# Le livre du jour : CYBERARNAQUES — a l'écoute des livres, Radio Massabielle (97.8 Mhz et 101.8 Mhz)



Comme les langues d'Esope, Internet peu être la meilleure et la pire des choses. En effet s'il permet de relier les femmes et les hommes à travers le monde, de travailler, de s'informer, etc.. il es également le point de toutes sortes d'escrocs. Aussi, en répondant à une annonce ou au message que vous pensez être envoyé par un ami, vous risquez de voir votre compte en banque vidé ou d'être victime d'un chantage. Les CYBERARNAQUES sont légion et il convient de s'informer pour mieux protéger votre famille et vos biens. Combien d'entre-nous n'on pas vérifié…[lire la suite]

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



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



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

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

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

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances

similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître ! Commandez sur Fnac.fr https://www.youtube.com/watch?v=lDw3kI7ra2s

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

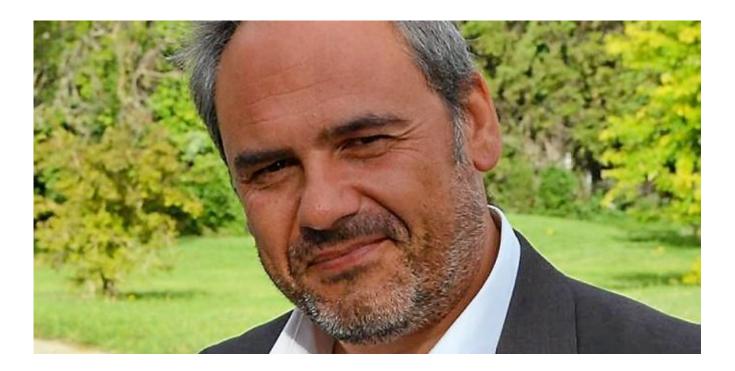
Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj\_HKcbzRuvIPdu3FktA

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

Commandez sur Fnac.fr

Source : Le livre du jour : CYBERARNAQUES — a l'écoute des livres

## Comment empêcher Android de

# sauvegarder automatiquement nos données personnelles ?



Nos smartphones et tablettes Android sauvegardent certaines de nos données personnelles sur les serveurs de Google sans forcément nous demander notre avis. Un système qui peut s'avérer aussi pratique pour certains qu'il peut être dérangeant pour d'autres. Encore faut-il savoir quelles sont les données sauvegardées par Google et celles qui ne le sont le pas. Nous allons donc aujourd'hui nous pencher sur la question.



N'avez-vous jamais remarqué que lorsque vous entrez-vos identifiants Google dans un nouvel appareil Android, ce dernier retrouvait automatiquement certaines de vos informations personnelles, notamment vos contacts. Pourtant, vous n'avez jamais rien fait pour, et pour cause puisque cette option est activée par défaut. Ce qui signifie que vous pouvez également la désactiver. La plupart des utilisateurs la conservent néanmoins activée pour des raisons de praticité.

Il faut dire que cette sauvegarde automatique peut s'avérer utile lorsque vous changez de smartphone, lorsque vous disposez de plusieurs appareils Android ou si par malheur, vous vous faisiez voler votre téléphone. Mais certains ne veulent pas que leur vie privée se retrouve sur le cloud de Google. Ce tutoriel est pour eux mais avant de passer à la pratique, un peu de théorie.

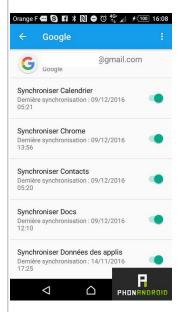
Les données automatiquement sauvegardées par Google Au sein de son OS, Google a intégré un outil du nom d'Android Backup Service qui sauvegarde certaines données liées aux services que vous utilisez. Ces données sont les suivantes :

