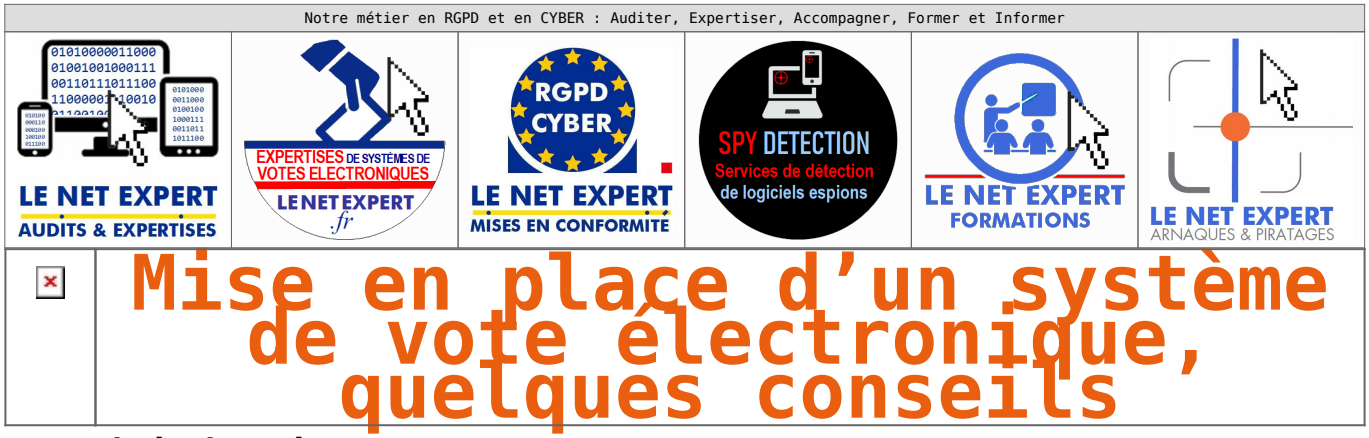
Mise en place d’un système de vote électronique, quelques conseils | Denis JACOPINI



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 lus 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.

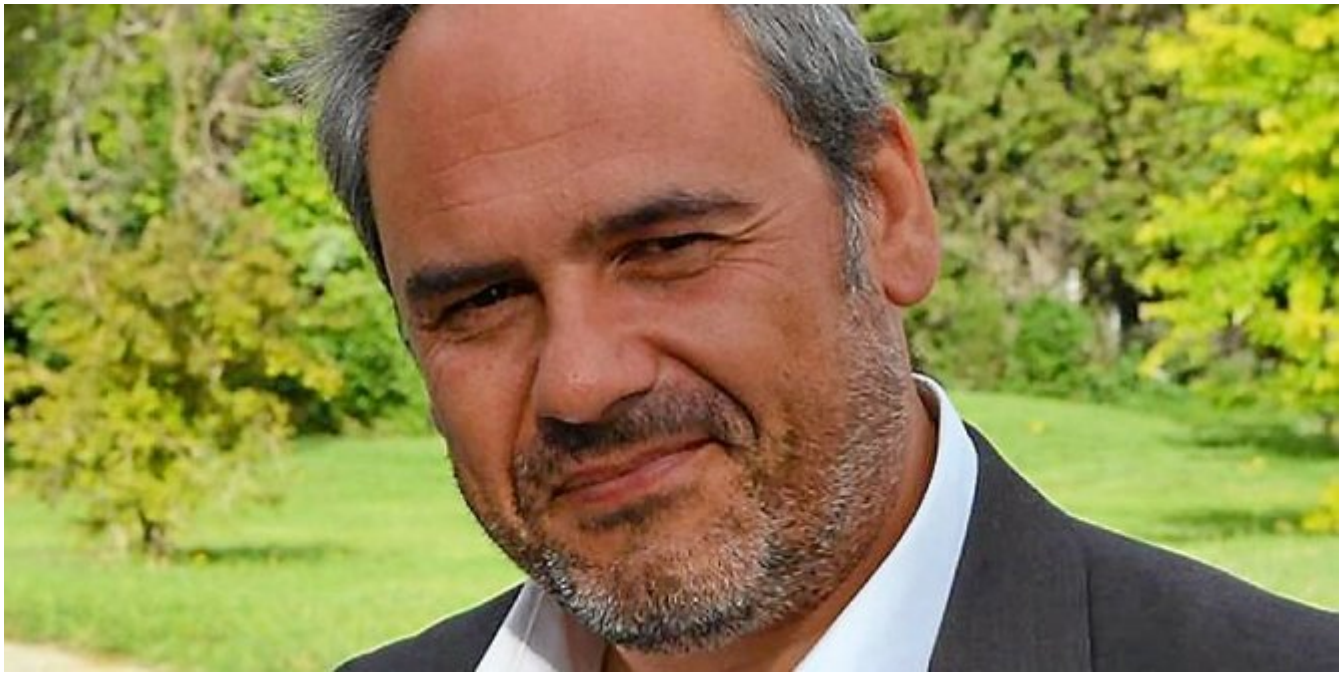
Si l’expertise peut couvrir un champ plus large que celui de la présente recommandation, le rapport d’expertise fourni au responsable de traitement doit comporter une partie spécifique présentant l’évaluation du dispositif au regard des différents points de la recommandation.

