Les meilleurs reportages vidéo sur la Cybercriminalité – A voir et à revoir | Denis JACOPINI

	Les meilleurs reportages vidéo sur la #Cybercriminalité – A voir et à revoir

Que ça soit sur la télévision ou déposé sur Internet sans passer par le petit écran, de nombreux reportages sont chargés de vous informer, avertir, sensibiliser.Ci-dessous, quelques reportages sélectionnés.Vous en connaissez d'autres ? N'hésitez pas à nous envoyer les liens pour les partager avec nos lecteurs ou les glisser dans les commentaires.

Envoyé spécial. Cyberattaques : les braqueurs de l'ombre – 14 décembre 2017 (France 2)
Les hold-up 2.0 par des « rançongiciels », logiciels de rançon, se multiplient : en France, une entreprise sur deux aurait déjà été piratée de cette façon. Enquête du magazine « Envoyé spécial » sur un fléau invisible en pleine explosion. Vous êtes tranquillement installé derrière votre ordinateur, vous ouvrez un mail anodin… et soudain, un message d'alerte apparaît : votre ordinateur est bloqué, tous vos documents sont cryptés, vous devez payer une rançon pour en retrouver l'usage. Vous venez de vous faire braquer par un « rançongiciel », ces programmes informatiques qui diffusent des virus et qui vous réclament de l'argent : 150 euros pour un particulier, 6 000 euros pour une PME, des millions d'euros pour une multinationale. Et vous n'avez que quelques heures pour payer, sinon vous perdez tout ! Une enquête de Clément Le Goff et Guillaume Beaufils.

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 Milions de victimes de la Cybercirminalité 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

M6 – Zone Interdite : Vie privée en danger
Est-il possible de rentrer chez nous, d'écouter nos conversations et de s'immiscer dans notre intimité sans y être invité ? Nous avons découvert qu'il suffit pour cela d'une simple connexion Internet. Ordinateur, téléphone portable, réseaux sociaux et même cartes bancaires : désormais nous sommes en permanence connectés les uns aux autres. Mais nos informations personnelles sont-elles réellement bien protégées ? Pas si sûr…

France 2 – Envoyé Spécial : Toute ma vie sur internet
La collecte d'informations personnelles – âge, sexe, centres d'intérêts – par les sites de réseaux sociaux est désormais connue et relativement acceptée par les utilisateurs. Le dernier exemple en date vient de Facebook, qui a annoncé, mercredi 26 novembre, une révision de ses conditions d'utilisation. Jugeant que ses 1,32 milliard de membres y consentiront aisément, le réseau social entend récolter ainsi encore plus de données personnelles qu'aujourd'hui, notamment des informations bancaires.

Réagissez à cet article

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

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 Milions 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

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

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

M6 – En quête d'actualité – Facebook,Twitter les réseaux : sociaux sont ils vraiment nos amis
Les réseaux sociaux sont en train de conquérir la planète entière. Après Facebook, d'autres sont apparus comme Twitter, Pinterest ou Foursquare. Quelles méthodes utilisent-ils pour faire de l'argent avec des données personnelles ? Raconter sa vie privée à tout le monde, est-ce sans danger ?

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :
Les 10 conseils pour ne pas se faire «hacker» pendant l'été
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, tweeter ? 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
- RÉCUPÉRATION 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 DDRTEFP (Numéro formateur n°93 84 03041 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 permanentes 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

Contactez-nous

France 2 – Envoyé Spécial : le côté obscur du Net Darknet
Plongée au coeur du Darknet, ce réseau internet caché où la seule règle est l'anonymat. Repaire pour les trafiquants d'armes ou de drogue, le Darknet est aussi un moyen d'échapper à la surveillance des dictatures.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.
« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

Quelques articles sélectionnés par nos Experts :
Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

France 2 – Envoyé Spécial : Les Objets Connectés à Internet WiFi / 4G
Les Objets Connectes WiFi / 4G / H+ / 3G, quels sont les conséquences aujourd'hui et ses prochaines années ?

Arte – Thema : Hackers, les nouveaux maîtres du monde
D'un côté, il y a les black hats (chapeaux noirs), les délinquants virtuels mus par l'appât du gain ; de l'autre, les white hats (chapeaux blancs) ou pirates .
Ici vous trouverez des documentaires sur l'histoire de l'informatique, du hacking et des jeux vidéo.

