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

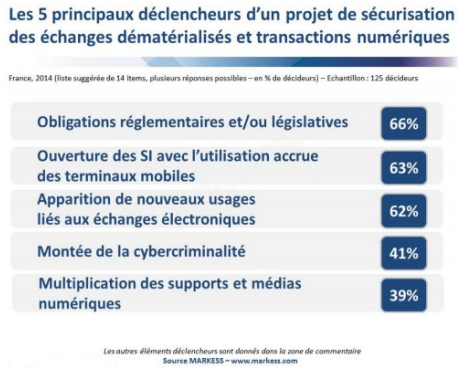
LE NET EXPERT AUDITS & EXPERTISES | EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES LE NET EXPERT .fr | RGPD CYBER LE NET EXPERT MISES EN CONFORMITÉ | SPY DETECTION Services de détection de logiciels espions | LE NET EXPERT FORMATIONS | LE NET EXPERT ARNAQUES & PIRATAGES

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

[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-dematerialises-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

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

Les données à caractère personnel du compte personnel de formation encadrées par la CNIL | Denis JACOPINI

À l'instar des données de santé, la gestion des données à caractère personnel par le système d'information du compte personnel de formation (SI-CPF) nécessite d'équilibrer principe de précaution et souplesse. Précisément ce que vient de faire la Commission nationale de l'informatique et des libertés (CNIL) en indiquant la possibilité d'une « autorisation unique ». Explications.

Choisie pour assurer fluidité et rapidité à la gestion des comptes personnels de formation, la dématérialisation de la gestion des droits inscrits ou mentionnés au CPF implique de nombreux acteurs. Parmi ceux-ci, des acteurs de la formation professionnelle non autorisés à traiter les numéros d'inscription des personnes au répertoire national d'identification des personnes physiques du titulaire d'un compte accompagné de son nom.

Le principe de « l'autorisation unique »
Saisie par le ministre du Travail, de l'Emploi, de la Formation professionnelle et du Dialogue social, la CNIL explique dans sa délibération du 9 juillet 2015 qu'il est toutefois possible de déroger : « dans la mesure où la connexion au SI-CPF est indispensable pour bénéficier d'une formation professionnelle et impose de renseigner le numéro d'inscription […], la Commission a souhaité alléger les formalités ». Aussi devient-il possible pour ces acteurs de bénéficier d'une « autorisation unique de traitements de données à caractère personnel mis en œuvre aux fins de gestion des comptes personnels de formation ».

Un spectre limité de données
Encadrée, cette autorisation bénéficie aux « organismes de droit privé habilités à intervenir dans le domaine de la formation professionnelle aux fins de mise en œuvre des CPF […] et de se connecter au SI-CPF […] ». Rappelant le concept de données « adéquates, pertinentes et non excessives au regard de la finalité poursuivie », la CNIL énumère de façon limitative les données susceptibles d'être collectées. Ceci, dans cinq domaines : informations personnelles du titulaire du compte ; données correspondantes aux comptes d'heures ; données des dossiers de formation ; passeports d'orientation, de formation et de compétences ; annuaires techniques des gestionnaires des organismes.

Des données à date de conservation limitée
L'article 3 de la délibération le précise, ces données « peuvent être conservées au maximum un mois à l'issue des opérations requises pour la gestion des comptes personnels de formation ».
Délibération n° 2015-227 du 9 juillet 2015 portant autorisation unique de traitements de données à caractère personnel mis en œuvre aux fins de gestion des comptes personnels de formation – JORF n° 1072 du 28 juillet 2015, texte n° 75 : format PDF – 136 ko

---

Source : http://www.actualite-de-la-formation.fr/rubriques/syntheses/la-cnil-encadre-la-gestion-des-donnees-personnelles-destinees-au-systeme-d.html

---

Bases essentielles pour

sécuriser son site web | Denis JACOPINI

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

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…

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

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

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : 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

LE NET EXPERT AUDITS & EXPERTISES | EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES LENETEXPERT.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

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

Le public doit-il être informé qu'il est filmé ? | Denis JACOPINI

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

Le public doit-il être informé qu'il est filmé ?

