

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



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

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

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

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

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

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

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

---

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

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

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

Contactez-nous

---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

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

---

# GDPR compliance: Request for costing estimate

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



**GDPR compliance:  
Request for  
costing estimate**

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

1. Are you looking for autonomy ? We can assist you to learn the essentials of European regulations relating to the Protection of Personal Data and the necessary to understand and start a compliance. Once the training is completed, you are independent but can always count on our support either in the form of personalized training, or in the form of personalized support. At the end of this training, we will give you a certificate proving the implementation of a process to bring your establishment into compliance with the GDPR (General Data Protection Regulations). For information, we are referenced to the CNIL.

2. Do you want to be accompanied for the implementation of compliance ? We carry out for you the audit which will highlight the points to be improved. At the end of this stage you can, if you wish, achieve compliance or let us proceed with the improvements that you have validated; At the end of this audit, we will give you a report proving the implementation of corrections as part of your process to bring your establishment into compliance with the GDPR (General Data Protection Regulations).

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

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

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

Your First Name / NAME (required)

Your Organization / Company (required)

Your email address (required)

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

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

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

#### YOUR ACTIVITY

Details about your activity :

Are you subject to professional secrecy?

Yes@NoI don't know

Does your activity depend on regulations?

Yes@NoI don't know

If "Yes", which one or which ones?

#### YOUR COMPUTER SYSTEM

Can you describe the composition of your computer system. We would like, in the form of an enumeration, to know the equipment which has any access to personal data with for each device ALL the software (s) used and their function (s) .

Examples :

- 1 WEB server with website to publicize my activity;

- 1 desktop computer with billing software to bill my clients;

- 2 laptops including:

> 1 with email software to correspond with clients and prospects + word processing for correspondence + billing software to bill my clients ...

> 1 with email software to correspond with customers and prospects + accounting software to do the accounting for my company ;

- 1 smartphone with email software to correspond with customers and prospects.

Do you have one or more websites?

Yes@NoI don't know

What is (are) this (those) website (s)?

Do you have data in the Cloud?

Yes@NoI don't know

Which cloud providers do you use?

#### YOUR PERSONAL DATA PROCESSING

If you have already established it, could you provide us with the list of processing of personal data (even if it is incomplete)?

#### SIZING YOUR BUSINESS

Number of employees in your structure :

How many of these employees use computer equipment ?

Number of departments or departments \*\* in your structure (example: Commercial service, technical service ...) :

Please list the services or departments \*\* of your structure:

#### SERVICE PROVIDERS & SUBCONTRACTORS

Do you work with sub-contractors?

Yes@NoI don't know

Please list these subcontractors :

Do you work with service providers who work on your premises or in your agencies (even remotely) ?

Yes@NoI don't know

Please list these providers :

How many IT companies do you work with ?

Please list these IT companies indicating the products or services for which they operate and possibly their country of establishment :

#### YOUR SITUATION TOWARDS THE GDPR

Does your establishment exchange data with foreign countries ?

Yes@NoI don't know

If "Yes", with which country(ies)?

Have you already been made aware of the GDPR ?

Yes@NoI don't know

Have people using IT equipment already been made aware of the GDPR ?

Yes@NoI don't know

If you or your employees have not been made aware of the GDPR, would you like to undergo training ?

Yes@NoI don't know

#### YOUR WORKPLACE

The analysis of the data processing conditions in your professional premises or your professional premises is part of the compliance process.

Do you have several offices, agencies etc. legally dependent on your establishment ?

Yes@No

If "Yes", how much ?

In which city (ies) (and country if not in France) do you or your employees work ?

#### TYPE OF SUPPORT DESIRED

We can support you in different ways.

A) We can teach you to become autonomous (training) :

B) We can support you at the start and then help you become independent (support, audit + training) :

C) We can choose to entrust us with the entire process of compliance (support) :

D) We can accompany you in a personalized way (thank you to detail your expectations).

IP barodatee est également collectée. What type of support do you want from us (A / B / C / D + details) ?

#### END OF QUESTIONNAIRE

If you wish, you can send us additional information such as:

- Emergency of your project;

- Any additional information that you deem useful to allow us to better understand your project.