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.

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

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 solution 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 rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

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

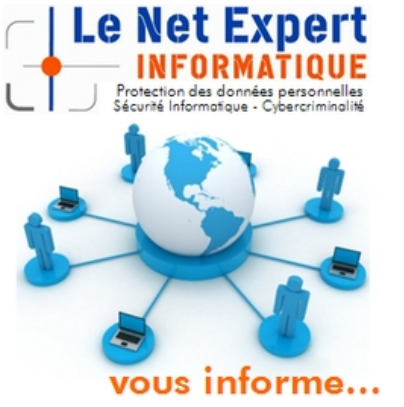
Contactez-nous

---

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



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

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

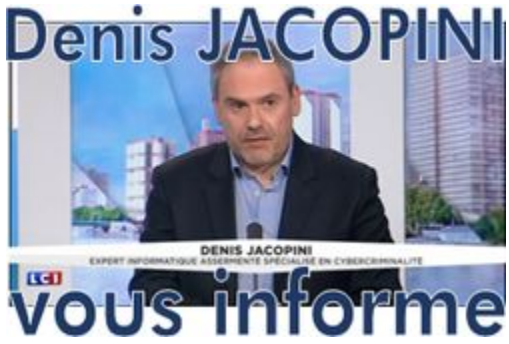
Les officiers de police judiciaire et les agents des douanes sont destinataires des résultats de la consultation du fichier, dans le cadre de leurs enquêtes.
Le FAED peut également être consulté, sous certaines conditions, par les agents des organismes internationaux de police judiciaire et par ceux des services de police ou de justice d'Etats étrangers.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous 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

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

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

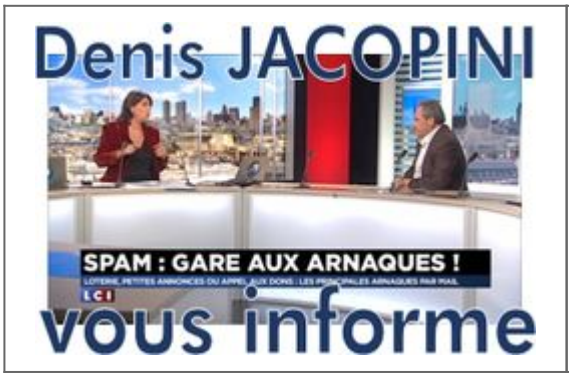
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Conseils de prévention sur Internet / Cybercrime / Dossiers / Actualités – Police nationale – Ministère de l’Intérieur

---

Comment bien se protéger contre les Cyberattaques ?



Comment bien se protéger contre les Cyberattaques ?

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 connait, 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 rechercher 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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle… ;
- Expertises de systèmes de vote électronique ;

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

ou suivez nous sur

Réagissez à cet article

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

?