Les personnes filmées dans un espace public (rue, gare, centre commercial, zone marchande, etc.) doivent en être informées, au moyen de panneaux affichés de façon visible comportant :
• Un pictogramme représentant une caméra ;
• Le nom ou la qualité et le numéro de téléphone du responsable.
• Ces panneaux doivent être affichés en permanence dans les lieux concernés et doivent être compréhensibles par tous les publics.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

S o u r c e :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=D6FE4EA8F8C2B622744249AD69FABBA1?name=Vid%C3%A9oprotection+%3A+le+public+doit-il+%C3%AAtre+inform%C3%A9+qu%27il+est+film%C3%A9+%3F&id=410

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

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

Un guide pour déjouer les cyber attaques | Denis JACOPINI

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

Les très petites et les moyennes entreprises (TPE et PME) seraient la cible de 77% des cyber attaques perpétrées en France

Un guide pour déjouer les cyber attaques

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 : configurez 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.

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

Piratage de votre boite mail, quelles peuvent être les conséquences sur votre vie personnelle

	Piratage de votre boite mail, quelles peuvent être les conséquences sur votre vie personnelle

Votre boite mail est souvent la clé qui permet d'accéder ou de vous inscrire aux services en ligne.Raison de plus pour la sécuriser au maximum !

Pour votre boite mail : un mot de passe solide

Vous devez utiliser un mot de passe propre et unique pour vous connecter à votre webmail et surtout ne pas l'utiliser pour un autre compte.

Pourquoi c'est important ?

Utiliser le même mot de passe pour votre compte de messagerie et votre compte de réseau social est une pratique risquée. Si votre fournisseur de réseau social est victime d'une fuite de données comprenant vos moyens d'authentification, une personne mal intentionnée pourrait les utiliser pour non seulement accéder à votre compte de réseau social mais aussi pour accéder à votre messagerie.
De plus, une fois l'accès à votre messagerie obtenu, il deviendra possible de voir la liste des messages d'inscriptions à vos comptes sur différents sites (si vous ne les avez pas supprimés de votre boîte). Il sera ainsi possible de connaître certains de vos identifiants de compte et d'utiliser la fonction d'oubli de mots de passe pour en prendre le contrôle.

Cette absence de sécurité ou l'utilisation d'un mot de passe faible vous expose à des risques :

• Usurpation de votre boite mail pour piéger votre liste de contacts ;
• Ajout d'une redirection de mail (souvent indétectable après la compromission d'une boite mail) : vos emails continuent de fuiter malgré tout changement de mot de passe ultérieur…
• Connexion du pirate à vos sites et applications tierces ;
• Utilisation de vos coordonnées bancaires pour payer ;
• Usurpation d'identité grâce aux données collectées dans votre boite mail ;
• Demande de rançon suite à des données compromettantes retrouvées dans votre boite mail ;
• …

[CONSEIL] – En parallèle d'un bon mot de passe :

• Il est déconseillé d'utiliser sa boite mail en tant qu'espace de stockage, notamment pour les données qui peuvent vous paraitre sensibles et notamment, les bulletin de paie, les justificatifs d'identité envoyés qui peuvent notamment contenir votre adresse postale personnelle, ou les mots de passe échangés en clair. Attention également aux photos qui permettent de vous ré-identifier sur des sites de réseaux sociaux et donnent la possibilité à une personne malveillante de se créer une fausse identité.
• Il convient de supprimer les emails reçus, envoyés ou enregistrés en tant que brouillon qui paraissent avoir une importance particulière ou de chiffrer les documents que vous mettez en pièce jointe.
• Enfin pour protéger votre identité, il est recommandé d'utiliser une boite mail sous pseudonyme pour l'inscription à des services que vous jugez intrusifs, ou particulièrement sensibles (site de jeux concours, site de rencontre …).

L'initiative

haveibeenpwened est un site conçu par Troy Int, informaticien indépendant. Il recense tous les mails compromis à l'occasion de fuite de données massive. L'utilisateur n'a qu'à entrer son email pour savoir s'il figure dans une base de données piratée et si ses mots de passes sont potentiellement entre les mains de personnes malveillantes.

***Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).*
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

5 conseils cyber pour vous protéger en vacances

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

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*

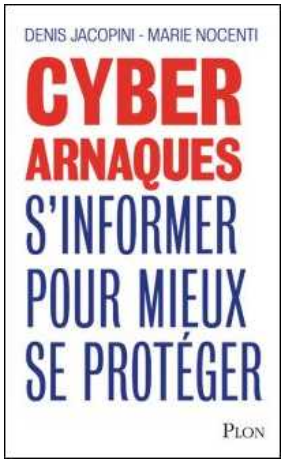
Autres conseils de Denis JACOPINI :

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 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