

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.gouv.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 activez 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

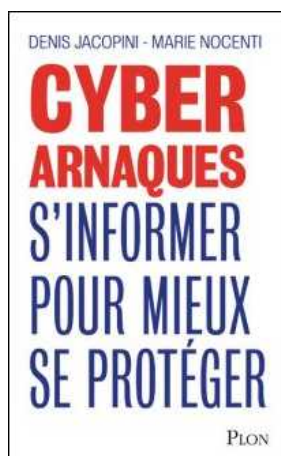
Rendez-vous sur cybermalveillance.gouv.fr, la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance. Que vous soyez un particulier, une entreprise ou une administration, retrouvez :

- 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]

[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)

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

Mon ordinateur ou mon

téléphone est-il espionné ? Des informations me sont-elles volées ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
 <p>Denis JACOPINI VOUS INFORME</p>	<p>Mon ordinateur ou mon téléphone est-il espionné ? Des informations me sont-elles volées ?</p>				

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



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.

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"]

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	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT RGPD CYBER MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
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 #divulgateion 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](#)

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 recoupement d'informations.

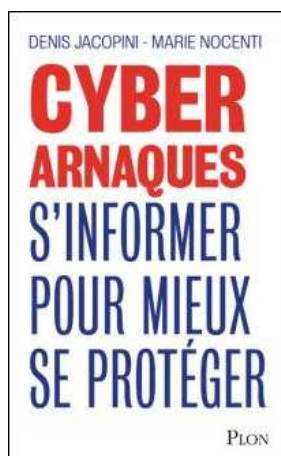
Anti-Virus-Pack PC Sécurité



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

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LE NET EXPERT fr</p>	 <p>RGPD CYBER LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<p>Sécuriser les échanges dématérialisés et les #transactions numériques est crucial pour les entreprises</p>				

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-sponsorisée 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 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.

[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



Denis JACOPINI



SPAM : GARE AUX ARNAQUES !

LOTTERIE, PETITES ANNONCES OU APPREZ, AUX DOSES, LES PRINCIPALES ARNAQUES PAR MAIL

LCI

vous informe

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 a 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

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

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
<input type="checkbox"/>	Les données à caractère personnel du #compte personnel de formation encadrées par la CNIL				

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

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 !

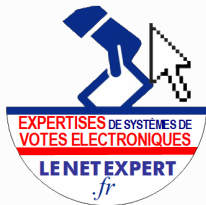
Source

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

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



Plus de 8 caractères
+ sans lien avec son détenteur
+ MAJUSCULES + ponctuation + chiffres

Exemple à suivre : la phrase mnémotechnique «un Utilisateur d'Internet averti en vaut deux » donnera le mot de passe 1Ud'laev2

D'autres informations et conseils pratiques sur www.cnil.fr / @CNIL

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 !

Source : <http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=D6FE4E8F8C2B62274429AD69FABBA1?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

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<h2>6 conseils pour #éviter la contamination du réseau par des ransomwares</h2>				

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.

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 plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

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