

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.



[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 ?



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>

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 ;



Contactez-nous

ou suivez nous sur



Réagissez à cet article

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

?

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

 <p>Your personal files are encrypted</p> <p>Info</p> <p>Your important files were encrypted on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.</p> <p>Encryption was produced using unique public key RSA-4096 generated for this computer. To decrypt files, you need to obtain private key.</p> <p>The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; the server will destroy the key within 72 hours after encryption completed. After that, nobody and never will be able to restore files!</p> <p>To retrieve the private key you need to pay 0.5 bitcoin</p> <p>Your files will be lost without payment!</p>	<p>Protégez vos ordinateurs Mac contre les virus et les ransomwares</p>
--	---

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 chiffants 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:



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.



[Contactez-nous](#)

Réagissez à cet article

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.

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.zdnet.fr/actualites/rombertik-un-virus-qui-detruit-le-pc-lorsqu-il-est-detecte-39818978.htm>

Comment réagir lorsque vous êtes victime de harcèlement en ligne ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES <i>.fr</i></p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
 <p>Denis JACOPINI vous informe LCI</p>	<p>Comment réagir lorsque vous êtes victime de harcèlement en ligne ?</p>				

Selon un rapport européen, près de 10 % de la population européenne a subi ou subira un harcèlement*. Voici quelques conseils si vous êtes victime de ces violences sur internet et les médias sociaux.

Qui sont les cyber-harceleurs ?

Un(e) internaute peut être harcelé(e) pour son appartenance à une religion, sa couleur de peau, ses opinions politiques, son comportement, ses choix de vie – Le harceleur peut revêtir l'aspect d'un « troll » (inconnu, anonyme) mais également faire partie de l'entourage de la victime (simple connaissance, ex-conjoint, camarade de classe, collègue, voisin, famille ...).

A quoi ressemble une situation de cyber-harcèlement ?

- Happy slapping : lynchage en groupe puis publication de la vidéo sur un site
- Propagation de rumeurs par téléphone, sur internet.
- Création d'un groupe, d'une page ou d'un faux profil à l'encontre de la personne.
- Publication de photographies sexuellement explicites ou humiliante
- Messages menaçants, insulte via messagerie privée
- Commande de biens/services pour la victime en utilisant ses données personnelles

Comment réagir ?

Ne surtout pas répondre ni se venger

Vous avez la possibilité de bloquer l'accès de cette personne à vos publications, de la signaler auprès de la communauté ou d'alerter le réseau social sur un comportement qui contrevient à sa charte d'utilisation.

Verrouiller l'ensemble de vos comptes sociaux

Il est très important de limiter au maximum l'audience de vos comptes sociaux. Des options de confidentialité existent pour « ne plus me trouver », « ne pas afficher/partager ma liste d'amis ». Il est également possible de « bannir » les amis indésirables. Sur Facebook, une option vous permet d'être avertis si un autre utilisateur mentionne votre nom sur une photo (tag).

Les paramètres conseillés sur Facebook :

PARAMÉTRAGE POSSIBLE	CHEMIN D'ACCÈS
Limiter la visibilité de vos photos	Ce type d'option ne fonctionne que photo par photo
Limiter la visibilité de vos informations de profil	Informations générales : page du profil > encart gauche > sélectionner « amis » ou « moi uniquement »
Cacher votre liste d'amis	Page du profil > onglet « amis » > « gérer section » > « modifier la confidentialité » > « liste d'amis » ou « moi uniquement »
Cacher vos mentions « j'aime »	Page du profil > Mentions j'aime (encart gauche) > « modifier la confidentialité » > « moi uniquement »
Être prévenu si quelqu'un vous « tague »	Paramètre > journal et identification > Paramètres d'identification et de journal > « examiner les identifications »
Limiter la visibilité de vos publications	Journal > sélectionner la publication > « moi uniquement » / ou « supprimer »
Examiner votre historique	Page du profil > « afficher l'historique personnel » > supprimer au cas par cas

Ces preuves servent à justifier votre identité, l'identité de l'agresseur, la nature du cyber-harcèlement, la récurrence des messages, les éventuels complices. Sachez qu'il est possible de faire appel à un huissier pour réaliser ces captures. Fiche pratique : comment réaliser une copie d'écran ?

