Bonnes pratiques face à une tentative de cyber-extorsion | Denis JACOPINI

	Bonnes pratiques face à une tentative de cyber-extorsion

Bonnes pratiques face à une tentative de cyber-extorsion

1. Typologie des différents cas de cyber-extorsion

Le type le plus répandu de cyber-extorsion est l'attaque par crypto-ransomware. Ce dernier est une forme de malware qui chiffre les fichiers présents sur la machine infectée. Une rançon est par la suite demandée afin d'obtenir la clef qui permet de déchiffrer les données compromises. Ces attaques touchent autant les particuliers que les acteurs du monde professionnel. Il existe cependant deux autres types de cyber-extorsion auxquels doivent faire face les sociétés.

Le premier cas est celui du chantage faisant suite à un vol de données internes. L'exemple le plus marquant de ces derniers mois est celui du groupe Rex Mundi : ce dernier dérobe des informations sensibles/confidentielles – comme une base clientèle – puis demande une rançon à sa victime sous peine de divulguer son butin et par conséquent de rendre public l'acte de piratage; ce qui peut être fortement compromettant pour la société ciblée comme pour sa clientèle. De nombreuses entreprises comme Dexia, Xperthis, Voo ou encore Labio ont été victimes des chantages du groupe Rex Mundi.

La deuxième pratique est celle du DDoS contre rançon, spécialité des pirates d'Armada Collective. Le modus operandi est simple et efficace : la cible reçoit un email l'invitant à payer une rançon en Bitcoin afin de ne pas se voir infliger une puissante attaque DDoS qui rendrait son site web indisponible à ses utilisateurs. La plupart des victimes sont des sociétés de taille intermédiaire dont le modèle économique est basé sur le principe de la vente en ligne – produits ou services – comme le fournisseur suisse de services de messagerie ProtonMail en novembre 2015.

2. Bonnes pratiques à mettre en place

En amont de la tentative de cyber-extorsion

Un ensemble de bonnes pratiques permet d'éviter qu'une attaque par ransomware se finalise par une demande de rançon.

Il convient de mettre en place une stratégie de sauvegarde – et de restauration – régulière des données. Ces back-ups doivent être séparés du réseau traditionnel des utilisateurs afin d'éviter d'être chiffrés en cas de déploiement d'un crypto-ransomware. Dans ce cas de figure, le système pourra être restauré sans avoir besoin de payer la rançon exigée.

La propagation d'un malware peut également être évitée par l'installation d'outils/solutions de cybersécurité notamment au niveau du client, du webmail et du système d'exploitation (antivirus). Ceci doit obligatoirement être couplé à une mise à jour régulière du système d'exploitation et de l'ensemble des logiciels installés sur le parc informatique.

L'être humain étant toujours le principal maillon faible de la chaîne, il est primordial de sensibiliser les collaborateurs afin qu'ils adoptent des comportements non-risqués. Par exemple : ne pas cliquer sur les liens et ne pas ouvrir les pièces-jointes provenant d'expéditeurs inconnus, ne jamais renseigner ses coordonnées personnelles ou bancaires à des opérateurs d'apparence légitimes (banques, fournisseurs d'accès Internet, services des impôts, etc.).

Ces bonnes pratiques s'appliquent également dans le cas d'un chantage faisant suite à un vol de données internes. Ces dernières sont en général dérobées via l'envoi dans un premier temps d'un spam contenant une pièce jointe malicieuse ou une URL redirigeant vers un site web compromis. Une fois le système d'information compromis, un malware est déployé afin de voler les informations ciblées.

La menace provient également de l'intérieur : un employé mal intentionné peut aussi mettre en place une tentative de cyber-extorsion en menaçant de divulguer des informations sensibles/confidentielles. Ainsi, il est important de gérer les accès par une hiérarchisation des droits et un cloisonnement.

