

# Les documents enregistrés dans un fichier « Mes documents », sont-ils inaccessibles à l'employeur ?

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

 <p><b>LE NET EXPERT</b> AUDITS &amp; EXPERTISES</p>	 <p><b>LE NET EXPERT</b> EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p><b>LE NET EXPERT</b> MISES EN CONFORMITE RGPD CYBER</p>	 <p><b>SPY DETECTION</b> Services de détection de logiciels espions</p>	 <p><b>LE NET EXPERT</b> FORMATIONS</p>	 <p><b>LE NET EXPERT</b> ARNAQUES &amp; PIRATAGES</p>
---	---	--	--	--	--



Les documents enregistrés dans un fichier « Mes documents », sont-ils inaccessibles à l'employeur ?

Les documents enregistrés dans un fichier « Mes documents », sont-ils inaccessibles à l'employeur ?

« Mes documents » est un terme générique. C'est encore une fois la mention « Personnel » qui permet de protéger un dossier ou un fichier. L'employeur ne peut donc pas en faire état, au risque d'avoir à payer des dommages et intérêts à son salarié. »

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**

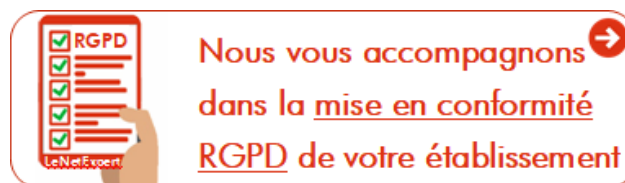
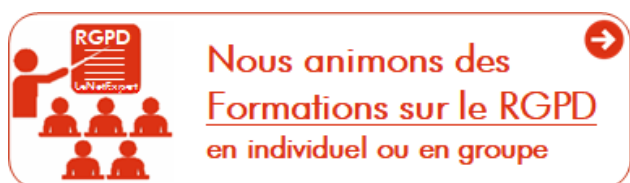
---

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)

---

[block id="24761" title="Pied de page HAUT"]

---

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

---

# Existe-t-il quelques mesures simples pour éviter que de mon ordinateur et mes boîtes mail se fassent pirater ? | Denis JACOPINI





Existe-t-il quelques mesures simples pour éviter que de mon ordinateur et mes boîtes mail se fassent pirater ?

**Il est très difficile de savoir si un ordinateur est piraté / piratable ou pas. Qu'il soit PC ou Mac, il possède ses failles qui peuvent sans limite être exploitées.**

**Il n'y a plus beaucoup de protections qui résistent aux plus grands hackers.**

La divulgation de documents dévoilant les techniques qu'utilise la NSA pour nous espionner (c.f. <http://www.lenetexpert.fr/les-10-outils-les-plus-incroyables-utilises-par-la-nsa-pour-nous-espionner-le-net-expert-informatique>) et les dessous de société d'espionnage informatique Hacking Team récemment piratée (c.f. <http://www.lenetexpert.fr/les-dessous-de-la-societe-despionnage-hacking-team-le-net-expert-informatique>) nous ont récemment démontré qu'il n'y a aucune limite au piratage.

**Mais alors, comment se protéger ?**

Comme pour votre maison ou votre appartement, il n'existe aucun moyen d'empêcher les voleurs de rentrer. Les moyens qu'ils utiliseront seront généralement à la hauteur de l'intérêt qu'ils y trouveront.

Cependant, les conseils que je peux donner, sont comme pour les moyens de protection de vos habitations. Au plus on met des barrières de sécurité, au plus on retarde l'intrusion et au plus on décourage l'auteur. Il sera en effet plus difficile de rentrer chez vous si vous avez la dernière serrure de protection avec les volets anti-effraction dernier cri, avec une alarme ultra perfectionnée etc. plutôt qu'un simple cadenas pour vous protéger.

**Pour sécuriser un système informatique**

1) J'analyse généralement ce qui, dans nos habitudes quotidiennes correspond à une attitude numérique dangereuse ou irresponsable. Pour cette phase, il est difficile de vous dire quoi faire exactement, puisque c'est généralement notre expérience, nos connaissances passées et notre intuition qui servent à produire une bonne analyse.

2) La phase suivante va consister à détecter la présence d'espions dans votre ordinateur. Compte tenu que la plupart des outils d'espionnage sont capables de détecter qu'on est en train de les détecter, vaut mieux déjà, faire des sauvegardes, puis couper d'internet votre appareil (du coup, il sera nécessaire de télécharger les logiciels de détection à partir d'un autre ordinateur, et les copier sur l'ordinateur à analyser à partir d'une clé USB par exemple). Cette phase de détection est très difficile. En effet, les logiciels espions, programmés pour espionner ce que vous tapez au clavier, ce que voit votre webcam ou entend votre micro, sont aussi programmés pour ne pas être détectés.

Le dernier outil connu pour réaliser une détection de logiciels espions est le logiciel **Detekt**. Ce logiciel a pour but de détecter des logiciels espions (spywares) sur un système d'exploitation Windows.

Les spywares actuellement détectés sont :

- DarkComet RAT ;
- XtremeRAT ;
- BlackShades RAT ;
- njRAT ;
- FinFisher FinSpy ;
- HackingTeam RCS ;
- ShadowTech RAT ;
- Gh0st RAT.

Attention, car les développeurs de ce logiciels précisent cependant :

*« Certains logiciels espions seront probablement mis à jour en réponse à la publication de Detekt afin d'éviter la détection. En outre, il peut y avoir des versions existantes de logiciels espions [...] qui ne sont pas détectés par cet outil ».*

Vous trouverez plus d'informations et le lien de téléchargement sur <http://linuxfr.org/news/detekt-un-logiciel-de-detection-de-logiciels-espions>

Sur Mac, il n'existe pas un tel outil. Vous pouvez cependant utiliser le logiciel MacScan pour des antispywares du commerce.

Cependant, que ça soit sur PC ou sur Mac, ce n'est qu'une analyse approfondie (et souvent manuelle) des fichiers systèmes, des processus en mémoire et qui se lancent au démarrage qui permettra de détecter les applications malveillantes installées sur votre ordinateur.

