

10 conseils pour garder vos appareils protégés pendant les vacances | Denis JACOPINI



**10 conseils pour
garder vos
appareils protégés
pendant
vos
vacances**

Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, voici un mini-guide conçu par les experts ESET pour voyager et surfer en toute tranquillité.

Serviette à dents ? ok.
Ordinateur, téléphone, tablette ? ok.
Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, méfiez-vous des menaces lorsque vous utilisez un Wi-Fi public pour vous connecter à votre banque en ligne, boutique en ligne ou tout simplement pour vérifier vos e-mails. Pas de panique ! Stephen Cobb et d'autres professionnels ESET ont créé un guide pour vous permettre de voyager en toute sécurité et garder ainsi toutes vos données personnelles et vos appareils protégés.

Conseils



1. Avant de prendre la route, assurez-vous d'effectuer une mise à jour complète du système d'exploitation ainsi que des logiciels, et de posséder une solution de sécurité de confiance.
2. Sauvegardez vos données et placez-les dans un endroit sûr. Pensez à déplacer les données sensibles du disque dur de votre ordinateur portable sur un disque dur externe chiffré à l'aide de vos vacances.
3. Ne laissez jamais vos appareils sous surveillance dans les lieux publics, activez la fonction entraîneur de vos appareils pour trier les appels et messages, et au besoin d'effacer les contenus à distance.
4. Mettez un mot de passe fort et activez la fonction « délai d'inactivité » sur tous vos appareils, que ce soit votre ordinateur portable, votre tablette ou votre téléphone. Retrouvez tous nos conseils pour un mot de passe efficace en cliquant ici.
5. Dans la mesure du possible, utilisez uniquement des accès internet de confiance. Demandez à votre hôtel ou l'endroit où vous logez le nom de leur Wi-Fi et utilisez exactement le même nom : faites attention aux arnaques qui essaient de ressembler aux Wi-Fi publics en ajoutant le mot « gratuit » au nom de la connexion Wi-Fi.
6. Si l'Internet de votre hôtel vous demande de mettre à jour un logiciel afin de pouvoir vous connecter, déconnectez-vous immédiatement et informez-en la réception.
7. Ne vous connectez pas à des connexions Wi-Fi qui ne sont pas chiffrées avec WPA2. Toutes les normes inférieures à celle-ci ne sont tout simplement pas assez sûres et peuvent être facilement piratées.
8. Si vous devez utiliser le Wi-Fi public pour vous connecter à votre réseau d'entreprise, utilisez toujours votre VPN (réseau virtuel privé).
9. Si ce n'est pas urgent, évitez les banques et boutiques en ligne quand vous utilisez le Wi-Fi public. Sinon, nous vous conseillons d'utiliser le partage de connexion de votre téléphone et de surfer en utilisant internet sur votre téléphone portable.
10. Si vous n'utilisez pas encore d'antivirus de confiance et suspectez votre ordinateur portable d'être infecté, vous pouvez utiliser gratuitement le scanner ESET Online qui ne nécessite aucune installation et peut être utilisé pour détecter et retirer des logiciels malveillants

Article original sur ESET

Cliquez ici



Denis JACOPINI est Expert Informatique Assermenté spécialisé en cybercriminalité et en protection des données personnelles.
• Expresses techniques (virus, espions, pirates, fraudeurs, arnaques Internet...) et pratiques (téléphonie mobile, réseaux sociaux, réseaux sociaux, contenus, détourneurs de clientèle...);
• Expresses de systèmes de vote électronique ;
• Formations et conférences en cybercriminalité ;
• Formations de C.I.L. (Correspondance Informatique et Liberté);
• Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : ESET – Actualités

Formations RGPD Protection des données personnelles et en Cybercriminalité

Parce que la Cybercriminalité et la Protection des données personnelles sont liés, nous couvrons ces sujets concomitamment.

