétré le réseau le plus discrètement possible, un virus actuel peut être commandé à distance et être utilisé au besoin par exemple comme actif d'un spambot de grande envergure voire même pour une attaque de cryptolockage.

**> Activation des liens URL de phishing après le passage du filtre**

En matière de phishing (phishing cible), les cybercriminels font également preuve de plus en plus d'intelligence pour faire évoluer leurs techniques. Ainsi, certains cybercriminels envoient des e-mails de phishing utilisant des liens URL activables à distance, une fois les outils de filtrage franchis. Cette technique permet aux e-mails de phishing de franchir le filtrage sans être détectés puisque les liens URL renvoient vers un contenu totalement légitime. Ce n'est qu'une fois les barrières franchies que les hackers vont les activer pour les faire renvoyer vers des sites de phishing frauduleux.

Cette technique de plus en plus utilisée est très efficace mais cependant encore peu répandue car elle n'est techniquement pas à la portée de tous les hackers.

Le hacking s'est fortement industrialisé ces dernières années. Les techniques utilisées pour diffuser du spam massivement et des virus sont de plus en plus intelligentes et dangereuses pour les entreprises. Pour se protéger mieux, l'éducation et la formation des utilisateurs sont des axes primordiaux d'où l'importance de rappeler quelques règles de base :

- N'ouvrir les pièces jointes suspectes (fichiers .zip, .xls ou .doc.) que si l'expéditeur est confirmé.
- Supprimer le message d'un expéditeur suspect inconnu sans y répondre.
- Refuser de confirmer l'accusé de réception dans le cas d'un expéditeur inconnu suspect. Cela risquerait de valider et diffuser l'adresse e-mail de l'utilisateur à son insu.
- Remonter les emails identifiés comme spam auprès de son service informatique. Ils seront ensuite transmis à l'entreprise chargée de la protection des messageries pour une prise en compte dans la technologie de filtrage.
- Et en cas de doute, contacter son service informatique.

---

## 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

Source : <http://www.journaldunet.com/solutions/expert/62660/diffusion-d-e-phishing-et-virus-3-nouvelles-techniques-identifiees.shtml>

# Les 6 conseils pour se protéger des Cryptovirus (Ransomwares)

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>Les 6 conseils pour se protéger des Cryptovirus (Ransomwares)</b>				

Alors que l'ANSSI vient d'annoncer un MOOC pour aider les entreprises à bien se protéger suite aux dernières attaques informatiques comme WannaCry, on réalise que la sécurité d'une entreprise doit être avant tout l'affaire de tous ses employés, et pas simplement des équipes dédiées au sein du service informatique. Après tout, la capacité de résistance de toute organisation dépend de son maillon le plus faible.

Une partie des financements devrait avoir pour objectif d'aider les entreprises à développer un programme de sensibilisation aux pratiques de cybersécurité spécialement adapté aux problématiques des PME. En effet, contrairement à leurs homologues des grandes entreprises, les dirigeants des PME sont généralement davantage impliqués dans des décisions d'ordres variés ce qui influe directement sur leur capacité à consacrer le temps ou l'attention nécessaires à la sécurité des systèmes d'information.

Tout programme conçu pour sensibiliser les employés aux méthodes de protection des menaces devrait en premier lieu viser à développer les connaissances des meilleures pratiques à tous les échelons hiérarchiques. Thibaut Behaghel, Spécialiste Produits International au sein du gestionnaire de mots de passe LastPass, nous explique à quoi pourrait ressembler un tel programme pour les petites et moyennes entreprises, et qu'elles devraient en être les priorités.

### **1. Respecter les principes de bases**

En matière de sécurité, il existe un certain nombre de principes de base à suivre pour toutes les organisations, à commencer par la mise en place de règles concernant la longueur, la complexité et la durée de validité des mots de passe...[lire la suite]

### **2. Gérer les accès des utilisateurs**

Quel que soit le nombre d'employés de votre entreprise, il est essentiel que chacun d'entre eux n'ait accès qu'aux informations et aux données qu'il est autorisé à consulter...[lire la suite]

### **3. Définir une politique de sécurité**

Toute organisation devrait créer une politique détaillant les mesures de sécurité prises à la fois au niveau de l'entreprise elle-même, et par l'ensemble de ses employés...[lire la suite]

