Un oeil sur vous, citoyens sous surveillance — Documentaire 2015 | Denis JACOPINI

Un oeil sur vous, citoyens sous
 surveillance − Documentaire
 2015 2h24

Des milliards de citoyens connectés livrent en permanence — et sans toujours s'en rendre compte — des informations sur leur vie quotidienne à des sociétés privées qui les stockent dans de gigantesques serveurs. Ces informations sont rendues accessibles aux États et vendues aux entreprises. Dans ce monde sous étroite surveillance, jusqu'où irons-nous en sacrifiant nos vies intimes et nos droits à la liberté individuelle ?

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 !

Votre boite e-mail a été piratée. Quelle attitude adopter ? | Denis JACOPINI



Votre boite e-mail a été piratée. Quelle attitude adopter ? Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée ?Quelle attitude adopter ?

Un choix s'offre à vous :

Vous protéger et faire cesser le piratage, ou bien rechercher l'auteur et porter plainte.

Vous protéger et faire cesser le piratage

Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée. Quels sont les éléments qui vous font penser ça ?

- Quelqu'un est au courant de choses dont il ne devrait pas être au courant qui n'apparaît que dans les e-mails?
- Vous constatez que des e-mails que vous n'avez pas lu sont tout de même « lus » ?
- Vous avez constaté dans l'historique des connexions une connexion qui ne semble pas être la votre ?
- 1°/ Pour vous protéger contre ça et faire cesser tout piratage, la première chose à faire est de lancer des outils de détection de virus, d'espions, keyloggers et autres logiciels malveillants.

Vous fournir une liste serait très compliqué car ceci engagerait quelque part ma responsabilité de vous conseiller un outil plutôt qu'un autre, alors qu'il en existe un grand nombre et aucun n'est fiable à 100%. Je ne peux vous conseiller que de rechercher sur Internet des « Antivirus Online », des Anti-Malwares, des Anti-espions... Toutefois, pour nos propres besoins nous avons une liste de liens accessible sur www.antivirus.lenetexpert.fr.

2°/ Une fois votre ordinateur nettoyé, vous pouvez procéder aux changements de mots de passe des différents services que vous utilisez régulèrement (e-mail, banque, blog, réseaux sociaux...). Une fois ces deux étapes réalisées, vous ne devriez plus être « espionné ».

Rechercher l'auteur et porter plainte

Si vous suspectez une personne en particulier et que vous souhaitez l'attraper la main dans le sac, sachez que votre action doit prendre la voie de la justice.

Soit vous avez les éléments techniques pouvant l'action de l'auteur clairement identifié, et vous pouvez faire constater par huissier, soit, vous n'avez comme élément qu'une adresse IP, au quel cas, il sera nécessaire de se rapprocher d'un avocat conseil qui rédigera une requête auprès du Tribunal Adhoc afin d'obtenir une ordonnance nous permettant, en tant qu'expert, de réaliser les démarches auprès des fournisseurs de services concernés par le piratage.

Une autre solution plus économique car gratuite mais à l'issue incertaine est de signaler les actes de piratages dont vous êtes victime aux services de Gendarmerie ou de Police en commissariat, en brigade ou sur le site Internet www.internet-signalement.gouv.fr. Cependant, s'il n'y a pas de très grosses sommes en jeu, d'actes délictueux auprès de mineurs ou en rapport avec des entreprises terroristes, vous comprendrez aisément que votre demande ne sera pas considérée comme prioritaire. Sachat que les opérateurs conservent les traces qui vous permettront d'agir en justice quelques mois, quelques semaines ou quelques jours, votre demande par cette voie risque fortement d'être classée sans suite.

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur

: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

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

Source : Denis JACOPINI

Arnaques, spams, phishing, sextape. Comment se protéger? | Denis JACOPINI



Arnaques, spams, phishing, sextape. Comment se protéger

Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée ?Quelle attitude adopter ?

Un choix s'offre à vous :

Vous protéger et faire cesser le piratage, ou bien rechercher l'auteur et porter plainte.