Réagissez à cet article

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

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 Milions 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

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

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

France 2 – Envoyé Spécial : Darknet, le côté obscur du Net
Au quotidien, avec les moteurs de recherche classique, vous n'avez accès qu'à une petite partie d'Internet. Il existe un internet parallèle, sans limites ni protection. Sur Darknet on trouve un supermarché de la drogue, des sites de cartes bleues volées, des sites pédopornographiques et même… des annonces de tueurs à gages.
Documentaire de Thomas LELONG, Marion CANTOR, Guillaume MAURICE, Antonin MARCEL, Jennifer ROLNIN et Lorraine De FOUCHER
Première diffusion le jeudi 29 novembre 2013

Arte – Théma : La Guerre invisible
Documentaire de Antoine Vitkine
Première diffusion le mercredi 03 octobre 2012

France 2 – Envoyé Spécial – Les cybercriminels
Reportage complet sur la cybercriminalité les hacker, les anonymous, le vols de carte bleu de compte d ejeux. les enjeu des hacker les risque qu'il encours toute les réponse a vos question.
Documentaire de Anne Richard, Jérôme Pavlovsky et Stéphane Rossi
Première diffusion le jeudi 7 mai 2009.

Réagissez à cet article

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

---

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 Milions de victimes de la Cybercirminalité 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

---

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

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

Vote électronique – Mode d'emploi | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	**Vote électronique – Mode d'emploi**				

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.

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. Pour éclairer les responsables de traitement, les fournisseurs de solution de vote et les experts sur les sécurités que la CNIL estime indispensables, une recommandation a été adoptée en 2003 et mise à jour en 2010.

Pour être valide, un système de vote électronique doit strictement respecter les obligations légales applicables aux systèmes de vote électronique, énoncées notamment dans le décret n° 2007-602 et l'arrêté correspondant du 25 avril 2007 relatifs aux conditions et aux modalités de vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise, et dans le décret n° 2011-595 du 26 mai 2011 relatif aux conditions et modalités de mise en œuvre du vote électronique par internet pour l'élection des représentants du personnel au sein des instances de représentation du personnel de la fonction publique de l'Etat.

Le système de vote électronique doit également respecter 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 qui précise notamment :

• Tout système de vote électronique doit faire l'objet d'une expertise indépendante.

• 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.).

• 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.

Réagissez à cet article

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :

• Expert en Informatique **assermenté et indépendant** ;

• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;

• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;

• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des 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

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

Devis pour la mise en conformité avec le RGPD de votre établissement

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

Devis pour la mise en conformité avec le RGPD de votre établissement

Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Vous souhaitez faire appel à un expert informatique qui vous accompagne dans la mise en conformité avec le RGPD de votre établissement ?

Je me présente : Denis JACOPINI. Je suis Expert en informatique assermenté et **spécialisé en RGPD (protection des Données à Caractère Personnel) et en cybercriminalité**. Consultant depuis 1996 et formateur depuis 1998, j'ai une expérience depuis 2012 dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données (DPO n°15845), en tant que praticien de la mise en conformité et formateur, je vous accompagne dans toutes vos démarches de mise en conformité avec le RGPD20.

« Mon objectif est de mettre à disposition toute mon expérience pour mettre en conformité votre établissement avec le RGPD. »

Pour cela, j'ai créé des services sur mesure :

Vous souhaitez vous mettre en conformité avec le Règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 (dit RGPD) et vous souhaitez vous faire accompagner. Au fil des années et depuis les mises en conformité avec la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nous avons constaté que les mises en conformité devaient se dérouler (et encore à ce jour avec le RGPD) selon 3 phases principales :

1. « Analyse du contexte » en vue d'établir la liste des traitements et les mesures correctives à adopter ;
2. « Mise en place de la conformité RGPD » avec amélioration des traitements en vue de les rendre acceptables ou conformes. Ceci inclue dans bien des cas l'analyse de risque ;
3. « Suivi de l'évolution des traitements » en fonction de l'évolution du contexte juridique relatif à la protection des Données à Caractère Personnel et des risques Cyber. Ce suivi a pour principal intérêt de maintenir votre conformité avec le RGPD dans le temps.

