

# Comment gérer les licences des logiciels installés par les salariés ? | Denis JACOPINI



Dès que l'on souhaite accueillir les terminaux personnels des collaborateurs dans l'entreprise, il faut absolument se pencher sur la question des licences logicielles pour éviter de cuisantes déconvenues.

Dès qu'un logiciel est présent, les risques liés aux licences sont forcément tapis dans l'ombre. Si l'on souhaite accueillir les terminaux personnels des collaborateurs avec un projet BYOD (Bring Your Own Device), il faut donc se pencher sur la question pour éviter de cuisantes déconvenues. Il en va de même avec les petits logiciels gratuits que les employés peuvent installer sur les équipements fournis par l'entreprise, qu'ils en soient ou non administrateurs.

Ces deux exemples, aussi concrets que courants, offrent quelques clefs pour mieux maîtriser un phénomène dont la complexité et l'ampleur ne cessent de croître.

## **Bring your own licence illégale**

Si l'on ne parvient pas à endiguer un phénomène, autant en tirer profit. C'est notamment le cas avec ces équipements informatiques personnels que les employés introduisent discrètement dans les systèmes d'information d'entreprise depuis des années. Las de lutter, les DSI cèdent à une nouvelle mode : le BYOD (Bring Your Own Device).

Certains se contentent de canaliser ces terminaux hétéroclites en veillant à la survie des équipes de support et à la sécurité de l'information : pas de support technique, connexion sur les accès Wi-Fi pour visiteur, etc. D'autres vont plus loin, comme dans cette grande organisation du secteur tertiaire dont je tairai le nom :

- Les collaborateurs peuvent utiliser leur matériel préféré à la place de celui fourni par la DSI ;
- Ils doivent alors y installer l'antivirus homologué dont une licence leur est allouée ;
- S'ils restituent le PC de la compagnie pour n'utiliser que le leur, ce dernier est subventionné ;
- En pareil cas, ils sont livrés à eux-mêmes en termes d'assistance et de logiciels ;
- Ils peuvent cependant bénéficier de l'accord passé avec Microsoft pour acquérir une licence Office à 13 €.

Remarquable exemple de modernité et d'ouverture, qui permet au passage de réduire les coûts de matériel, de logiciel et de support. Le tout est savamment enrobé d'une communication du plus bel effet vantant les mérites d'une transformation digitale soucieuse des collaborateurs et de leur bien-être.

Comme d'habitude, le diable est dans les détails, en l'occurrence dans les conditions d'utilisation de la licence Microsoft Office à 13 €. En effet, elle couvre l'usage secondaire du logiciel sur un PC personnel si une licence entreprise est octroyée à l'utilisateur. Dans notre cas, l'utilisateur n'a plus de licence entreprise puisqu'il l'a restituée en même temps que son PC.

Voilà comment une organisation peut pousser ses collaborateurs à agir illégalement, sans s'exposer directement puisque les logiciels et les terminaux incriminés ne lui appartiennent pas. Les employés mis en défaut par Microsoft pourront cependant prouver qu'ils ont respecté les préconisations relayées par leur hiérarchie. Il n'est pas certain que cela engendre l'atmosphère voulue : décontractée et propice au travail.

## **La gratuité peut coûter cher**

Une autre situation classique, en apparence anodine, peut faire des remous si l'on n'y prend pas garde : les logiciels gratuits, si pratiques et si sympathiques.

Ainsi, un collègue m'a récemment présenté les bienfaits d'un petit freeware qui le comblait d'aise. Il m'a vivement conseillé de l'installer sur mon PC professionnel. Je l'ai donc téléchargé depuis le site de l'éditeur. Avant de lancer l'installation, j'ai lu les conditions d'utilisation (vous auriez évidemment fait la même chose à ma place). Au milieu de cette prose, j'ai découvert que le produit ne devait pas être utilisé en entreprise. Que l'on travaille sur un terminal personnel ou mis à disposition par la DSI ne change rien puisqu'il s'agit toujours d'un usage « en entreprise ». Utiliser ainsi la version gratuite du logiciel est donc illégal.