Quelques exemples de sanctions et condamnations prononcées par la CNIL | Denis JACOPINI

	**Quelques sanctions CNIL prononcées auprès de sociétés commerciales**

Quelques sanctions CNIL prononcées auprès de sociétés commerciales

- Société JEAN MARC PHILIPPE (DELIBERATION n°2009-201 du 16 avril 2009) : 10 000 euros d'amende d'amende pour avoir installé une vidéosurveillance permanente des salariés (COMMERCE VÊTEMENTS MAGASIN + SITE EN LIGNE PARIS)
  En outre, le directeur général de la société JEAN MARC PHILIPPE s'étant opposé au contrôle de la CNIL, a été condamné par le Tribunal correctionnel de Paris à une peine d'amende de 5 000 euros pour délit d'entrave.
- DirectAnnonces : 40 000 euros d'amende pour pratiques déloyales Cette société est spécialisée dans la compilation d'annonces immobilières de particuliers sur

internet pour revente à des professionnels (pratique jugée déloyale puisqu'elle se faisait à l'insu des personnes). (ANNONCES IMMOBILIERES PARIS)

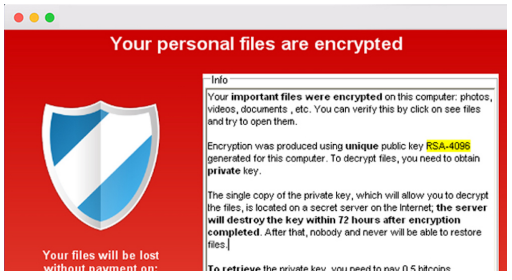
- CDISCOUNT (30.000 € d'amende) et ISOTHERM (30.000 € d'amende) pour démarchage commercial par courriel et téléphone abusif. Sanctions prononcées en novembre 2008 et rendues publiques en juin 2009. Ces deux sociétés ne prenaient pas en compte efficacement les demandes de désinscription des personnes ne souhaitant plus être démarchées alors que la loi informatique et libertés prévoit un droit d'opposition à la prospection commerciale. (MAGASIN EN LIGNE BORDEAUX)
- KEOLIS RENNES : avertissement public pour le passe Korrigo de Rennes (prononcé le 20 janvier 2009 et rendu public le 17 juin 2009). Un contrôle sur place a souligné de véritables obstacles pour souscrire un passe anonyme. (TRANSPORT PUBLIC DE VOYAGEURS RENNES)
- Entreparticuliers.com : Par décision du 20 mai 2008, la CNIL, a prononcé un avertissement à l'égard de la société en raison de plusieurs manquements à la loi informatique et libertés, dont des défauts de sécurité. Information rendue publique le 17 novembre 2008. (ANNONCES IMMOBILIERES LEVALLOSIS PERET)
- Société Leclerc ARCYDIS SA : 30 000 € d'amende + Publication de la sanction sur son site internet et sur la base Légifrance – juillet 2008 (CENTRE LECLERC BOIS D'ARCY 78390)
- Société Neuf Cegetel : 7 000 € d'amende + Publication de la sanction sur son site internet et sur la base Légifrance – juin 2008 (OPERATEUR TELEPHONIQUE 92)
- Société VPC KHADR : 5 000 € d'amende + Publication de la sanction dans le quotidien La Nouvelle République du Centre Ouest – février 2008 (VENTE DE MOBILIE REN LIGNE ARGENTON SUR CREUSE 36)*****
- SERVICE INNOVATION GROUP France : Société spécialisée dans la force de vente et le marketing : 40 000 € d'amende – décembre 2007 (78140 VELIZY VILLACOUBLAY)