Vous protéger et faire cesser le piratage

Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée. Quels sont les éléments qui vous font penser ca ?

- Quelqu'un est au courant de choses dont il ne devrait pas être au courant qui n'apparaît que dans les e-mails ?
- Vous constatez que des e-mails que vous n'avez pas lu sont tout de même « lus » ?
- Vous avez constaté dans l'historique des connexions une connexion qui ne semble pas être la votre ?
- l°/ Pour vous protéger contre ça et faire cesser tout piratage, la première chose à faire est de lancer des outils de détection de virus, d'espions, keyloggers et autres logiciels malveillants.

Vous fournir une liste serait très compliqué car ceci engagerait quelque part ma responsabilité de vous conseiller un outil plutôt qu'un autre, alors qu'il en existe un grand nombre et aucun n'est fiable à 100%. Je ne peux vous conseiller que de rechercher sur Internet des « Antivirus Online », des Anti-Malwares, des Anti-espions… Toutefois, pour nos propres besoins nous avons une liste de liens accessible sur www.antivirus.lenetexpert.fr.

2°/ Une fois votre ordinateur nettoyé, vous pouvez procéder aux changements de mots de passe des différents services que vous utilisez régulèrement (e-mail, banque, blog, réseaux sociaux...).

Une fois ces deux étapes réalisées, vous ne devriez plus être « espionné ».

Rechercher l'auteur et porter plainte

Si vous suspectez une personne en particulier et que vous souhaitez l'attraper la main dans le sac, sachez que votre action doit prendre la voie de la justice.

Soit vous avez les éléments techniques prouvant l'action de l'auteur clairement identifié, et vous pouvez faire constater par huissier, soit, vous n'avez comme élément qu'une adresse IP, au quel cas, il sera nécessaire de se rapprocher d'un avocat conseil qui rédigera une requête auprès du Tribunal Adhoc afin d'obtenir une ordonnance nous permettant, en tant qu'expert, de réaliser les démarches auprès des fournisseurs de services concernés par le piratage.

Une autre solution plus économique car gratuite mais à l'issue incertaine est de signaler les actes de piratages dont vous êtes victime aux services de Gendarmerie ou de Police en commissariat, en brigade ou sur le site Internet www.internet-signalement.gouv.fr. Cependant, s'il n'y a pas de très grosses sommes en jeu, d'actes délictueux auprès de mineurs ou en rapport avec des entreprises terroristes, vous comprendrez aisément que votre demande ne sera pas considérée comme prioritaire. Sachat que les opérateurs conservent les traces qui vous permettront d'agir en justice quelques mois, quelques semaines ou quelques jours, votre demande par cette voie risque fortement d'être classée sans suite.

Denis JACOPINI est Expert Informatique assermenté, pratiquant à la demande de particuliers d'entreprises ou de Tribunaux. Il est consultant et formateur en sécurité informatique et en mise en conformité de vos déclarations à la CNTI.

Nos domaines de compétence :

- Expertises et avis techniques en concurrence déloyale, litige commercial, piratages, arnaques Internet...;
- Consultant en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- Formateur et chargé de cours en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source : Denis JACOPINI

Déplacements professionnels. Attention au Wi-Fi de l'hôtel…



De nos jours, qui réussirait à se passer d'Internet plus d'une journée, en vacances, en déplacement, lors d'une conférence ou au travail ? Nos vies aujourd'hui digitalisées nous poussent à nous connecter quasi automatiquement au premier réseau Wi-Fi disponible, quitte à mettre la confidentialité de nos données en danger.

Cela devient d'autant plus problématique lorsque nous voyageons : une étude Kaspersky Lab révélait récemment que 82% des personnes interrogées se connectent à des réseaux Wi-Fi gratuits non sécurisés dans des terminaux d'aéroports, des hôtels, des cafés ou des restaurants.