Les informations recueillies sont enregistrées dans la messagerie électronique et le système informatique de LenetExpert pour les traitements correspondant à la gestion de vos demandes et la proposition de services correspondant à votre demande. Le lieu de traitement de stockage et de sauvegarde se situe en France et auprès d'établissements respectant le bouclier de protection des données UE-Etats-Unis (en anglais : EU-US Privacy Shield). Elles sont conservées 3 ans après notre dernier échange et sont destinées aux services internes. Une démarche de mise en conformité a été entamée en interne depuis 2019 et jusqu'à ce jour par des formations régulières, l'identification des traitements, la réalisation d'un registre des traitements, une analyse de risques sur nos traitements manipulant des données sensibles ou des « données à caractère hautement personnel » pour lesquels leur violation pourrait avoir de graves conséquences dans la vie quotidienne des personnes concernées et un suivi semestriel. Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 dit RGPD (Règlement Général sur la Protection des Données), à la loi n°78-17 dite «Informatique et Libertés» du 6 janvier 1978 et à la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier en contactant Le Net Expert, Monsieur le Délégué à la Protection des Données - 1 les Magnolias - 84300 CAVAILLON par Remandé avec accusé de réception. Enfin, sur le fondement des articles 131-13, 222-17, 222-18, 222-18-1, 322-12, 322-13, R-621-1, R-621-2, R-623-1, R-624-3, R-624-4, R-631-1 et R634-1 du code Pénal et l'article 29 de la loi du 29 juillet 1881 sur la liberté de la presse, votre adresse IP barodatee est également collectée.

Sauf indication contraire ou information publique, nous nous engageons à la plus totale discrétion et la plus grande confidentialité concernant les informations que vous nous communiquez.

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

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

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




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

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

---

**RGPD : Que se passe t-il si le 25 mai 2018 nous n'avons pas terminé notre mise en conformité ?**

	<b>RGPD : Que se passe t-il si le 25 mai 2018 nous n'avons pas terminé notre mise en conformité ?</b>
---	---

---

**Le Net Expert : Denis JACOPINI, vous êtes spécialisé dans l'accompagnement des PME dans la mise en conformité avec le RGPD depuis plusieurs années. Que se passe t-il si le 25 mai 2018 nous n'avons pas terminé notre mise en conformité avec Le RGPD ?**

Si le 25 mai 2018 vous n'avez pas terminé votre mise en conformité avec le RGPD ou pire, vous venez à peine de l'initier pour votre entreprise, association ou administration, stricto sensu, en tant que responsable de traitement pénalement responsable, vous devenez amendable et les sanctions encourues, forcément pécuniaires selon les cas, pourraient être accompagnées de peines de prison comme le précise l'article 226-17 du Code pénal.

Ainsi, le Règlement sera « obligatoire dans tous ses éléments et directement applicable dans tout État membre », dont la France dès le 25 mai 2018, et puisqu'il s'agit d'un règlement, celui-ci entrera directement en vigueur, sans nécessiter de législation de transposition.

En réalité, avant que soient engagées des sanctions à votre encontre, vous serez contacté par la CNIL, laquelle vous demandera certainement de justifier les mesures prises à l'égard du Règlement Européen. Il est clair qu'au plus vous faites preuve de négligence, de mauvaise foi et de résistance, les sanctions risquées se rapprocheront du maximum à savoir la plus grande valeur entre 4% de votre chiffre d'affaire mondial ou 20 millions d'euros.

Si par contre, vous avez entamé une démarche de mise en conformité à savoir au minimum commencé à suivre une formation, désigné officiellement une personne (interne ou externe à votre entreprise) à cette démarche réglementaire et même si vous en êtes seulement au stade où vous avez commencé à établir la liste de vos traitements avec les risques inhérents à la vie privée et aux libertés fondamentales des propriétaires des données à caractère personnel et si possible vous avez commencé à mettre en place des mesures correctives, vous montrerez ainsi à l'autorité administrative indépendante de contrôle du bon respect de la réglementation relative à la protection des données à caractère personnel (la CNIL en France) que vous avez pris en compte cette démarche dans votre organisation, pris au sérieux des défaillances en matière juridique ou technique de votre organisation et que des améliorations sont en cours. L'ensemble des démarches accomplies même après le 25 mai 2018 joueront en votre faveur en anéantissant les risques de sanction, bien évidemment à condition que vous ne fassiez aucune victime en cas de fuite de données avant.