Pour chacune des phases, nous vous laissons une totale liberté et vous choisissez si vous souhaitez :

• « Apprendre à faire » (nous vous apprenons pour une totale autonomie) ;
• « Faire » (nous vous apprenons et vous poursuivez le maintien de la mise en conformité tout en ayant la sécurité de nous avoir à vos cotés si vous en exprimez le besoin) ;
• ou « Nous laisser faire » (nous réalisons les démarches de mise en conformité de votre établissement en totale autonomie et vous établissons régulièrement un rapport des actions réalisées opposable à un contrôle de la CNIL).

contactez-nous avec le formulaire ci-dessous

Pour ceux qui veulent apprendre à faire, nous proposons 3 niveaux de formation

1. Une formation d'une journée pour vous sensibiliser au RGPD : « **Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer** » ;
2. Une formation de deux jours pour les futurs ou actuels DPO : « **Je veux devenir le Délégué à la Protection des Données de mon établissement** » ;
3. Une formation sur 4 jours pour les structures qui veulent apprendre à mettre en conformité leurs clients : « **J'accompagne mes clients dans leur mise en conformité avec le RGPD** ».

Afin de vous communiquer une indication du coût d'un tel accompagnement, nous aurons besoin d'éléments sur votre structure : Durée dépendant de la taille, de l'activité et des ressources de votre établissement.

Cliquez ici pour accéder à notre formulaire de demande d'informations

Source : Denis JACOPINI

Comment détecter e-mail malveillant

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

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

	Comment détecter e-mail malveillant

Via votre messagerie ou votre boîte mail, certaines personnes malintentionnées tentent de mettre la main sur vos données personnelles en utilisant des techniques d'hameçonnage (phishing) ou d'escroquerie de type fraude 419 (scam) ! Ces techniques d'attaque évoluent constamment. Les conseils suivants vous aideront à déterminer si un message est légitime ou non.

Comment repérer une arnaque reçue dans votre messagerie ou votre boîte mail ?

• **Est-ce que le message/courriel vous est réellement destiné ?**
1. Généralement, les messages malveillants sont envoyés à destination d'un grand nombre de cibles, ils ne sont pas ou peu personnalisés.
2. Le message évoque un dossier, une facture, un thème qui ne vous parle pas ? Il s'agit certainement d'un courriel malveillant.
• **Attention aux expéditeurs inconnus** : soyez particulièrement vigilants sur les courriels provenant d'une adresse électronique que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact.
• **Soyez attentif au niveau de langage du courriel** : même si cela s'avère de moins en moins vrai, certains courriels malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées, c'est qu'il n'est pas l'œuvre d'un organisme crédible (banque, administration …).
• **Vérifiez les liens dans le courriel** : avant de cliquer sur les éventuels liens, laissez votre souris dessus*. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime. Ne faites pas confiance aux noms de domaine du type impots.gouvv.fr, impots.gouvfr.biz, infocaf.org au lieu de www.caf.fr.* *A noter : cette manipulation est impossible à effectuer depuis un écran de smartphone.*
• **Méfiez vous des demandes étranges** : posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n'a le droit de vous demander votre code carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.
• **L'adresse de messagerie source n'est pas un critère fiable** : une adresse de messagerie provenant d'un ami, de votre entreprise, d'un collaborateur peut facilement être usurpée. Seule une investigation poussée permet de confirmer ou non la source d'un courrier électronique. Si ce message semble provenir d'un ami – par exemple pour récupérer l'accès à son compte – contactez-le sur un autre canal pour vous assurer qu'il s'agit bien de lui !

Comment réagir ?

Si vous avez un doute sur un message reçu, il y a de fortes chances que celui-ci ne soit pas légitime :
• N'ouvrez surtout pas les pièces jointes et ne répondez-pas;
• Si l'escroquerie que vous souhaitez signaler vous est parvenue par un spam (pourriel), rendez-vous sur www.signal-spam.fr;
• Supprimez le message puis videz la corbeille;
• S'il s'agit de votre compte de messagerie professionnel : transférez-le au service informatique et au responsable de la sécurité des systèmes d'information de votre entreprise pour vérification. Attendez leur réponse avant de supprimer le courrier électronique.

