

Les bonnes pratiques contre les Cyberattaques | Denis JACOPINI

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

 LE NET EXPERT AUDITS & EXPERTISES	 EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LENETEXPERT .fr	 RGPD CYBER LE NET EXPERT MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
<input checked="" type="checkbox"/>	Les bonnes pratiques contre les Cyberattaques				

Pour se prémunir des cyberattaques, la meilleure solution consiste à mettre en place quelques bonnes pratiques de base.

Encourager une gestion rigoureuse des mots de passe

Mettez en place des outils qui forcent les utilisateurs à choisir des mots de passe forts. Ceux-ci comprennent au moins huit caractères, des majuscules et des minuscules, des chiffres et des symboles du clavier (!, @, \$, etc.), mais aucun mot entier. Ils doivent aussi être changés régulièrement, même si ça cause de la grogne.

Sensibiliser les employés

Souvent considérés comme la porte d'entrée des cybercriminels, les employés doivent être formés, par exemple au moyen de modules d'apprentissage vidéo, sur les risques d'attaques possibles et les différentes formes qu'elles peuvent prendre.

Effectuer régulièrement des tests

Une façon de vérifier si les campagnes de sensibilisation auprès des employés fonctionnent consiste à les tester en simulant, par exemple, l'envoi d'un courriel frauduleux. N'oubliez pas de l'envoyer aussi – et même surtout – à ceux qui occupent des postes stratégiques.

Limiter l'accès à l'information confidentielle

Ne donnez accès aux renseignements confidentiels qu'à ceux qui en ont réellement besoin dans l'entreprise.

Contrôler les processus de sécurité

Rien ne sert d'avoir des systèmes informatiques à la fine pointe si on ne les teste pas régulièrement. Il vaut mieux impartir la tâche à des experts si on ne possède pas les ressources nécessaires à l'interne. Les fournisseurs de solutions infonuagiques disposent d'une infrastructure de sécurité informatique qui peut bien souvent dépasser celle des entreprises.

Installer les mises à jour logicielles rapidement

Beaucoup d'attaques exploitent des vulnérabilités connues depuis plusieurs mois par les fournisseurs d'antivirus, qui d'ailleurs offrent déjà des correctifs pour les contrer. Prévoyez l'installation des mises à jour dans un délai optimal de 48 heures, ou d'au plus une semaine.

Nous vous conseillons les ouvrages suivants :

Guide de la survie de l'Internaute	Anti-Virus-Pack PC Sécurité
	 Moyen pour détecter et chasser les Virus et autres Spyware, ou Protéger Votre PC avant qu'il ne soit TROP tard ...



Dans ce guide pratique, vous trouverez des conseils et un vrai savoir faire dans le domaine de l'identité Internet et de la recherche par recoupement d'informations.

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

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 ?

[block id="24760" title="Pied de page BAS"]

Source : <http://www.lesaffaires.com/dossier/gestion-des-risques/cyberattaques-toutes-les-bonnes-pratiques/579165>

Comment bien sécuriser ses e-mails ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LE NET EXPERT .fr	 RGPD CYBER LE NET EXPERT MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
<input checked="" type="checkbox"/> 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 évitez 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

Nous vous conseillons les ouvrages suivants :

Guide de la survie de l'Internaute



Dans ce guide pratique, vous trouverez des conseils et un vrai savoir faire dans le domaine de l'identité Internet et de la recherche par recouplement d'informations.

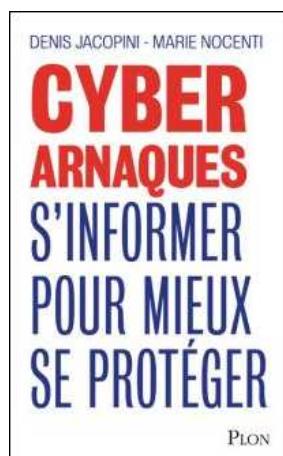
Anti-Virus-Pack PC Sécurité



Moyen pour détecter et chasser les Virus et autres Spyware, ou Protéger Votre PC avant qu'il ne soit TROP tard ...