Disposer des droits d'administrateur sur son ordinateur n'est pas forcément nécessaire pour installer un tel produit. L'entreprise peut donc se retrouver dans une posture inavouable, même si elle a correctement sécurisé son parc informatique. Pour mettre un peu de piment, ajoutons que ces installations occultes passent inaperçues lors des inventaires logiciels, puisqu'ils sont le plus souvent conçus pour détecter ce qui est connu, et non pour découvrir l'inconnu.

De nos jours, les logiciels communiquent presque tous avec leur éditeur via Internet au moyen de protocoles réseau qui franchissent allègrement les dispositifs de sécurité. Il peut s'agir de rechercher des mises à jour ou de fournir des données vous concernant. C'est légal puisque spécifié dans le contrat de licence accepté *de facto* lors de l'installation, qu'il ait été lu ou non. Il suffit alors d'un nombre significatif de PC communiquant depuis votre réseau d'entreprise pour mettre la puce à l'oreille de l'éditeur. Il a alors tout le loisir de vous retrouver grâce à vos adresses IP publiques et de réclamer le manque à gagner en faisant jouer la clause d'audit inscrite, elle aussi, aux conditions générales d'utilisation. Elle lui offre en effet la possibilité de contrôler votre système d'information pour vérifier que les logiciels utilisés sont dûment payés.

Les petits logiciels gratuits peuvent ainsi coûter fort cher à des DSI qui en ignoraient jusqu'à l'existence car les grands éditeurs ne sont plus les seuls à développer leurs ventes par un nouveau canal : l'audit.

## **L'effort fait les forts**

Ces deux cas d'école montrent que la compréhension des contrats de licences est indispensable pour éviter des complications désagréables. C'est par ailleurs un préalable à la gestion des actifs logiciels (Software Asset Management, SAM). Comment, en effet, maîtriser le droit d'usage contractuel d'un produit dont on ignore le contrat ?

En ces temps de crise, la chasse au manque à gagner est ouverte pour de nombreux éditeurs. Tout changement impliquant l'informatique concerne forcément des composants logiciels. Il convient donc d'être prudent et de prendre en considération leur dimension contractuelle. Bien des projets ont vu leur retour sur investissement réduit à néant, voire inversé, après un audit d'éditeur.

En définitive, qu'il s'agisse d'adopter le BYOD, d'utiliser un freeware ou de transformer le système d'information, le SAM renforce la position du client face aux éditeurs de logiciels car, comme disait Marcel Pagnol : « Comme on est faible quand on est dans son tort ! »... [Lire la suite]



Réagissez à cet article

# Les TPE et les PME, cibles privilégiées des cybercriminels | Denis JACOPINI



Les TPE et les PME, cibles privilégiées des cybercriminels

**Selon le spécialiste de la sécurité Symantec, 71 % des TPE et les PME qui font l'objet d'une cyber-attaque ne s'en remettent pas. Pourtant, la sécurité du système informatique ne fait pas partie des priorités des petites et moyennes entreprises, même si c'est un enjeu majeur pour leur survie.**

Face à des systèmes d'information de plus en plus ouverts, un usage généralisé d'internet et des terminaux mobiles connectés, les entreprises doivent mettre en œuvre des politiques de sécurité informatique de plus en plus exigeantes. Pourquoi les cybercriminels s'en prennent d'avantage aux TPE et aux PME ? Explication.

La cybercriminalité n'est pas un fait nouveau. Pourtant depuis quelques années, nous sommes tous devenus ultra-connectés et multi-équipés. Ce constat n'épargne pas les entreprises qui ont vu apparaître de nouveaux outils qui permettent aux salariés de rester connectés en étant plus mobile et plus productif. Ces nouveaux modes de travail, sont aujourd'hui autant de failles de sécurité possibles et donc d'attaques possibles. Cette forme de criminalité ne concerne plus les grandes entreprises qui ont majoritairement mis en place des moyens coûteux pour lutter contre le piratage. La nouvelle cible privilégiée des hackers serait les TPE et les PME qui seraient plus simple à attaquer.