- · Contacts qui sont sauvegardés au sein de Google Contacts. Vous pouvez ainsi les retrouver sur tous vos appareils et même sur votre PC en vous connectant simplement à votre compte.
- Emails qui sont sauvegardés au sein de Gmail
- Documents, ce qui vous permet d'ailleurs d'éditer vos documents sauvegardés dans le cloud à partir de n'importe lequel de vos appareils
- Calendriers
- Chrome : vos favoris et votre historique de navigation sont synchronisés avec votre compte. Idem pour vos mots de passe si vous avez activé la fonction Smart Lock
- Hangouts : vos conversations sont sauvegardées
- Google Play Store : les applications que vous avez téléchargées sont automatiquement sauvegardées. Vous pouvez ensuite les retrouvez dans l'onglet « Mes applications » de la boutique. C'est très pratique lorsque vous changez de smartphone car vous n'avez pas besoin de les rechercher une par une, en outre, les applications achetées sont également sauvegardées
- Vos photos et vidéos, à condition d'utiliser l'application Google Photos et d'avoir activé la sauvegarde automatique de vos médias
- Certaines données d'applications

### Comment empêcher Google de sauvegarder vos données

Vous n'êtes pas ravis à l'idée que Google en sache autant sur vous et vous souhaiteriez que certaines de vos données ne soient pas sauvegardées ? Et bien rassurez-vous, c'est possible et en quelques clics. Il vous suffit pour cela de :

- Vous rendre dans le menu Paramètres > Personnel > Comptes de votre smartphone
- Sélectionner votre compte Google
- Décocher toutes les données que vous ne voulez pas que Google sauvegarde



Et pour aller plus loin, n'hésitez pas à jeter un œil à notre tutoriel comment préserver sa vie privée sur Android.

### Les données non sauvegardées par Google

Les données listées ci-dessous ne sont pas sauvegardées par Google. Pour éviter de les perdre en changeant de smartphone, il faudra donc utiliser une application tierce mais nous y viendrons après.

- Les SMS, il est néanmoins possible de sauvegarder ses SMS sur Android en utilisant une application
- Google Authentificator : pour des raisons de sécurité, les données d'authentification Google en deux étapes ne sont pas sauvegardées
- Réglages : les paramètres personnalisés de de votre smartphone ne sont pas sauvegardés
- Bluetooth : Android ne synchronise pas les périphériques Bluetooth appairés vers votre smartphone

### Comment sauvegarder toutes ses données personnelles

Bien que Google ne le permette pas par défaut, il est tout à fait possible de sauvegarder toutes les données de votre smartphone Android à l'aide de notre précédent tutoriel. Certaines de vos données iront directement sur votre support externe, d'autres seront sauvegardées en ligne afin de pouvoir ensuite être réintégrées à votre nouveau smartphone si votre but est de sauvegarder vos données pour les retrouver sur un nouvel appareil.

N'oubliez pas non plus de jeter un œil à notre sélection d'applications pour sauvegarder ses données personnelles. Certaines nécessiteront que votre téléphone soit rooté, d'autres non, et elles vous permettront de sauvegarder toutes vos applications et pas seulement les données.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.









Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec 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, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de mise en conformité avec le RGPD.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





### Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles

### en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

Source :

http://www.phonandroid.com/comment-empecher-android-sauvegarde
r-automatiquement-donnees-personnelles.html

# Denis JACOPINI sur LCI : Les techniques des cybercriminels pour pirater votre CB





# Denis JACOPINI sur LCI : Les techniques des cybercriminels pour pirater votre CB

Denis Jacopini, expert informatique assermenté spécialisé en cybercriminalité, explique que quoi que l'on fasse, les fraudeurs auront une longueur d'avance. Néanmoins, il y a des failles dans le système, et en particulier au niveau du cryptogramme visuel.

En direct sur LCI avec Serge Maître Maître, président de l'AFUB (Association Française des Usagers des Banques) et Nicolas CHATILLON, Directeur du développement-fonctions transverses du groupe BPCE et Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité débattent le 7 mars 2016 sur les techniques des cybercriminels pour vous pirater votre CB.









http://lci.tfl.fr/france/societe/cartes-bancaires-les-fraudeurs-ont-toujours-une-longueur-d-avance-8722056.html

Une liste non exhaustive avec 10 techniques de cybercriminels pour vous pirater votre carte bancaire : http://www.lenetexpert.fr/10-techniques-de-cybercriminels-pour-vous-pirater-votre-carte-bancaire/

[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 (Symantec) 13,8 Milions de victimes Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj\_HKcbzRuvIPdu3FktA

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

Commandez sur Fnac.fr

Source : Cartes bancaires : « Les fraudeurs ont toujours une longueur d'avance » — Société — MYTF1News

### Voici 320 millions de mots de

# passe … à éviter pour votre cybersécurité !



Le spécialiste en sécurité informatique Troy Hunt a mis à disposition un nouvel outil recensant 320 millions de mots de passe corrompus. Une base de données impressionnante qui devrait limiter de futurs impairs.