Pendant la tentative de cyber-extorsion

Lors d'un chantage faisant suite à un vol de données internes, il est important de se renseigner sur la véracité des informations qui ont été dérobées. Certains groupes de pirates se spécialisent dans des tentatives de cyber-extorsion basées sur de fausses informations et abusent de la crédulité de leurs victimes. Il en va de même concernant l'origine du corbeau : de nombreux usurpateurs imitent le style du groupe Armada Collective et envoient massivement des emails de chantage à des TPE/PME. Ces dernières cèdent fréquemment à ces attaques qui ne sont pourtant que des canulars.

Il est vivement recommandé de ne jamais payer une rançon car le paiement ne constitue pas une garantie. De nombreuses victimes sont amenées à payer une somme bien plus conséquente que la rançon initialement demandée. Il n'est pas rare de constater que les échanges débutent de manière très cordiale afin de mettre la cible en confiance. Si cette dernière cède au premier chantage, l'attaquant n'hésite pas à profiter de sa faiblesse afin de lui soutirer le plus d'argent possible. Il abuse de techniques basées sur l'ingénierie sociale afin d'augmenter ses profits. Ainsi, l'escroc gentil n'existe pas et le paiement de la rançon ne fait que l'encourager dans sa démarche frauduleuse.

De nombreuses victimes refusent de porter plainte et cela pour plusieurs raisons. Elles estiment à tort que c'est une perte de temps et refusent également de communiquer sur les résultats et conséquences d'une attaque qui ne feraient que nuire à leur image auprès des clients, fournisseurs ou partenaires. Pourtant cette mauvaise stratégie ne fait que renforcer le sentiment d'impunité des attaquants, les confortent dans le choix de leurs modes opératoires et leur permet de continuer leurs actions malveillantes. Il est ainsi vital de porter plainte lors de chaque tentative de cyber-extorsion. L'aide de personnes qualifiées permet de faciliter ce genre de démarches.

En cas d'attaque avérée, il est essentiel pour la victime de s'appuyer sur un panel de professionnels habitués à gérer ce type de situation. La mise en place d'une politique de sauvegarde ou bien la restauration d'un parc informatique n'est pas à la portée de toutes les TPE/PME. Il est nécessaire de faire appel à des prestataires spécialisés dans la réalisation de ces opérations complexes.

Par ailleurs, en cas de publication de la part de l'attaquant de données sensibles/confidentielles, il convient de mettre en place un plan de gestion de crise. La communication est un élément central dans ce cas de figure et nécessite l'aide de spécialistes.

Article original de Adrien Petit

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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Bonnes pratiques face à une tentative de cyber-extorsion [Par Adrien Petit, CEIS] | Observatoire FIC

LeNetExpert a intégré la plateforme cybermalveillance.gouv.fr

---

Parce que les victimes doivent pouvoir compter sur des professionnels habitués à réagir face à des actes de piratage, des escroqueries ou vols de données etc., nous avons tenu à soutenir le projet cybermalveillance.gouv.fr. à mettant à leur disposition le meilleur de nos compétences.

2017 sera probablement l'année qui comptera le plus de victimes de rançongiciels. Les initiatives que l'on peut identifier sur le cyberespace ayant pour objectif de combattre ce fléau démontrent une réelle prise de conscience à toutes les strates de l'économie et de l'état. Vous trouverez ci-dessous un guide pdf spécialement fait pour vous aider à anticiper et à réagir face de telles menaces. Cette fiche réflexe est destinée à toutes les catégories de publics. Elle présente cette catégorie d'attaque informatique, les principales mesures à prendre pour s'en protéger, les actions à entreprendre lorsque l'on en est victime, ainsi que les infractions et sanctions pénales auxquelles s'exposent ceux qui les utilisent.