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

A Lire aussi :

Mise en conformité RGPD : Mode d'emploi

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

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

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

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)

**Notre métier :** Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles



Réagissez à cet article

Source : Denis JACOPINI (Expert Informatique spécialisé RGPD)

# Comment déjouer les arnaques aux distributeurs automatiques de billets (DAB)

**Comment déjouer les arnaques aux distributeurs automatiques de billets (DAB) ?**

---

**Déjouer les escroqueries au DAB et adopter les bons gestes pour s'en prémunir, par la brigade des fraudes aux moyens de paiement**

**Denis JACOPINI :**

Parce que nous considérons que notre connaissance des risques et le premier rempart contre les pirates, nous avons souhaité partager avec vous cette vidéo.

N'hésitez pas à nous contacter pour l'organisation de sessions de formations ou de conférences de sensibilisation aux risques informatiques, pour apprendre à vous protéger des pirates, des arnaques et limiter ainsi votre exposition à ces pièges.

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

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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



Réagissez à cet article

---

**Attaque informatique TV5  
Monde – Denis JACOPINI  
interviewé par un journaliste**

# de Canal Plus pour le JT de Direct8 | Denis JACOPINI

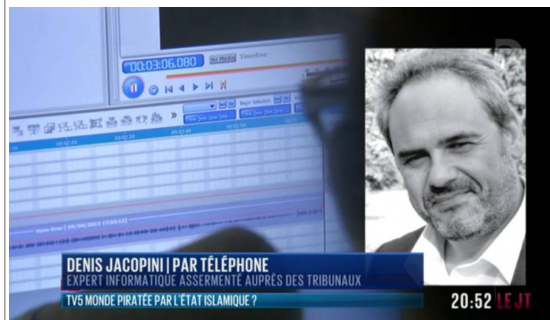
Attaque  
informatique TV5  
Monde - Denis  
JACOPINI, interviewé  
par un journaliste  
de Canal Plus pour  
le JT de Direct8



A la suite de l'attaque informatique ayant visé TV5 Monte, le 9 avril dernier, pendant qu'il se trouvait à un Colloque international sur la Cybercriminalité à Montpellier organisé par Adel JOMNI, Denis JACOPINI a été interviewé par un journaliste de Canal Plus et certains propos retenus pour le JT de 20h45 sur Direct 8.

**D'après-vous, pourquoi les pirates ont choisi la chaîne de télévision TV5 Monde comme cible de leur attaque informatique ?** Lorsque des pirates ou des cybercriminels décident d'attaquer un système informatique, il le font principalement pour les raisons suivantes :- A la suite d'une sorte de défi qu'ils se sont lancés afin de prouver leur capacité à pirater un système qui s'est par exemple déclaré comme système inviolable...- Afin de récolter de l'argent soit en menaçant de diffuser des informations secrètes, soit en vendant les informations piratées, soit en prenant en otage un serveur en le bloquant et tout cela, contre rançon.

- Ou bien, dans le but de diffuser un message idéologique, prônant un message politique, religieux... Dans ce cas, l'objectif premier des cyber-attaquants est la diffusion à grande échelle d'un message (c.f. les defacements de plus de 25000 sites Internet à la suite des attentats contre Charlie Hebdo). Que le plus de personnes possibles puisse prendre connaissance d'un message en y associant une sensation de puissance, tel a été le type d'attaque contre TV5 Monde. Cette attaque, a été destinée avant tout à diffuser un message idéologique, en touchant un média à couverture mondiale pour qu'on parle le plus possible des attaquant et de leur symbole.