Consultez la liste de nos formations et services sur le RGPD



RGPD = RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

NOS SERVICES :

- Formations **RGPD** (Règlement Général sur la Protection des Données) ;
- Formations en **Cybercriminalité** ;
- **Sensibilisations** à la cybercriminalité ;
- **État des lieux RGPD** ;
- **Mise en conformité RGPD** ;
 - **Analyses de risques** (PIA / DPIA) ;
- **Audits sécurité** ;

VOTRE PROFIL :

- **CLUB D'ENTREPRISES, ORDRES, FÉDÉRATIONS, CORPORATION** : Quelles sont vos responsabilités, quels sont vos risques, quelles devraient être vos priorités ? Que ça soit en matière de Protection des Données Personnelles (RGPD) ou de cybercriminalité, faisons ensemble un état des lieux. Agir sur vos équipements ? Sensibiliser votre personnel ? Libre à vous ensuite d'agir en fonctions de nos recommandations sur les points qui vous sembleront prioritaires.
- **ÉTABLISSEMENTS / CENTRES DE FORMATION / ORGANISATEURS D'ÉVÉNEMENTS** : Que ça soit en protection des données personnelles ou en Cybercriminalité, permettez à vos stagiaires de découvrir les notions essentielles ;

- **CHEFS D'ENTREPRISE / ÉQUIPE INFORMATIQUE** : Nous vous formons dans vos locaux et réalisons en collaboration avec votre équipe informatique une analyse détaillée de vos installation à la recherche de failles et d'axes d'amélioration conformément aux règles de l'art ou de la réglementation en vigueur (RGPD).

LES SUJETS DE FORMATION :



Consultez notre catalogue

COMMENT PROTÉGER VOTRE ORGANISME DE LA CYBERCRIMINALITÉ

Durée : 2 jours ou 4 jours (2 jours tout public + 2 jours approfondissement pour techniciens/informaticiens)

VIRUS, DEMANDES DE RANÇONS, VOL DE DONNÉES... PROTÉGEZ-VOUS !

Durée : 1 jour

LES ARNAQUES INTERNET À CONNAÎTRE POUR NE PLUS SE FAIRE AVOIR

Durée : 1 jour

COMMENT BIEN UTILISER LE CLOUD

Durée : 1 jour

COMMENT PROTÉGER VOTRE IDENTITÉ ET VOTRE VIE PRIVÉE SUR

INTERNET

Durée : 1 jour

DÉCOUVREZ 50 LOGICIELS GRATUITS À CONNAÎTRE ABSOLUMENT

Durée : 1 jour

RGPD CE QU'IL FAUT SAVOIR POUR NE PAS LE PAYER CHER

Durée : 1 jour

RGPD : ANALYSONS CE QUE VOUS AVEZ COMMENCÉ

Durée : 1 jour (il est recommandé d'avoir déjà mis en pratique une mise en conformité au moins 15 jours avant)

COMMENT BIEN UTILISER LES DONNÉES DANS LE CLOUD

Durée : 1 jour

À LA DÉCOUVERTE DU DARKNET (LE WEB CLANDESTIN)

Durée : 1 jour

DÉTECTER ET GÉRER LES CYBER-ATTAQUES

Durée : 2 jours

APPRENEZ À RÉALISER DES AUDITS SÉCURITÉ SUR VOTRE SYSTÈME INFORMATIQUE

Durée : 2 jours

APPRENEZ À RÉALISER DES TESTS D'INTRUSION SUR VOTRE SYSTÈME INFORMATIQUE

Durée : 2 jours

Remarque :

Un sujet peut être traité en quelques heures mais aussi en quelques jours.

Malgré un minimum de théorie à connaître, nous pouvons réaliser un mélange de ces thèmes afin de vous proposer un contenu personnalisé en fonction des thèmes et durées globales souhaités.

EN FORMAT CONFÉRENCE :

QUE NOUS RÉSERVE LA CYBERCRIMINALITÉ DANS LES 12 PROCHAINS MOIS ?

Conférence personnalisable en général sur 1h30 + 30min Questions / réponses) (Demandez le programme détaillé)

RGPD – CE QU'IL FAUT SAVOIR POUR NE PAS LE PAYER

Conférence personnalisable en général sur 1h30 + 30min Questions / réponses) (Demandez le programme détaillé)

FONCTIONNEMENT :

- Vous organisez des formations dans votre établissement ou dans des locaux adaptés : Nous pouvons animer de 1 à 6 jours de formation sur les sujets ci-dessus ;
- Vous organisez un forum ou un salon, nous pouvons préparer une conférence de 20 minutes à 1h30 ou

- participer à des tables rondes ;
- En faculté ou établissement scolaire, nos interventions seront de 3 à 35 heures.
 - Pour une journée de formation, nos interventions sont prévues sont prévues généralement prévues du mardi au jeudi (Lundi, Vendredi et Samedi sous conditions).
 - Nos formations d'une journée sont prévues pour une durée de 7 heures par jour maximum.