Comment s'en prémunir ?

• Utilisez un logiciel de filtre anti-pourriel ou activer l'option d'avertissement contre le filoutage présent sur la plupart des navigateurs.
• Installez un anti-virus et mettez-le à jour.
• Désactivez le volet de prévisualisation des messages.
• Lisez vos messages en mode de texte brut.

Si vous êtes victime d'une escroquerie en ligne ?

Signalez les escroqueries auprès du site www.internet-signalement.gouv.fr, la plateforme d'harmonisation, d'analyse de recoupement et d'orientation des signalements. **Pour s'informer sur les escroqueries** ou pour signaler un site internet ou un courriel d'escroqueries, un vol de coordonnées bancaires ou une tentative d'hameçonnage : contacter Info Escroqueries au 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile) – Du lundi au vendredi de 9h à 18h

Rendez-vous sur cybermalveillance.gouv.fr , la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance. Que vous soyez un particulier, une entreprise ou une administration, retrouvez :
• des conseils / vidéos pour sensibiliser votre entourage professionnel ou personnel,
• des services de proximité en cas de dommages causés par une attaque informatique.
…[lire la suite]

Réagissez à cet article

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

---

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 Milions de victimes de la

Cybercirminalité 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

---

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

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

Source : *Phishing : détecter un message malveillant | CNIL*

Comment bien sécuriser ses e-mails ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Comment bien sécuriser ses e-mails ?				

Peut-on encore se passer de l'e mail dans le cadre de nos activités professionnelles ? Je ne le crois pas. Il est pratique et instantané. Cependant, peu sécurisé en standard, sans précautions, il pourrait bien vous attirer des ennuis.

Selon une étude récente de SilverSky, Email Security Habits Survey Report, 53 % des employés ont déjà reçu des données sensibles d'entreprise non cryptées par e mail ou en pièces jointes, que 21 % des employés déclarent envoyer des données sensibles sans les chiffrer et que 22 % des entreprises sont concernées chaque année par la #perte de données via e-mail.

Inquiétant vous direz-vous ? Catastrophique quand on sait que tout détenteur de données à caractère personnel est tenu à la sécurisation de ces données, conformément à la loi informatique et libertés, encadrée par la CNIL.
Et c'est encore pire quand on prend en compte les informations soumises au secret professionnel ou revêtues de confidentialité que nous échangeons quotidiennement… (plus de 100 milliards d'e-mails sont échangées chaque jour…)
Un des derniers incidents en date : la récente #divulgation des numéros de passeport de 31 leaders mondiaux…
Malgré l'évolution du contexte législatif il est bien étonnant que les entreprises ne soient pas plus nombreuses à choisir de sécuriser leurs échanges par e-mail.

Des solutions ?
Oui, heureusement, et je vais partager avec vous mes conseils :
Mettez en place des procédés de signature numérique et le chiffrement des e-mails garantissent la confidentialité d'un message.
Vous éviterez ainsi que des données sensibles ne tombent dans de mauvaises mains.
Avantage pour le destinataire : l'assurance de l'identité réelle de l'expéditeur de l'e-mail et que le contenu du message n'a pas été modifié après son envoi.
L'utilisation simultanée de ces procédés vous permettront ainsi de répondre à un besoin de Confidentialité (par le chiffrement) et un besoin d'Intégrité (par la signature électronique).

Enfin, aucun de ces deux procédés vous assurera une protection contre la fuite d'informations ou de données confidentielles à votre insu. POur cela, nous vous recommandons d'utiliser des système de « Protection contre la fuite des données » ou de « Data Leak Protection ».*

Plus d'info sur la confidentialité des e-mails ici

Réagissez à cet article

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

---

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 Milions de victimes de la Cybercirminalité 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