#### **Quelle a été la technique utilisée lors de l'attaque des serveurs de TV5 Monde ?**

Les cybercriminels utilisent généralement 2 types de méthodes pour pénétrer dans un système informatique :

- la recherche de failles
- la naïveté d'un destinataire à un e-mail

C'est un voire même plusieurs e-mails, de type phishing qui semblent être à l'origine, depuis probablement plusieurs semaines ou mois, de l'intrusion du système informatique de TV5 monde par les cybercriminels. Une fois introduits dans le système informatique, l'accès invisible ou silencieux à des informations confidentielles ou secrètes permet ensuite de trouver les clefs autorisant de se répandre dans un réseau et contaminer ainsi le plus possibles d'organes sensibles ou stratégiques.

Une fois tous ces accès ainsi possibles, il suffit de coordonner une attaque simultanée de tous ces fruits devenus véreux pour donner l'impressionnante vision d'un arbre prêt à tomber.

*« Il suffit d'envoyer tous les jours un email avec un virus auprès de différentes personnes de différents services et à un moment ou un autre il va bien y a voir quelqu'un qui va l'ouvrir.*

*Son vrai travail va commencer lorsque quelqu'un aura mordu à l'hameçon »*

#### **Peut-on conclure que n'importe quelle chaînes de télévision peuvent être victime de cyber-attaques telles que celle dont a été victime TV5 monde ?**

La faille qu'ont exploité les cybercriminels dans le cadre de l'attaque informatique de TV5 monde est une faille humaine. En effet, recevoir un e-mail nous incitant à cliquer sur un lien qui va contre notre volonté et de manière complètement invisible changer dans son ordinateur un logiciel malveillant chargé, de manière tout aussi silencieuse, de prendre le contrôle de notre ordinateur est devenu le moyen d'attaque le plus utilisé.

Les systèmes informatiques des chaînes de télévision sont certes équipées de moyens de protection techniques contre les virus, les codes malveillants et autres types d'attaques, mais les cybercriminels auront toujours un coup d'avance en exploitant la faille humaine, principalement par manque de connaissance ou manque de formation de la part des utilisateurs.

#### **Existe t-il un moyen de se protéger contre ce type d'attaque ?**

Les organismes et entreprises ont pris trop de retard pour mettre en place des politiques de sécurité informatique. Quand on voit qu'en 2013, moins de 100 000 entreprises en France s'étaient mises en conformité avec la CNIL, excellent point de départ pour mettre en place des mesures de sécurité sur les données personnelles, il y a de quoi s'inquiéter sur la manière dont nos données (mot de passe y compris) sont sécurisées.

Commencer par se mettre en conformité avec la CNIL serait un bon début...

<http://www.lenetexpert.fr/wp-content/uploads/2015/04/Denis-JACOPINI-interviewé-par-journaliste-Canal-plus-pour-JT-de-Direct-8.mp4>

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

Après cette lecture, quel est votre avis ?  
Cliquez et laissez-nous un commentaire...

Source : <http://www.bfmtv.com/culture/l-attaque-contre-tv5monde-enclenchee-des-fin-janvier-877334.html>

---

**Que faire en cas de fraude sur sa carte bancaire ?**

<input type="checkbox"/>	<b>Que faire en cas de fraude sur sa carte bancaire ?</b>
--------------------------	---

---

**De plus en plus d'usagers de la banque sont victimes de l'utilisation frauduleuse de leur carte alors même qu'ils ne l'utilisent pas pour leur achat sur le net. Pourtant il arrive de plus en plus fréquemment que certains d'entre eux constatent des sommes prélevées sur leur compte bancaire en consultant leur relevé bancaire.**

Que faire en cas de fraude sur sa carte ? Quelles sont les démarches pour déclarer une utilisation frauduleuse de sa carte bancaire ?

Selon les disposition de l'article L 133-24 du Code Monétaire et Financier, la responsabilité du propriétaire d'une carte bancaire n'est pas engagée dans le cas où la carte a été contrefaite ou si l'achat contesté n'a pas été effectué avec l'utilisation physique de la carte.

Les titulaires de carte victimes d'une utilisation frauduleuse sur Internet ont un délai de 13 mois pour contester les sommes prélevées sur leur compte bancaire. Ils doivent se rendre auprès de sa banque et s'opposer formellement aux transactions effectuées ou au paiement des opérations en question.