Dans la tribune ci-dessous, Tanguy de Coatpont, Directeur général de Kaspersky Lab France et Afrique du Nord analyse les vulnérabilités des réseaux Wi-Fi dans les hôtels, une mine d'or pour des cybercriminels en quête de données personnelles ou d'informations confidentielles.

Depuis 10 ans, le cyber crime s'est largement professionnalisé pour devenir une véritablement industrie, portée sur la rentabilité. Les cybercriminels sont en quête permanente de victimes qui leur assureront un maximum de gains pour un minimum d'investissements techniques.

De son côté, l'industrie hôtelière a passé la dernière décennie à se transformer pour répondre aux nouvelles attentes digitales de ses clients. Alors que plus d'un quart d'entre eux annoncent qu'ils refuseraient de séjourner dans un hôtel ne proposant pas de Wi-Fi, la technologie n'est plus un luxe mais bien une question de survie pour les établissements hôteliers. Face aux ruptures liées à la numérisation, il a donc fallu repenser les modèles existants et s'équiper, parfois en hâte, de nouvelles technologies mal maîtrisées. Il n'était donc pas surprenant de voir émerger rapidement des problèmes de sécurité, dans les hôtels bon marché comme dans les 5 étoiles.

Par Tanguy de Coatpont, Directeur général de Kaspersky Lab France et Afrique du Nord

Le paradoxe du Wi-Fi à l'hôtel : privé mais public

Ils ont beau être déployés dans des établissements privés, les Wi-Fi d'hôtels restent des points d'accès publics. Ils sont même parfois complètement ouverts. Le processus de connexion, qui nécessite le plus souvent de confirmer son identité et son numéro de chambre, limite l'accès au réseau mais ne chiffre pas les communications. Il ne garantit pas non plus leur confidentialité. Est-ce que cela signifie que nos informations sont à la portée de tous ? La réalité n'est pas aussi sombre, mais elles sont à la portée de n'importe quel criminel équipé d'un logiciel de piratage, dont certains sont disponibles gratuitement en ligne, et disposant de connaissances techniques de base.

Concrètement, il suffit à un criminel de se positionner virtuellement entre l'utilisateur et le point de connexion pour récupérer toutes les données qui transitent par le réseau, qu'il s'agisse d'emails, de données bancaires ou encore de mots de passe qui lui donneront accès à tous les comptes de l'internaute. Une approche plus sophistiquée consiste à utiliser une connexion Wi-Fi non sécurisée pour propager un malware, en créant par exemple des fenêtres pop-up malveillantes qui invitent faussement l'utilisateur à mettre à jour un logiciel légitime comme Windows.

Le mythe de la victime idéale

En 2014, le groupe de cybercriminels Darkhotel avait utilisé une connexion Wi-Fi pour infiltrer un réseau d'hôtels de luxe et espionner quelques-uns de leurs clients les plus prestigieux. Un an plus tard, les activités de ce groupe étaient toujours en cours, continuant d'exfiltrer les données des dirigeants d'entreprises et dignitaires. Pour autant, les cybercriminels ne ciblent pas que des victimes à hauts profils. Beaucoup d'utilisteurs continuent de penser qu'ils ne courent aucun risque car les informations qu'ils partagent sur Internet ne méritent pas d'être piratées. C'est oublier que la rentabilité d'une attaque repose aussi sur le nombre de victimes. Parmi les 30 millions de clients pris en charge par l'hôtellerie française chaque année, seuls 20% sont des clients d'affaires. Les 80% de voyageurs de loisirs représentent donc une manne financière tout aussi importante pour des cybercriminels en quête de profit.

Dans certains cas, une faille Wi-Fi peut même exposer l'hôtel lui-même, en servant de porte d'entrée vers son réseau. Si l'on prend le cas d'une chaîne d'hôtellerie internationale qui disposerait d'un système de gestion centralisé et automatisé, une intrusion sur le réseau pourrait entrainer le vol à grande échelle d'informations confidentielles et bancaires sur les employées, le fonctionnement de l'hôtel et ses clients.