#### **Des cibles plus accessibles**

Les enquêtes le confirment : les gérants de TPE et PME ont une vision assez exacte du piratage informatique, mais ils se sentent peu concernés. Selon eux, cette forme moderne de criminalité menace surtout les grandes entreprises. Pourtant, les délits constatés contredisent cette perception. Plus encore, le pourcentage des attaques vers les entreprises de moins de 250 salariés progressent. Selon le rapport Symantec Security Threat, elles seraient passées de 18% à 31% en 4 ans. Or ce sont justement les entreprises de moins de 250 salariés qui doivent protéger leurs données. Le constat est le suivant : 40% de la valeur des entreprises est issue des informations qu'elles détiennent. Ce qui intéresse les cybercriminels : dossiers clients, listes de contacts, renseignements sur le personnel et informations bancaires de l'entreprise, cartes de crédit comprises et propriétés intellectuelles. Elles représentent aussi des passerelles d'accès à leurs partenaires.

#### **Un frein pour travailler avec les grandes entreprises**

Loin des considérations financières et ne se sentant pas concernées, les TPE et PME s'estiment à l'abri de ces attaques. En conséquence, leurs infrastructures ne sont pas adaptées. Elles sont alors des cibles idéales permettant d'attaquer leurs différents partenaires qui sont parfois des grandes entreprises ou des administrations. Elles deviennent alors un moyen d'accéder à leurs systèmes d'information. Et cela peut constituer un frein à la compétitivité. Les Grandes Entreprises, ne pouvant contrôler le système d'information de leurs partenaires, exigent alors de leurs sous traitants un matériel informatique similaire afin de contrôler les flux.

#### **Des attaques virales invisibles**

Les attaques les plus fréquentes sont de natures virales. A l'insu des utilisateurs, elles visent à installer de petits programmes capables d'identifier les mots de passe (via des enregistreurs de frappe), d'accéder aux services bancaires en ligne de l'entreprise (Chevaux de Troie bancaires), de contrôler à distance les ordinateurs de l'entreprise pour lancer des attaques commandées (réseaux de zombies ou botnet) ou d'espionner les employés pour connaître leurs habitudes, leurs mots de passe ou leurs préférences (Spyware)...

#### **De nouvelles attaques plus structurées**

Les techniques de piratages évoluent et le matériel n'est plus l'unique faille. On voit apparaître de nouveaux types d'attaques basées sur les failles humaines et sociales. Les environnements de travail des salariés sont ciblés à travers les postes de travail des salariés. A titre d'exemple, les hackers identifient le lien entre les entreprises et leurs partenaires. Des mails sont envoyés depuis les réseaux sociaux type LinkedIn ou Viadeo au nom du partenaire. L'email sera donc ouvert sans réel méfiance de la part du salarié. Cette technique, appelée « social engineering », permet alors au pirate d'accéder au poste de travail de l'utilisateur en premier lieu pour ensuite évoluer dans le système d'information de l'entreprise.

#### **Des règles simples de cyber-stratégie**

Il n'est pas rare qu'en entreprise les salariés utilisent des outils réservés aux particuliers. Ce type de pratique multiplie les dangers d'intrusion car les systèmes peuvent être piratés. Ils pointeront vers l'installation de « maliciels » (logiciels malveillants conçus pour infiltrer un ordinateur et y réaliser des activités non autorisées). Il en est de même pour tous les outils connectés. Malheureusement, ce n'est souvent qu'une question de temps avant qu'un hacker arrive à ses fins. Il est donc primordial de faire preuve de plus de rigueur pour gagner du temps afin de décourager l'intrusion. Une entreprise qui connaît les risques et montre qu'elle a pris des mesures de sécurité simples, décourage les pirates. Il existe aujourd'hui des services de sécurité informatiques adaptés aux TPE/PME. A titre d'exemple, des prestataires proposent des offres sous forme de machine virtuelle, un proxy complet et simple. Le service permet de filtrer les pages internet en se basant sur des listes préétablies.