#### **Quelles sont les démarches à faire auprès de sa banque ?**

En cas d'usurpation des données de sa carte bancaire, il faut :

- Appeler sa banque le plus rapidement possible pour le signaler par téléphone.
- Envoyer à sa banque une lettre qui confirme la mise en opposition de la carte utilisée frauduleusement,
  - Un document qui décrit toutes les opérations contestées, les coordonnées bancaires et le motif de l'opposition de la carte,
- Une attestation (AFFIDAVIT) certifiant que la carte a toujours été en sa possession et qu'elle n'a jamais été cédée ou prêtée.

La loi de 2001 sur la protection du consommateur n'exige pas de dépôt de plainte auprès de la gendarmerie. Il n'est donc pas nécessaire de porter plainte pour que la banque procède aux remboursement des sommes usurpées.

Selon les articles L133-19 et L 133-20, la banque doit rembourser toutes les sommes prélevées à compter de la date d'opposition ainsi que tous les frais liés à l'opposition de la carte bancaire.

#### **Pour éviter une usurpation de sa CB, voici quelques conseils et certaines mesures de sécurité à prendre :**

- ne jamais laisser la carte bancaire à la vue d'un quelconque public (ex :
  - exposée la CB dans la voiture ou sur un bureau),
- penser à reprendre sa carte bancaire dans les terminaux de paiement après chaque achat,
- détruire les tickets de paiement avant de les jeter car ils comportent le code de la carte bancaire,
  - ne jamais dire le numéro ni le code secret de la carte bancaire à quiconque,
  - ne pas oublier de signer au dos de la carte bancaire.

Source : Banque-en-ligne.fr *Que faire en cas de fraude sur sa carte bancaire ?*

#### **LE NET EXPERT**

- **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**
  - ANALYSE DE VOTRE ACTIVITÉ
  - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
    - IDENTIFICATION DES RISQUES
    - ANALYSE DE RISQUE (PIA / DPIA)
  - MISE EN CONFORMITÉ RGPD de vos traitements
  - SUIVI de l'évolution de vos traitements
  - **FORMATIONS / SENSIBILISATION :**
    - CYBERCRIMINALITÉ
  - PROTECTION DES DONNÉES PERSONNELLES
    - AU RGPD
    - À LA FONCTION DE DPO
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
  - ORDINATEURS (Photos / E-mails / Fichiers)
  - TÉLÉPHONES (récupération de Photos / SMS)
    - SYSTÈMES NUMÉRIQUES
  - **EXPERTISES & AUDITS** (certifié ISO 27005)
    - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
    - SÉCURITÉ INFORMATIQUE
    - SYSTÈMES DE VOTES ÉLECTRONIQUES

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

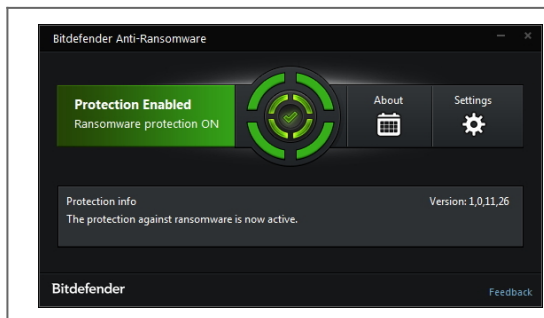
Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des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



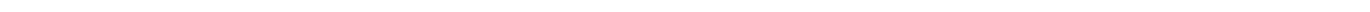
Réagissez à cet article

---

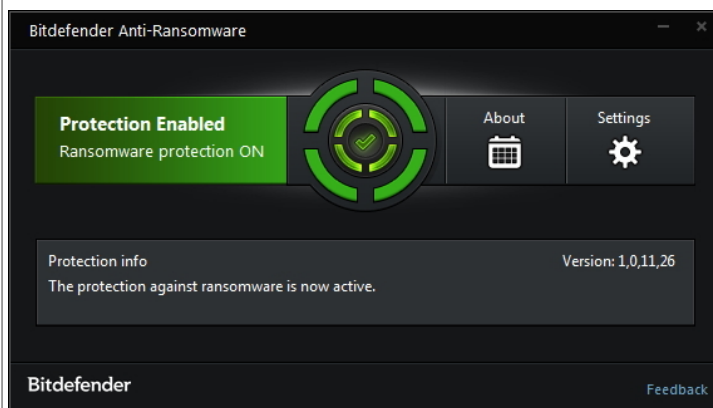
# Comment protéger votre ordinateur du virus Locky avec un outil Gratuit ? | Denis JACOPINI



