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 Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…) | Denis JACOPINI



Une « phrase de passe » est beaucoup plus difficile à pirater qu'un « mot de passe ». Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes et mettraient… plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Atlantico : Selon de nombreuses études menées par des chercheurs de l'Université américaine Carnegie-Mellon, un long mot de passe facile à retenir tel que « ilfaitbeaudanstoutelafrancesaufdanslebassinparisien » serait plus difficile à pirater qu'un mot de passe relativement court mais composé de glyphes de toutes sortes, tel que « p8)J#&=89pE », très difficiles à mémoriser. Pouvez-vous nous expliquer pourquoi ?

Denis Jacopini : La plupart des mots de passe sont piratés par une technique qu'on appelle « la force brute ». En d'autres termes, les hackers vont utiliser toutes les combinaisons possibles des caractères qui composent le mot de passe.

Donc, logiquement, plus le mot de passe choisi va avoir de caractères (majuscule, minuscule, chiffre, symbole), plus il va être long à trouver. Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes via la technique de « la force brute », et mettraient… plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Un long mot de passe est donc plus difficile à pirater qu'un mot de passe court, à une condition cependant : que la phrase choisie comme mot de passe ne soit pas une phrase connue de tous, qui sort dès qu'on en tape les premiers mots dans la barre de recherche de Google. Les pirates du Net ont en effet des bases de données où ils compilent toutes les phrases, expressions ou mots de passe les plus couramment utilisés, et essayent de hacker les données personnelles en les composant tous les uns derrière les autres. Par exemple, mieux vaut avoir un mot de passe court et complexe plutôt qu'une « phrase de passe » comme « Sur le pont d'Avignon, on y danse on y danse... ».

Il faut également bien veiller à ce que cette « phrase de passe » ne corresponde pas trop à nos habitudes de vie, car les pirates du Web les étudient aussi pour arriver à leur fin. Par exemple, si vous avez un chien qui s'appelle « Titi » et que vous habitez dans le 93, il y a beaucoup de chance que votre ou vos mots de passe emploient ces termes, avec des associations basiques du type : « jevaispromenermonchienTITIdansle93 ».

De plus, selon la Federal Trade Commission, changer son mot de passe régulièrement comme il est habituellement recommandé aurait pour effet de faciliter le piratage. Pourquoi ?

Changer fréquemment de mot de passe est en soi une très bonne recommandation, mais elle a un effet pervers : plus les internautes changent leurs mots de passe, plus ils doivent en inventer de nouveaux, ce qui finit par embrouiller leur mémoire. Dès lors, plus les internautes changent fréquemment de mots de passe, plus ils les simplifient, par peur de les oublier, ce qui, comme expliqué plus haut, facilite grandement le piratage informatique.

Plus généralement, quels seraient vos conseils pour se prémunir le plus efficacement du piratage informatique ?

Je conseille d'avoir une « phrase de passe » plutôt qu'un « mot de passe », qui ne soit pas connue de tous, et dont on peut aisément en changer la fin, pour ne pas avoir la même « phrase de passe » qui vérouille nos différents comptes.

Enfin et surtout, je conseille de ne pas se focaliser uniquement sur la conception du mot de passe ou de la « phrase de passe », parce que c'est très loin d'être suffisant pour se prémunir du piratage informatique. Ouvrir par erreur un mail contenant un malware peut donner accès à toutes vos données personnelles, sans avoir à pirater aucun mot de passe. Il faut donc rester vigilant sur les mails que l'on ouvre, réfléchir à qui on communique notre mot de passe professionnel si on travail sur un ordinateur partagé, bien vérrouiller son ordinateur, etc...

Article original de Denis JACOPINI et Atlantico

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger**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



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 : Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…) | Atlantico.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

Comment sécuriser Firefox efficacement en quelques clics de souris ?



Vous utilisez Firefox est vous souhaitez que cet excellent navigateur soit encore plus sécurisé lors de vos surfs sur Internet ? Voici quelques astuces qui supprimerons la géolocalisation, le profilage de Google ou encore que vos données offline disparaissent du regard d'espions locaux.

C'est sur le blog des Télécoms que j'ai vu pointer l'information concernant le réglage de plusieurs paramètres de Firefox afin de rendre le navigateur de la fondation Mozilla encore plus sécurisé. L'idée de ce paramétrage, empêcher par exemple Google de vous suivre à la trace ou de bloquer la géolocalisation qui pourrait être particulièrement big brotherienne.