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

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN :
2259264220



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

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

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

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

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

Commandez sur Fnac.fr

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

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

Commandez sur Fnac.fr

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).

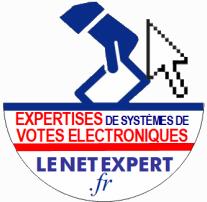
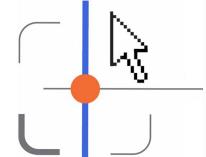
Commandez sur [Fnac.fr](https://www.fnac.fr)

**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

 LE NET EXPERT AUDITS & EXPERTISES	 EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES LE NET EXPERT .fr	 RGPD CYBER LE NET EXPERT MISES EN CONFORMITÉ	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité vous informe...					

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-sponsoriisée 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.

Les 5 principaux déclencheurs d'un projet de sécurisation des échanges dématérialisés et transactions numériques

France, 2014 (liste suggérée de 14 items, plusieurs réponses possibles – en % de décideurs) – Echantillon : 125 décideurs



Les autres éléments déclencheurs sont donnés dans la zone de commentaire
Source MARKESS – www.markess.com

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 cœur 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.

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

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 ?

[block id="24760" title="Pied de page BAS"]

Source :
<http://www.infodsi.com/articles/152936/securiser-echanges-demanterialises-transactions-numeriques-est-crucial-entreprises.html>
par infoDSI.com

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





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

vous informe

Aéroports, hôtels, cafés... Le WiFi public est très utilisé, mais pas sans risque. 30 % des managers ont fait les frais d'un acte cyber criminel 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 cyber criminel (malware, vol de données, usurpation d'identité...) lorsqu'ils étaient à l'étranger.

Droit ou devoir de déconnexion ?

« Les businessmen assurent 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



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.



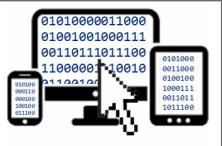
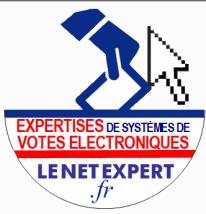
[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Les voyageurs d'affaires

ignorent les risques du WiFi public

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					
 LE NET EXPERT AUDITS & EXPERTISES	 EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LENETEXPERT .fr	 RGPD CYBER LE NET EXPERT MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité vous informe...	6 conseils pour #éviter la contamination du réseau par des ransomwares				

6 conseils pour éviter la contamination du réseau par des ransomwaresUne 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.

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

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.itrmobiles.com/index.php/articles/157764/6-conseils-eviter-contamination-reseau-ransomwares.html>

Un guide pour déjouer les cyber attaques | Denis JACOPINI

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

 LE NET EXPERT AUDITS & EXPERTISES	 EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LENETEXPERT .fr	 RGPD CYBER LENETEXPERT MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
			Un guide pour déjouer les cyber attaques		
Les très petites et les moyennes entreprises (TPE et PME) seraient la cible de 77% des cyber attaques perpétrées en France					

Plus de trois quarts des intrusions malveillantes par Internet visent des petites et moyennes entreprises. Le risque augmente et le coût des dégâts aussi.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI), en partenariat avec la CGPME (Confédération générale des petites et moyennes entreprises), a publié en début d'année un « Guide des bonnes pratiques de l'informatique » (<http://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique>).

Ce document de douze « recommandations » doit aider les petites entreprises à protéger leurs fichiers, déjouer les escroqueries financières, le sabotage de leurs sites de vente en ligne, surveiller leur image de marque sur les réseaux sociaux...

Comment se protéger des piratages ?

Premier conseil : le mot de passe. Le guide recommande d'en choisir un avec « 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance...) et ne figurant pas dans le dictionnaire ».