**Et si on dispose d'un Mac plutôt que d'un PC ?**

Il y a quelques années, avoir un Mac « garantissait » d'être un peu à l'abri des virus et des pirates informatiques. En effet, pourquoi un pirate informatique perdrait du temps à développer un logiciel malveillant et prendrait des risques pour seulement 5% de la population numérique mondiale. Désormais, avec l'explosion d'Apple, de ses téléphones, tablettes et aussi ordinateur, les systèmes IOS se sont répandus sur la planète numérique. De plus, c'est très souvent les plus fortunés qui disposent de ces types d'appareils... une aubaine pour les pirates qui trouvent tout de suite un intérêt à développer des dangereuxwares.

3) La troisième et dernière phase de ces recommandations est la protection. Une fois votre système considéré comme sain (il est complètement inutile de protéger un système qui est infecté car ça ne soignera pas l'équipement et les conséquences pourraient être pires), il est temps d'adopter l'attitude d'un vrai utilisateur responsable et paranoïaque.

• Mettez à jour votre système d'exploitation (Windows, MacOS, IOS, Androïd, Linux...) avec la version la plus récente. En effet, l'enchaînement des mises à jour des systèmes d'exploitation est peu souvent fait pour améliorer le fonctionnement ou ajouter des fonctions à votre appareil. Le ballet incessant des « updates » sert prioritairement à corriger les « boulettes » qu'ont fait volontairement ou involontairement les informaticiens « développeurs » détectés par d'autres informaticiens plus « contrôleurs ».

• Mettez à jour vos logiciels avec leurs versions les plus récentes (et particulièrement pour vos navigateurs Internet et les logiciels Adobe). En effet, la plupart des intrusions informatiques se font pas des sites Internet malveillants qui font exécuter sur votre ordinateur un code informatique malveillant chargé d'ouvrir un canal entre le pirate et vous. Ces codes informatiques malveillants utilisent les failles de vos logiciels pour s'exécuter. Lorsque l'utilisation d'une faille inconnue (sauf par les pirates) d'un logiciel est détectée par les « Gardiens de la paix numérique », un correctif (ou patch) est généralement développé par l'éditeur dans les jours qui suivent leur découverte. Ceci ne vous garantira pas une protection absolue de votre ordinateur, mais renforcera son blindage. Les pirates utilisent parfois d'anciens serveurs ou d'anciens postes de travail connectés sur le réseau, qui ont de vieux systèmes d'exploitation qui ne se mettent plus à jour et qui ont des failles ultra-connues pour pénétrer votre réseau et des postes pourtant ultra-sécurisés. Pensez donc à les déconnecter du réseau ou à copier le contenu ou les virtualiser sur des systèmes plus récents et tenus à jour.

• Mettez à jour les firmwares des matériels et objets connectés. Pour les mêmes raisons qu'il est important de mettre à jour vos logiciels avec leurs versions les plus récentes, il est aussi important de mettre à jour les logiciels de vos matériels et objets connectés (routeurs, modems, webcams etc.).

• Adoptez une politique sécurisée dans l'utilisation des mots de passe. Vos mots de passe doivent être longs, complexes et doivent changer souvent. Conseil primordial dans l'utilisation des mots de passe au bureau : Il doit être aussi précieux et aussi secret que le code de votre carte bancaire. Personne ne doit le connaître, sinon... quelqu'un pourra facilement se faire passer pour vous et vous faire porter le chapeau pour ses actes malveillants.

• Méfiez-vous des sites Internet proposant des vidéos gratuites, du streaming gratuit ou autres services inespérément gratuits. Les sites sont souvent piégés et ont destinés soit à collecter des données personnelles, soit contaminer votre ordinateur par des petits codes malveillants.

• Méfiez-vous également des e-mails douteux de demande d'aide (même d'un ami) ou autre participation humanitaire utilisant le paiement par Manda Cash, Western Union ou monnaie virtuelle telle le Bitcoin. Ce sont des moyen de paiement qui sont généralement utilisés par les pirates pour se faire payer et disparaître dans la nature. Les emails destinés à vous hameçonner auront aussi quelques détails qui devraient vous mettre la puce à l'oreille (Faute d'orthographe, huissier ou directeur ayant une adresse e-mail yahoo ou gmail).

• Vous avez un doute, vous pensez que votre ordinateur ou votre boîte e-mail est victime d'intrusion, changez immédiatement de mot de passe. Certains systèmes de messagerie permettent d'avoir un historique des accès et des connexions. L'analyse de cet historique pourrait bien vous donner une indication pour savoir si quelqu'un d'autre a accès à votre messagerie (alias, double diffusion, collecte d'un compte mail sur un autre compte etc).

**Conclusion**

Voilà, vous avez maintenant toute une liste de recommandations qui peut vous rassurer (ou non) et vous permettre de prendre conscience de la complexité qu'est à ce jour la lutte de la #cybercriminalité.

Si maintenant tout ceci vous semble complexe, rassurez-vous, c'est notre métier. Nous serons donc en mesure de vous accompagner dans la sensibilisation des utilisateurs, la détection ou la protection contre ces « ennuiwares ».

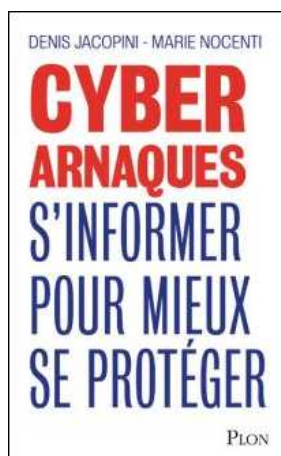
Contactez-moi

[block id="24761" title="Pied de page HAUT"]

---

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

Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



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

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

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

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

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

Commandez sur [Fnac.fr](http://Fnac.fr)

---

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur [Fnac.fr](http://Fnac.fr)

---

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

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

Comment se protéger des arnaques Internet

Commandez sur [amazon.fr](http://amazon.fr)

---



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

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

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

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

Source : Denis JACOPINI

---

# Un Employeur peut-il examiner

# Les messages échangés par ses employés sur leur téléphone professionnel ?



Un Employeur  
peut-il  
examiner les  
messages  
échangés par  
ses employés  
sur leur  
téléphone  
professionnel  
?

## Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel ?

Dès lors que le téléphone du salarié est professionnel, l'employeur a ce droit, à moins d'avoir mentionné avant le message «personnel». Dans ce cas, l'employeur n'a plus le droit. Mais souvent, on n'oublie de l'écrire... »

**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>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



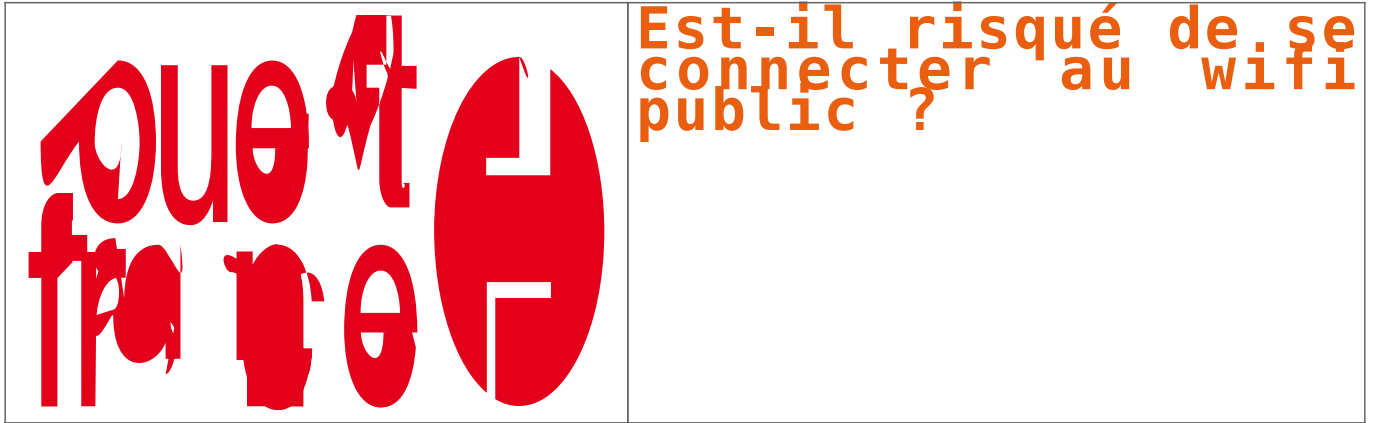
[Contactez-nous](#)



Réagissez à cet article

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

# Est-il risqué de se connecter au wifi public ? | Denis JACOPINI



**Nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants... Mais y a-t-il un risque à partager ces accès sans fil à internet avec d'autres ? Peut-on se faire pirater ses données ? Le point avec Denis Jacopini, expert en cybercriminalité.**

Avec les smartphones ou ordinateurs portables d'aujourd'hui, se connecter au réseau wifi d'une gare ou d'un hôtel, quand on est en déplacement, est devenu presque banal. À l'étranger, c'est même la solution la plus simple pour surfer sur internet et relever ses e-mails, sans risquer d'exorbitants frais de « roaming » (coûts de connexion au réseau mobile local, facturés ensuite par l'opérateur français). Résultat, on a tendance à surfer sur ces réseaux wifi avec la même insouciance qu'à la maison, sans aucune précaution. Ce qui n'est pas bien malin. Denis Jacopini, expert judiciaire en sécurité informatique, nous explique pourquoi.



Denis Jacopini, créateur du site LeNetExpert.fr et correspondant Cnil (Commission nationale de l'informatique et des libertés), est aussi formateur en protection des données personnelles et en sécurité informatique. (Photo : DR)

#### **À quoi faut-il faire attention, quand on se connecte à une borne wifi publique ou semi-publique, en ville ou dans un hôtel ?**

Si possible, il faut choisir un réseau wifi où la connexion se fait avec un nom d'identifiant et un mot de passe personnalisés, différents pour chaque utilisateur. En cas d'utilisation malveillante du réseau par quelqu'un, cette identification fournit une piste, sur le plan judiciaire, pour remonter jusqu'à l'auteur. Avec les wifi qui proposent un identifiant et un mot de passe identiques pour tout le monde, on est moins protégé. Les réseaux wifi les plus dangereux sont ceux qui sont complètement ouverts, sans aucun mot de passe, où les utilisateurs sont impossibles à tracer.

#### **Quel est le danger ? Se faire espionner ?**

Tout à fait. À partir du moment où quelqu'un se trouve connecté au même point wifi que vous, il a techniquement la possibilité d'accéder aux informations qui transitent sur le réseau, il peut « voir » ce qui entre et qui sort. Les pirates utilisent pour cela des logiciels espions, appelés « sniffers », ou « renifleurs » en bon français. Ces programmes sont désormais très faciles à trouver et à télécharger sur internet. Plus ou moins sophistiqués, ils permettent de capter, trier et interpréter le « bruit » informatique qui transite par le wifi.



Le wifi public, c'est pratique, mais pas très sécurisé. (Photo : Flickr/Richard Summers)

#### **La confidentialité de la navigation n'est donc pas garantie ?**

En effet. Et pas uniquement sur les réseaux wifi, d'ailleurs. C'est ainsi depuis la création d'internet : les protocoles de communication du web ne sont pas cryptés. Mais de plus en plus de sites « sensibles » – par exemple les messageries électroniques, les banques, les boutiques en ligne, etc. – ont désormais des adresses commençant par « https » au lieu de « http ». Le « s », souvent associé avec un petit cadenas dans la barre du navigateur, signifie que les communications sont sécurisées. Quand on navigue sur internet via un wifi, il faut donc privilégier ces sites.

#### **Le risque de se faire voler ses mots de passe, ou ses coordonnées bancaires, est donc bien réel ?**

Oui, mieux vaut éviter de saisir des données confidentielles quand on navigue sur internet via un wifi public ou semi-public. On a ainsi vu des hommes d'affaires se faire voler des informations importantes, car ils utilisaient en toute confiance un wifi d'hôtel... sur lequel étaient aussi connectés des pirates !