---

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

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

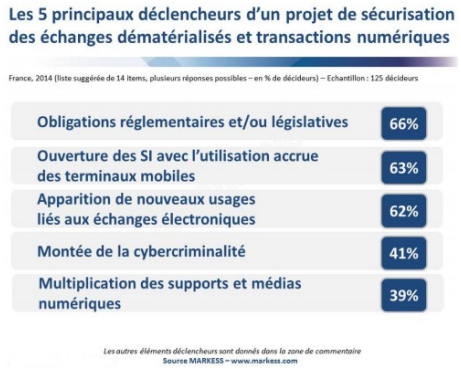
Sécuriser les échanges dématérialisés et les transactions numériques est crucial pour les entreprises | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	**Sécuriser les échanges dématérialisés et les #transactions numériques est crucial pour les entreprises**				

Des dizaines de milliers de dossiers RH de fonctionnaires américains (dont certains habilités au secret défense) piratés, tout autant de documents confidentiels volés à Sony Pictures, 7 millions d'identifiants Dropbox volés et publiés en ligne, 56 millions de cartes de paiement compromises lors d'une intrusion dans le système de paiement de l'américain Home Depot, 83 millions de clients de la banque JB Morgan Chase & Co dont les données personnelles ont été piratées…, de tels chiffres sont régulièrement rapportés par les médias et renforcent clairement les besoins en sécurisation des données. Aussi, il n'est pas surprenant que 85% des décideurs interviewés par Markess fin 2014 estiment avoir de forts, voire de très forts, besoins dans ce domaine.

La société d'études indépendante spécialisée dans l'analyse des marchés du numérique et des stratégies de modernisation des entreprises et administrations, annonce la parution de sa nouvelle étude intitulée : "Solutions de confiance pour sécuriser les échanges dématérialisés et les transactions numériques" et co-sponsonsorisée par ChamberSign France, Oodrive et OpenTrust. Conduite auprès de 125 décideurs d'entreprises privées et d'administrations, elle appréhende les nouveaux risques associés à l'introduction du numérique dans les échanges et les transactions avec les employés, les clients et les partenaires, les meilleures approches pour les contrer ainsi que les solutions mises en place en regard.

Sécuriser les échanges dématérialisés et les transactions numériques en réponse à d'autres facteurs que la cybercriminalité
Rapport Lemoine(1) sur la transformation numérique, actions du G29(2) en faveur de la protection des données, règlement eIDAS(3) visant à développer les échanges numériques au niveau européen…, les initiatives sont nombreuses afin d'instaurer le climat de confiance indispensable à la mutation des organisations vers le numérique et à l'essor d'usages innovants associés. La montée de la cybercriminalité n'apparaît qu'en 4ème position des éléments déclenchant un projet de sécurisation des échanges dématérialisés et des transactions numériques. Les contraintes imposées par la loi ou des réglementations quant à la dématérialisation de certains documents ou au recours au numérique pour le traitement de nombreux processus, ainsi que l'utilisation des terminaux mobiles de type smartphone ou tablette pour accéder aux applications métiers de l'entreprise arrivent en tête de ces déclencheurs fin 2014.



De nouveaux usages avec le numérique… entraînant de nouveaux risques
L'innovation constante dans le domaine du numérique favorise également le développement de nouveaux usages adressant aussi bien le grand public que la sphère professionnelle (partenaires commerciaux, clients BtoB, fournisseurs, employés ou agents…). Ces nouveaux usages numériques déclenchent en parallèle la mise en oeuvre de projets visant à sécuriser les échanges et les transactions qu'ils génèrent.
Pour 62% des décideurs interrogés, l'apparition de nouveaux usages est un déclencheur de tels projets dans les entreprises. "La contractualisation en ligne, la dataroom virtuelle, les services en ligne pour les citoyens, le vote électronique, la saisie et la transmission d'un constat d'accident depuis un smartphone, le paiement par téléphone mobile… sont autant d'usages innovants qui répondent à de réelles attentes mais qui aussi accroissent les risques" selon Hélène Mouiche, Analyste senior auteur de cette étude chez Markess. "Or, parmi les organisations interrogées, nombre d'entre elles ne sont pas prêtes aujourd'hui à y faire face. Demain, avec le développement des objets connectés, c'est la porte ouverte à de nouveaux risques difficiles à évaluer !".
Pour autant, la grande majorité des décideurs interviewés, et particulièrement les décideurs métiers, ont pleinement conscience que ces risques existent : près d'un décideur sur deux indique ainsi que son organisation aurait déjà évalué les risques encourus avec l'introduction du numérique dans les échanges et les transactions.