Hôtels indépendants vs. chaînes hôtelières : des contraintes différentes pour un même défi

Pour une industrie aussi fragmentée que celle de l'hôtellerie, la sécurité est sans aucun doute un défi. Les hôtels indépendants ont une capacité d'accueil réduite et traitent donc moins de données. Le revers de la médaille est qu'ils disposent souvent d'une expertise informatique limitée et leur taille ne permet pas de réaliser les économies d'échelle qui rentabiliseraient un investissement important dans la sécurité informatique. Quant aux grands groupes, qui comptent des ressources humaines et financières plus importantes, ils sont mis à mal par l'étendue de leur écosystème, qui rend difficile l'harmonisation d'une politique de sécurité sur des centaines, voire des milliers de sites.

Il est important que tous les hôtels, quelle que soit leur taille ou leur catégorie, respectent quelques règles simples à commencer par l'isolation de chaque client sur le réseau, l'utilisation de technologies de chiffrement et l'installation de solutions de sécurité professionnelles. Enfin, le réseau Wi-Fi offert aux clients ne doit jamais être connecté au reste du système informatique de l'hôtel, afin d'éviter qu'une petite infection ne se transforme en épidémie généralisée. En respectant ces règles, la sécurité pourrait devenir un argument commercial au moins aussi efficace que le Wi-Fi.

Article original de Robert Kassous

Denis JACOPINI est Expert Informatique et aussi **formateur en Cybercriminalité** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous pouvons vous animer des **actions de sensibilisation ou de formation** à la Protection des Données Personnelles, au risque informatique, à l'hygiène informatique et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles

Denis JACOPINI



Denis JACOPINI est Expert Informatique asserment spécialisé en cybercriminalité et en protection de données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentions désphones, de licentés.)
- 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 : Etude Kaspersky sur le Wi-Fi à l'hôtel… | InfoTravel.fr

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques



| CONTINUE OF THE PROPERTY OF TH |
|--|
| |
| Care of a 12 miles of the control of |
| Stream or you're a your require to the stream of the stream or the strea |
| Figure and the control of the contro |
| Commit daire or protings 7 |
| has a filter order of the control of |
| Section 1. |
| Traching part was on any part of the contract |
| E. MINITAL ON AND AND AND AND AND AND AND AND AND AN |
| THE CONTROL OF THE PROPERTY OF |
| The Contract of Contraction is a possible part in a transition of Contraction is a possible part in a transition of Contraction of Contraction is a possible part in a contraction of Cont |
| Analogue in projection part on the case of |
| a straight of states of the straight of the st |
| L Transport register (uniform to inflamentary registers (uniform to inflamentary registers) and the second of the |
| - Command and the command of the com |
| The principle of the control of the |
| the great printer of contribution of an information and inform |
| And analysis recommenced in the commenced in the commence |
| I repair or a con an final design and an inflammation and an an inflammation and an inflammation in repair or an inflammation and an inflammation in repair or an inflammation and an inflammation in repair or an inflamma |
| The STREET COUNTY OF A CHARMA OF FEMORE AND ADDRESS OF A CHARMA OF A CHA |
| |
| A profile of an extra declaration of the second of the sec |
| Principalities a principal parallel in princ |
| the control of the co |
| And the state of t |
| PRIMATE AND MANAGE. From the of general to, regarder 1.0 follows and one, produced with supply come primate with supply |
| In case the residence of these analysis of the residence |
| or its regarded as a decrease of the contract |
| |
| 1. A MANAGEMENT AND THE SETTING CONTINUES AND ADDRESS OF THE SETTING CONTINUES AND AD |
| |
| The contract of the contract o |
| A STATE OF AN ADMINISTRATION OF THE PROPERTY OF THE ADMINISTRATION |
| Subject to 1 for all continues and the size of the si |
| William and the second |
| - TAMENDA TO A MARKET AND THE PROPERTY A |
| 1. A SEPTION AND AND ADDRESS A |
| The is a relative to a self-or processing depth on a comparability to the comparability of th |
| |
| To the life of the control of the co |
| To case the part of the definition in the case of the |
| 9. NOTE AND TO PRODUCE AND COPING OCCUPANT (MATERIAL OF ANY AND THE ANY AND TH |
| A SEA OF A S |
| 1 IN THE A THING A PHYSICAL AND A THING AND AND A SHEET AND A SHEE |
| The control of the co |
| The EA TO A STATE AND ADDRESS |
| |
| Market or Market of an admitted by Market State of Market State of Anna Admitted State of Anna Admittant Admitted State of Anna Admitted |
| 2 Notice in the content of authorized to application content on the first to the content of authorized to to the conte |
| in region in part of mark that a second of the contract of part of mark that a second of the contract of the c |
| 24. DEFEZ FERLENT CHICA D'UN PARRINTE UNE DEFENDIT |
| Let, ORDER LEGISLATI UNIT AUTOMAT UNIT PROGRAMMAT UNIT AUTOMATE DE LEGISLATI UNIT AUTOMAT UNIT A |
| A continue to present or a contra ment to contra ment to contra ment to the contra ment to the contra ment to c |
| A serior to reconstant or former for the reconstant of the reconst |
| In Additional to the second of |
| 1-1. THANDWING AND PRODUCTION, SPECIALLY AND |
| THE THE PART OF MARKET THE PART |
| 1 MAN, AMERICAN Transform and amenintry Minimized and American State Organization and American |
| 27,7347100 |
| |
| Figure 1000 to the part page. |
| ************************************** |
| ** ** ** ** ** ** ** ** ** ** ** ** ** |
| The state of the s |
| AND ADMINISTRATION OF STREET AND ADMINISTRATI |
| List tripper |
| |
| |
| CL DEFENDENCE TO THE PROPERTY OF THE PROPERTY |