Mais bien avant de se consacrer à la sécurisation du matériel de travail, la première mesure à prendre concernera celle des bonnes pratiques des salariés. Des mesures de protection humaines sont nécessaires. « Il est surtout important de sensibiliser ses collaborateurs aux bonnes pratiques », assure Philippe Trouchaud, associé PricewaterhouseCoopers, spécialiste de la cyber sécurité. Le gouvernement met à disposition un Guide d'Hygiène et de Sécurité de l'ANSSI, il fournit les bases de la sécurité pour les utilisateurs au sein des entreprises.

Aussi une politique de sécurité consistera tout d'abord à mener de front trois actions :

- Identifier les points de vulnérabilité généralement utilisés par les criminels informatiques pour s'introduire dans les systèmes d'information,
- Définir les règles de prudence à appliquer au quotidien par l'entreprise et son personnel,
- Mettre en œuvre systèmes de protection électroniques adéquats. Le tout devant être organisé et planifié dans la durée.

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

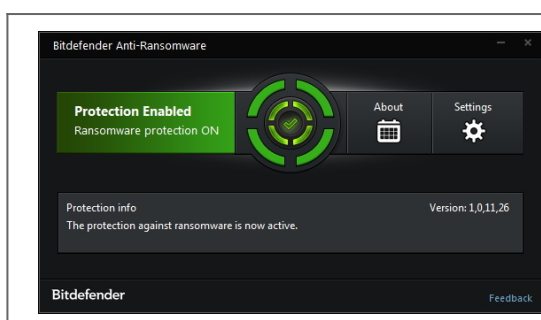
Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

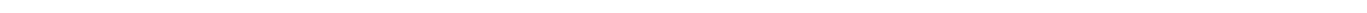
Source : <http://www.axione-limousin.fr/actualites/tpe-et-pme-cibles-privilegiees-des-cybercriminels-57.xhtml>

---

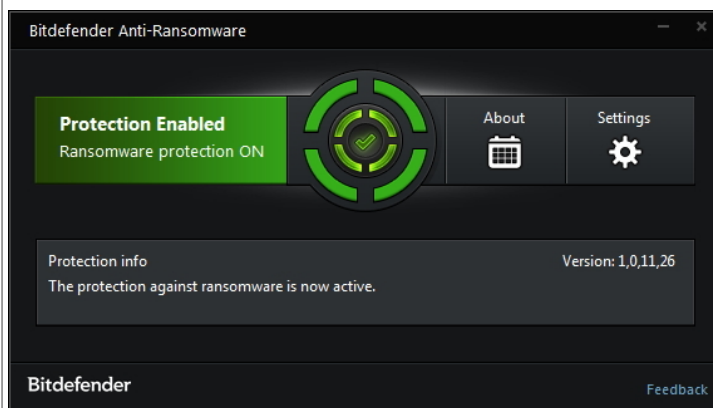
# Comment protéger votre ordinateur du virus Locky avec un outil Gratuit ? | Denis JACOPINI



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*

---

# Comment vérifier si votre site Internet a été victime d'un Hackeur | Denis JACOPINI



Que ça soit à cause d'une simple erreur de frappe ou du fait que votre site Internet a été Hacké, l'auteur, l'éditeur ou le rédacteur en chef d'un site Internet peut être pénalement responsable des conséquences causées par son contenu non désiré.

Afin de vérifier si votre site Internet a été Hacké, voici quelques conseils pour vérifier si votre site Internet a été victime d'un Hackeur :

Que votre site Internet ait été victime d'un hackeur ou que votre site Internet ait été victime d'un pirate sont deux choses différentes.

Le pirate va pomper une partie ou la totalité du contenu de votre site Internet. Le hackeur va modifier le contenu de votre site Internet dans un but de malveillance.