Portez plainte auprès de la Gendarmerie/Police si le harcèlement est très grave

Vous avez la possibilité de porter plainte auprès du commissariat de Police, de Gendarmerie ou du procureur du tribunal de grande instance le plus proche de votre domicile.

En parler auprès d'une personne de confiance

La violence des termes employés par l'escroc et le risque d'exposition de votre vie privée peuvent être vécus comme un traumatisme. Il est conseillé d'en parler avec une personne de confiance.

Si quelqu'un d'autre est harcelé ?

Le fait de « partager » implique votre responsabilité devant la loi. Ne faites jamais suivre de photos, de vidéos ou de messages insultants y compris pour dénoncer l'auteur du harcèlement. Un simple acte de signalement ou un rôle de conseil auprès de la victime est bien plus efficace ! Le chiffre : 61% des victimes indiquent qu'elles n'ont reçu aucun soutien quel qu'il soit de la part d'organismes ou d'une personne de leur réseau personnel. * Source: rapport européen sur le cyber-harcèlement (2013)

Si vous êtes victime et avez moins de 18 ans ...

Composez le 3020. Il est ouvert du lundi au vendredi de 9h à 18h (sauf les jours fériés). Le numéro vert est géré par la plateforme nonaharcelement.education.gouv.fr qui propose de nombreuses ressources pour les victimes, témoins, parents et professionnels (écoles, collèges, lycées). Si le harcèlement a lieu sur internet, vous pouvez également composer le 0800 200 000 ou vous rendre sur netecoute.fr. La plateforme propose une assistance gratuite, anonyme, confidentiel par courriel, téléphone, chat en ligne, Skype. Une fonction « être rappelé par un conseiller » est également disponible. La réponse en ligne est ouverte du lundi au vendredi de 9h à 19h. Un dépôt de plainte est envisagé ? Renseignez vous sur le dépôt de plainte d'un mineur. Celui-ci doit se faire en présence d'un ou de plusieurs parents ou d'un représentant légal. N'hésitez pas à contacter les télé-conseillers du fil santé jeune au 8000 235 236.

Quelles sanctions encourues par l'auteur de ces violences en ligne ?

L'auteur de tels actes est susceptible de voir sa responsabilité engagée sur le fondement du Droit civil, du Droit de la presse ou du Code pénal. Quelques exemples de sanctions :

- Une injure ou une diffamation publique peut être punie d'une amende de 12.000€ (art. 32 de la Loi du 29 juillet 1881).
- Pour le droit à l'image, la peine maximum encourue est d'un an de prison et de 45.000 € d'amende (art. 226-1, 226-2 du Code pénal).
- L'usurpation d'identité peut être punie d'un an d'emprisonnement et de 15.000€ d'amende (art. 226-4-1 du Code pénal).

Quels sont les recours auprès de la CNIL ?

La qualification et la sanction de telles infractions relève de la seule compétence des juridictions judiciaires. En parallèle de telles démarches, vous pouvez demander la suppression de ces informations à chaque site ou réseau social d'origine, en faisant valoir votre droit d'opposition, pour des motifs légitimes, sur le fondement de l'article 38 de la loi du 6 janvier 1978 modifiée dite « Informatique et Liberté ». Le responsable du site dispose d'un délai légal de deux mois pour répondre à votre demande. La majorité des sites propose un bouton « signaler un abus ou un contenu gênant ». Si aucun lien n'est proposé, contactez directement par courriel ou par courrier le responsable du site en suivant la procédure expliquée sur notre site. Par ailleurs, si ces informations apparaissent dans les résultats de recherche à la saisie de vos prénom et nom, vous avez la possibilité d'effectuer une demande de déréférencement auprès de Google en remplissant le formulaire. En cas d'absence de réponse ou de refus, vous pourrez revenir vers la CNIL en joignant une copie de votre demande effectuée auprès du moteur de recherche incluant le numéro de requête Google. Pour plus d'informations, consultez la fiche. Source : CNIL

Régissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

- Les meilleurs conseils pour choisir vos mots de passe
- Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
- Victime d'usurpation d'identité sur facebook, twitter ? Portez plainte mais d'après quel article de loi ?
- Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à se mettre en conformité avec la réglementation numérique (dont le RGPD) et à se protéger des pirates informatiques.