Deuxième élément important : configuez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible. Sinon, téléchargez les correctifs de sécurité disponibles.

Troisième point crucial, « éviter le Wi-Fi dans le cadre de l'entreprise », préconise le guide. Si vous souhaitez quand même en profiter, le WEP est à bannir absolument puisqu'un chiffrement de ce type peut être cassé en quelques minutes seulement. Il faudra donc lui préférer du WPA/WPA2 avec une clé suffisamment longue de « plus de 20 caractères de types différents ».

Enfin, le guide donne quelques conseils lorsque votre machine a un « comportement étrange », laissant penser à un piratage : « déconnectez la machine du réseau, pour stopper l'attaque. En revanche, maintenez là sous tension et ne la redémarrez pas, pour ne pas perdre d'informations utiles pour l'analyse de l'attaque ». Ensuite, prévenez le responsable informatique ou un prestataire compétent si besoin.

Les PME, premières cibles des cyber attaques

Si chacun a en tête l'exemple récent de Ryanair, délesté de 4,5 millions d'euros par des hackers chinois, ou de la chaîne TV5 monde privée de diffusion, les attaques par Internet ne sont pas réservées aux seules grandes entreprises. Les très petites et les moyennes entreprises (TPE et PME) seraient la cible de 77% des cyber attaques perpétrées en France, selon le Syntec, le syndicat de l'ingénierie et des services informatiques.

La raison est connue : les PME, qui travaillent souvent pour des grands comptes, détiennent des informations capitales, mais insuffisamment sécurisées, faute de moyens. Les hackers s'attaquent donc d'abord à ce « maillon faible ».

Des risques en hausse de 66%

Le 14 avril dernier, à la CCI de Bordeaux, lors d'une réunion d'information sur les « risques nouveaux et émergents » a été présentée une enquête réalisée en 2014 par Ipsos pour l'assureur Axa entreprises. Menée auprès de 500 dirigeants, elle a montré que, si les sociétés de 10 à 500 salariés placent l'environnement (pollution de l'air ou de l'eau) en tête de leurs risques, celui lié à Internet se situe immédiatement après.

Depuis 2009, le nombre d'incidents sur la toile de ce type augmente de 66% en moyenne par an, estime le cabinet d'audit PwC. Il a atteint le nombre de 117 339 attaques dans le monde en 2014. Le coût de la « réparation » et de la mise en place d'une meilleure protection augmente année après année et varie de quelques dizaines de milliers d'euros à plusieurs millions d'euros en fonction de la taille de l'entreprise et des dégâts. Et, il faut compter un délai de 30 à 40 jours pour un retour total à la normale.

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

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

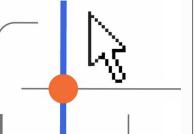
Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.sudouest.fr/2015/05/07/un-guide-pour-aider-les-pme-a-dejouer-les-cyber-attaques-1914431-705.php>
par Michel Monteil

5 conseils cyber pour vous protéger en vacances

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

 LE NET EXPERT AUDITS & EXPERTISES	 LENETEXPERT fr EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 RGPD CYBER LE NET EXPERT MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Denis JACOPINI DENIS JACOPINI EXPERT INFORMATIQUE ASSESSMENT SPECIALISE EN CYBERCRIMINALITE vous informe		5 conseils cyber pour vous protéger en vacances			

Les attaques sur internet ne prennent pas de vacances, il faut être vigilant toute l'année. Protégez vos ordinateurs, installez un anti-virus et suivez nos conseils.

L'été bat son plein et chaque année les Français s'exposent sans le savoir à de nombreux cyber risques pendant les vacances. Norton by Symantec souligne l'importance de rester vigilant lorsque vous êtes connecté à internet et propose ci-dessous une liste de 6 conseils, utiles pour toute la famille :

En voyage, sur quel réseau WiFi se connecter en toute sécurité ?