Original de l'article mis en page : Conseils aux usagers | Gouvernement.fr

Victime d'une arnaque sur Internet ? Faites-nous part de votre témoignage



Vous êtes victime d'une arnaque ou d'un piratage sur Internet ? Votre témoignage nous permettra peut-être de vous aider.

Devant une explosion de cas d'arnaques et de piratages par Internet et des pouvoirs publics débordés par ce phénomène, nous avons souhaité apporter notre pierre à l'édifice.

Vous souhaitez nous faire part de votre témoignage, contactez-nous.

Vous devez nous communiquer les informations suivantes (<u>tout message incomplet et correctement rédigé ne sera pas traité)</u>:

- une présentation de vous (qui vous êtes, ce que vous faites dans la vie et quel type d'utilisateur informatique vous êtes) ;
- un déroulé chronologique et précis des faits (qui vous a contacté, comment et quand et les différents échanges qui se sont succédé, sans oublier l'ensemble des détails même s'ils vous semblent inutiles, date heure, prénom nom du ou des interlocuteurs, numéro, adresse e-mail, éventuellement numéros de téléphone ;
- Ce que vous attendez comme aide (je souhaite que vous m'aidiez en faisant la chose suivante :)
 - Vos nom, prénom et coordonnées (ces informations resteront strictement confidentielles).

Contactez moi

Conservez précieusement toutes traces d'échanges avec l'auteur des actes malveillants. Ils me seront peut-être utiles.



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

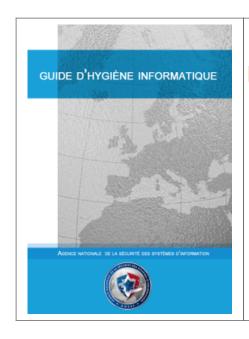
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation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



Contactez-nous

Réagissez à cet article

Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique | Denis JACOPINI



Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique Vous voulez éviter que le parc informatique soit utilisé pour affaiblir votre organisation ? L'un des guides publiés par l'ANSSI vous aidera à vous protéger.