Boites mail corrompues, comptes piratés… chaque jour les cas se multiplient : virus et hackers sont bien présents, et ce, partout sur la toile. Personne n'est à l'abri et sans le savoir, vous utilisez peut-être vous-même un mot de passe corrompu. L'expert en sécurité informatique Troy Hunt en a détecté 320 millions!

Sur son site *Have I been pwned* ?, il était déjà possible de savoir si un compte avait été compromis. En indiquant son adresse mail ou son nom d'utilisateur, sans révéler le mot de passe associé, vous pouvez savoir si votre compte a été piraté et fait l'objet d'une fuite de données.

Depuis ce jeudi, le site propose désormais l'outil inverse : une collection de 320 millions de mots de passe consultables, déjà compromis, sans les identifiants associés. Car avec la multiplication des fuites de données, mieux vaut être armé. La CNIL conseille ainsi d'utiliser au moins 12 caractères et 4 types différents (minuscules, majuscules, chiffres et caractères spéciaux). Il faut également en changer régulièrement…[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 : Cyber-sécurité : voici 320 millions de mots de passe ... à éviter ! — LCI

## Pouvez-vous refuser la carte sans contact délivrée par votre banque ? | Denis JACOPINI



La Cnil rappelle que les banques doivent informer leurs clients que leur carte bancaire dispose de la fonction paiement sans contact, une option que ces derniers sont libres de refuser.

En France, plus de 33 millions de cartes de paiement ont des fonctionnalités sans contact, ce qui représente plus de 50 % des cartes en circulation, rappelle la Cnil (Commission nationale de l'informatique des libertés). Grâce à ce système, il est possible d'utiliser sa carte bancaire sans avoir à taper son code secret lorsque les achats sont inférieurs à 20 euros. Depuis la recommandation de la Cnil de juillet 2013, les porteurs de ce type de carte doivent être clairement informés de la fonctionnalité sans contact et doivent pouvoir la refuser.

Comment exercer son droit d'opposition ?

Dans un premier temps, le client doit se tourner vers sa banque pour lui demander la désactivation ou la réédition gratuite d'une nouvelle carte dépourvue de la fonctionnalité paiement sans contact.

Les banques sont libres de choisir les moyens à engager pour respecter ce droit d'opposition. Certaines proposent de distribuer une nouvelle carte identique aux anciens modèles, d'autres incitent à une désactivation via le site internet de la banque.

Si la banque ne respecte pas son devoir d'information ou si elle refuse de désactiver le paiement sans contact, le client peut alors s'adresser au service des plaintes de la Cnil, sur le site internet de la Commision, en appelant le 01 53 73 22 22 (du lundi au vendredi de 10h à 12h et de 14h à 16h) ou en écrivant un courrier à la Cnil – Service des plaintes – 8, rue Vivienne – CS 30223- 75083 Paris cedex 02

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



DÉSIGNATION N° DPO-15945





# Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec 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, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





### Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

# Comment bâtir et préserver son e-réputation ? | Denis JACOPINI



A l'heure où les médias ne détiennent plus le monopole de l'information, il serait dangereux de penser qu'on arrive à bâtir, maîtriser et préserver sa réputation sans tenir compte d'Internet qui accélère, modifie, invente, et déstabilise les acquis. Etre capable de préserver son e-réputation nécessite donc de modifier ses repères, faire preuve d'humilité, contrôler ses tribus et ses communautés, adapter ses messages, et redoubler de vigilance. Car, si bâtir une bonne réputation demande du temps et de l'investissement, son anéantissement peut s'effectuer en quelques jours.

L'e-réputation est déterminée par la circulation sur le Web d'informations, d'échanges, d'avis, de commentaires, d'articles, de rumeurs qui forgent une opinion commune. L'identité d'une marque telle qu'elle est diffusée à ses différents publics par tous les moyens de médiatisation, ajoutée à la perception que les internautes en ont, créé l'e-réputation. Avec plusieurs milliards de contenus diffusés et partagés chaque jour rien que sur Facebook, la réputation d'une marque ou d'une enseigne échappe totalement à son contrôle.