Les conseils que je vais vous donner concernent le cas où un site Internet a été Hacké.

### **DU CONTENU ETRANGE APPARAIT ?**

En premier lieu, consultez votre site Internet sur plusieurs ordinateurs ayant des systèmes d'exploitation et des navigateurs différents afin de vérifier si un affichage anormal apparaît.

### **UN ANTIVIRUS DECLENCHE UNE ALERTE A L'OUVERTURE DE VOTRE SITE INTERNET ?**

Un message d'alerte de votre antivirus est aussi un bon indicateur de la présence éventuelle d'un code suspicieux sur votre site Internet.

Première solution : Depuis votre dernière sauvegarde vous n'avez plus fait de modifications :

Restaurez les pages Web ou la base de donnée contaminée.

Seconde solution : Vous n'avez pas de Sauvegarde de votre site Internet ou la sauvegarde est trop vieille :

Dans ce cas, vous allez devoir résoudre le problème à la main.

### **COMMENT TESTER VOTRE SITE INTERNET**

Enfin, si vous ne savez pas si votre site Internet a été hacké, vous pouvez le vérifier en utilisant les outils suivants :



<https://www.virustotal.com/url>

VirusTotal est un service gratuit qui *analyse les fichiers et URL suspects*, et facilite la détection rapide des virus, vers, trojans et tous types de malwares.

<http://www.urlvoid.com>

URLVoid.com is a free service developed by NoVirusThanks Company Srl that allows users to scan a website address with multiple website reputation engines and domain blacklists to facilitate the detection of possible dangerous websites, used to distribute malware and spyware or related to fraudulent activities.

<http://urlquery.net>

Query.net is a service for detecting and analyzing web-based malware. It provides detailed information about the activities a browser does while visiting a site and presents the information for further analysis.

<http://wepawet.iseclab.org/>

Dans ce cas, vous allez devoir résoudre le problème à la main.

### **COMMENT SE PROTEGER D'UN HACKEUR ?**

Voici quelques astuces simples vous aideront a protéger votre site efficacement contre les pirates et hackers de l'internet :

Ces techniques sont efficace contre les hackers débutants.

- Avoir un hébergeur de qualité et lui même utilisant des surveillances automatiques et permanentes.
- Mettez à jour systématiquement le système d'exploitation de votre serveur ainsi que toutes les applications liées à l'hébergement des sites internet, du FTP, des messageries et des bases de données.
- Supprimer l'utilisateur « admin » des logiciels et créez

le votre

- Mot de passe sécurisé (minuscules, majuscules, chiffres et symboles)

**Cet article vous à plu ? Laissez-nous un commentaire  
(notre source d'encouragements et de progrès)**

---

# **Se mettre en conformité avec la CNIL. Quel est le rôle de l'audit ? | Denis JACOPINI**

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



---

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.

---

MISES EN CONFORMITÉ



PROTECTION  
DES  
DONNÉES PERSONNELLES

**CNIL**

Se mettre en  
conformité avec la  
CNIL. Quel est le  
rôle de l'audit ?

Depuis le 6 janvier 1978, les établissements public ou privés, les associations, les entreprises etc. doivent se mettre en conformité avec la Loi Informatique et Libertés. Un règlement européen entrant dans quelques mois en vigueur risquant de responsabiliser et sanctionner bien plus lourdement les concernés, il nous semblait important de vous détailler les étapes indispensables pour se mettre en conformité avec la CNIL.

Art. 226-16 de la Loi Informatique et Libertés

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

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, l'**#audit CNIL**, indépendant de la démarche de contrôle de la CNIL.