Des besoins autour de la protection des données et de la gestion de l'identité numérique
Les risques encourus sont variés (perte de données confidentielles, atteinte à l'image et à la réputation de l'entreprise, perte de confiance des clients, non respect de la vie privée, perte de la valeur authentique des documents…). Ils peuvent très rapidement entraîner des conséquences désastreuses tant pour les entreprises que pour leurs partenaires impliqués dans les échanges électroniques.
Aussi, les décideurs interrogés cherchent à se prémunir en mettant en oeuvre des solutions de :
• protection et sécurisation des données :
si les données personnelles sont très souvent au coeur des enjeux de confiance, quel que soit le profil des organisations, la sécurisation de nombreux autres contenus et documents numériques – contrats, factures électroniques, commandes, bulletins de paie, pièces de marchés publics, données de santé, demandes de citoyens…, est également jugée cruciale.
• gestion des identités numériques tant au niveau des personnes que des objets connectés.
Alors que plus de 50% des décideurs interviewés mentionnent que leur organisation a déjà investi, à fin 2014, dans des solutions d'authentification par mot de passe, de certificat de signature électronique et de certificat SSL, les projets d'investissement d'ici 2016 devraient porter sur d'autres typologies de solutions plus en phase avec les évolutions en cours : coffre-fort numérique, authentification forte par téléphone mobile, gestion des identités et des accès (IAM – Identity and Access Management), chiffrement (ou cryptage) et transfert sécurisé de documents. L'étude de Markess passe en revue le recours et les projets des organisations concernant près de 20 types de solutions couvrant tout ou partie de la chaîne de la confiance numérique afin de d'identifier, accéder, authentifier, prouver, protéger et échanger les documents et contenus numériques et ainsi aider les organisations à bâtir le socle de confiance indispensable à leur transformation numérique.

(1) "La nouvelle grammaire du succès – La transformation numérique de l'économie française" – Novembre 2014
(2) Groupe des autorités européennes de protection des données dont fait partie la CNIL
(3) electronic Identification And trust Services : règlement européen, adopté le 23 juillet 2014 par le Conseil de l'UE.

Le lien pour télécharger en ligne la synthèse de l'étude : http://bit.ly/markessREF_CONFNUM14

Réagissez à cet article

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

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
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, tweeter ? 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
  - RÉCUPÉRATION 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 DDRTEFP (Numéro formateur n°93 84 03041 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 permanentes 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

Source : http://www.infodsi.com/articles/152936/securiser-echanges-dematerialises-transactions-numeriques-est-crucial-

Ce qu’il faut savoir avant de se connecter sur du WiFi public | Denis JACOPINI

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

Ce qu’il faut savoir avant de se connecter sur du WiFi public

Aéroports, hôtels, cafés… Le WiFi public est très utilisé, mais pas sans risque. 30 % des managers ont fait les frais d'un acte cybercriminel lors d'un voyage à l'étranger, selon Kaspersky Lab.
Spécialiste des solutions de sécurité informatique, Kaspersky Lab publie les résultats d'une enquête réalisée par l'agence Toluna auprès de 11 850 salariés, cadres et dirigeants dans 23 pays, sur leur utilisation de terminaux et Internet à l'étranger. Tous ont voyagé à l'international l'an dernier, à titre professionnel ou personnel. Premier constat : 82 % ont utilisé des services WiFi gratuits, mais non sécurisés (aucune authentification n'étant nécessaire pour établir une connexion réseau), depuis un aéroport, un hôtel, un café… Or, 18 % des répondants, et 30 % des managers, ont fait les frais d'un acte cybercriminel (malware, vol de données, usurpation d'identité…) lorsqu'ils étaient à l'étranger.
Droit ou devoir de déconnexion ?
« Les businessmen assument que leurs terminaux professionnels sont plus sûrs du fait de la sécurité intégrée », a souligné l'équipe de Kaspersky Lab dans un billet de blog. Et si cela n'est pas le cas, ils considèrent que ce n'est pas leur problème. Ainsi « un répondant sur quatre (et plus de la moitié des managers) pense qu'il est de la responsabilité de l'organisation, plutôt que de celle de la personne, de protéger les données. En effet, à leurs yeux, si les employeurs envoient du personnel à l'étranger, ils doivent accepter tous les risques de sécurité qui vont avec ».
Si des données sont perdues ou volées durant leur voyage, la plupart des managers seraient prêts à blâmer leur département informatique. Et ce pour ne pas avoir recommandé l'utilisation de moyens de protection comme un réseau privé virtuel (VPN), des connexions SSL ou encore la désactivation du partage de fichiers lors d'une connexion WiFi… Quant au droit à la déconnexion, lorsqu'il existe, il se pratique peu. Pour 59 % des dirigeants et 45 % des managers « intermédiaires », il y une attente de connexion quasi continue de la part de leur employeur.
Article original de Ariane Beky