Si le site de l'enseigne est le premier vecteur de la création de l'e-réputation, elle se forge aussi via son personnel interne, des articles publiés sur les sites de médias importants, les informations diffusées sur les blogs d'influence, les forums, les réseaux sociaux, les libres commentaires sur les sites communautaires, mais aussi via des plateformes de vidéo et photos.

### Rester accessible évite le dénigrement

La majeure partie des problèmes d'e-réputation vient du fait que l'enseigne ne donne pas la possibilité à un client mécontent d'entrer directement et rapidement en contact avec elle. Dépité et frustré, il se tourne alors vers des canaux simples d'accès tels que Twitter, des blogs ou des sites de consommateurs. Afin d'éviter ce genre de dérive, il faut afficher clairement toutes les informations de contacts et non pas un simple formulaire, et apporter rapidement des solutions au client insatisfait. Un portail Web de service client peut aider à fluidifier l'information.

### Créer du contenu positif

Diffuser des messages qui inspirent la sympathie, valoriser les produits par des témoignages utilisateurs, donner la possibilité d'ajouter des avis, ou encore certifier les modes de paiement… autant de moyens servant à sensibiliser et fidéliser une communauté. En pratiquant une politique de marketing social, les consommateurs « heureux » prennent le pouvoir, défendent la marque, se diffusent entre eux les bons plans, les promotions, les nouveautés et donc contribuent à bâtir comme une trainée de poudre la e-réputation. Mais attention, dans ce cas, à ne pas perdre le contrôle de son image !

### S'emparer du contenu négatif

Les clients mécontents redoublant d'imagination pour faire savoir à un plus grand nombre les problèmes rencontrés avec une marque, ou par pure volonté de nuire, n'hésitent pas à créer des blogs, voire même des sites structurés portant l'URL de l'enseigne suivi d'un terme de type « problèmes » : www.nomdelenseigne-problemes.com .

Acheter des noms de domaine négatifs permet de recenser en un clic la mauvaise réputation car au final vous offrez aux mécontents la possibilité de s'exprimer tout en maîtrisant les problématiques.

Plus simple, créez une page « Foire aux questions » ou « service clients » et engagez-vous à répondre aux critiques ou aux avis négatifs dans un délai raisonnable. Pour garder le client, un geste commercial peut montrer de la considération à son égard et faire basculer du négatif au positif.

Enfin, un démenti public contre une rumeur permet de retrouver une forme de crédibilité et d'afficher une grande transparence dans sa manière de fonctionner.

### Pratiquer la technique de l'enfouissement

Trop, c'est trop ! Si de nombreux commentaires négatifs apparaissent sur les premières pages de Google ou autre moteur de recherche lorsqu'on tape votre nom, il est vraiment temps de réagir ! Il faut alors pratiquer la technique dite « de l'enfouissement » qui consiste à créer du contenu positif pour faire baisser dans le référencement tous les liens négatifs. Il est en effet assez rare qu'un internaute dépasse la page 3 ou 4 lorsqu'il souhaite se renseigner sur une marque.

Une politique suivie de Relations Presse aide aussi à diffuser du contenu porteur, à crédibiliser l'offre, à redorer son blason et à nettoyer la toile.

Si la liberté d'expression permet de faire, défaire et refaire des réputations, il faut se dire que c'est une grande richesse. Alors pourquoi se contenter d'être simplement populaire alors qu'il est possible aujourd'hui de devenir influent.

## 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"]

# Wifi gratuit: Attention à vos données personnelles!





### Wifi gratuit: Attention à vos données personnelles

Les utilisateurs de réseaux de wifi du monde entier ne sont pas à l'abri du danger. D'après une enquête réalisée par Norton by Symantec, la grande majorité des internautes de l'Hexagone adoptent des comportements dangereux pour leur sécurité comme pour leur confidentialité.