- Société JPSM (nom commercial « Stock Premium ») : 5000 € d’amende – novembre 2007 (BOUTIQUE VÊTEMENTS NANCY)
- Société B&M : Société de Conseils – 10 000 € d’amende – octobre 2007 (LA RICHE 37)
- Cabinet d’enquêtes privées (non public) : Recherche de débiteurs – 50 000 € d’amende – juin 2007
- FRDT – Entreprise spécialisée dans l’immobilier : 15 000 € d’amende – mai 2007 (TOULON 83)
- Studio Replay – Entreprise de vente à distance : 10 000 € d’amende – mars 2007
- Cabinet de recouvrement de créances : 5 000 € d’amende – mars 2007
- BANQUE DES ANTILLES FRANCAISES : 30 000 € d’amende – mars 2007 (PARIS)
- Opérateur télécom (Non Public) : 10 000 € d’amende – mars 2007
- Entreprise de vente à distance (Non public) : 5 000 € d’amende – déc. 2006
- La société Tyco HealthCare (Matériel médical) : 30 000 € d’amende – déc. 2006. (PLAISIR 78)
- Deux enseignes spécialisées dans la vente de fenêtres (Non public) : 60 000 € d’amendes – Déc. 2006
- Le Crédit Agricole Centre France : 20 000 € d’amende – Nov. 2006
- Etablissement financier (Non Public) : 1 000 € d’amende – Sept. 2006
- Entreprise d’électricité (non public) : 1 500 € d’amende – Sept. 2006

- Expertise financière Cabinet de conseil : 500 € d’amende – Sept. 2006
- Prestataire internet (Non Public) : 300 € d’amende- Sept. 2006
- Etude d’huissiers de justice (Non Public) : 5000 € d’amende- Juin 2006
- LCL (anciennement Le Crédit Lyonnais) : 45 000 € d’amende – Juin 2006

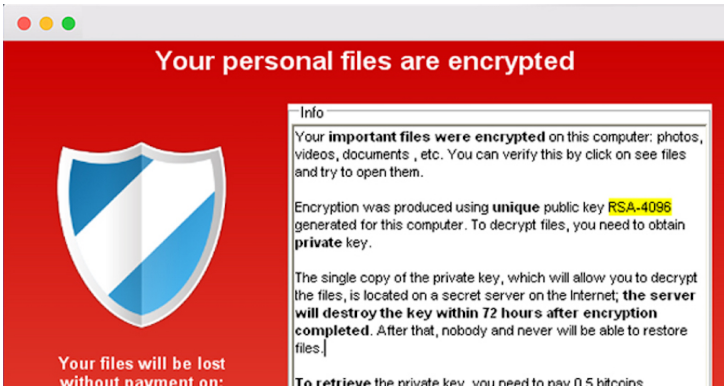
Cet article vous à plu ? Laissez-nous un commentaire (notre source d’encouragements et de progrès)

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



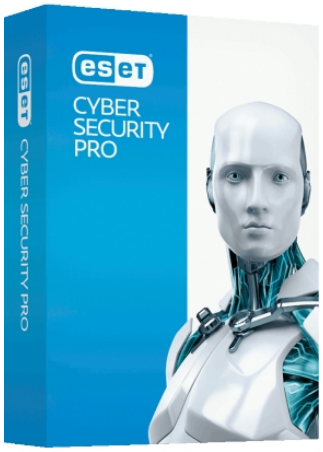
Protégez vos ordinateurs Mac contre les virus et les ransomwares

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 !

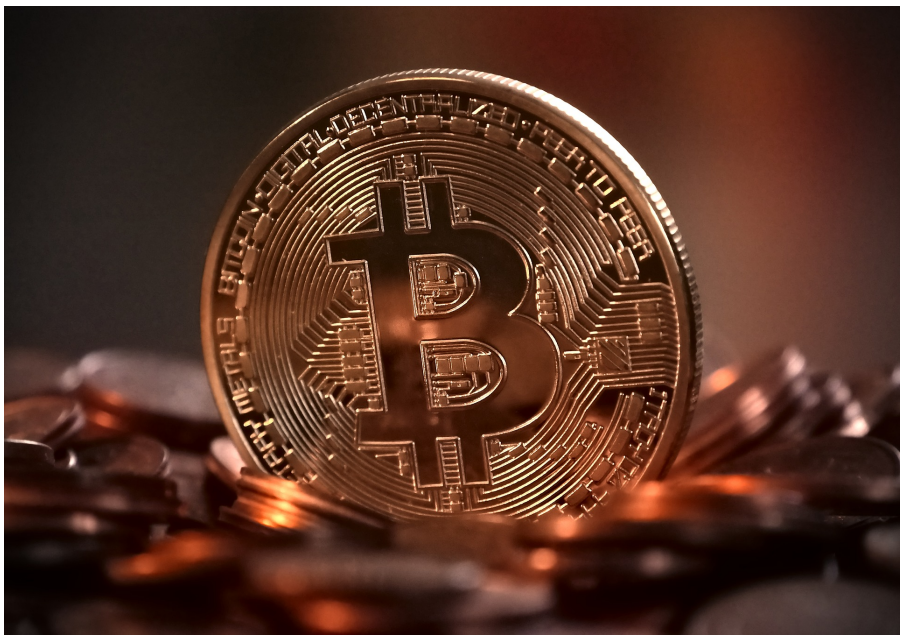
Pour protéger votre Mac des Virus, des ransomwares, veillez à avoir une bonne sauvegarde automatique, contrôlée, automatisée et historisée et aussi vous pouvez utiliser l'application de sécurité pour Mac :