Quel sont nos principales activités ?

- RGPD
- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)
- CYBERCRIMINALITÉ
- FORMATIONS / SENSIBILISATION D'UTILISATEURS
- RECHERCHE DE PREUVES
- EXPERTISES
- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RECUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en Cybercriminalité, Recherche de preuves et en Protection des données personnelles. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DORTEFP (Numéro formateur n°93 84 03941 84).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanents car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme. Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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

- Mise en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Expertise (et sensibilisation) à la Sécurité Informatique (normes ISO 27001 et ISO 27005) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves : Téléphones, disques durs, e-mails, contenus, détournements de données ;
- Expertise de systèmes de vote électronique ;



Contactez-nous

Les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données | Denis JACOPINI

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<p>Les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données</p>
---	---

Varonis a mené une enquête en mars auprès des informaticiens professionnels participant au CeBIT, le plus grand salon IT d'Allemagne, afin de recueillir leur opinion sur la nouvelle réglementation régissant la protection des données qui doit entrer en vigueur cette année ou l'année prochaine. Le constat est sans appel : les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données. Les professionnels interrogés par Varonis ne pensent pas que leurs entreprises soient en mesure de respecter les délais imposés par l'UE pour la notification des violations de données.

Il ressort de cette enquête que 80 % des personnes interrogées pensent qu'une banque sera très probablement la première entreprise à être frappée par l'amende maximale de 100 millions d'euros pour non-respect de la réglementation européenne sur la protection des données. À la question concernant le pays le plus probable de cette banque, les répondants indiquent l'Allemagne (30 %), les États-Unis (28 %) et 22 % mentionnent un autre pays européen. 48 % seulement des personnes interrogées pensent que leur entreprise pourrait signaler une violation dans le délai obligatoire de 72 heures. Seuls 31 % disposent d'un plan leur permettant de se conformer à la nouvelle législation et seulement un tiers des personnes enquêtées a mis en place les processus et la technologie nécessaires pour empêcher leur entreprise de se voir infliger une amende importante dans le cadre de cette loi. 71 % des répondants sont incapables de dire ce que les entreprises doivent faire pour se conformer à la nouvelle réglementation.

Seuls 22 % des répondants savaient que l'amende maximale prévue par la nouvelle législation est de 100 millions d'euros, 41 % pensaient qu'elle ne serait que de 10 millions d'euros et 32 % l'estimaient à 1 million d'euros, avec un nombre réduit de personnes interrogées croyant qu'elle pouvait s'élever à un milliard d'euros. Un tiers a déclaré que la réglementation européenne sur la protection des données entrera en vigueur en 2015, 28 % ont indiqué que tel serait le cas en 2016, 7 % estiment que la loi ne verra jamais le jour et 32 % des personnes interrogées ont dit ne pas savoir quand la loi entrerait en vigueur.

« Nous pouvons attendre une refonte majeure de la loi européenne sur la protection des données au cours des prochains 12 à 24 mois », déclare David Gibson, vice-président du marketing de Varonis. « Les amendes devraient s'élever à 2 % du revenu annuel avec un plafond de 100 millions d'euros ou de dollars pour la non-protection des données personnelles des citoyens européens. Il pourrait également y avoir un nombre important de plaintes individuelles en plus des amendes et les sommes mises en jeu pourraient donc représenter des coûts substantiels, même pour les grandes entreprises. La nouvelle loi marquera aussi le passage d'un environnement autoréglementé à un régime d'application obligatoire qui aura une incidence sur toute entreprise stockant des informations d'identification personnelle concernant les citoyens européens (y compris sur les sociétés américaines menant des activités dans l'UE). Les entreprises doivent être préparées à protéger les données de leurs clients et prouver qu'elles le font avec le soin approprié, rendre compte de toute violation et supprimer les données à la demande des citoyens de l'UE. »