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

Numéro de formateur
93 84 03041 84




Data**dock**
Organisme **validé**
et **référencé**

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

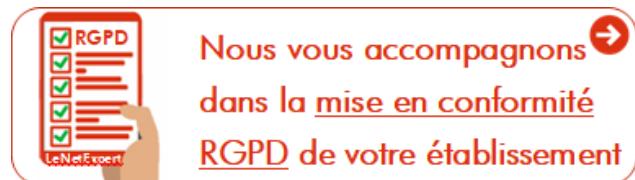
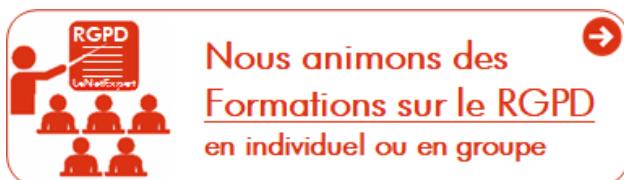
?

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 aisément 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"]

Recherche de preuves dans les téléphones, smartphones,

tabletes, ordinateur PC, Mac... retrouver des documents, photos ou SMS effacés

RECHERCHE DE PREUVES

DANS LES TÉLÉPHONES – SMARTPHONES - TABLETTES

RÉCUPÉRATION SMS & IMAGES SUPPRIMÉS



Denis JACOPINI – LE NET EXPERT

Recherche de preuves dans les téléphones, smartphones, tablettes, ordinateur PC, Mac... retrouver des documents, photos ou SMS effacés

Doutes, soupçons ? Vous pensez que quequ'un vous a volé des données ? Vous pensez que votre conjoint(e) ou enfant a quelque chose à vous cacher ? Vous pensez que le téléphone contient les preuves qu'il vous faut ? Pour mettre un terme à ces interrogations, Denis JACOPINI vous permet une récupération des preuves et un usage judiciaire si vous le désirez.

Denis JACOPINI, Expert de justice en Informatique. Assermenté par les tribunaux, il est inscrit sur les listes des Tribunaux de Commerce, Tribunaux d'Instance, de Grande Instance et Administratif sur les catégories suivantes :

- E-01.02 Internet et Multimédia
- E-01.03 Logiciels et Matériels
- E-01.04 Systèmes d'information (mise en oeuvre)
- G-02 Investigations scientifiques et techniques
- G-02.05 Documents Informatiques (Investigations Numériques)

Diplômé en Droit de l'Expertise Judiciaire, en Cybercriminalité, Certifié en Gestion des Risques sur les Systèmes d'information (ISO 27005 Risk Manager), équipé des meilleurs équipements utilisé en Investigation Numérique par les Polices du monde entier, il vous permettra de retrouver des traces et des preuves dans de nombreux supports (e-mails, fichiers, appels émis, reçus, sms, mms, photos, vidéos etc... même effacés de la quasi totalité des téléphones du marché).

Avec les meilleurs équipements utilisés par les Polices du monde entier, ils est enfin possible de faire parler vos équipements numériques.



Rechercher de preuves dans un téléphone, un smartphone ou une tablette

You souhaitez rechercher des preuves dans un téléphone, un smartphone ou une tablette ?
Contactez-vous

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



- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)

ou suivez nous sur

Réagissez à cet article

Fausses applications Pokémon GO. Comment se protéger ? | Denis JACOPINI



Les chercheurs ESET découvrent des fausses applications sur Google Play qui cible les utilisateurs de Pokémons GO. L'une d'entre elles utilise pour la première fois une application qui verrouille l'écran (Lockscreen) sur Google Play. Les deux autres applications utilisent la fonctionnalité scareware qui oblige l'utilisateur à payer pour des services inutiles.

Toutes les fausses applications découvertes par ESET et détectées grâce à ESET Mobile Security (application lockscreen nommée « Pokémons GO Ultimate » et les applications scareware « Guide & Cheats for Pokémons GO » et « Install Pokemongo ») ne sont plus disponibles sur Google Play. Elles ont été retirées de l'app Store suite à l'alerte donnée par ESET. Même si ces fausses applications ne sont pas restées longtemps sur le Google Play, elles ont généré quelques milliers de téléchargements. L'application « Pokémons GO Ultimate », a piégé entre 500 et 1.000 victimes, « The Guide & Cheats for Pokémons GO » en a atteint entre 100 et 500, et la plus dangereuse d'entre elles, « Install Pokemongo » a atteint entre 10.000 et 50.000 téléchargements.