Commençons par du simple. Il suffit de taper dans la barre de navigation de votre Firefox la commande about:config. Une alerte s'affiche, pas d'inquiétude, mais lisez là quand même. recherchez ensuite la ligne security.tls.version. Les valeurs affichées doivent osciller entre 1 et 3. Ensuite, recherchez la ligne geo.enabled pour annuler la géolocalisation. Passez le « true » en « False ». Pour que les sites que vous visitiez ne connaisse pas la dernière page que vous avez pu visiter, cherchez la ligne network.http.sendRefererHeader et mettre la valeur 1. Elle est naturellement placée à 2. Passez à False la ligne browser.safebrowsing.malware.enabled.

Ici, il ne s'agit pas d'autoriser les malwares dans Firefox, mais d'empêcher Google de vous tracer en bloquant les requêtes vers les serveurs de Google. Pour que Google cesse de vous profiler, cherchez la ligne browser.safebrowsing.provider.google.lists et effacez la valeur proposée.

Pour finir, vos données peuvent être encore accessibles en « offlire », en mode hors connexion. Cherchez les lignes offline-apps.allow_by_default et offline-apps.quota.warn. La première valeur est à passer en Fasle, la seconde valeur en 0.

Il ne vous reste plus qu'à tester votre navigateur via le site de la CNIL ou celui de l'Electronic Frontier Foundation.

Article original de Damien Bancal



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 : Sécuriser Firefox efficacement en quelques clics de souris — Data Security BreachData Security Breach 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

Compte Facebook piraté : Quelles sont les bons réflexes à avoir ? | Denis JACOPINI

21



Il arrive parfois de se faire pirater son compte Facebook. Soit parce qu'on a oublié de se déconnecter du site sur un ordinateur public, soit parce qu'on s'est fait voler d'une manière ou d'une autre son mot de passe. Il arrive aussi que des personnes se fassent passer pour vous et ouvrent un profil à votre nom avec vos informations et photos personnelles.

Dans ces cas de piratage ou d'usurpation d'identité, il importe de réagir rapidement pour empêcher toute possibilité de nuisance. Première chose à faire : signaler le compte piraté ou usurpé à Facebook.

Si votre compte a été piraté



Rendez-vous sur la page Signaler un compte piraté.

Indiquez l'identifiant de votre compte puis suivez les instructions. Vous serez notamment amené à taper votre ancien mot de passe et Facebook vous posera quelques questions pour vérifier votre identité.

Dans le pire des cas, vous pourrez faire appel à contacts de confiance pour récupérer votre compte.

Si votre identité (ou celle d'une autre personne) a été usurpée

Rendez-vous sur la page du profil suspicieux et cliquez sur le bouton contenant 3 petits points, juste en dessous de la photo de couverture. Sélectionnez Signaler.



Dans la fenêtre qui s'affiche alors, sélectionnez l'option Signaler ce compte et cliquez sur Continuer.



Dans l'écran suivant, sélectionnez ensuite l'option Ce journal se fait passer pour quelqu'un que je connais.



Vous êtes amené ensuite à préciser votre cas.



S'il s'agit de votre propre identité, sélectionnez l'option Moi. Vous pouvez alors demander à fermer le compte.

Si l'identité de quelqu'un d'autre a été usurpée, sélectionnez l'option Une personne que je connais ou éventuellement Une célébrité.

Cliquez sur Continuer pour valider et suivez les instructions.

Aller plus loin et porter plaine

Si vous estimez qu'il y a préjudice, vous pouvez aller porter plainte au Commissariat de police ou à la Gendarmerie de votre lieu d'habitation. N'hésitez pas à faire des captures d'écran pour nourrir votre dossier.

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 protection juridique du chef d'entreprise.

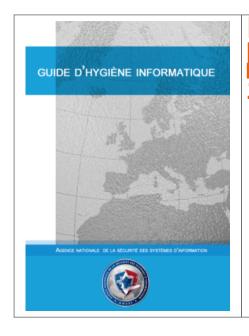
Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire…

Source : http://www.aussitot.fr/facebook/signaler-compte-pirate-usurpation-identite-facebook.html

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/

Votre responsabilité engagée en cas de piratage de vos données | Denis JACOPINI



Votre responsabilité engagée en cas de piratage de vos données



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



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