Initialement destinés aux professionnels de la sécurité informatique, les guides et recommandations de l'ANSSI constituent des bases méthodologiques utiles à tous. Vous trouverez sans peine votre chemin en utilisant les motsclés, qu'un glossaire vous permet d'affiner, ou le menu thématique.

LISTE DES GUIDES DISPONTBLES

- Guide pour une formation sur la cybersécurité des systèmes industriels
- Profils de protection pour les systèmes industriels
- Sécuriser l'administration des systèmes d'information
- Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du rgs
- Recommandations pour le déploiement sécurisé du navigateur mozilla firefox sous windows
- Cryptographie les règles du rgs
- Recommandations de sécurité concernant l'analyse des flux https
- Partir en mission avec son téléphone sa tablette ou son ordinateur portable
- Recommandations de sécurité relatives à active directory
- Recommandations pour le déploiement sécurisé du navigateur microsoft internet explorer
- l'homologation de sécurité en neuf étapes simples,
- bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,
- · recommandations pour le déploiement sécurisé du navigateur google chrome sous windows,
- usage sécurisé d'(open)ssh,
- la cybersécurité des systèmes industriels,
- sécuriser une architecture de téléphonie sur ip,
- mettre en œuvre une politique de restrictions logicielles sous windows,
- prérequis à la mise en œuvre d'un système de journalisation,
- vulnérabilités 0-day, prévention et bonnes pratiques,
- le guide des bonnes pratiques de configuration de bgp,
- sécuriser son ordiphone,
- sécuriser un site web,
- sécuriser un environnement d'exécution java sous windows,
- définition d'une politique de pare-feu,
- sécuriser les accès wi-fi,
- sécuriser vos dispositifs de vidéoprotection,
- guide d'hygiène informatique,
- la sécurité des technologies sans contact pour le contrôle des accès physiques,
- recommandations de sécurité relatives à ipsec,
- la télé-assistance sécurisée,
- sécurité des systèmes de virtualisation,
- sécurité des mots de passe,
- définition d'une architecture de passerelle d'interconnexion sécurisée,
- ebios expression des besoins et identification des objectifs de sécurité,
- la défense en profondeur appliquée aux systèmes d'information,
- externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques,
- archivage électronique… comment le sécuriser ?
- pssi guide d'élaboration de politiques de sécurité des systèmes d'information,
- tdbssi guide d'élaboration de tableaux de bord de sécurité des systèmes d'information,
- guide relatif à la maturité ssi,
- gissip guide d'intégration de la sécurité des systèmes d'information dans les projets

Expert Informatique 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 protection juridique du chef d'entreprise.

Contactez-nous

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

Source : http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/

Attention aux démarchages trompeurs « Mise en conformité RGPD »



Des courriers « Mise en conformité — RELANCE » ou « Mise en conformité — dernier rappel » avec le logo usurpé de la CNIL ou des fax « RGPD — Mise en conformité » invitent à appeler un numéro de téléphone pour ensuite facturer la fausse mise en conformité au règlement européen.



D'après des témoignages récents, après avoir appelé au numéro indiqué sur leur document affichant fièrement une bande bleu / blanc / rouge, ils ont posé quelques questions sur l'entreprise puis envoyé par mail un facture proforma demandant de s'en acquitter sous 72h. Les escrocs vont même jusqu'à dire qu'en payant cette facture, la CNIL fera une « levée de contrôle et de sanction » sur votre société.

Puis, une fois le paiement effectué, vous aurez un entretien de 15 minutes durant lequel 50 questions vous seront posées puis sous 30 jours un « délégué syndical du département» prendra contact et clôturera définitivement la mise a jour.

Tous ces arguments sont strictement faux !

La mise en conformité au RGPD nécessite plus qu'un simple échange ou l'envoi d'une documentation. Elle suppose un vrai accompagnement, par une personne qualifiée en protection des données personnelles, pour identifier les actions à mettre en place et assurer leur suivi dans le temps. Il est nécessaire, avant tout engagement, de chercher en ligne des informations sur la société qui prend contact avec vous. Si le doute persiste, vous pouvez contacter la CNIL au 01 53 73 22 22.