« Pokémons GO Ultimate » cultive son extrême ressemblance avec la version officielle du célèbre jeu mais ses fonctionnalités sont très différentes : elle verrouille l'écran automatiquement après le démarrage de l'application. Dans de nombreux cas, réinitialiser le téléphone ne fonctionne pas parce que l'application se superpose à toutes les autres, ainsi qu'aux fenêtres du système. Les utilisateurs doivent redémarrer leurs appareils en retirant la batterie ou en utilisant Android Device Manager. Après la réinitialisation, l'application malveillante fonctionne en arrière-plan, à l'insu de sa victime, en cliquant silencieusement sur des annonces à caractère pornographique. Pour se débarrasser de l'application, l'utilisateur doit aller dans Réglages -> Gestion des Applications -> Pi Réseau et la désinstaller manuellement.

« Pokémons GO Ultimate » est la première fausse application sur Google Play qui utilise avec succès une fonction de verrouillage d'écran. Comme la fonctionnalité principale de cette application est le clic sur des annonces pornographiques, il n'y a pas de réels dommages. Mais il suffit de peu pour que la fonction de verrouillage d'écran évolue et ajoute un message de rançon, pour créer le premier ransomware par lockscreen sur Google Play.», explique Lukáš Štefanko, Malware Researcher chez ESET.

Alors que l'application « Pokémons GO Ultimate » porte les signes d'un screenlocker et d'un pornclicker, les chercheurs ESET ont également trouvé un autre malware sur Pokémons GO dans Google Play. Les fausses applications nommées « Guide & Cheats for Pokémons GO » et « Install Pokemongo » sur Google Play, appartiennent à la famille des Scarewares. Ils escroquent leurs victimes en leur faisant payer des services inutiles. En leur promettant de leur gérer des Pokecoins, Pokeballs ou des œufs chanceux – jusqu'à 999.999 chaque jour – ils trompent les victimes en leur faisant souscrire à de faux services onéreux. (Cette fonctionnalité a récemment été décrite dans un article publié sur WeLiveSecurity).

« Pokémons GO est un jeu si attrayant que malgré les mises en garde des experts en sécurité, les utilisateurs ont tendance à accepter les risques et à télécharger toutes les applications qui leur permettraient de capturer encore plus de Pokémons. Ceux qui ne peuvent pas résister à la tentation devraient au moins suivre des règles de sécurité élémentaires. » recommande Lukáš Štefanko.

Conseils des experts en sécurité ESET pour les aficionados de Pokémons GO :

- téléchargez uniquement ce qui vient d'une source connue
- lisez les avis en prêtant attention aux commentaires négatifs (gardez en tête que les commentaires positifs ont pu être créés par le développeur)
- lisez les termes et conditions de l'application, concentrez-vous sur la partie qui concerne les permissions requises
- utilisez une solution de sécurité mobile de qualité pour vérifier toutes vos applications

Conseils de Denis JACOPINI

Pour anticiper et vous protéger pour moins de 10€ (10€ est prix de la licence initiale. Une forte réduction sera appliquée au moment du renouvellement au bout d'un an)



Article original de ESET



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques à Internet...) et judiciaires (Investigation Téléphones, disques durs, e-mails, conteneurs, décomptes 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.