Sans solution sécurité et VPN ou sur un accès Wi-Fi ouvert, un internaute/mobinaute, ainsi que ses enfants, peuvent être confrontés à certains risques...

Enfants sur internet : rester vigilant même pendant les vacances

De nombreuses plateformes d'hébergement de contenu vidéos notamment permettent de configurer un contrôle parental, également, ne pas hésiter à prendre connaissance du contenu consulté par les plus jeunes.

Modifier régulièrement ses mots de passe

Il est d'importance critique d'avoir un mot de passe complexe ou d'utiliser un gestionnaire de mot de passe pour éviter d'être victime d'une usurpation d'identité. Le bon réflexe est donc de créer des mots de passe forts et uniques qui ne peuvent être facilement devinés, voire, d'utiliser un gestionnaire de mots de passe tel que Identity Safe de Norton...

Les logiciels et applications doivent toujours être à jour

Plusieurs menaces peuvent être contrées par de simples mises à jour de vos applications et appareils...

Effectuer une sauvegarde physique et dans le cloud de ses données.

Que ce soit le contenu qui reste à la maison ou le contenu apporté en vacances, le vol d'un appareil s'accompagne du vol des données qu'il contient – il est donc vital d'être en mesure de les récupérer rapidement.

Source : *Cyber sécurité : 5 conseils pour protéger toute la famille en vacances – Femme Actuelle*

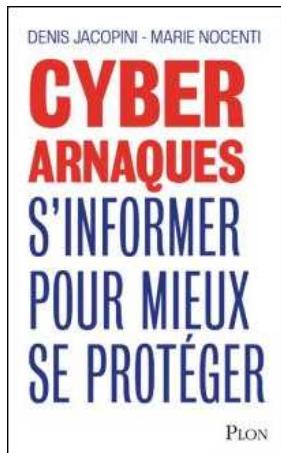
Autres conseils de Denis JACOPINI :

Et comme toujours, attention aux arnaques !

Apprenez à détecter de faux e-mails, de faux sites internet ou des sites internet piégés. Votre meilleur ennemi c'est vous, celui qui est imprudent, qui clique sans vérifier face à un e-mail qui vous fait peur ou qui vous annonce un cadeau...

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

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN :
2259264220



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

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

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

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

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

Commandez sur Fnac.fr

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

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

Commandez sur Fnac.fr

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

Hotspot Shield le logiciel

VPN pour Windows MacOs IOS Android Apple Samsung pour accéder de manière sécurisée à un Wifi public | Denis JACOPINI

#Hotspot Shield le #logiciel VPN
pour Windows MacOs IOS Android Apple
Samsung pour accéder de manière
sécurisée à un Wifi public

En période de vacances ou lors de déplacements professionnels, nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants... En juillet 2015, nous vous avions publié un article « Est-il risqué de se connecter au wifi public ? » pour vous informer des principaux risques à partager ces accès sans fil à internet avec d'autres. Cette fois, nous allons parler des solutions pour surfer sécurisé en utilisant les réseaux Wifi publics.

RAPPEL DU PRINCIPAL RISQUEUn pirate peut se connecter tout aussi facilement que vous sur un réseau Wifi Public et espionner les données qui y transitent.

Il peut ainsi, en fonction des données qu'il récupère, accéder à toutes les informations qui sortent et qui entrent de votre ordinateur (le protocole tcp/ip n'étant pas protégé par défaut).

LA SOLUTION ?

Utiliser une connexion Wifi qui sera cryptée au moyen d'un logiciel VPN (ce ctyptage n'a aucun rapport avec les clés Wifi) .

La connexion Wifi ainsi créée étant crypté, toutes les informations qui véhiculeront (identifiants, adresses email, mots de passe, numéros de cartes bancaires...) seront illisibles pour tous les pirates qui seront connectés sur le même point d'accès wifi.