### **4. Former les salariés**

Une fois la politique de sécurité mise en place, il est nécessaire de former les employés afin qu'ils en connaissent les règles et qu'ils sachent comment les respecter...[lire la suite]

### **5. Sécuriser les réseaux sans fil**

Les PME doivent utiliser des mots de passe administrateurs et d'accès aux réseaux forts, et choisir des protocoles de chiffrement éprouvés (WPA2 et AES)...[lire la suite]

### **6. Savoir reconnaître le phishing**

En cas de doute, il ne faut prendre aucun risque. Les entreprises doivent montrer à leurs employés comment repérer et signaler des e-mails suspects...[lire la suite]

[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** ;



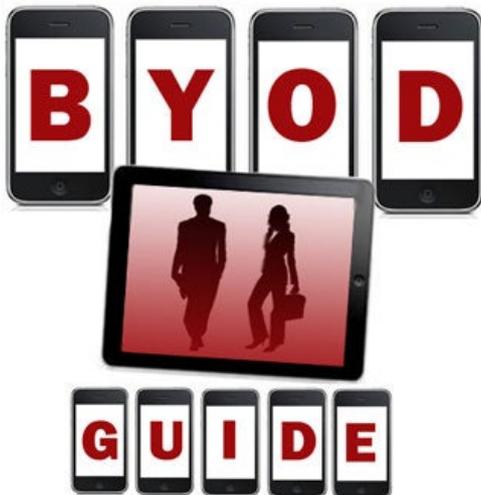
[Contactez-nous](#)



Source : *Ransomware : les 6 conseils pour se protéger*

# BYOD Matériel personnel au travail et matériel professionnel à la maison : 12 points pour une bonne sécurité | Denis JACOPINI

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



BYOD  
Matériel  
personnel au  
travail et  
matériel  
professionnel à  
la maison : 12  
points pour une  
bonne sécurité

Si l'on parle souvent des avantages et des désagréments du BYOD, la base reste après tout d'adopter la politique qui correspond aux besoins de l'entreprise. Cela permet ainsi de savoir si l'on applique un BYOD total ou un CYOD (Choose Your Own Device) voire un COPE (Corporate Owned, Personally Enabled).

Et pour arriver aux bonnes conclusions, il faut se poser les bonnes questions.

## **1. Le BYOD : mais pour qui ?**

C'est en premier lieu une question fondamentale. Faut-il permettre le BYOD à l'intégralité des employés, ou juste certains métiers, uniquement les cadres voire seulement les principaux dirigeants ? Répondre à cette question est primordial avant de mettre en place une bonne politique de BYOD, car de cette réponse découleront bien des conséquences.

Il faut toutefois bien avoir en tête que si tout le monde n'est pas autorisé à pratiquer le BYOD, cela n'empêchera pas certains d'amener leurs appareils sans prévenir qui que ce soit, ce qui pourrait créer quelques complications par la suite. Intégrer une telle donnée est indispensable.

## **2. Quels appareils ?**

Une fois le personnel concerné enfin déterminé, il convient de se poser une question équivalente sur les appareils. Faut-il tous les accepter ? Se limiter à une marque ou un système d'exploitation particulier ? Aujourd'hui, même si les Androphones et les iPhone captent la majeure partie du marché, cibler les appareils acceptés est aussi un élément majeur qui simplifiera la vie du DSI et du patron.

Par exemple, n'autoriser que des appareils sous iOS dont la dernière version a été installée impliquera une gestion moins complexe que de permettre tous les Androphones, vieux comme récents, qui ne fonctionneront même pas sous la même version d'Android et qui comptent des dizaines de marques différentes. Et la logique est similaire pour les tablettes tactiles.

### **3. Quelles applications ?**

On connaît désormais qui pourra exploiter le BYOD et quels appareils seront concernés. Très bien. Reste désormais à régler la question tout aussi fondamentale des logiciels. Quelles applications seront acceptées ? Certaines bien spécifiques devront-elles être installées ? Seront-elles extérieures à l'entreprise ou programmées en interne spécifiquement pour les employés ? Est-il utile ou non de passer par une interface multi-OS et multi-écran à la Exo U ?

Là encore, afin de mettre en place une bonne politique de BYOD, toujours en fonction des besoins de l'entreprise, cibler les applications autorisées est primordial. Mais là encore, le risque que l'employé utilise d'autres applications est réel et doit être pris en compte. Plus on impose de limite et plus les mauvaises surprises sont multipliées. L'avantage de laisser une liberté totale est donc que les parades à cette liberté seront calculées.