Comment protéger votre ordinateur du virus Locky avec un outil Gratuit ?



Antivirus firm Bitdefender has released a free tool that can prevent computers from being infected with some of the most widespread file-encrypting ransomware programs: Locky, TeslaCrypt and CTB-Locker.



Antivirus firm Bitdefender has released a free tool that can prevent computers from being infected with some of the most widespread file-encrypting ransomware programs: Locky, TeslaCrypt and CTB-Locker.

The new Bitdefender Anti-Ransomware vaccine is built on the same principle as a previous tool that the company designed to prevent CryptoWall infections. CryptoWall later changed the way in which it operates, rendering that tool ineffective, but the same defense concept still works for other ransomware families.

While security experts generally advise against paying ransomware authors for decryption keys, this is based more on ethical grounds than on a perceived risk that the keys won't be delivered.

In fact, the creators of some of the most successful ransomware programs go to great lengths to deliver on their promise and help paying users decrypt their data, often even engaging in negotiations that result in smaller payments. After all, the likelihood of more users paying is influenced by what past victims report.

Many ransomware creators also build checks into their programs to ensure that infected computers where files have already been encrypted are not infected again. Otherwise, some files could end up with nested encryption by the same ransomware program.

The new Bitdefender tool takes advantage of these ransomware checks by making it appear as if computers are already infected with current variants of Locky, TeslaCrypt or CTB-Locker. This prevents those programs from infecting them again.

The downside is that the tool can only fool certain ransomware families and is not guaranteed to work indefinitely. Therefore, it's best for users to take all the common precautions to prevent infections in the first place and to view the tool only as a last layer of defense that might save them in case everything else fails.

Users should always keep the software on their computer up to date, especially the OS, browser and browser plug-ins like Flash Player, Adobe Reader, Java and Silverlight. They should never enable the execution of macros in documents, unless they've verified their source and know that the documents in question are supposed to contain such code.

Emails, especially those that contain attachments, should be carefully scrutinized, regardless of who appears to have sent them. Performing day-to-day activities from a limited user account on the OS, not from an administrative one, and running an up-to-date antivirus program, are also essential steps in preventing malware infections.

« While extremely effective, the anti-ransomware vaccine was designed as a complementary layer of defense for end-users who don't run a security solution or who would like to complement their security solution with an anti-ransomware feature, » said Bogdan Botezatu, a senior e-threat analyst at Bitdefender, via email... [Lire la suite]



Réagissez à cet article

Source : *Free Bitdefender tool prevents Locky, other ransomware infections, for now | Computerworld*

---

# Qu'est-ce que le registre RGPD ?

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>Qu'est-ce que le registre RGPD ?</b>				

---

**Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité.**

Document de recensement et d'analyse, il doit refléter la réalité de vos traitements de données personnelles et vous permet d'identifier précisément :

- les parties prenantes (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données,
- les catégories de données traitées,
- à quoi servent ces données (ce que vous en faites),
- qui accède aux données et à qui elles sont communiquées,
- combien de temps vous les conservez,
- et comment elles sont sécurisées.

Au-delà de la réponse à l'obligation prévue par l'article 30 du RGPD, le registre est un outil de pilotage et de démonstration de votre conformité au RGPD. Il vous permet de documenter vos traitements de données et de vous poser les bonnes questions : ai-je vraiment besoin de cette donnée dans le cadre de mon traitement ? Est-il pertinent de conserver toutes les données aussi longtemps ? Les données sont-elles suffisamment protégées ? Etc.