Réagissez à cet article

Original de l’article mis en page : Les voyageurs daffaires ignorent les risques du WiFi public

---

Bases essentielles pour sécuriser son site web | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Bases essentielles pour sécuriser son site web				

Il faut savoir qu'internet peut se révéler vulnérable. La sécurité d'un site n'est pas à prendre à la légère, c'est quelque chose de très compliqué qui requiert des connaissances techniques approfondies afin de pouvoir identifier les vulnérabilités et mettre en place les mesures de protection nécessaires.

La sécurité d'un site web est un enjeu crucial et essentiel pour tout administrateur système soucieux de préserver et protéger son site. Les hackers sont toujours à la recherche de nouvelles failles, mais de multiples solutions de sécurité s'offrent à vous de plus simples et de plus pointues qui vous permettront de lutter contre les pirates et les hackers et protéger son site internet.

Voici quelques simples conseils sous forme d'une liste de bonnes pratiques qu'un professionnel doit appliquer à la rigueur pour se défendre des attaques automatiques et **empêcher ceux qui visent votre site web d'y pénétrer** :

1. Veiller sur la mise à jour de votre site web

Il faut d'abord veiller à mettre à jour correctement le serveur web qui héberge le site. Si vous faites appel à un hébergeur professionnel, c'est son travail. Par contre, si vous héberger votre site vous-même c'est à vous de faire les mises à jour nécessaires. Ensuite, le système de gestion du site doit également être à jour, ainsi que toutes les applications qui jouent un rôle dans l'administration du site.

Certains systèmes de gestion de contenu comme WordPress permettent d'effectuer facilement les mises à jour automatiquement. Comme ils offrent aussi une quantité très importante de plugins dont certains peuvent présenter des failles flagrantes. Je vous conseille alors de **bien vous renseigner sur la qualité et l'efficacité d'un plugin avant de l'installer**.

2. S'assurer du sauvegarde et de la protection

N'oubliez jamais d'effectuer une sauvegarde régulière pour votre site web et aussi que pour toutes les autres informations. Sa fréquence dépendra de la fréquence de la mise à jour du site, c'est-à-dire que **vous devrez faire une sauvegarde de votre site à chaque fois que vous le mettez à jour**. Vous vous rendrez compte de la grande valeur de cette sauvegarde le jour où votre site sera piraté malgré les précautions que vous avez prises.

Enfin, vous devez protéger l'accès au serveur web pour éviter les tentatives d'attaque du site. Par exemple, l'authentification http et l'une des pratiques sur laquelle vous pouvez compter pour protéger votre serveur web.

3. Protéger les données sensibles

Lorsque vous collectez des données personnels, mots de passe, données financières, il faut veiller sur leur sécurité mieux que tout le reste. Il s'agit non seulement d'une obligation vis-à-vis de vos utilisateurs mais aussi d'une contrainte légale.

Il est indispensable que vous **chiffriez toutes les données stockées sur vos serveurs**. Il faut aussi chiffrer la connexion (SSL) pour éviter que des données soient interceptées lors de le communication entre l'utilisateur et votre site.

Vous devez faire des mots de passe l'objet d'un soin tout particulier pour assurer plus de sécurité, pour cela ils doivent être encryptés avant d'être stockés.