### Les Français parmi les mauvais élèves

Un sondage a été réalisé par Norton by Symantec sur un échantillon de 1 000 personnes environ dans chacun des 15 pays supervisés, dont la France et les Etats-Unis. L'enquête a tenté de mettre en avant les dangers d'une connexion à des réseaux de wifi gratuit. Il a été révélé que les internautes prennent de très gros risques pour leur sécurité et leur confidentialité par le biais du troc connexion-information. Ce dernier se manifeste sous plusieurs formes : adresse email à fournir, coordonnées, géolocalisation à accepter ou encore publicité à voir. Selon l'étude, la quasi-totalité des internautes de l'Hexagone (87%) ne cesse de multiplier les comportements dangereux pour leur sécurité comme pour leur confidentialité.

# Les comportements dangereux des mobinautes

L'étude a mis en avant le comportement des internautes du monde entier. Ainsi, 43% des sondés sont impatients de se connecter à peine installés au restaurant, au café, à l'hôtel, dans un magasin ou même chez un ami. Plus encore, l'envie est si pressante que 25% avouent avoir déjà tenté de se connecter sans la permission du propriétaire du réseau. Les 7% ont déjà tenté de pirater ou deviner le mot de passe (7%), rapporte *LCI*. Pour avoir une bonne **connexion**, 55% des personnes enquêtées accepteraient de fournir n'importe quelle information...[lire la suite]

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 (Symantec) 13,8 Milions de victimes Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj\_HKcbzRuvIPdu3FktA

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

### Commandez sur Fnac.fr

Source

http://www.linfo.re/magazine/high-tech/722259-wifi-gratuit-hal te-a-vos-donnees-personnelles »>Wifi gratuit: attention à vos données personnelles! — LINFO.re — Magazine, High-Tech Existe-t-il quelques mesures simples pour éviter que de mon ordinateur et mes boites mail se fassent pirater ? |
Denis JACOPINI



Il est très difficile de savoir si un ordinateur est piraté / piratable ou pas. Qu'il soit PC ou Mac, il possède ses failles qui peuvent sans limite être exploitées.

Il n'y a plus beaucoup de protections qui résistes aux plus grands hackers.

La divulgation de documents dévoilant les techniques qu'utilise la NSA pour nous espionner (c.f. http://www.lenetexpert.fr/les-10-outils-les-plus-incroyables-utilises-par-la-nsa-pour-nous-espionner-le-net-expert-informatique) et les dessous de société d'espionnage informatique Hacking Team récemment piratée (c.f. http://www.lenetexpert.fr/les-dessous-de-la-societe-despionnage-hacking-team-le-net-expert-informatique) nous ont récemment démontré qu'il n'y a aucune

limite au piratage.

### Mais alors, comment se protéger ?

Comme pour votre maison ou votre appartement, il n'existe aucun moyen d'empêcher les voleurs de rentrer. Les moyens qu'ils utiliseront seront généralement à la hauteur de l'intérêt qu'ils y trouveront.

Cependant, les conseils que je peux donner, sont comme pour les moyens de protection de vos habitions. Au plus on met des barrières de sécurité, au plus on retarde l'intrusion et au plus on décourage l'auteur. Il sera en effet plus difficile de rentrer chez vous si vous avez la dernière serrure de protection avec les volets anti-effraction dernier cri, avec une alarme ultra perfectionnée etc. plutôt qu'un simple cadenas pour vous protéger.

### Pour sécuriser un système informatique

1) J'analyse généralement ce qui, dans nos habitudes quotidiennes correspond à une attitude numérique dangereuse ou irresponsable. Pour cette phase, il est difficile de vous dire quoi faire exactement, puisque c'est généralement notre expérience, nos connaissances passées et notre intuition qui servent à produire une bonne analyse.

2) La phase suivante va consister à détecter la présence d'espions dans votre ordinateur. Compte tenu que la plupart des outils d'espionnage sont capables de détecter qu'on est en train de les détecter, vaut mieux déjà, faire des sauvegardes, puis couper d'internet votre appareil (du coup, il sera nécessaire de télécharger les logiciels de détection à partir d'un autre ordinateur, et les copier sur l'ordinateur à analyser à partir d'une clé USB par exemple). Cette phase de détection est très difficile. En effet, les logiciels espions, programmés pour espionner ce que vous tapez au clavier, ce que voit votre webcam ou entend votre micro, sont aussi programmés pour ne pas être détectés.