Un café Starbucks à Londres, très apprécié pour sa connexion wifi gratuite. (Photo : Stefan Wermuth/Reuters)

#### **Peut-on se faire abuser par une fausse borne wifi ?**

Oui, c'est une raison supplémentaire de se méfier des réseaux complètement ouverts : certains pirates créent leur propre borne wifi à partir d'un simple ordinateur portable. Les passants se connectent dessus, par facilité, sans se douter qu'il ne s'agit pas du tout d'une « vraie » borne. Ensuite, la personne mal intentionnée n'a plus qu'à récupérer les informations qui transitent par le réseau qu'elle a créé... Aujourd'hui, c'est très facile de devenir pirate !

#### **Comment se protéger ?**

En s'abstenant de réaliser des opérations sensibles, comme des achats en ligne ou des opérations bancaires, sur un wifi public. Si on le peut, mieux vaut utiliser le réseau 3G ou 4G pour se connecter à internet en mobilité. Les informations qui transitent par cette voie sont beaucoup moins faciles à pirater. Il y a aussi la solution consistant à installer, sur son smartphone ou son ordinateur, ce qu'on appelle un « VPN ». C'est un logiciel qui crée un « réseau privé virtuel », une sorte de tunnel crypté pour vos communications internet. Cela ralentit un peu la connexion, mais c'est beaucoup plus sûr.



Zone de wifi gratuit à New York : en France comme à l'étranger, mieux vaut se connecter sur un nom de réseau connu, éventuellement signalé via l'affichage public. (Photo : Keith Bedford/Reuters)

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 plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.ouest-france.fr/leditiondusoir/data/492/reader/reader.html?t=1431534138729#!preferred/1/package/492/pub/493/page/7>

Par Corinne Bourbeillon



# Peut-on être licencié pour ce

# qu'on y a écrit dans les réseaux sociaux ? | Denis JACOPINI



Peut-on être licencié pour ce qu'on y a écrit dans les réseaux sociaux ?

Peut-on être licencié pour ce qu'on y a écrit dans les réseaux sociaux ?

Oui.

Dans une affaire concernant trois salariés licenciés pour avoir dénigré leur hiérarchie sur Facebook, un Conseil des prud'hommes a considéré que les propos publiés sur le mur d'un des salariés étaient publics car accessibles aux « amis d'amis ».

Ces propos ont perdu leur caractère privé du fait qu'ils étaient accessibles à des personnes non concernées par la discussion.

Soyez donc vigilant lorsque vous publiez des commentaires sur un réseau social !

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 plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

<https://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=D48813C492DFE134132210B5E195173E?id=199&back=true>

# Detekt un logiciel pour supprimer des programmes espions | Denis JACOPINI



#Detekt, un logiciel pour  
supprimer des programmes  
espions

**Voilà un logiciel qui va vous aider à supprimer les RAT que vous pouvez trouver éventuellement sur vos PC.** Les RAT sont des programmes espions ( Remote Administration Tool, ou Outil d'Administration Distante ), ce sont des programmes qui peuvent effectuer une prise de contrôle à distance de votre ordinateur, sans que vous sachiez même que ce programme est sur votre machine.

Le logiciel proposé est le logiciel Detekt, il est également disponible avec son code source et vous aidera grandement à scanner votre PC et à éradiquer les RAT facilement de votre machine.

**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.**



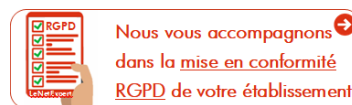
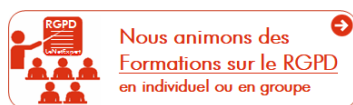
**Besoin d'un expert pour vous mettre en conformité avec le RGPD ?**

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)

---

# Loi Renseignement : la boîte à outils pour apprendre à protéger votre vie privée, en chiffrant vos données et communications | Denis JACOPINI

✘ Loi Renseignement : la boîte à outils pour apprendre à protéger votre vie privée, en chiffrant vos données et communications

**Maintenant que la Loi Renseignement est votée, et en attendant la suite du processus législatif, apprenons à résister à la surveillance de masse avec quelques outils cryptographiques plus ou moins simples, mais efficaces et légaux.**

Nous sommes le soir du mardi 5 mai, et c'est un jour funeste pour la démocratie. La France s'était autoproclamée « pays des Lumières » parce qu'il y a 250 ans notre pays éclairait l'Europe et le monde grâce aux travaux philosophiques et politiques de Montesquieu, qui prônait la séparation des pouvoirs, et de Voltaire et Rousseau.

À dater d'aujourd'hui, jour du vote en première lecture du projet de loi sur le renseignement, à cause d'une classe politique d'une grande médiocrité, s'enclenche un processus au terme duquel le peuple français va probablement devoir subir une loi dangereuse, qui pourrait s'avérer extrêmement liberticide si elle tombait entre de mauvaises mains, par exemple celles de l'extrême droite.

Même si la loi doit encore passer devant le Sénat puis peut-être revenir en seconde lecture à l'Assemblée Nationale, même si une saisine du Conseil Constitutionnel va être déposée par une soixantaine de courageux députés en complément de celle déjà annoncée par François Hollande, mieux vaut se préparer au pire, en imaginant que cette loi sera un jour promulguée. En faisant un peu de mauvais esprit, j'ai imaginé un nom pour le dispositif qui sera chargé de collecter nos données personnelles afin de détecter les comportements suspects : « Surveillance Totale Automatisée via des Systèmes Informatiques » et bizarrement l'acronyme est STASI !

Dès lors, à titre préventif et sans préjuger de l'avenir, il me semble important d'apprendre à protéger sa vie privée. Ceci passe par le chiffrement de ses communications, qu'il s'agisse d'échanges sur Internet ou via SMS, et cela peut se faire au moyen de différents outils à la fois efficaces et légaux.