Pour vous rassurer, Denis JACOPINI et son équipe réalisent des démarches de mise en conformité des établissements avec la réglementation relative aux données à caractère Personnel depuis 2012. Plus d'informations ici

Nos conseils

Mettre en conformité nécessitera dans la plupart des cas une analyse de vos process, une sensibilisation du personnel, des interviews personnalisés et nous recommandons a minimas une rencontre. Ces organismes ne semblent pas répondre à ces recommandations.

Au regard de pratiques commerciales trompeuses, la DGCCRF et la CNIL formulent plusieurs recommandations qui visent à :

- vérifier l'identité des entreprises démarcheuses qui ne sont en aucun cas, contrairement à ce que certaines prétendent, mandatées par les pouvoirs publics pour proposer à titre onéreux des prestations de mise en conformité au RGPD ;
- vérifier la nature des services proposés :
- la mise en conformité au RGPD nécessite plus qu'un simple échange ou l'envoi d'une documentation. Elle suppose un vrai accompagnement par un professionnel qualifié en protection des données personnelles, pour identifier les actions à mettre en place et assurer leur suivi dans le temps ;
 - Dans certains cas, il peut aussi s'agir de manœuvres pour collecter des informations sur une société en vue d'une escroquerie ou d'une attaque informatique.

Principaux réflexes à avoir en cas de démarchage

Si vous recevez ce type de sollicitations, vous devez :

- demander des informations sur l'identité de l'entreprise démarcheuse permettant de faire des vérifications sur internet ou auprès des syndicats de votre profession ;
- demander le numéro SIRET de l'organisme ;
- demander les conditions générales de vente de l'organisme ou les termes du contrat que vous devrez signer ;
- consulter le site internet et vérifier les mentions légales ;
- vérifier l'ancienneté du nom de domaine (un nom de domaine récent indique la création récente du service avec un risque de manque d'expérience ou la création d'un nom de domaine spécialement pour l'arnaque.
 vous méfier de telles communications prenant les formes d'une information officielle émanant d'un service public;
- lire attentivement les dispositions contractuelles ou pré-contractuelles ;

prendre le temps de la réflexion et de l'analyse de l'offre ;

- · diffuser ces conseils de vigilance auprès de vos services et des personnels qui sont appelés à traiter ce type de courrier dans l'entreprise ;
- ne payer aucune somme d'argent au motif qu'elle stopperait une éventuelle action contentieuse…

Pour vous aider dans votre mise en conformité au RGPD, la CNIL publie des contenus pratiques. Vous pouvez notamment consulter « RGPD : ce qui change pour les pros » ainsi que le nouveau « Guide de sensibilisation pour les petites et moyennes entreprises » élaboré en partenariat avec la BPI. Pour information, voici les 6 phases recommandées par la CNIL

https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

et notre méthode de mise en conformité avec le RGPD :

- « Comment se mettre en conformité avec le RGPD ? »
- « Mise en conformité RGPD : Accompagnement personnalisé par un Expert »
- « Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants ».



Je me présente : Denis JACOPINI. Je suis Expert de justice en informatique spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel), consultant depuis 1996 et formateur depuis 1998. J'ai bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, j'ai été ensuite Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délègué à la Protection des Données, en tant que praticien de la mise en conformité et formateur.

récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur.

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

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 : Vigilance : Démarchages trompeurs « Mise en conformité RGPD » | CNIL

Illustration issue d'un témoignage

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits | Denis JACOPINI



Wi-Fi Attention au piratage sur les vrais et taux réseaux gratuits Ce sont les vacances mais nombre de touristes ne se séparent pas de leurs smartphones, tablettes ou ordinateurs portables. Et pour se connecter à l'internet, quoi de mieux qu'attraper un wi-fi gratuit. Une pratique qui peut se révéler très dangereuse. Des proies faciles pour les « sniffeurs » de données. Explications de Laurent Heslault, expert sécurité chez Symantec.