Sa création et sa mise à jour sont ainsi l'occasion d'identifier et de hiérarchiser les risques au regard du RGPD. Cette étape essentielle vous permettra d'en déduire un plan d'action de mise en conformité de vos traitements aux règles de protection des données.

## **Qui est concerné ?**

L'obligation de tenir un registre des traitements concerne tous les organismes, publics comme privés et quelle que soit leur taille, dès lors qu'ils traitent des données personnelles.

### **Dispositions pour les organismes de moins de 250 salariés**

Les entreprises de moins de 250 salariés bénéficient d'une dérogation en ce qui concerne la tenue de registres. Ils doivent inscrire au registre les seuls traitements de données suivants :

- les traitements non occasionnels (exemple : gestion de la paie, gestion des clients/prospects et des fournisseurs, etc.) ;
- les traitements susceptibles de comporter un risque pour les droits et libertés des personnes (exemple : systèmes de géolocalisation, de vidéosurveillance, etc.)
- les traitements qui portent sur des données sensibles (exemple : données de santé, infractions, etc.).

**En pratique, cette dérogation est donc limitée à des cas très particuliers de traitements, mis en œuvre de manière occasionnelle et non routinière, comme par exemple une campagne de communication à l'occasion de l'ouverture d'un nouvel établissement, sous réserve que ces traitements ne soulèvent aucun risque pour les personnes concernées. En cas de doute sur l'application de cette dérogation à un traitement, la CNIL vous recommande de l'intégrer dans votre registre.**

## **Un registre spécifique pour les activités de sous-traitance des données personnelles**

Les organismes qui traitent des données personnelles pour le compte d'un autre organisme (les sous-traitants comme, par exemple, des prestataires de services informatiques ou des agences de marketing ou de communication qui traitent des données personnelles pour le compte de leurs clients) doivent également tenir un registre de leurs activités de sous-traitant impliquant le traitement de données.

Pour plus de précisions : voir le guide RGPD pour les sous-traitants

## **Que contient le registre ?**

L'article 30 du RGPD prévoit des obligations spécifiques pour le registre du responsable de traitement de données personnelles et pour le registre du sous-traitant. Si votre organisme agit à la fois en tant que sous-traitant et responsable de traitement, votre registre doit donc clairement distinguer les deux catégories d'activités.

**En pratique, dans cette hypothèse, la CNIL vous recommande de tenir 2 registres :**

1. un pour les traitements de données personnelles dont vous êtes vous-même responsable,
2. un autre pour les traitements que vous opérez, en tant que sous-traitant, pour le compte de vos clients.

[lire la suite]

**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 : *Le registre des activités de traitement*

---

# Mise en place d'un système de vote électronique, quelques conseils | Denis JACOPINI

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>Mise en place d'un système de vote électronique, quelques conseils</b>				

La délibération n° 2010-371 du 21 octobre 2010 de la CNIL portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique indique que tout système de vote électronique doit faire l'objet d'une expertise indépendante.

---

Le vote électronique, souvent via internet, connaît un développement important depuis plusieurs années, notamment pour les élections professionnelles au sein des entreprises.

La mise en place des traitements de données personnelles nécessaires au vote doit veiller à garantir la protection de la vie privée des électeurs, notamment quand il s'agit d'élections syndicales ou politiques.

La CNIL souligne que le recours à de tels systèmes doit s'inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin (sauf pour les scrutins publics), le caractère personnel, libre et anonyme du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle a posteriori par le juge de l'élection. Ces systèmes de vote électronique doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.

Les mesures de sécurité sont donc essentielles pour un succès des opérations de vote mais mettent en œuvre des mesures compliquées, comme par exemple l'utilisation de procédés cryptographiques pour le scellement et le chiffrement.

La délibération n° 2010-371 du 21 octobre 2010 de la CNIL portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique indique que **tout système de vote électronique doit faire l'objet d'une expertise indépendante.**

Par ailleurs, l'article R2314-12 du Code du Travail créé par Décret n°2008-244 du 7 mars 2008 – art. (V) fixe très clairement que préalablement à sa mise en place ou à toute modification substantielle de sa conception, **un système de vote électronique est soumis à une expertise indépendante.** Le rapport de l'expert est tenu à la disposition de la Commission

nationale de l'informatique et des libertés.