### **4. Impliquer toutes les branches de l'entreprise**

Une fois les trois premiers points enfin réglés, si l'on souhaite que la politique de BYOD se passe pour le mieux, il faut impliquer toutes les branches de l'entreprise. Que ce soit les ressources humaines, les juristes, évidemment le DSI, etc. Pourquoi ? Tout simplement, et c'est toujours la même chose, pour une question de besoin, mais aussi ici de précision.

Le responsable des RH apportera forcément un regard différent du DSI, qui lui-même ne pensera pas aux mêmes problématiques que le juriste. L'un insistera pour que les règlements quant au BYOD traitent bien des différences entre les données privées et professionnelles. Un autre pensera à l'aspect technique,

tandis que son voisin préviendra des différents risques de plaintes.

## **5. Mettre en place une infrastructure réseau suffisante**

Vous savez qui utilisera quoi et comment. Vous pouvez donc prévoir (à peu près) quel sera le trafic qui sera utilisé dans votre entreprise tous les jours. Et qui dit BYOD dit généralement une utilisation bien plus forte des réseaux mobiles, que ce soit en Wi-Fi ou en 3G/4G. Une augmentation qu'il faut donc prévoir si vous voulez éviter que vos employés commencent sérieusement à s'agacer des débits.

Sachant que certains employés peuvent avoir deux, trois voire quatre appareils en même temps connectés, il est capital de mettre en place l'infrastructure suffisante pour assurer un réseau de qualité. Augmenter ses débits fixes et obtenir des routeurs Wi-Fi puissants sera probablement indispensable. Il faudra de plus s'assurer que les forfaits mobiles des employés soient suffisamment volumineux.

## **6. Simplifiez, soyez clair et prévoyez**

Lorsque vous allez commencer à mettre au point vos règles de politique de BYOD, il faut à la fois penser à la simplifier tout en prévoyant le futur. Faire simple, être direct et clair permet d'éviter les failles et les abus de ces dernières. Utiliser les mots justes et précis, c'est s'assurer que les règles seront bien appliquées.

Enfin, il faut absolument prévoir. Le marché évolue à grande vitesse et vos règles du jour ne seront peut-être pas viables dans trois ans ou peut-être même moins. Il faut donc là encore

ne pas être trop spécifiques aux produits du moment et généraliser afin d'englober les appareils et les applications du futur.

## **7. La sécurité**

C'est l'évidence même, on ne cesse d'en parler, c'est généralement la priorité numéro un des entreprises (BYOD ou non), la sécurité est un point majeur à régler. Elle dépendra évidemment des sujets 1, 2 et 3 évoqués dans notre précédent article, à savoir ceux rapportés aux utilisateurs de BYOD, aux appareils autorisés et aux applications permises.

La sécurité pour le BYOD, ce sont des règles de bonnes conduites et des règles techniques. Que ce soit par rapport au cloud, à l'accès aux données sensibles selon les réseaux utilisés, aux mises à jour des logiciels, aux mots de passe, aux protections, à la perte de l'appareil, etc. Tout doit être réglé au millimètre et prévoir toutes les catastrophes possibles est indispensable.

Et surtout, la sécurité implique un rapport de confiance entre l'employé et sa direction. La pire des situations seraient que l'employé se soit rendu compte qu'il a subi un vol de données et qu'il ne dise rien. La transparence et la rapidité sont ainsi indispensables pour assurer un maximum de sécurité.

## **8. La question des données personnelles**

Outre le plan sécuritaire, celui du droit et du respect des données privées doit aussi être réglé. S'arranger pour séparer les données privées/personnelles des données professionnelles dans les appareils est ainsi plus que conseillé. L'entreprise

doit le faire pour ses employés mais aussi pour elle-même, ne serait-ce que pour éviter quelques désagréments et plaintes dans le futur.

### **9. Avoir la mainmise sur l'appareil**

Certes, dans le cadre du BYOD, le PC portable, le smartphone ou la tablette appartient à l'employé. Néanmoins, comme pour les données personnelles, dès lors que le professionnel s'intègre dans l'appareil, l'entreprise a donc un droit de regard.