Bien évidemment, les « vrais méchants » que sont les terroristes, djihadistes, gangsters et autres trafiquants connaissent et utilisent déjà ces outils : vous vous doutez bien qu'ils n'ont pas attendu ce billet de blog pour les découvrir...



#### **Une boîte à outils pour protéger votre vie privée**

##### **Anonymat sur Internet**

Pour protéger votre identité sur Internet et notamment sur le web, vous pouvez combiner l'utilisation d'un réseau privé virtuel, ou VPN, et de TOR, un système d'anonymisation qui nécessite l'installation d'un logiciel spécifique, TOR Browser. Je ne vous donne pas de référence particulière en matière de VPN, car l'offre est pléthorique.

MAJ : un lecteur m'a indiqué l'existence de La Brique Internet, un simple boîtier VPN couplé à un serveur. Pour que la Brique fonctionne, il faut lui configurer un accès VPN, qui lui permettra de créer un tunnel jusqu'à un autre ordinateur sur Internet. Une extension fournira bientôt aussi en plus un accès clé-en-main via TOR en utilisant la clé wifi du boîtier pour diffuser deux réseaux wifi : l'un pour un accès transparent via VPN et l'autre pour un accès transparent via Tor.

##### **Chiffrement des données**

Pour chiffrer le contenu de vos données, stockées sur les disques durs de vos ordinateurs ou dans les mémoires permanentes de vos smartphones, vous pouvez mettre en œuvre des outils tels que LUKS pour les systèmes Linux ou TrueCrypt pour les OS les plus répandus : même si TrueCrypt a connu une histoire compliquée, son efficacité ne semble pas remise en cause par le dernier audit de code effectué par des experts.

Je vous signale aussi que l'ANSSI – Agence nationale de la sécurité des systèmes d'information – signale d'autres outils alternatifs comme Cryhod, Zed !, ZoneCentral, Security Box et StormShield. Même si l'ANSSI est un service gouvernemental il n'y a pas de raison de ne pas leur faire confiance sur ce point ☐

##### **Chiffrement des e-mails et authentification des correspondants**

GPG, acronyme de GNU Privacy Guard, est l'implémentation GNU du standard OpenPGP. Cet outil permet de transmettre des messages signés et/ou chiffrés ce qui vous garantit à la fois l'authenticité et la confidentialité de vos échanges. Des modules complémentaires en facilitent l'utilisation sous Linux, Windows, MacOS X et Android.

MAJ : un lecteur m'a signalé PEPS, une solution de sécurisation française et Open Source, issue d'un projet mené par la DGA – Direction générale de l'armement – à partir duquel a été créée la société MLState.

##### **Messagerie instantanée sécurisée**

OTR, Off The Record, est un plugin à greffer à un client de messagerie instantanée. Le logiciel de messagerie instantanée Jitsi, qui repose sur le protocole SIP de la voix sur IP, intègre l'outil de chiffrement ZRTP.

##### **Protection des communications mobiles**

A défaut de protéger les métadonnées de vos communications mobiles, qu'il s'agisse de voix ou de SMS, vous pouvez au moins chiffrer les données en elles-mêmes, à savoir le contenu de vos échanges :

RedPhon est une application de chiffrement des communications vocales sous Android capable de communiquer avec Signal qui est une application du même fournisseur destinée aux iPhone sous iOS.

TextSecure est une application dédiée pour l'échange sécurisé de SMS, disponible pour Android et compatible avec la dernière version de l'application Signal. Plus d'information à ce sujet sur le blog de Stéphane Bortzmeyer.

MAJ : un lecteur m'a indiqué l'application APG pour Android qui permet d'utiliser ses clés GPG pour chiffrer ses SMS.

##### **Allez vous former dans les « cafés Vie Privée »**

Si vous n'êtes pas geek et ne vous sentez pas capable de maîtriser ces outils sans un minimum d'accompagnement, alors le concept des « cafés Vie Privée » est pour vous : il s'agit tout simplement de se réunir pour apprendre, de la bouche ceux qui savent le faire, comment mettre en œuvre les outils dont je vous ai parlé plus haut afin de protéger sa vie privée de toute intrusion, gouvernementale ou non.

Tout simplement, il s'agit de passer un après-midi à échanger et à pratiquer la cryptographie. Pour cela sont proposés des ateliers d'une durée minimum de 1 heure, axés autour de la sécurité informatique et de la protection de la vie privée.

Et comme le disent avec humour les organisateurs, « les ateliers sont accessibles à tout type de public, geek et non-geek, chatons, poneys, loutres ou licornes. ». Bref, le « café Vie Privée » est à la protection de la vie privée ce que la réunion Tupperware était à la cuisine ☐



Voilà, vous avez je l'espère suffisamment d'éléments pratiques pour commencer à protéger votre vie privée... en espérant vraiment que le Conseil Constitutionnel abrogera les points les plus contestables de cette loi et nous évitera d'avoir à déployer un tel arsenal sécuritaire.

PS : l'image « 1984 was not a manual » a été créée par Arnaud Velten aka @Bizcom.

---

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

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

Source : <http://www.zdnet.fr/actualites/loi-renseignement-la-bo-te-a-outils-pour-apprendre-a-protoger-votre-vie-privee-en-chiffrent-vos-donnees-et-communications-39818894.htm>  
Par Pierre Col

---

# Vidéosurveillance en entreprise : règles et limites | Denis JACOPINI

✖ #Vidéosurveillance en entreprise :  
règles et limites

**Un système de vidéosurveillance en entreprise se doit d'observer certaines limites pour rester dans un cadre de protection des biens et personnes.**

#### **Le cadre législatif de la vidéosurveillance**

C'est la loi dite « informatique et libertés » du 6 janvier 1978, modifiée par la loi du 6 août 2004, qui fixe le cadre de mise en place d'une vidéosurveillance sur un lieu à usage professionnel.

Ainsi dans des lieux non accessibles au public (bureaux, entrepôts, réserves, locaux d'administration) l'installation d'une vidéosurveillance doit faire l'objet d'une déclaration à la CNIL (Commission Nationale Informatique et Libertés).