> Comment se passe un contrôle de la CNIL

Une fois cet **audit CNIL** réalisé, l'établissement connaissant enfin les actions qu'il doit mener va pouvoir prévoir deux actions de formation entrant dans notre cursus :

**Se mettre en conformité avec la CNIL, mode d'emploi**

- sensibiliser le personnel de l'établissement en lui expliquant la raison d'une démarche de mise en conformité CNIL et le comportement qu'il se verra adopter pour favoriser cette action ;
  - former le futur correspondant CNIL (CIL) à devenir autonome en lui inculquant :
    - les notions clés et grands principes de la loi informatique et libertés ;
    - les principes de base en matière de sécurité des systèmes d'information ;
    - le traitement des demandes et les modalités d'instruction d'une plainte ;
    - les contrôles et les procédures de sanction de la CNIL
  - La mise en application de la mise en conformité sur des cas concrets sur le système informatique de votre entreprise.
- Au terme de ces démarches, un nouvel **audit CNIL** peut être réalisé afin de vérifier la conservation de la conformité dans le temps.



**Intéressé par une démarche de mise en conformité avec la CNIL ?**

Contatez-nous

Denis JACOPINI

formateur n°93 84 03041 84

**Notre métier** : Denis JACOPINI est Expert indépendant, Expert judiciaire en Informatique spécialisé en protection des données personnelles. Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Nous pouvons également 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 : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



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

Sources : Denis JACOPINI

<https://www.cnil.fr/fr/comment-se-passe-un-contrôle-de-la-cnil>

---

# 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

×

×

×

×

×

×

×

**Mise en place d'un système de vote électronique, quelques conseils**

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

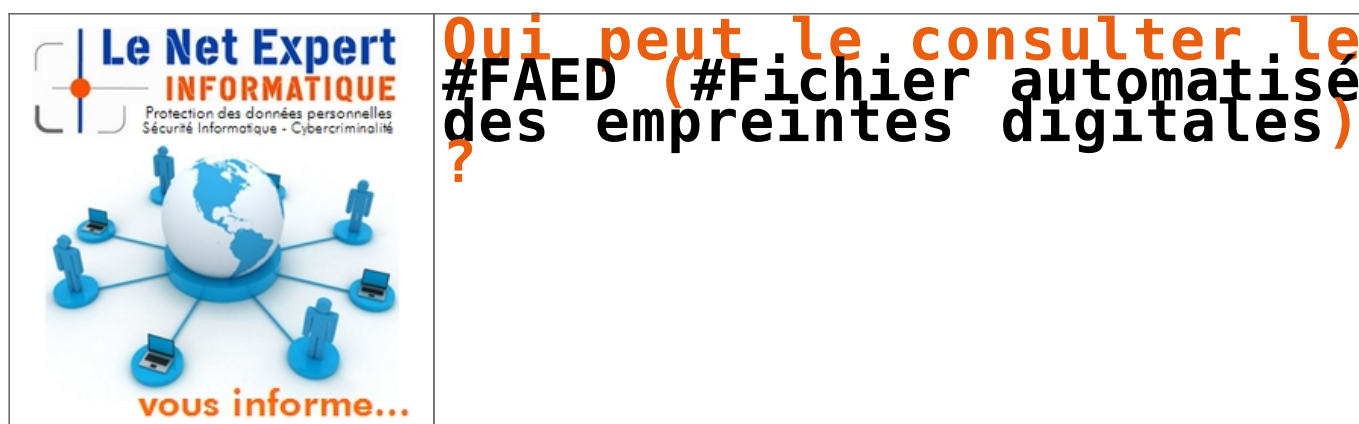
---

<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



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 plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

[http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=A8D0FF1FEB6BB72CCAD5DFA090DF59F2?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=A8D0FF1FEB6BB72CCAD5DFA090DF59F2?name=FAED+(Fichier+automatis%C3%A9+des+empreintes+digitales)+%3A+qui+peut+le+consulter+%3F&id=423)

---

## Quelques conseils pour surfer

# un peu plus tranquille sur Internet

✕	Quelques conseils pour surfer un peu plus tranquille sur Internet
---	---

---

Quelques conseils de bon sens pour se protéger au mieux des attaques liées à l'utilisation d'Internet.

## Des mises à jour régulières et automatiques

L'un des meilleurs moyens de se prémunir des risques de piratage, est de **maintenir son matériel informatique et ses logiciels à jour** avec les derniers correctifs de sécurité et les dernières mises à jour.