Il faut donc bien faire comprendre à l'employé que son appareil personnel peut être surveillé et que l'entreprise peut avoir accès à certaines données, y compris personnelles. Clarifier ce point dès le départ évite ainsi les mauvaises surprises.

### **10. Quelles solutions MDM ?**

MDM, signifie Mobile Device Management, que l'on peut traduire en gestion des terminaux mobiles. Les solutions MDM sont indispensables pour toutes les entreprises (surtout les grandes) qui disposent d'une flotte importante d'appareils, qu'ils appartiennent ou non à l'employé par ailleurs.

Dans le cadre strict du BYOD, les solutions MDM ont souvent l'avantage d'être multiplateforme et sont l'une des armes pour sécuriser son réseau et ses données. Elles permettent en effet d'identifier les terminaux mobiles connectés, de les activer et les désactiver comme on le souhaite, d'installer des applications à distance, de les mettre à jour, de bloquer les appareils à distance ou des applications spécifiques, de

géolocaliser les appareils, d'imposer des mots de passe ou même le chiffrement des données, etc. En somme, un BYOD sans MDM paraît presque impensable.

### **11. En cas de casse ou de vol**

Même si l'appareil n'appartient pas à l'entreprise, il faut néanmoins prévoir le cas où ce dernier casserait, tomberait en panne ou tout simplement serait volé. Les données présentes sur l'appareil ou disponibles à distance peuvent être sensibles et prévoir une telle éventualité est obligatoire quand on sait que les cas de casses et de vols sont nombreux.

Bien entendu, un système de blocage à distance est indispensable en cas de vol, tout comme le fait de chiffrer ses données. Pour la casse, moins il y a de données stockées directement dans l'appareil (sans copie en ligne), moins la situation sera catastrophique.

### **12. En cas de départ**

Enfin, on n'y pense pas toujours, mais si l'employé vient avec son appareil, il repart évidemment avec en cas de départ, de fin de contrat ou de licenciement. C'est un point crucial à ne pas manquer dès le début de la politique de BYOD.

Il faut ainsi prévoir à l'avance le futur départ de l'employé et par conséquent le rapatriement de toutes les données qu'il détient, en sus de leur suppression sur son ou ses appareils. Dans le même esprit, il faudra donc l'empêcher d'avoir accès via ses appareils aux réseaux et serveurs de l'entreprise. Cela peut là encore éviter certains désagréments.

---

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.zdnet.fr/actualites/12-points-a-traiter-pour-une-bonne-politique-de-byod-1-2-39804195.htm>

# Un employeur peut-il consulter les courriels d'une messagerie professionnelle d'un de ses salariés ?

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

x

x

x

x

x

x

x

Un employeur peut-il consulter les courriels d'une messagerie professionnelle d'un de ses salariés ?

**Un employeur peut-il consulter les courriels d'une messagerie professionnelle d'un de ses salariés ?**

« L'employeur ne peut, hors présence du salarié, consulter ses messages sans son autorisation. Car, potentiellement, il pourrait y trouver des messages dits «personnels». Le principe, c'est qu'une messagerie ne peut pas être 100 % professionnelle. Quand on écrit un message à son conjoint pour le prévenir qu'on va être en retard par exemple. C'est donc toléré mais il ne faut pas en abuser. La seule condition pour l'employeur est dans le cas d'un danger grave : concurrence déloyale ou terrorisme. Mais, dans ce cas, cela nécessite la présence d'un huissier. »

---

Réagissez à cet article

**Quelques articles sélectionnés par nos Experts :**

Quels sont les droits et devoirs des salariés en matière de sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

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

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

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)

---

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

**Besoin d'une formation pour apprendre à vous mettre en conformité avec le RGPD ?**

## Contactez-nous

---



Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a 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 facile pour moi d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.

*« Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services. ».*

Source : *Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord*

---

# Denis JACOPINI en direct sur LCI vendredi pour nous parler Cybercriminalité | Denis JACOPINI



Invité de l'émission d'information de Valérie Expert « Choisissez votre camp », Denis JACOPINI nous présentera Vendredi un état des lieux de la cybercriminalité et les différentes formes d'arnaques par Internet.

Sur le plateau de LCI nous parlerons Fichier infecté, arnaques et phishing, arnaques par Internet et aussi par téléphone avec un représentant de 60 millions de consommateurs.

A vendredi.

---

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 : Denis JACOPINI