Comme vous devez aussi « hacher » les mots de passe avec un algorithme approprié comme «**bcrypt** » ou « **scrypt** » qui sont difficiles à être attaqués, et évitez les usuels MD5 et SHA1 qui sont plus vulnérables.

4. Vérifier la sécurité de votre hébergeur

C'est une astuce de sécurité d'ordre plus général, il est très important que votre hébergeur vous propose des versions plus récentes de Apache, MySQL et PHP. Renseignez-vous auprès de votre hébergeur ou utiliser un fichier PHP pour obtenir ces informations cruciales.

5. Créer votre site web avec Wix

Vous pouvez choisir des outils qui vont sécuriser votre site à votre place.

Pour ceux qui veulent se simplifier la vie et choisir une solution aussi sécurisé que pratique, il existe **Wix**. Lire la suite…

Réagissez à cet article

Original de l’article mis en page : Bases essentielles pour sécuriser son site web | FunInformatique

---

Qu’est ce qu’un bon mot de passe ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	**Qu’est ce qu’un #bon mot de passe ?**				

Un mot de passe efficace =

1. Plus de 8 caractères
2. sans lien avec son détenteur
3. MAJUSCULES
4. ponctuation
5. chiffres
6. unique pour chaque site (si possible)

Au travers de conférences ou de formations, Denis JACOPINI vous propose de vous sensibiliser, responsable de la stratégie de l'entreprise qui DOIT désormais intégrer le risque informatique comme un fléau à combattre et à enrayer plutôt qu'une fatalité.
Contactez-nous

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

Source : https://twitter.com/cnil/status/545603180487131136

6 conseils pour éviter la contamination du réseau par des ransomwares | Denis JACOPINI

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

6 conseils pour #éviter la contamination du réseau par des ransomwares

6 conseils pour éviter la contamination du réseau par des ransomwares Une étude réalisée par Bitdefender aux États-Unis montre que les APT (Advanced Persistent Threats), le spear phishing et les ransomware sont les types d'incidents les plus craints dans les entreprises.

Cette étude montre, en effet, qu'en termes d'importance, les APT (techniques complexes d'intrusion réseau) sont en tête des préoccupations : 19,7% des managers interrogés les estiment difficiles à gérer.
Les ransomware arrivent en seconde position (13,7%) avec les rootkits. Ces derniers préoccupent plus les DSI que les menaces 0-day.
Le Spear Phishing (des e-mails soigneusement préparés, destinés à des individus spécifiques au sein de l'entreprise) sont mentionnées par à peu près 13% des personnes interrogées. Reste qu'il s'agit là d'une des techniques les plus utilisées pour pénétrer la sécurité de l'entreprise et diffuser des malwares.
Quant aux incidents générés par le BYOD (Bring Your Own Device, l'utilisation de son appareil personnel dans le cadre du travail) et aux vulnérabilités zero-day, ils semblent moins inquiétants, puisque 11,3% des personnes interrogées voient le BYOD comme un risque potentiel pour leur entreprise, tandis que 10,3% des managers pensent que les attaques zero-day sont sources de menaces pour la sécurité de leur entreprise.
BitDefender fait donc 6 recommandations pour que les entreprises puissent limiter les risques d'infection :
1. Mettre en garde les employés contre les nouvelles menaces et leur expliquer comment déceler un e-mail de spear phishing et d'autres attaques d'ingénierie sociale.
2. Installer, configurer et maintenir à jour la solution de sécurité de l'entreprise.
3. Bloquer l'exécution de certains programmes vecteurs d'infections, comme par exemple des logiciels de téléchargement illégal ou de P2P au bureau.
4. Utiliser un pare-feu pour bloquer les connections entrantes vers des services qui n'ont pas lieu d'être publiquement accessibles via Internet.
5. S'assurer que les utilisateurs aient les droits les plus faibles possible pour accomplir leurs missions. Lorsqu'une application requiert des droits d'administrateur, il faut être certain que l'application soit légitime.
6. Activer la restauration système afin de retrouver les versions précédentes des fichiers qui ont été chiffrés, une fois que la désinfection a eu lieu.

Source : http://www.itrmobiles.com/index.php/articles/157764/6-conseils-eviter-contamination-reseau-ransomwares.html