Information complémentaire : Les articles R2314-8 à 21 et R2324-4 à 17 du Code du Travail indiquent de manière générale les modalités du vote électronique lors du scrutin électoral de l'élection des délégués du personnel et des délégués du personnel au comité d'entreprise.

Ces dispositions ont été complétées par la délibération 2010-371 de la CNIL du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.

L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).

L'expertise doit porter sur l'ensemble des mesures décrites dans la présente délibération et notamment sur :

- le code source du logiciel y compris dans le cas de l'utilisation d'un logiciel libre,
- les mécanismes de scellement utilisés aux différentes étapes du scrutin (voir ci-après),
- le système informatique sur lequel le vote va se dérouler, et notamment le fait que le scrutin se déroulera sur un système isolé ;
- les échanges réseau,
- les mécanismes de chiffrement utilisé, notamment pour le chiffrement du bulletin de vote sur le poste de l'électeur.

L'expertise doit être réalisée par un expert indépendant, c'est-à-dire qu'il devra répondre aux critères suivants :

- Être un informaticien spécialisé dans la sécurité ;
- Ne pas avoir d'intérêt financier dans la société qui a créé la solution de vote à expertiser, ni dans la

société responsable de traitement qui a décidé d'utiliser la solution de vote ;

- Posséder une expérience dans l'analyse des systèmes de vote, si possible en ayant expertisé les systèmes de vote électronique d'au moins deux prestataires différents ;
- Avoir suivi la formation délivrée par la CNIL sur le vote électronique.

Le rapport d'expertise doit être remis au responsable de traitement. Les prestataires de solutions de vote électronique doivent, par ailleurs, transmettre à la CNIL les rapports d'expertise correspondants à la première version et aux évolutions substantielles de la solution de vote mise en place.

Si l'expertise peut couvrir un champ plus large que celui de la présente recommandation, le rapport d'expertise fourni au responsable de traitement doit comporter une partie spécifique présentant l'évaluation du dispositif au regard des différents points de la recommandation.

L'expert doit fournir un moyen technique permettant de vérifier a posteriori que les différents composants logiciels sur lesquels a porté l'expertise n'ont pas été modifiés sur le système utilisé durant le scrutin. La méthode et les moyens permettant d'effectuer cette vérification doivent être décrits dans le rapport d'expertise.

---

[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 systèmes de vote de prestataires différents.

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 rapports

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

---

<http://www.cnil.fr/les-themes/vie-citoyenne/vote-electronique/>  
<http://www.cnil.fr/documentation/deliberations/deliberation/delib/249/>

<http://infosdroits.fr/la-cnil-sanctionne-un-employeur-pour-defaut-de-securite-du-vote-electronique-pendant-une-election-professionnelle/>

---

**Qui peut le consulter le FAED  
(Fichier automatisé des  
empreintes digitales) ? |  
Denis JACOPINI**





**vous informe...**

# Qui peut le consulter le #FAED (#Fichier automatisé des empreintes digitales) ?

Seuls les agents habilités des services de l'identité judiciaire de la police nationale et des unités de recherches de la gendarmerie nationale ont directement accès au FAED, pour procéder aux opérations d'identification.

Les officiers de police judiciaire et les agents des douanes sont destinataires des résultats de la consultation du fichier, dans le cadre de leurs enquêtes.

Le FAED peut également être consulté, sous certaines conditions, par les agents des organismes internationaux de police judiciaire et par ceux des services de police ou de justice d'Etats étrangers.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

S o u r c e

[http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=ABD0FF1FEB6BB72CCAD5DFA090DF59F2?name=FAED+\(Fichier+automatis%C3%A9+des+empreintes+digitales\)+%3A+qui+peut+le+consulter+%3F&id=423](http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=ABD0FF1FEB6BB72CCAD5DFA090DF59F2?name=FAED+(Fichier+automatis%C3%A9+des+empreintes+digitales)+%3A+qui+peut+le+consulter+%3F&id=423)