

Nos ordinateurs ont-ils la mémoire courte ? Vidéo



Nos
ordinateurs
ont-ils la
mémoire
courte ?
Vidéo

Que trouveront les archéologues du futur, d'ici quelques siècles ou quelques milliers d'années ? Des pierres taillées du paléolithique, des hiéroglyphes, des rouleaux de parchemins probablement, des livres peut-être.

Quelles images, quels sons, quels écrits de notre société restera-t-il dans 2000 ans ? Auront-ils résisté aux épreuves du temps et aux mutations technologiques comme l'ont fait la première photo, le premier film, le premier enregistrement sonore. Mais que deviendront les milliards d'informations engrangées dans les disques durs qui se démagnétisent, et sur les CD ou DVD, qui redoutent la lumière du soleil ?[lire la suite]

LE NET EXPERT

:

- **MISE EN CONFORMITÉ RGPD / CNIL**
- AUDIT RGPD ET CARTOGRAPHIE de vos traitements
- MISE EN CONFORMITÉ RGPD de vos traitements
- SUIVI de l'évolution de vos traitements
- FORMATIONS / SENSIBILISATION :
 - CYBERCRIMINALITÉ
- PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (réécupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité, Recherche de preuves et en Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

Attention, l'employeur peut lire les SMS des téléphones professionnels | Denis JACOPINI

23

Attention, l'employeur peut lire les SMS des téléphones professionnels

Une décision de la Cour de cassation permet désormais à une entreprise de lire les messages reçus et envoyés sur un téléphone professionnel. Comme elle pouvait déjà le faire avec les e-mails. ☒
Gare aux sanctions si vous refusez l'accès à vos SMS à votre employeur.

Appelée à statuer sur le litige opposant deux sociétés de courtage, la Cour de cassation a pris une décision qui va concerner des centaines de milliers de salariés : elle a validé le principe selon lequel les SMS envoyés ou reçus par un téléphone mis à la disposition par une entreprise sont « présumés avoir un caractère professionnel ». Par conséquent, les employeurs sont autorisés à lire ces messages, même hors de la présence des salariés.

« Cet arrêt est dans la droite ligne de décisions prises depuis quelques années, nous explique Olivier Iteanu, avocat à la cour d'appel de Paris. Peu à peu la jurisprudence en vient à plus protéger l'entreprise que le salarié. »

L'avocat rappelle ainsi qu'en 2012, un employeur avait été autorisé à consulter le contenu de la clé USB d'un salarié car celui-ci l'avait branchée sur le système informatique de l'entreprise. Un an plus tard, la Cour de cassation confirmait que les employeurs pouvaient consulter les e-mails de la boîte professionnelle de leurs salariés, même hors de leur présence, s'ils n'étaient pas identifiés comme personnels.

Concrètement, grâce à la décision prise en ce mois de février 2015, un employeur ayant « un motif légitime » peut vérifier les SMS en prenant le téléphone de son salarié ou « placer, en passant par des outils de Mobile Device Management (gestion de terminaux mobiles), des logiciels qui vont monitorer ce qui se passe sur le smartphone, pour en extraire les SMS qui pourront être analysés », nous précise Jean Pujol, manager au sein de l'entité conseil en stratégie SI du cabinet Kurt Salmon. « Les SMS peuvent aussi être stockés sur des serveurs centraux, comme cela était le cas dans l'affaire jugée par la Cour de cassation. »

Refuser le contrôle entraînera une sanction

Pour Me Martine Ricouart-Maillet, vice-présidente de l'Association française des correspondants à la protection des données personnelles et associée au sein du cabinet BRM Avocats, « afin d'éviter tout litige, le salarié doit être informé de l'usage qu'il peut faire des outils mis à sa disposition dans la charte informatique de l'entreprise. Cette charte doit aussi l'avertir des moyens de surveillance dont dispose son employeur. »

« Et s'il refuse de se soumettre à ce contrôle, ajoute Me Iteanu, le salarié pourra être sanctionné. » La sanction « suprême » étant le licenciement. Pour lui, cette décision risque d'induire des comportements abusifs de la part de certains employeurs. « Les juges devront très probablement se saisir de cas pour rétablir l'équilibre entre les parties », estime-t-il.

La seule solution pour protéger certains SMS est de les identifier comme personnels. Même si cela n'interdit pas à l'employeur de les lire, cela l'empêche de les utiliser contre un employé. Autre méthode, plus radicale : disposer de deux appareils, un professionnel et un personnel.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source :

<http://www.01net.com/editorial/646337/attention-votre-employeur-va-pouvoir-lire-les-sms-de-votre-telephone-pro/>
Par Cécile Bolesse

Piratage de ses comptes sociaux : prévenir, repérer

et réagir | Denis JACOPINI

Piratage de ses comptes sociaux : prévenir, repérer et réagir !