Par ce biais, le risque d'intrusion est minimisé. Il est donc très important de **configurer son ordinateur** pour que le système d'exploitation se mette **régulièrement et automatiquement à jour**.

## Une bonne configuration matérielle et des logiciels adaptés

Les **niveaux de sécurité** de l'ordinateur doivent être **réglés au plus haut** pour minimiser les risques d'intrusions. Les **paramètres des navigateurs** et des **logiciels de messageries** électroniques peuvent aussi être configurés avec des niveaux de sécurité élevés.

L'utilisation d'un **anti-virus à jour** et d'un **pare-feu (firewall)** assureront un niveau de protection minimum pour surfer sur la toile. Le **firewall** permet de filtrer les données échangées entre votre ordinateur et le réseau. Il peut être réglé de manière à bloquer ou autoriser certaines connexions.

## Utiliser un bon mot de passe

Les mots de passe sont une **protection incontournable** pour sécuriser l'ordinateur et ses données ainsi que tous les accès au service sur Internet.

Mais encore faut-il en choisir un bon. Un bon mot de passe doit être difficile à deviner par une personne tierce et facile à retenir pour l'utilisateur.

Lire nos conseils pour choisir un bon mot de passe .

## Se méfier des courriers électroniques non-sollicités et leurs pièces jointes

A la réception d'un mail dont l'**expéditeur est inconnu**, un seul mot d'ordre : **prudence !**

Les courriers électroniques peuvent être accompagnés de **liens menant vers des sites frauduleux** (voir l'article sur le *phishing*) ou de **pièces jointes piégées**. **Un simple clic sur une image suffit pour installer à votre insu un logiciel ou code malveillant** (cheval de Troie) sur votre ordinateur. La pièce jointe piégée peut être : une page html, une image JPG, GIF, un document word, open office, un PDF ou autre.

Pour se protéger de ce type d'attaque, la règle est simple : **ne jamais ouvrir une pièce jointe dont l'expéditeur est soit inconnu, soit d'une confiance relative**.

En cas de doute, une recherche sur internet permet de trouver les arnaques répertoriées.

## Que faire si j'ai déjà cliqué sur la pièce jointe?

**Déconnectez-vous d'internet** et **passez votre ordinateur à l'analyse anti-virus** (à jour) pour détecter l'installation éventuelle d'un logiciel malveillant.

Pour tout renseignement ou pour signaler une tentative d'escroquerie :



---

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

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

Plus sur  
d'informations

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Conseils de prévention sur

# Comment bien se protéger contre les Cyberattaques ?

	<b>Comment bien se protéger contre les Cyberattaques ?</b>
---	--

---

**On l'a encore vu récemment, aucun système informatique n'est à l'abri d'une faille...**

Et en matière de cybercriminalité, les exemples nous montrent que l'attaque semble toujours avoir un coup d'avance sur la défense. L'enjeu, pour les institutions et les entreprises, est d'anticiper et de se préparer à ces situations de crise en développant, en amont, une stratégie à-même de minorer au maximum leurs conséquences.

Demande de rançons, fraudes externes, défiguration de sites web, vols ou fuites d'informations, cyber-espionnage économique ou industriel..., en 2016 huit entreprises françaises sur dix ont été victimes de cybercriminels, contre six en 2015. La tendance n'est malheureusement pas à l'amélioration et l'actualité récente regorge d'exemples frappants : le logiciel malveillant WannaCry qui vient de frapper plus de 300 000 ordinateurs dans 150 pays avec les conséquences désastreuses que l'on connaît, l'attaque du virus Adylkuzz qui ralentit les systèmes informatiques, le vol de la copie numérique du dernier opus de la saga « Pirates des Caraïbes » quelques jours avant sa sortie mondiale..., les exemples de cyberattaques ne cessent de défrayer la chronique.