« Compte tenu de la vaste portée de la nouvelle réglementation et de l'importance accrue des amendes, cette enquête révèle des inquiétudes très importantes quant aux efforts que les entreprises sont prêtes à fournir pour se conformer aux conditions de la réglementation et gérer les scénarios de violation de données », indique Mark Deem, partenaire de Cooley LLP au Royaume-Uni. « En fait, l'échelle des amendes potentielles sera plus proche de celles infligées pour corruption ou violation antitrust, ou dans le secteur des services financiers. La conformité en matière de protection des données sera tout aussi importante que la conformité aux réglementations de la FCA. Même si la législation n'entre pas en vigueur avant 2017, un travail considérable doit être accompli par ceux qui souhaitent offrir des biens et des services aux habitants de l'UE et s'assurer qu'ils se trouvent dans la meilleure situation possible pour respecter la loi. »

Varonis propose 7 conseils pour garantir la conformité des données non structurées et permettre aux entreprises de se préparer à la réglementation européenne sur la protection des données :

1. Minimiser la collecte des données : la proposition de loi de l'UE comporte de fortes exigences en ce qui concerne la limitation des données recueillies auprès des consommateurs.
2. Favoriser le signalement des violations de données : la notification des atteintes à la protection des données constitue une nouvelle exigence que les entreprises européennes devront respecter.
3. Conserver les données avec attention : les règles de minimisation de la nouvelle loi concernent non seulement l'étendue des données collectées, mais aussi leur durée de rétention. En d'autres termes, une entreprise ne doit pas stocker les données plus longtemps que nécessaire aux fins prévues.
4. Nouvelle définition des identifiants personnels : l'UE a étendu la définition des identifiants personnels et ce changement s'avère important parce que les lois de l'UE portent sur la protection de ces identifiants.
5. Employez un langage clair : il faudra à une entreprise le consentement préalable et explicite des consommateurs lors de la collecte des données.
6. Bouton d'effacement : le « droit d'effacement » signifie qu'en cas de retrait du consentement accordé par les consommateurs, les sociétés devront supprimer les données concernées.
7. Le Cloud computing n'échappe pas à cette nouvelle loi de l'UE, car celle-ci suit les données.

Méthodologie de l'enquête

Les 145 personnes interrogées constituent un échantillon représentatif des participants du plus grand salon informatique d'Allemagne qui a compté 221 000 visiteurs en mars 2015. Parmi les répondants, 16 % sont issus de banques allemandes, 3 % de banques américaines, 3 % de banques européennes, 45 % d'entreprises allemandes hors du secteur financier, 26 % d'entreprises européennes hors du secteur financier et 7 % d'entreprises américaines.

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 plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.infodsi.com/articles/157046/entreprises-sont-pas-pretres-nouvelle-legislation-europeenne-protection-donnees.html>

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

communications
JACOPINI

|

Denis

x	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-chiffrant-vos-donnees-et-communications-39818894.htm>
Par Pierre Col

Un outil gratuit pour analyser et nettoyer votre ordinateur



Un outil gratuit pour analyser et nettoyer votre ordinateur

Avec plus de 40.000 visiteurs uniques par an, ESET Online Scanner apparaît comme l'un des outils gratuits les plus plébiscités par les internautes soucieux de leur sécurité. Fort de ce constat, ESET améliore son scanner basé sur le moteur d'analyse ThreatSense® permettant d'analyser et nettoyer son ordinateur sans contrainte d'installation logicielle.