Le dernier outil connu pour réaliser une détection de logiciels espions est le logiciel Detekt. Ce logiciel a pour but de détecter des logiciels espions (spywares) sur un système d'exploitation Windows.

Les spywares actuellement détectés sont :

- DarkComet RAT;XtremeRAT;BlackShades RAT;
- BlackShades RAT;njRAT;
- FinFisher FinSpy;HackingTeam RCS;
- ShadowTech RAT;
- Gh0st RAT.

Attention, car les développeurs de ce logiciels précisent cependant :

« Certains logiciels espions seront probablement mis à jour en réponse à la publication de Detekt afin d'éviter la détection. En outre, il peut y avoir des versions existantes de logiciels espions […] qui ne sont pas détectés par cet outil ».

Vous trouverez plus d'informations et le lien de téléchargement sur http://linuxfr.org/news/detekt-un-logiciel-de-detection-de-logiciels-espions

Sur Mac, il n'existe pas un tel outil. Vous pouvez cependant utiliser le logiciel MacScan pou des antispaywares du commerce.

Cependant, que ça soit sur PC ou sur Mac, ce n'est qu'une analyse approfondie (et souvent manuelle) des fichiers systèmes, des processus en mémoire et qui se lancent au démarrage qui permettra de détecter les applications malveillantes installées sur votre ordinateur.

### Et si on dispose d'un Mac plutôt que d'un PC ?

Il y a quelques années, avoir un Mac « garantissait » d'être un peu à l'abris des virus et des pirates informatiques. En effet, pouquoi un pirate informatique perdrait du temps à développer un logiciel malveillant et prendrait des risques pour seulement 5% de la population numérique mondiale. Désormais, avec l'explosion d'Apple, de ses téléphones, tablettes et aussi ordinateur, les systèmes IOS se sont répandu sur la planète numérique. De plus, c'est très souvent les plus fortunés qui disposent de ces types d'appareils… une aubaine pour les pirates qui trouvent tout de suite un intérêt à développer des dangereuxwares.

- 3) La troisième et dernière phase de ces recommandations est la protection. Une fois votre système considéré comme sain (il est complètement inutile de protéger un système qui est infecté car ça ne soignera pas l'équipement et les conséquences pourraient être pires), il est temps d'adopter l'attitude d'un vrai utilisateur responsable et paranoïaque.
- Mettez à jour votre système d'exploitation (Windows, MasOs, IOS, Androis, Linux...) avec la version la plus récente. En effet, l'enchaînement des mises à jour des systèmes d'exploitation est peu souvent fait pour améliorer le fonctionnement ou ajouter des fonctions à votre appareil. Le ballet incessant des « updates » sert prioritairement à corriger les « boulettes » qu'ont fait volontairement ou involontairement les informaticiens « développeurs » détectées par d'autres informaticiens olus « contrôleurs ».
- Mettez à jour vos logiciels avec leurs versions les plus récentes (et particulièrement pour vos navigateurs Internet et les logiciels Adobe). En effet, la plupart des intrusions informatiques se font pas des sites Internet malveillants qui font exécuter sur votre ordinateur un code informatique malveillant chargé d'ouvrir un canal entre le pirate et vous. Ces codes informatiques malveillants utilisent les failles de vos logiciels pour s'exécuter. Lorsque l'utilisation d'une faille inconnue (sauf par les pirates) d'un logiciel est détectée par les « Gardiens de la paix numérique », un correctif (ou patch) est généralement développée par l'éditeur dans les jours qui suivent leur découverte. Ceci ne vous garantira pas une protection absolue de votre ordinateur, mais renforcera son blindage.Les pirates utilisent parfois d'anciens serveurs ou d'anciens postes de travail connecté sur le réseau, qui ont de vieux systèmes d'exploitation qui ne se mettent plus à jour et qui ont des failles ultra-connues pour pénétrer votre réseau et des postes pourtant ultra-sécurisés. Pensez donc à les déconnecter du réseau ou à copier le contenu ou les virtualiser sur des systèmes plus récents et tenus à jour.
- Mettez à jour les firmwares des matériels et objets connectés. Pour les mêmes raisons qu'il est important de mettre à jour vos logiciels avec leurs versions les plus récentes, il est aussi important de mettre à jour les logiciels de vos matériels et objets connectés (routeurs, modems, webcams etc.).
- Adoptez une politique sécurisée dans l'utilisation des mots de passe. Vos mots de passe doivent êtres longs, complexes et doivent changer souvent. Conseil primordial dans l'utilisation des mots de passe au bureau : Il doit être aussi précieux et aussi secret que le code de votre carte bancaire. Personne ne doit le connaître, sinon… quelqu'un pourra facilement se faire passer pour vous et vous faire porter le chapeau pour ses actes malveillants.
- Méfiez-vous des sites Internet proposant des vidéos gratuites, du streaming gratuit ou autres services inespérément gratuit. Les sites sont souvent piégés et ont destinés soit à collecter des données personnelles, soit contaminer votre ordinateur par des petits codes malveillants.
- Méfiez-vous également des e-mails douteux de demande d'aide (même d'un ami) ou autre participation humanitaire utilisant le paiement par Manda Cash, Western Union ou monnaie virtuelle telle le Bitcoin. Ce sont des moyen de paiement qui sont généralement utilisés par les pirates pour se faire payer et disparaître dans la nature. Les emails destinés à vous hameçonner auront aussi quelques détails qui devraient vous mettre la puce à l'oreille (Faute d'orthographe, huissier ou directeur ayant une adresse e-mail yahoo ou gmail).
- Vous avez un doute, vous pensez que votre ordinateur ou votre boite e-mail est victime d'intrusion, changez immédiatement de mot de passe. Certains systèmes de messagerie permettent d'avoir un historique des accès et des connexions. L'analyse de cet historique pourrait bien vous donner une indication pour savoir si quelqu'un d'autre à accès à votre messagerie (alias, double diffusion, collecte d'un compte mail sur un autre compte etc).