Sur les réseaux sociaux, la plus grande vigilance est requise si l'on veut protéger ses données personnelles.

Les réseaux sociaux se multipliant de façon considérable, il convient de se montrer attentif à la protection des données personnelles, car ces dernières peuvent d'autant plus facilement être piratées.

A ce titre, la Commission nationale de l'informatique et des libertés (CNIL) publie une fiche pratique, agrémentée de liens directs vers les principaux réseaux sociaux, afin de mettre en oeuvre le contrôle des données personnelles.

Parmi les conseils donnés par la Commission, citons :

- le choix de mots de passe complexes, mais aussi différents les uns des autres, et avec un sens n'ayant aucun rapport avec une donnée personnelle relative à la vie privée du titulaire du compte (comme une date de naissance, etc...) ;
- l'absence totale de communication du mot de passe à une tierce personne ;
- l'activation d'un dispositif d'alerte en cas d'intrusion (dans ce cas, la personne titulaire du compte et qui se connecte depuis un poste informatique inconnu doit confirmer l'accès en entrant un code, reçu préalablement par sms ou par mail) ;
- la déconnexion à distance des terminaux encore liés au compte ;
- la désactivation des applications tierces encore connectées au compte ;
- le réglage précis des paramètres de confidentialité.

En outre, la CNIL donne des astuces pour repérer le piratage d'un compte. Des signes doivent en effet alerter l'utilisateur, par exemple un mot de passe invalide, ou des comportements inhabituels ayant lieu sur le compte, sans consentement préalable (comme suivre, se désabonner, ou encore bloquer...).

En cas de piratage, il convient donc :

- en premier lieu, de signaler le compte piraté auprès du réseau social ;
- cette première étape franchie, il convient alors de demander une réinitialisation du mot de passe. Si la réponse apportées par les modérateurs du réseau n'est pas satisfaisante, la CNIL peut être saisie.

Consultez la fiche pratique de la CNIL

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 plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.net-iris.fr/veille-juridique/actualite/34642/comment-prevenir-le-piratage-de-son-compte-en-ligne.php>
© 2015 Net-iris

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

Wi-Fi.
Attention
au
piratage
sur les
vrais et
faux
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 Heslaut tire le signal d'alarme. « Rien de plus simple que de pirater les données qui transitingent 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 transitingent sur le Wi-Fi ne sont pas chiffrées. Sauf quand vous vous connectez 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

Mon employeur peut-il enregistrer ou écouter mes conversations téléphoniques à mon insu ? | Denis JACOPINI

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité informatique - Cybercriminalité</p> <p>vous informe...</p>	<p>Mon employeur peut-il enregistrer ou écouter mes conversations téléphoniques à mon insu ?</p>
<p>Un employeur n'a le droit ni d'enregistrer ni d'écouter les conversations téléphoniques de ses employés s'ils n'en sont pas informés. S'il le fait, il commet un délit et risque des sanctions pénales.</p>	
<p>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</p>	
<p>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</p>	
<p>Cet article vous plaît ? Partagez ! Un avis ? Laissez-nous un commentaire !</p> <p>Source : http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=4FBDF806985B62BC62EB3DEBC567BF6F?name=Mon+employeur+peut-il+enregistrer+ou+%C3%A9couter+mes+conversations+t%C3%A9l%C3%A9phoniques+%C3%A0+mon+insu+%3F&id=106</p>	

Comment savoir si je suis fiché au FNAEG (Fichier national des empreintes

génétiques) ? | Denis JACOPINI



Comment savoir si je suis fiché au #FNAEG (#Fichier national des empreintes génétiques) ?

Pour avoir ces informations, vous devez écrire (en joignant une copie d'une pièce d'identité) à l'adresse suivante :
Directeur central de la police judiciaire
Ministère de l'Intérieur
11 Rue des Saussaies
75800 Paris Cedex 08
Si vous n'avez pas de réponse dans un délai de 2 mois ou si votre demande est refusée, vous pouvez adresser une plainte à la CNIL ou porter plainte auprès des services de police, de gendarmerie ou du procureur de la République.
L'effacement de votre inscription est possible dans certains cas, en vous adressant au procureur de la République du Tribunal de grande instance compétent.