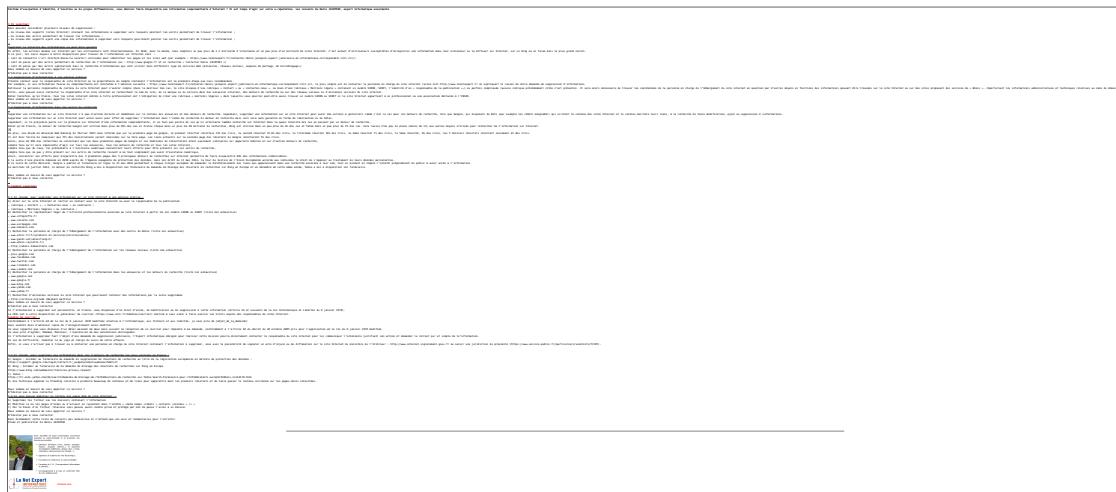


Réagissez à cet article

Suppression d'un contenu web : comment procéder ? | Denis JACOPINI



Suppression d'un contenu web : comment procéder ?



LIENS SOURCES

Utilisation des moteurs de recherche en France

<http://www.journaldunet.com/ebusiness/le-net/1087481-parts-de-marche-des-moteurs-de-recherche-en-france/>

Taux de clic en fonction de la position dans les résultats

<http://www.mathiasp.fr/blog/seo/quel-est-le-taux-de-clic-en-fonction-des-positions-dans-google/544>

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





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

Que ce soit à la suite d'un licenciement ou tout simplement en raison d'un conflit, il se peut que la personne en face de vous souhaite savoir à tout prix quelles sont les informations et les documents à votre disposition ou quelle est votre ligne de défense.

Quelqu'un sait des choses qu'il ne devrait pas savoir ?

Comment savoir si mon ordinateur est espionné ?

Comment savoir si mes informations personnelles volées sur mon ordinateur ?

Comment savoir si je suis victime de fuites d'informations ?

Il est clair que si vous êtes en conflit avec quelqu'un, il y a de fortes chances, qu'il cherchera, tout comme vous, à savoir ce qui peut bien se mijoter chez la partie adverse. Le premier réflexe que vous aurez probablement de penser que votre ordinateur est espionné et que votre téléphone est espionné. Sauf à ce que vous ayez anticipé la fuite d'informations en placant dans votre installation informatique des systèmes destinés à détecter la fuite d'informations et éventuellement à vous alerter, il faudra passer votre téléphone ou votre ordinateur au peigne fin pour détecter à posteriori les traces d'infiltration ou des traces d'exfiltration de données.

Quelle est notre technique ?

Notre technique consiste à trouver des pistes et éléments secrets, mais notre technique est basée sur la recherche et la détection de détails et fonctionnements anormaux. C'est par une bonne connaissance des techniques utilisées par les pirates informatiques et par une connaissance approfondie d'un système afin que nous puissions identifier un système modifié, altéré, trafiqué, piégé... Nos informations dans le système d'exploitation (base de registre, journaux des événements, journaux divers) et dans tous les lieux dans lesquels le malveillant peut laisser des traces, sont collectées, analysées et traitées. Une analyse sur une « Timeline » des actions déroulées dans votre ordinateur permet aussi parfois de pouvoir découvrir la chronologie des actions et confondre les éléments recueillis avec d'autres preuves.

Comment devrez-vous organiser ?

Afin de vous aider à en tirer le meilleur sur l'existence ou non d'éléments doux dans votre système, il est d'abord indispensable de pouvoir disposer des équipements à expertiser. Nous nous organisons pour vous priver de votre appareil le moins possible mais cette étape est nécessaire pour faire une photocopy de votre appareil et les premières mesures.

En fonction de vos besoins, il peut aussi que nous déposions dans vos locaux un appareil enregistreur avec lequel nous pourrons collecter en temps réel l'ensemble des données suspectes.

Nos rapports sont-ils utilisables en justice ?

Si vous avez besoin de la rédaction d'un rapport d'expertise privée (non judiciaire), nous le construirons sur le même modèle que les rapports d'expertise que nous produisons pour la justice. Si par la suite vous avez décidé d'aller en justice, le juge qui sera en charge de votre affaire, même s'il ne pourra pas se fier aux seuls éléments figurant dans notre rapport expertise, aura tout de même l'obligation de le tenir compte dans son jugement.