C'est également une obligation pour les guichets de réception de clients et les commerces, lorsque le système enregistre les images dans un fichier et permettant de conserver d'identité des personnes filmées.

Si toutefois les fichiers ne sont pas conservés à des fins d'identification, un assouplissement de la loi permet de solliciter une simple autorisation préfectorale (pour les lieux accueillant du public).

#### **Information des salariés et du public**

Une information préalable est requise auprès des représentants des salariés avant toute installation d'un dispositif de vidéosurveillance, en mettant l'accent sur les objectifs de sécurité et en spécifiant que les enregistrements ne sont pas conservés plus d'un mois.

De la même manière, l'entreprise doit mettre en place une signalisation informant les visiteurs de la présence d'un système de vidéosurveillance.

Cet affichage doit se faire dès l'entrée dans l'établissement, en précisant les raisons ainsi que les coordonnées de l'autorité ou de la personne chargée de l'exploitation du système et en rappelant les modalités d'exercice du droit d'accès des personnes filmées aux enregistrements qui les concernent (loi du 6 août 2004).

#### **Le principe de proportionnalité**

On pourrait dire aussi principe de bon sens. L'employeur doit en premier lieu démontrer l'intérêt légitime à la mise en place d'un système de surveillance. Il peut s'agir de la nécessité de protéger des personnes ou des biens, ou de se prémunir contre des risques tels que le vol.

Partant de là, le dispositif installé doit être proportionnel au regard des intérêts à protéger.

Il y a une différence notable entre installer une caméra dans un entrepôt à des fins de sécurité et le fait d'en installer une permettant d'observer en permanence des postes de travail.

Bien évidemment des caméras installées dans des lieux de repos des salariés ou dans des toilettes constituent une surveillance excessive. La CNIL a récemment mis à l'amende des entreprises pour des situations de surveillance jugées excessives et non proportionnées par rapport aux risques à prévenir.

La CNIL a fait valoir que des caméras peuvent être installées au niveau des entrées et sorties des bâtiments, des issues de secours et des voies de circulation, ou encore filmer les zones où de la marchandise ou des biens de valeur sont entreposés. Pas question en revanche de filmer en permanence un employé sur son poste de travail, sauf si celui-ci manipule par exemple de l'argent, en vertu du principe de proportionnalité.

En synthèse, bien que frappée du sceau du bon sens, la mise en place d'un système de vidéosurveillance doit s'accompagner de certaines précautions. Eventuellement prenez avis auprès de votre conseiller en assurances, qui saura vous orienter vers un prestataire de vidéosurveillance homologué et bien au fait des contraintes législatives.

---

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.comptanoo.com/assurance-prevention/actualite-tpe-pme/23794/videosurveillance-entreprise-regles-et-limites>

:

---

# Windows 8 : Identifier les applications malveillantes à partir des services par défaut | Denis JACOPINI

x	Windows 8 : Identifier les applications malveillantes à partir des services par défaut
---	--