### Conclusion

Voila, vous avez maintenant toute une liste de recommandations qui peut vous rassurer (ou non) et vous permettre de prendre conscience de la complexité qu'est à ce jour la lutte de la #cybercriminalité.

Si maintenant tout ceci vous semble complexe, rassurez-vous, c'est notre métier. Nous seront donc en mesure de vous accompagner dans la sensibilisation des utilisateurs, la détection ou la protection contre ces « ennuiwares ».

Contactez-moi

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 (Symantec) 13,8 Milions de victimes Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj\_HKcbzRuvIPdu3FktA

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

Commandez sur Fnac.fr

Source : Denis JACOPINI

## Un Employeur peut-il examiner

# les messages échangés par ses employés sur leur téléphone professionnel ?



Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel ?

Dès lors que le téléphone du salarié est professionnel, l'employeur a ce droit, à moins d'avoir mentionné avant le message «personnel». Dans ce cas, l'employeur n'a plus le droit. Mais souvent, on n'oublie de l'écrire… »

**Notre métier**: Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations

sur

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



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

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



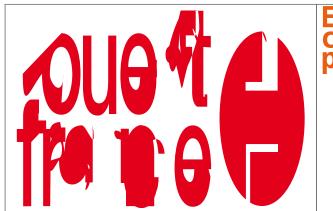
Contactez-nous

×

Réagissez à cet article

Source : Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? — La Voix du Nord

# Est-il risqué de se connecter au wifi public ? | Denis JACOPINI



Est-il risqué de se connecter au wifi public ? Nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants... Mais y a-t-il un risque à partager ces accès sans fil à internet avec d'autres ? Peut-on se faire pirater ses données ? Le point avec Denis Jacopini, expert en cybercriminalité.

Avec les smartphones ou ordinateurs portables d'aujourd'hui, se connecter au réseau wifi d'une gare ou d'un hôtel, quand on est en déplacement, est devenu presque banal. À l'étranger, c'est même la solution la plus simple pour surfer sur internet et relever ses e-mails, sans risquer d'exorbitants frais de « roaming » (coûts de connexion au réseau mobile local, facturés ensuite par l'opérateur français). Résultat, on a tendance à surfer

on a tendance à surfer sur ces réseaux wifi avec la même insouciance qu'à la maison, sans aucune précaution. Ce qui n'est pas bien malin. Denis Jacopini, expert judiciaire en sécurité informatique, nous explique pourquoi.