Réagissez à cet article

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

Conseils pour bien se protéger des demandes de rançon informatiques / rançongiciels / ransomwares / cryptovirus ?



Conseils pour bien se protéger des demandes de rançon informatiques / rançongiciels / ransomwares / cryptovirus ?

Les rançongiciels (ransomware en anglais) sont une catégorie particulière de logiciels malveillants qui bloquent l'ordinateur des internautes et réclament le paiement d'une rançon pour en obtenir à nouveau l'accès.
Depuis 2013, une variante est apparue avec des virus chiffrants ou crypto-virus (cryptolocker, cryptoDefense, cryptorBit et plus récemment locky, petya ou WannaCry). Cette forme de rançongiciels chiffre les documents se trouvant sur l'ordinateur cible, voire sur des serveurs qui hébergent les données. Les cybercriminels communiquent parfois la clé de déchiffrement une fois le paiement de la rançon effectué, mais ce n'est jamais une garantie.
Cliquez ci-dessous pour en savoir plus:


CYBERMALVEILLANCE.GOUV.FR
VOUS ÊTES VICTIME D'UN RANÇONGICIEL ?

Victime d'un rançongiciels / ransomwares / cryptovirus ou d'une demandes de rançon informatiques ? Contactez-nous

---

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 ».

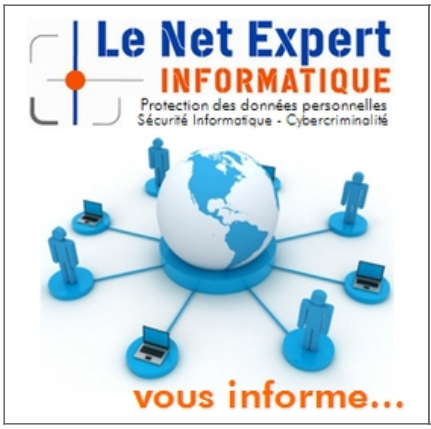
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation 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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Les rançongiciels ou ransomware – ANSSI – Plateforme Cyber Malveillance*

L’absence de formalité auprès de la CNIL, lorsqu’elle est obligatoire, peut constituer une infraction pénale | Denis JACOPINI



L’absence de formalité auprès de la CNIL, lorsqu’elle est obligatoire, peut constituer une infraction pénale

L’absence de formalité auprès de la CNIL, lorsqu’elle est obligatoire, peut constituer une infraction pénale.
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. 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.
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?name=D%C3%A9clarer%C2%A0%C3%A0+la+CNIL%2C+c%27est+obligatoire+%3F&id=335

Alerte Virus ! Rombertik détruit le PC lorsqu’il est détecté | Denis JACOPINI

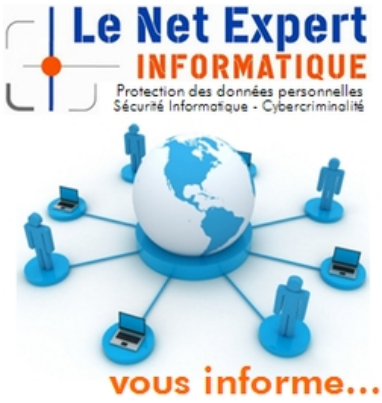
Alerte Virus ! Rombertik détruit le PC lorsqu’il est détecté