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 91 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 plaît ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
[http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=65372FC5C6502D0A6ED2239F1706AE63?name=FNAEG+\(Fichier+national+des+empreintes+g%C3%A9n%C3%A9tiques\)+%3A+comment+savoir+si+je+suis+fich%C3%A9+id=256](http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=65372FC5C6502D0A6ED2239F1706AE63?name=FNAEG+(Fichier+national+des+empreintes+g%C3%A9n%C3%A9tiques)+%3A+comment+savoir+si+je+suis+fich%C3%A9+id=256)

Windows 10 : Identifier les applications malveillantes à partir des services par

défaut | Denis JACOPINI

Windows 10 Identifier les malveillantes à partir des applications par défaut

[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"]

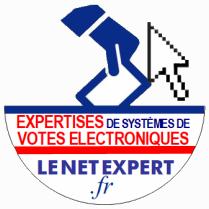
Source

: <https://www.winhelponline.com/blog/windows-10-default-services-configuration>

Mon ordinateur ou mon téléphone est-il espionné ? Des informations me sont-elles volées ? | Denis JACOPINI



LE NET EXPERT
AUDITS & EXPERTISES



EXPERTISES DE SYSTEMES DE
VOTES ELECTRONIQUES
LE NET EXPERT
.fr



RGPD CYBER
LE NET EXPERT
MISES EN CONFORMITE



SPY DETECTION
Services de détection
de logiciels espions



LE NET EXPERT
FORMATIONS



LE NET EXPERT
ARNAQUES & PIRATAGES



Mon ordinateur ou mon téléphone est-il espionné ? Des informations me sont-elles volées ?

Original de l'article mis en page : Comment se protéger contre la fuite d'informations avec le départ des collaborateurs ? – Lexsi Security Hub

Comment bien sécuriser ses e-mails ? | Denis JACOPINI

Peut-on encore se passer de l'e mail dans le cadre de nos activités professionnelles ? Je ne le crois pas. Il est pratique et instantané. Cependant, peu sécurisé en standard, sans précautions, il pourrait bien vous attirer des ennuis.

Selon une étude récente de SilverSky, Email Security Habits Survey Report, 53 % des employés ont déjà reçu des données sensibles d'entreprise non cryptées par e mail ou en pièces jointes, que 21 % des employés déclarent envoyer des données sensibles sans les chiffrer et que 22 % des entreprises sont concernées chaque année par la #perte de données via e-mail.

Inquiétant vous direz-vous ? Catastrophique quand on sait que tout détenteur de données à caractère personnel est tenu à la sécurisation de ces données, conformément à la loi informatique et libertés, encadrée par la CNIL.

Et c'est encore pire quand on prend en compte les informations soumises au secret professionnel ou revêtues de confidentialité que nous échangeons quotidiennement... (plus de 100 milliards d'e-mails sont échangées chaque jour...)

Un des derniers incidents en date : la récente #divulgation des numéros de passeport de 31 leaders mondiaux...

Malgré l'évolution du contexte législatif il est bien étonnant que les entreprises ne soient pas plus nombreuses à choisir de sécuriser leurs échanges par e-mail.

Des solutions ?

Oui, heureusement, et je vais partager avec vous mes conseils :

Mettez en place des procédés de signature numérique et le chiffrement des e-mails garantissent la confidentialité d'un message.

Vous évitez ainsi que des données sensibles ne tombent dans de mauvaises mains.

Avantage pour le destinataire : l'assurance de l'identité réelle de l'expéditeur de l'e-mail et que le contenu du message n'a pas été modifié après son envoi.

L'utilisation simultanée de ces procédés vous permettront ainsi de répondre à un besoin de Confidentialité (par le chiffrement) et un besoin d'Intégrité (par la signature électronique).

Enfin, aucun de ces deux procédés vous assurera une protection contre la fuite d'informations ou de données confidentielles à votre insu. Pour cela, nous vous recommandons d'utiliser des système de « Protection contre la fuite des données » ou de « Data Leak Protection ».*

Plus d'info sur la confidentialité des e-mails ici

Nous vous conseillons les ouvrages suivants :

Guide de la survie de l'Internaute



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

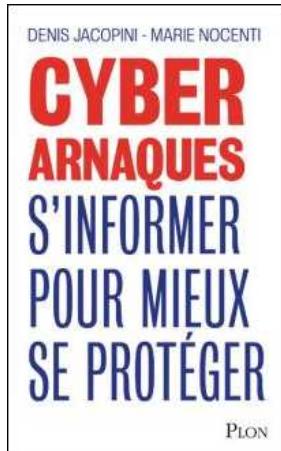
Anti-Virus-Pack PC Sécurité



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

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

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



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

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

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

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

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

Commandez sur Fnac.fr

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

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

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

**Hotspot Shield le logiciel
VPN pour Windows MacOs IOS**

Android Apple Samsung pour accéder de manière sécurisée à un Wifi public | Denis JACOPINI

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

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

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

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

LA SOLUTION ?

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

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

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

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

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

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

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

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

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

Téléchargez et testez gratuitement HotSpot Shield



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

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