Table of Contents

Page	Section	Page	Section	Page
1	Introduction	1	Introduction	1
2	1.1 Objectives	2	1.1 Objectives	2
3	1.2 Scope	3	1.2 Scope	3
4	1.3 Methodology	4	1.3 Methodology	4
5	1.4 Deliverables	5	1.4 Deliverables	5
6	2. Literature Review	6	2. Literature Review	6
7	2.1 Background	7	2.1 Background	7
8	2.2 Related Work	8	2.2 Related Work	8
9	2.3 Research Gaps	9	2.3 Research Gaps	9
10	3. System Architecture	10	3. System Architecture	10
11	3.1 Overview	11	3.1 Overview	11
12	3.2 Components	12	3.2 Components	12
13	3.3 Data Flow	13	3.3 Data Flow	13
14	3.4 Security	14	3.4 Security	14
15	3.5 Performance	15	3.5 Performance	15
16	4. Implementation	16	4. Implementation	16
17	4.1 Environment	17	4.1 Environment	17
18	4.2 Tools	18	4.2 Tools	18
19	4.3 Design	19	4.3 Design	19
20	4.4 Development	20	4.4 Development	20
21	4.5 Testing	21	4.5 Testing	21
22	4.6 Deployment	22	4.6 Deployment	22
23	5. Results and Discussion	23	5. Results and Discussion	23
24	5.1 Findings	24	5.1 Findings	24
25	5.2 Analysis	25	5.2 Analysis	25
26	5.3 Comparison	26	5.3 Comparison	26
27	5.4 Limitations	27	5.4 Limitations	27
28	5.5 Future Work	28	5.5 Future Work	28
29	6. Conclusion	29	6. Conclusion	29
30	6.1 Summary	30	6.1 Summary	30
31	6.2 Final Thoughts	31	6.2 Final Thoughts	31
32	7. References	32	7. References	32
33	7.1 Bibliography	33	7.1 Bibliography	33
34	7.2 Citations	34	7.2 Citations	34
35	7.3 Sources	35	7.3 Sources	35
36	7.4 Acknowledgments	36	7.4 Acknowledgments	36
37	7.5 Appendix	37	7.5 Appendix	37
38	7.6 Glossary	38	7.6 Glossary	38
39	7.7 Index	39	7.7 Index	39
40	7.8 Appendix A	40	7.8 Appendix A	40
41	7.9 Appendix B	41	7.9 Appendix B	41
42	7.10 Appendix C	42	7.10 Appendix C	42
43	7.11 Appendix D	43	7.11 Appendix D	43
44	7.12 Appendix E	44	7.12 Appendix E	44
45	7.13 Appendix F	45	7.13 Appendix F	45
46	7.14 Appendix G	46	7.14 Appendix G	46
47	7.15 Appendix H	47	7.15 Appendix H	47
48	7.16 Appendix I	48	7.16 Appendix I	48
49	7.17 Appendix J	49	7.17 Appendix J	49
50	7.18 Appendix K	50	7.18 Appendix K	50
51	7.19 Appendix L	51	7.19 Appendix L	51
52	7.20 Appendix M	52	7.20 Appendix M	52
53	7.21 Appendix N	53	7.21 Appendix N	53
54	7.22 Appendix O	54	7.22 Appendix O	54
55	7.23 Appendix P	55	7.23 Appendix P	55
56	7.24 Appendix Q	56	7.24 Appendix Q	56
57	7.25 Appendix R	57	7.25 Appendix R	57
58	7.26 Appendix S	58	7.26 Appendix S	58
59	7.27 Appendix T	59	7.27 Appendix T	59
60	7.28 Appendix U	60	7.28 Appendix U	60
61	7.29 Appendix V	61	7.29 Appendix V	61
62	7.30 Appendix W	62	7.30 Appendix W	62
63	7.31 Appendix X	63	7.31 Appendix X	63
64	7.32 Appendix Y	64	7.32 Appendix Y	64
65	7.33 Appendix Z	65	7.33 Appendix Z	65
66	7.34 Appendix AA	66	7.34 Appendix AA	66
67	7.35 Appendix AB	67	7.35 Appendix AB	67
68	7.36 Appendix AC	68	7.36 Appendix AC	68
69	7.37 Appendix AD	69	7.37 Appendix AD	69
70	7.38 Appendix AE	70	7.38 Appendix AE	70
71	7.39 Appendix AF	71	7.39 Appendix AF	71
72	7.40 Appendix AG	72	7.40 Appendix AG	72
73	7.41 Appendix AH	73	7.41 Appendix AH	73
74	7.42 Appendix AI	74	7.42 Appendix AI	74
75	7.43 Appendix AJ	75	7.43 Appendix AJ	75
76	7.44 Appendix AK	76	7.44 Appendix AK	76
77	7.45 Appendix AL	77	7.45 Appendix AL	77
78	7.46 Appendix AM	78	7.46 Appendix AM	78
79	7.47 Appendix AN	79	7.47 Appendix AN	79
80	7.48 Appendix AO	80	7.48 Appendix AO	80
81	7.49 Appendix AP	81	7.49 Appendix AP	81
82	7.50 Appendix AQ	82	7.50 Appendix AQ	82
83	7.51 Appendix AR	83	7.51 Appendix AR	83
84	7.52 Appendix AS	84	7.52 Appendix AS	84
85	7.53 Appendix AT	85	7.53 Appendix AT	85
86	7.54 Appendix AU	86	7.54 Appendix AU	86
87	7.55 Appendix AV	87	7.55 Appendix AV	87
88	7.56 Appendix AW	88	7.56 Appendix AW	88
89	7.57 Appendix AX	89	7.57 Appendix AX	89
90	7.58 Appendix AY	90	7.58 Appendix AY	90
91	7.59 Appendix AZ	91	7.59 Appendix AZ	91
92	7.60 Appendix BA	92	7.60 Appendix BA	92
93	7.61 Appendix BB	93	7.61 Appendix BB	93
94	7.62 Appendix BC	94	7.62 Appendix BC	94
95	7.63 Appendix BD	95	7.63 Appendix BD	95
96	7.64 Appendix BE	96	7.64 Appendix BE	96
97	7.65 Appendix BF	97	7.65 Appendix BF	97
98	7.66 Appendix BG	98	7.66 Appendix BG	98
99	7.67 Appendix BH	99	7.67 Appendix BH	99
100	7.68 Appendix BI	100	7.68 Appendix BI	100
101	7.69 Appendix BJ	101	7.69 Appendix BJ	101
102	7.70 Appendix BK	102	7.70 Appendix BK	102
103	7.71 Appendix BL	103	7.71 Appendix BL	103
104	7.72 Appendix BM	104	7.72 Appendix BM	104
105	7.73 Appendix BN	105	7.73 Appendix BN	105
106	7.74 Appendix BO	106	7.74 Appendix BO	106
107	7.75 Appendix BP	107	7.75 Appendix BP	107
108	7.76 Appendix BQ	108	7.76 Appendix BQ	108
109	7.77 Appendix BR	109	7.77 Appendix BR	109
110	7.78 Appendix BS	110	7.78 Appendix BS	110
111	7.79 Appendix BT	111	7.79 Appendix BT	111
112	7.80 Appendix BU	112	7.80 Appendix BU	112
113	7.81 Appendix BV	113	7.81 Appendix BV	113
114	7.82 Appendix BW	114	7.82 Appendix BW	114
115	7.83 Appendix BX	115	7.83 Appendix BX	115
116	7.84 Appendix BY	116	7.84 Appendix BY	116
117	7.85 Appendix BZ	117	7.85 Appendix BZ	117
118	7.86 Appendix CA	118	7.86 Appendix CA	118
119	7.87 Appendix CB	119	7.87 Appendix CB	119
120	7.88 Appendix CC	120	7.88 Appendix CC	120
121	7.89 Appendix CD	121	7.89 Appendix CD	121
122	7.90 Appendix CE	122	7.90 Appendix CE	122