ADUS (4)

Die 69

Benis Jacopini, créateur du site LeNetExpert.fr et correspondant Cnil (Commission nationale de l'informatique et des libertés), est aussi formateur en protection des données personnelles et en sécurité informatique. (Photo : DR)

À quoi faut-il faire attention, quand on se connecte à une borne wifi publique ou semi-publique, en ville ou dans un hôtel ? Si possible, il faut choisir un réseau wifi où la connexion se fait avec un nom d'identifiant et un mot de passe personnalisés, différents pour chaque utilisateur. En cas d'utilisation malveillante du réseau par quelqu'un, cette identification fournit une piste, sur le plan judiciaire, pour remonter jusqu'à l'auteur. Avec les wifi qui proposent un identifiant et un mot de passe identiques pour tout le monde, on est moins protégé. Les réseaux wifi les plus dangereux sont ceux qui sont complètement ouverts, sans aucun mot de passe, où les utilisateurs sont impossibles à tracer.

### Ouel est le danger ? Se faire espionner ?

Tout à fait. À partir du moment où quelqu'un se trouve connecté au même point wifi que vous, il a techniquement la possibilité d'accéder aux informations qui transitent sur le réseau, il peut « voir » ce qui entre et qui sort. Les pirates utilisent pour cela des logiciels espions, appelés « sniffers », ou « renifleurs » en bon français. Ces programmes sont désormais très faciles à trouver et à télécharger sur internet. Plus ou moins sophistiqués, ils permettent de capter, trier et interpréter le « bruit » informatique qui transite par le wifi.

OLO (Le wifi public, c'est pratique, mais pas très sécurisé. (Photo : FlickR/Richard Summers)

La confidentialité de la navigation n'est donc pas garantie ?
En effet. Et pas uniquement sur les réseaux wifi, d'ailleurs. C'est ainsi depuis la création d'internet : les protocoles de communication du web ne sont pas cryptés. Mais de plus en plus de sites « sensibles » — par exemple les messageries électroniques, les banques, les boutiques en ligne, etc. — ont désormais des adresses commençant par « https » au lieu de « http ». Le « s », souvent associé avec un petit cadenas dans la barre du navigateur, signifie que les communications sont sécurisées. Quand on navigue sur internet via un wifi, il faut donc privilégier ces sites.

### Le risque de se faire voler ses mots de passe, ou ses coordonnées bancaires, est donc bien réel ?

Oui, mieux vaut éviter de saisir des données confidentielles quand on navigue sur internet via un wifi public ou semi-public. On a ainsi vu des hommes d'affaires se faire voler des informations importantes, car ils utilisaient en toute confiance un wifi d'hôtel… sur lequel étaient aussi connectés des pirates !

Pug 4

Un café Starbucks à Londres, très apprécié pour sa connexion wifi gratuite. (Photo : Stefan Wermuth/Reuters)

### Peut-on se faire abuser par une fausse borne wifi ?

Oui, c'est une raison supplémentaire de se méfier des réseaux complètement ouverts : certains pirates créent leur propre borne wifi à partir d'un simple ordinateur portable. Les passants se connectent dessus, par facilité, sans se douter qu'il ne s'agit pas du tout d'une « vraie » borne. Ensuite, la personne mal intentionnée n'a plus qu'à récupérer les informations qui transitent par le réseau qu'elle a créé… Aujourd'hui, c'est très facile de devenir pirate !

### Comment se protéger ?

En s'abstenant de réaliser des opérations sensibles, comme des achats en ligne ou des opérations bancaires, sur un wifi public. Si on le peut, mieux vaut utiliser le réseau 3G ou 4G pour se connecter à internet en mobilité. Les informations qui transitent par cette voie sont beaucoup moins faciles à pirater. Il y a aussi la solution consistant à installer, sur son smartphone ou son ordinateur, ce qu'on appelle un « VPN ». C'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 c'est beaucoup plus sûr.

Zone de wifi gratuit à New York : en France comme à l'étranger, mieux vaut se connecter sur un nom de réseau connu, éventuellement signalé via l'affichage public. (Photo : Keith Bedford/Reuters)

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.

Cet article vous plait ? Partagez !

Source : http://www.ouest-france.fr/leditiondusoir/data/492/reader/reader.html?t=1431534138729#!preferred/1/package/492/pub/493/page/7 Par Corinne Bourbeillon

Pue 4