Vous êtes sur votre lieu de vacances et vous avez envie de vous connecter à l'internet. Pour consulter votre messagerie ou vos réseaux sociaux, envoyer des photos à vos proches, surfer sur le net ou consulter votre compte en banque ou faire une réservation.

Solution la plus simple : se connecter à un réseau Wi-Fi gratuit. Dans votre hôtel, camping, à la terrasse d'un café ou d'un restaurant… Les accès gratuits pullulent et se généralisent.

Expert en sécurité à Symantec, Laurent Heslault tire le signal d'alarme. « Rien de plus simple que de pirater les données qui transitent sur un réseau Wi-Fi gratuit » assure-t-il. « Par exemple, je m'installe à la terrasse d'un café et je crée un vrai faux point d'accès gratuit en empruntant le nom du café. Des gens vont s'y connecter et je n'ai plus qu'à récupérer toutes les données qui m'intéressent. Des mots de passe, des identifiants… »

Des sniffeurs de données

Il exagère ? Non. « L'expérience a été faite à la terrasse d'un café. Nous avons installé un logiciel qui permet de sniffer tous les appareils qui se branchaient sur le Wi-Fi. Ensuite, des complices, qui se faisaient passer pour des magiciens, allaient voir les gens en disant que par magie, ils avaient réussi à changer le code de leur téléphone ou leur image sur Facebook. Ils étaient étonnés ! » Rien de magique mais des logiciels de piratage qui se trouvent facilement sur le net.

Les données sur le Wi-Fi ne sont pas chiffrées

« Les données qui transitent sur le Wi-Fi ne sont pas chiffrées. Sauf quand vous vous connectés à un site sécurisé avec le protocole HTTPS. Donc ce sont des données faciles à intercepter. » Danger sur les vrais faux points d'accès Wi-Fi mais aussi sur les vrais qui ne sont, dans la grande majorité des cas, pas chiffrés non plus. « Par contre pas de problème pour une connexion 3G ou 4G qui sont chiffrées. Mais pour économiser leur forfait, les gens préfèrent se connecter au Wi-Fi ».

Conseils

Alors quels conseils ? « **Ne jamais, sur un Wi-Fi public, entrer un mot de passe. D'autant que la plupart des internautes utilisent le même mot de passe pour tous leurs sites.** » En clair, limiter les dégâts en ne consultant que des sites qui ne demandent aucune identification.

Autre solution : protéger son smartphone ou sa tablette en y installent un logiciel qui va chiffrer toutes les données qui vont en sortir. Plusieurs types de logiciels existent dont le Wi-Fi Privacy de Norton qui est gratuit pendant 7 jours et peut s'installer sur des périphériques fonctionnant sous Ios et Androïd. Article original de Samuel NOHRA.

Nous prodiguons une multitude d'autres conseils durant les formations que nous animons à destination des élus, chef d'entreprises, agents publics et salariés. [Consultez la liste de nos formations]



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 : Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

« Vous avez été en contact avec une personne testée positive au Covid-19 » : Attention aux arnaques sur les smartphones



MÉFIEZ-VOUS ! — La crise sanitaire liée à la pandémie est perçue comme une opportunité par les pirates informatiques qui jouent sur les craintes et les angoisses des citoyens pour les piéger. Attention donc si vous recevez des messages liés au Covid-19 sur votre téléphone.

A l'approche de la levée du confinement, profitant de l'inquiétude qui règne au sein de la population, les pirates informatiques agissent, multipliant fraudes et arnaques sur le web, notamment à travers la pratique de l'hameçonnage (ou « phishing » en anglais), particulièrement lucrative. Pour rappel, cette technique consiste à « piéger » une personne en le poussant à cliquer sur un lien dans le but d'installer un logiciel malveillant sur son appareil ou de collecter ses informations personnelles. ...[lire la suite]

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 : « Vous avez été en contact avec une personne testée positive au Covid-19 » : attention aux arnaques sur les smartphones | LCI