Conçue pour être conviviale, cette dernière version devient complètement indépendante des navigateurs Internet. De plus, l'installation est désormais possible sans les droits d'administrateur, ce qui rend l'analyse et le nettoyage des ordinateurs contenant des logiciels malveillants encore plus simples.

ESET Online Scanner améliore l'élimination des logiciels malveillants, par l'ajout de ces nouvelles fonctions :

- **Analyse des emplacements de démarrage automatique** et du secteur d'amorçage pour les menaces cachées – choix de cette option dans setup / cibles d'analyse avancées
 - **Nettoyage du registre système** – Supprime les traces des logiciels malveillants du registre système
 - **Nettoyage après analyse lors du redémarrage** – Si nécessaire, ESET Online Scanner est capable de repérer les malwares les plus persistants afin de les nettoyer après redémarrage
- Pour plus d'informations sur l'outil gratuit ESET Online Scanner, contactez-nous ou rendez-vous sur <http://www.eset.com/fr/home/products/online-scanner/>

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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Boîte de réception (10) – denis.jacopini@gmail.com – Gmail

Les conseils pour faire connaître son site Internet et les outils pour Webmasters | Denis JACOPINI



AUDIT DE CONTENU DE SITES INTERNET

Google Webmaster Tools

Google Webmaster Tools est un outil pertinent et facile d'utilisation pour les éditeurs qui cherchent à optimiser le référencement naturel de leurs pages web. De l'exploration des pages par les robots, à l'analyse des mots-clés, en passant par la qualité/quantité des liens retours et le positionnement des pages : il analyse de nombreux paramètres SEO décisifs pour améliorer la visibilité d'un site web sur Google.

Screaming Frog

Disponible pour Mac et PC, Screaming Frog audite un site, ses liens, images, CSS et scripts pour en ressortir des indicateurs utiles à l'indexation et au SEO. Au-delà des erreurs HTTP rencontrées lors du crawl, l'outil va également faire remonter les balises Title, H1 ou H2 manquantes, dupliquées ou trop longues. L'ancre des liens rencontrés est précisée, tout comme leur éventuel attribut *nofollow*.

Bing pour Webmasters

Certes, « Bing Webmaster » est plus intéressant pour des sites positionnés dans des pays où Bing a une part de marché significative, mais même en France, il a plusieurs intérêts. Puisqu'il peut par exemple auditer un site, ou retrouver des liens pointant vers n'importe quelle page.

MajesticSEO

MajesticSEO analyse des liens entrants de n'importe quel site web. Ses indicateurs maison, le score de citation (« Citation Flow ») et le score de crédibilité (« Trust Flow »), sont souvent cités par les SEO pour évaluer la qualité d'un site web et de ses liens sortants. Bâti sur des centaines de milliards d'URL crawlées, le service est régulièrement actualisé, et propose souvent de nouvelles fonctionnalités.

Open Site Explorer

Open Site Explorer ou OSE est un outil est bien connu pour ses analyses de backlinks et de l'autorité de leur origine. OSE peut être utilisé gratuitement, mais en version bridée. L'analyse complète, et certains indicateurs, comme ceux concernant les partages sociaux d'une page, sont cependant réservés à la version payante.

Moz

Certains outils de cette suite sont gratuits, comme la météo des pages de résultats de Google.com ou l'analyse des comptes Twitter. Mais les plus utiles (analyse de mot clé, crawl et audit de site, suivi de position...) nécessitent un abonnement, facturé à partir de 99 dollars par mois.

AUDIT DE TEST DE SITE INTERNET

WebPageTest – Mesure de vitesse d'ouverture des pages

FAIRE CONNAITRE SON SITE INTERNET SUR LES RESEAUX SOCIAUX

15/04/2014 26 idées pour obtenir plus d'abonnés Google+

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

Références :

28/02/2014

<http://www.journaldunet.com/solutions/seo-referencement/seo-les-meilleurs-outils/google-webmaster-tools.shtml>

27/02/2014

<http://ecommerce-live.net/event/nouvelle-strategie-de-referencement-en-2014-quand-le-virtuel-rencontre-le-reel-3/>

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