Pour bien se protéger contre les Cyberattaque, nous vous conseillons de suivre les étapes suivantes :

1. Faire ou faire faire un état des lieux des menaces et vulnérabilités risquant de mettre en danger votre système informatique ;
2. Faire ou faire faire un état des lieux des failles aussi bien techniques qu'humaines ;
3. Mettre en place les mesures de sécurité adaptées à vos priorités et aux moyens que vous souhaitez consacrer ;
4. Assurer une surveillance des mesures de sécurité et s'assurer de leur bon fonctionnement et de leur adaptation au fil de vos évolutions aussi bien techniques que stratégiques.

- Vous souhaitez faire un point sur l'exposition de votre entreprise aux risques cyber ?
- Vous souhaitez sensibiliser votre personnel aux différentes arnaques avant qu'il ne soit trop tard ?
- Vous recherchez une structure en mesure de mettre en place une surveillance de votre réseau, de votre installation, de vos ordinateurs ?

Contactez-vous

---

**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>

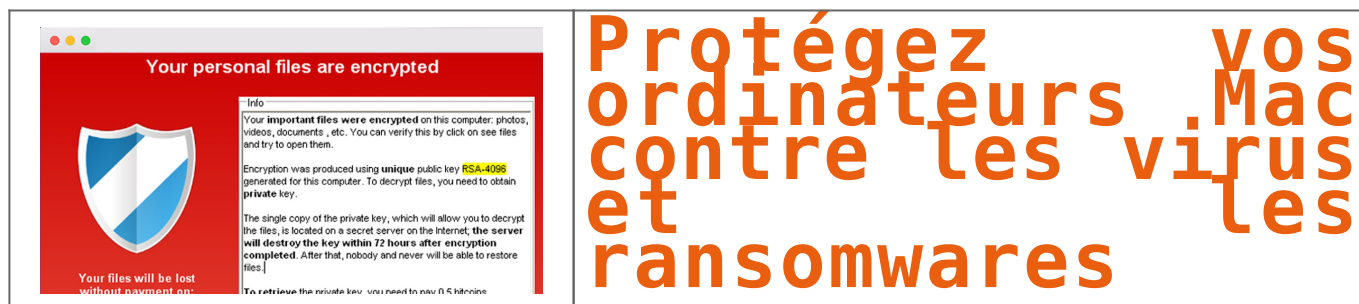


Réagissez à cet article

Source : *Cyberattaque, comment faire pour limiter les risques ?*

---

# Protégez vos ordinateurs Mac contre les virus et les ransomwares | Denis JACOPINI





Vous pensiez que les appareils Apple étaient moins sujets au virus et autres méchancetés informatiques ? Voici un ransomware !



Un ransomware pleinement fonctionnel sévit actuellement sur OS X. Le fonctionnement est toujours le même : une fois installé sur votre machine, il chiffre tous vos fichiers et demande une rançon pour débloquer lesdits fichiers...

Oui, il y a bien un ransomware en action sur OS X mais... Pour l'heure, celui-ci a été découvert dans la dernière version du logiciel de torrent Transmission. Le virus restait dormant durant trois jours avant d'utiliser un client Tor pour se connecter et commencer à verrouiller des fichiers importants. La rançon s'élève ensuite à un bitcoin (environ 400\$).

Mais attention, pour pouvoir implanter ce virus dans Transmission, il aura fallu pénétrer sur le site ou dans le code de l'application... ce qui est plutôt simple à détecter, et à corriger. D'ailleurs, Apple avait très rapidement révoqué le certificat de signature de l'application, laquelle ne pouvait donc plus être installée sur les machines de la firme de Cupertino.

Une nouvelle version de Transmission est déjà disponible sur le site officiel, et sans ransomware !

Pour protéger votre Mac des Virus, des ransomwares, veillez à avoir une bonne sauvegarde automatique, contrôlée, automatisée et historisée et aussi vous pouvez utiliser l'application de sécurité pour Mac :



Réagissez à cet article

Source : *Les ransomwares débarquent sur Mac OS X !*