Vous pouvez certes partager la connexion 3G ou 4G de votre smartphone, mais l'utilisation d'un logiciel VPN est recommandé.

Un logiciel « VPN » (Virtual Private Network) est un logiciel qui crée un « réseau privé virtuel », une sorte de tunnel crypté pour vos communications internet. Cela ralentit un peu la connexion, mais elle est du coup sécurisée.

Nous utilisons régulièrement un logiciel VPN #HotSpotShield. C'est un logiciel qui coûte moins de 25 euros et qui vous rendra les connexions Wifi publiques sécurisées.

HotSpot Shield existe pour Windows pour protéger par un logiciel VPN les connexions Wifi des ordinateurs assemblés, Acer, Asus, IBM, Dell ;

HotSpot Shield existe aussi pour MacOs X Lion pour protéger par un logiciel VPN les connexions Wifi des ordinateurs Apple ;

HotSpot Shield existe aussi pour Android pour protéger par un logiciel VPN les connexions Wifi des smartphones Samsung, HTC, Archos, LG, Acer, Wiko, Sony, Asus, Alcatel, ZTE... ;

Enfin, HotSpot Shield existe aussi pour IOs pour protéger par un logiciel VPN les connexions Wifi des smartphones Apple.

Téléchargez et testez gratuitement HotSpot Shield



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.

Denis JACOPINI interviewé par une journaliste de Ouest France | Denis JACOPINI



Est-il risqué de se connecter au wifi public ?

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

Avec les smartphones ou ordinateurs portables d'aujourd'hui, se connecter au réseau wifi d'une gare ou d'un hôtel, quand on est en déplacement, est devenu presque banal. À l'étranger, c'est même la solution la plus simple pour surfer sur internet et relever ses e-mails, sans risquer d'exorbitants frais de « roaming » (coûts de connexion au réseau mobile local, facturés ensuite par l'opérateur français).

Résultat, on a tendance à surfer sur ces réseaux wifi avec la même insouciance qu'à la maison, sans aucune précaution. Ce qui n'est pas bien malin. Denis Jacopini, expert judiciaire en sécurité informatique, nous explique pourquoi.



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

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

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

Quel est le danger ? Se faire espionner ?

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



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

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

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

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

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



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

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

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

Comment se protéger ?

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



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

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

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 ?

[block id="24760" title="Pied de page BAS"]

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

Par Corinne Bourbeillon



Est-ce utile de protéger la WebCam et le microphone de son ordinateur avec de l'adhésif ? | Denis JACOPINI



Est-ce utile de protéger Webcam et microphone son ordinateur avec l'adhésif ?

Cela peut sembler absurde, mais c'est une mesure de précaution élémentaire, probablement conseillée par la direction en charge de la sécurité de Facebook, sur tous les ordinateurs portables susceptibles d'être attaqués.

En 2013, des chercheurs en sécurité informatique de l'université John Hopkins, aux Etats-Unis, avaient démontré qu'il était possible de prendre le contrôle des webcams des Mac, ce qui est aussi chose fréquente sur les PC.

La firme Symantec avait même alerté, la même année, sur ce qu'elle désignait comme des « creepwares », « Certaines personnes mettent un morceau d'adhésif sur la webcam de leur portable, peut-être vous-mêmes le faites. Sont-elles trop prudentes, paranoïaques, un peu étranges ? (...) »

Beaucoup d'entre nous ont entendu des histoires de gens qui étaient espionnés sur leur ordinateur (...). Mais ces histoires sont-elles vraies et les précautions prises par des gens en apparence paranoïaques sont elles justifiées ? Malheureusement la réponse est oui », écrivait alors Symantec. L'éditeur a même publié une vidéo de prévention :

Source Numerama

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

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 ?

[block id="24760" title="Pied de page BAS"]

Original de l'article mis en page : Pourquoi Mark Zuckerberg met du scotch sur la webcam et le micro de son Mac – Tech – Numerama