Que faire avant qu'il ne soit trop tard ?

Vous pouvez être espionné, déjà par l'intermédiaire de votre ordinateur ou de votre téléphone ? N'attendez pas, il est nécessaire de réagir vite, compte tenu que les traces peuvent disparaître rapidement. Deux priorités se présentent à vous et en fonction de votre choix, des actions différentes seront menées.:

1. restaurer l'outil de défense de votre entreprise
2. faire stopper l'acte de surveillance illégale;

Article de Denis JACOPINI (expert informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles).

 Denis JACOPINI est un consultant informatique spécialisé en cybersécurité et en protection des données personnelles. Il a une vaste expérience dans l'industrie et le secteur public, ayant travaillé pour de grands groupes internationaux. Ses compétences couvrent l'analyse de systèmes, la détection d'attaques et la mise en œuvre de stratégies de sécurité. Il est également formateur et a participé à de nombreux projets de recherche et développement dans le domaine de la sécurité informatique.

 [Le Net Expert](#) | INFORMATIQUE | CONSULTANCE

Réagissez à cet article

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

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.

Denis JACOPINI interviewé par une journaliste de Ouest France | 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 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.



Denis 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.

Quel 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.



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 !



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)

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

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

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

Par Corinne Bourbeillon



Quelles sont les mentions obligatoires sur un site internet ? | Denis JACOPINI

Quelles sont les #mentions obligatoires sur un site internet ?

Tous les sites internet édités à titre professionnel, qu'ils proposent des ventes en ligne ou non, doivent obligatoirement indiquer les mentions légales suivantes :

- pour un entrepreneur individuel : nom, prénom, domicile
- pour une société : raison sociale, forme juridique, adresse de l'établissement ou du siège social (et non pas une simple boîte postale), montant du capital social
- adresse de courrier électronique et numéro de téléphone
- pour une activité commerciale : numéro d'inscription au registre du commerce et des sociétés (RCS)
- pour une activité artisanale : numéro d'immatriculation au répertoire des métiers (RM)
- numéro individuel d'identification fiscale : numéro de TVA intracommunautaire
- pour une profession réglementée : référence aux règles professionnelles applicables et au titre professionnel
- nom et adresse de l'autorité ayant délivré l'autorisation d'exercer quand celle-ci est nécessaire
- nom du responsable de la publication
- coordonnées de l'hébergeur du site : nom, dénomination ou raison sociale, adresse et numéro de téléphone
- pour un site marchand, conditions générales de vente (CGV) : prix (exprimé en euros et TTC), frais et date de livraison, modalité de paiement, service après-vente, droit de rétractation, durée de l'offre, coût de la technique de communication à distance
- numéro de déclaration simplifiée Cnil, dans le cas de collecte de données sur les clients

Avant de déposer ou lire un cookie, les éditeurs de sites ou d'applications doivent :

- informer les internautes de la finalité des cookies,
- obtenir leur consentement,
- fournir aux internautes un moyen de les refuser.

La durée de validité de ce consentement est de 13 mois maximum. Certains cookies sont cependant dispensés du recueil de ce consentement.

Le manquement à l'une de ces obligations peut être sanctionné jusqu'à un an d'emprisonnement, 75 000 € d'amende pour les personnes physiques et 375 000 € pour les personnes morales.

Remarque : Depuis l'entrée en application du RGPD, Règlement Général sur la Protection des Données), vous devez également prévoir des mentions relatives à la protection des données à caractère Personnel ainsi que prévoir des précautions relatives à la demande de consentement des internautes à utiliser leurs coordonnées.

Consultez notre dossier consacré à la demande de consentement

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://vosdroits.service-public.fr/professionnels-entreprises/F31228.xhtml>

Comment se connecter de manière sécurisée à un wifi public ? | Denis JACOPINI



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) ;
- vous voler, crypter des documents ou exercer un chantage pour que vous puissiez les récupérer ;
- usurper votre identité et réaliser des actes illégaux ou terroristes sous votre identité ;
- accéder à des informations bancaires et vous spolier de l'argent.

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 et conseillons le logiciel VPN HotSpot Shield.
Ce logiciel rendra vos connections Wifi publiques tranquilles.
Téléchargez et découvrez gratuitement HotSpot Shield
Notre page de présentation de 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.