123	7.91 Appendix CF	123	7.91 Appendix CF	123
124	7.92 Appendix CG	124	7.92 Appendix CG	124
125	7.93 Appendix CH	125	7.93 Appendix CH	125
126	7.94 Appendix CI	126	7.94 Appendix CI	126
127	7.95 Appendix CJ	127	7.95 Appendix CJ	127
128	7.96 Appendix CK	128	7.96 Appendix CK	128
129	7.97 Appendix CL	129	7.97 Appendix CL	129
130	7.98 Appendix CM	130	7.98 Appendix CM	130
131	7.99 Appendix CN	131	7.99 Appendix CN	131
132	7.100 Appendix CO	132	7.100 Appendix CO	132
133	7.101 Appendix CP	133	7.101 Appendix CP	133
134	7.102 Appendix CQ	134	7.102 Appendix CQ	134
135	7.103 Appendix CR	135	7.103 Appendix CR	135
136	7.104 Appendix CS	136	7.104 Appendix CS	136
137	7.105 Appendix CT	137	7.105 Appendix CT	137
138	7.106 Appendix CU	138	7.106 Appendix CU	138
139	7.107 Appendix CV	139	7.107 Appendix CV	139
140	7.108 Appendix CW	140	7.108 Appendix CW	140
141	7.109 Appendix CX	141	7.109 Appendix CX	141
142	7.110 Appendix CY	142	7.110 Appendix CY	142
143	7.111 Appendix CZ	143	7.111 Appendix CZ	143
144	7.112 Appendix DA	144	7.112 Appendix DA	144
145	7.113 Appendix DB	145	7.113 Appendix DB	145
146	7.114 Appendix DC	146	7.114 Appendix DC	146
147	7.115 Appendix DD	147	7.115 Appendix DD	147
148	7.116 Appendix DE	148	7.116 Appendix DE	148
149	7.117 Appendix DF	149	7.117 Appendix DF	149
150	7.118 Appendix DG	150	7.118 Appendix DG	150
151	7.119 Appendix DH	151	7.119 Appendix DH	151
152	7.120 Appendix DI	152	7.120 Appendix DI	152
153	7.121 Appendix DJ	153	7.121 Appendix DJ	153
154	7.122 Appendix DK	154	7.122 Appendix DK	154
155	7.123 Appendix DL	155	7.123 Appendix DL	155
156	7.124 Appendix DM	156	7.124 Appendix DM	156
157	7.125 Appendix DN	157	7.125 Appendix DN	157
158	7.126 Appendix DO	158	7.126 Appendix DO	158
159	7.127 Appendix DP	159	7.127 Appendix DP	159
160	7.128 Appendix DQ	160	7.128 Appendix DQ	160
161	7.129 Appendix DR	161	7.129 Appendix DR	161
162	7.130 Appendix DS	162	7.130 Appendix DS	162
163	7.131 Appendix DT	163	7.131 Appendix DT	163
164	7.132 Appendix DU	164	7.132 Appendix DU	164
165	7.133 Appendix DV	165	7.133 Appendix DV	165
166	7.134 Appendix DW	166	7.134 Appendix DW	166
167	7.135 Appendix DX	167	7.135 Appendix DX	167
168	7.136 Appendix DY	168	7.136 Appendix DY	168
169	7.137 Appendix DZ	169	7.137 Appendix DZ	169
170	7.138 Appendix EA	170	7.138 Appendix EA	170
171	7.139 Appendix EB	171	7.139 Appendix EB	171
172	7.140 Appendix EC	172	7.140 Appendix EC	172
173	7.141 Appendix ED	173	7.141 Appendix ED	173
174	7.142 Appendix EE	174	7.142 Appendix EE	174
175	7.143 Appendix EF	175	7.143 Appendix EF	175
176	7.144 Appendix EG	176	7.144 Appendix EG	176
177	7.145 Appendix EH	177	7.145 Appendix EH	177
178	7.146 Appendix EI	178	7.146 Appendix EI	178
179	7.147 Appendix EJ	179	7.147 Appendix EJ	179
180	7.148 Appendix EK	180	7.148 Appendix EK	180
181	7.149 Appendix EL	181	7.149 Appendix EL	181
182	7.150 Appendix EM	182	7.150 Appendix EM	182
183	7.151 Appendix EN	183	7.151 Appendix EN	183
184	7.152 Appendix EO	184	7.152 Appendix EO	184
185	7.153 Appendix EP	185	7.153 Appendix EP	185
186	7.154 Appendix EQ	186	7.154 Appendix EQ	186
187	7.155 Appendix ER	187	7.155 Appendix ER	187
188	7.156 Appendix ES	188	7.156 Appendix ES	188
189	7.157 Appendix ET	189	7.157 Appendix ET	189
190	7.158 Appendix EU	190	7.158 Appendix EU	190
191	7.159 Appendix EV	191	7.159 Appendix EV	191
192	7.160 Appendix EW	192	7.160 Appendix EW	192
193	7.161 Appendix EX	193	7.161 Appendix EX	193
194	7.162 Appendix EY	194	7.162 Appendix EY	194
195	7.163 Appendix EZ	195	7.163 Appendix EZ	195
196	7.164 Appendix FA	196	7.164 Appendix FA	196
197	7.165 Appendix FB	197	7.165 Appendix FB	197
198	7.166 Appendix FC	198	7.166 Appendix FC	198
199	7.167 Appendix FD	199	7.167 Appendix FD	199
200	7.168 Appendix FE	200	7.168 Appendix FE	200
201	7.169 Appendix FF	201	7.169 Appendix FF	201
202	7.170 Appendix FG	202	7.170 Appendix FG	202
203	7.171 Appendix FH	203	7.171 Appendix FH	203
204	7.172 Appendix FI	204	7.172 Appendix FI	204
205	7.173 Appendix FJ	205	7.173 Appendix FJ	205
206	7.174 Appendix FK	206	7.174 Appendix FK	206
207	7.175 Appendix FL	207	7.175 Appendix FL	207
208	7.176 Appendix FM	208	7.176 Appendix FM	208
209	7.177 Appendix FN	209	7.177 Appendix FN	209
210	7.178 Appendix FO	210	7.178 Appendix FO	210
211	7.179 Appendix FP	211	7.179 Appendix FP	211
212	7.180 Appendix FQ	212	7.180 Appendix FQ	212
213	7.181 Appendix FR	213	7.181 Appendix FR	213
214	7.182 Appendix FS	214	7.182 Appendix FS	214
215	7.183 Appendix FT	215	7.183 Appendix FT	215
216	7.184 Appendix FU	216	7.184 Appendix FU	216

---

# Un oeil sur vous, citoyens sous surveillance – Documentaire 2015 | Denis JACOPINI

x	Un oeil sur vous, citoyens sous surveillance – Documentaire 2015 2h24
---	---

**Des milliards de citoyens connectés livrent en permanence – et sans toujours s'en rendre compte – des informations sur leur vie quotidienne à des sociétés privées qui les stockent dans de gigantesques serveurs. Ces informations sont rendues accessibles aux États et vendues aux entreprises. Dans ce monde sous étroite surveillance, jusqu'où irons-nous en sacrifiant nos vies intimes et nos droits à la liberté individuelle ?**

---

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 !