La menace a de quoi faire froid dans le dos. Les équipes de chercheurs de Talos (Cisco) viennent de repérer un nouveau type de malware capable de mettre à genoux un PC et les données qu'il contient. Rien de neuf, me direz-vous…

Mais Rombertik, c'est son petit nom, a été pensé pour contourner les protections mises en place, qu'elles soient système ou liées à un anti-virus. Pire, il devient particulièrement agressif lorsqu'il est chatouillé ou en phase d'être repéré.
Comme d'habitude, Rombertik se loge dans votre PC via un mail (spam ou phishing) contenant un lien piégé, souvent un faux PDF. Une fois exécuté, le malware fait le tour du propriétaire et s'assure de ne pas être enfermé dans une sandbox. Après s'être déployé, il est ensuite capable de s'insérer dans le navigateur utilisé pour collecter des données personnelles, même sur un site en https, et les expédier vers un serveur distant. Classique.
Dans le même temps, et c'est à ce moment qu'il est le plus dangereux, le malware vérifie qu'il n'est pas en cours d'analyse mémoire. Si c'est le cas, il va alors tenter de détruire le Master Boot Record (MBR), endommageant gravement le PC. Ce composant est essentiel pour démarrer une machine Windows.
S'il ne parvient pas à ses fins, il s'attaquera alors aux fichiers présents dans le dossier utilisateurs, fichiers qui seront alors cryptés avec une clé RC4 aléatoire. La machine est alors rebootée mais entre dans une boucle infinie. Bref, les dégâts sont majeurs. Et une analyse anti-virus aura les mêmes effets. la réinstallation du système est alors le seul moyen d'accéder à sa machine.
« Ce qui est intéressant avec ce malware, c'est qu'il n'a pas une fonction malveillante, mais plusieurs », souligne les experts de Talos. « Le résultat est un cauchemar », ajoutent-ils.
Comment alors se protéger ? « Etant donné que Rombertik est très sensible à la traditionnelle sandboxing réactive, il est crucial d'utiliser des systèmes de défense modernes – prédictifs. Des systèmes qui n'attendent pas qu'un utilisateur clique pour déclencher un téléchargement potentiel de Rombertik. », explique Charles Rami, responsable technique Proofpoint..
« De plus, comme le malware peut être expédié via de multiples vecteurs – comme Dyre, via des URL ou des fichiers .doc ou .zip/exe etc. – il est crucial d'utiliser des systèmes qui examinent l'ensemble chaîne destructrice, et bloquent l'accès des utilisateurs aux URL et pièces jointes envoyées par emails avant ceux-ci ne cliquent dessus. Enfin, les aspects « autodestruction » de Rombertik état susceptibles d'être déclenchés par les technologies telles que les antivirus, il est crucial que les entreprises utilisent des systèmes automatisés de réponse aux menaces – des systèmes qui peuvent localiser et bloquer l'exfiltration de données par Rombertik – sans – déclencher d'action sur le PC, et alerter les équipes de sécurité pour répondre rapidement aux dommages pouvant être causés », poursuit-il.

Source : http://www.zdnet.fr/actualites/rombertik-un-virus-qui-detruit-le-pc-lorsqu-il-est-detecte-39818978.htm

Utilisation des photos des élèves : faut-il l’accord des parents ? | Denis JACOPINI



Utilisation des photos des élèves : faut-il l’accord des parents ?

Toute personne dispose sur son image et sur l'utilisation qui en est faite d'un droit exclusif et peut s'opposer à sa reproduction et à sa diffusion.

Si un établissement scolaire veut utiliser les photographies de ses élèves dans le journal de l'école, sur un trombinoscope ou sur son site, il doit donc obligatoirement obtenir le consentement des parents ou représentants légaux des mineurs. Cet accord doit être écrit. De plus, le traitement informatique des photographies (numérisation, diffusion à partir d'un site web, etc.) doit être déclaré auprès de la CNIL, sauf si l'établissement a désigné un Correspondant Informatique et Libertés (CIL).

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. 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

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : http://www.aide.cnil.fr/selfcnil/site/template.do?id=272&back=true