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

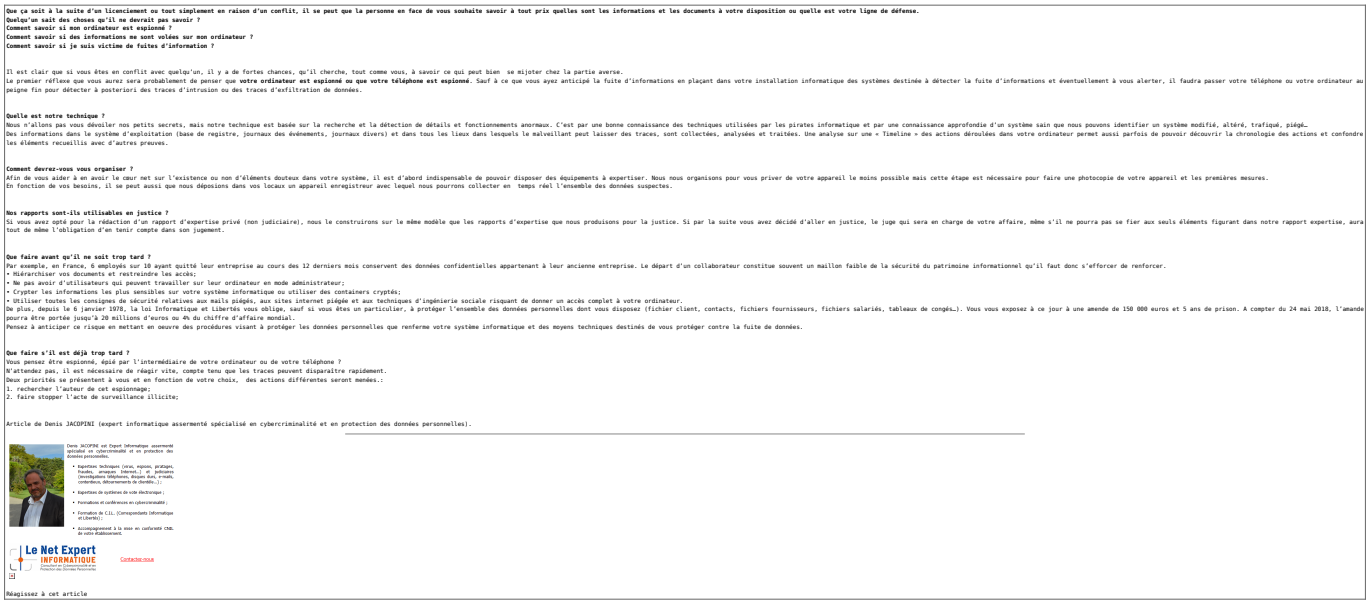
Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des 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).

LE NET EXPERT
:
• **SENSIBILISATION / FORMATIONS** :
- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**
• **MISE EN CONFORMITÉ RGPD / CNIL**
- **ÉTAT DES LIEUX RGPD** de vos traitements)
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération 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

Réagissez à cet article

Source : *Fiche rançongiciels (cryptolocker)*

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



Que ça 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 des informations me sont volées sur mon ordinateur ?
Comment savoir si je suis victime de fuites d'information ?

Il est clair que si vous êtes en conflit avec quelqu'un, il y a de fortes chances, qu'il cherche, tout comme vous, à savoir ce qui peut bien se mijoter chez la partie averse.
Le premier réflexe que vous aurez sera probablement de penser que **votre ordinateur est espionné ou que votre téléphone est espionné**. Sauf à ce que vous ayez anticipé la fuite d'informations en plaçant dans votre installation informatique des systèmes destinée 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 des traces d'intrusion ou des traces d'exfiltration de données.

Quelle est notre technique ?
Nous n'allons pas vous dévoiler nos petits 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 informatique et par une connaissance approfondie d'un système sain que nous pouvons identifier un système modifié, altéré, trafiqué, piégé…
Des 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 vous organiser ?
Afin de vous aider à en avoir le cœur net sur l'existence ou non d'éléments douteux 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 photocopie de votre appareil et les premières mesures.
En fonction de vos besoins, il se 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 opté pour la rédaction d'un rapport d'expertise privé (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 d'en tenir compte dans son jugement.

Que faire avant qu'il ne soit trop tard ?
Par exemple, en France, 6 employés sur 10 ayant quitté leur entreprise au cours des 12 derniers mois conservent des données confidentielles appartenant à leur ancienne entreprise. Le départ d'un collaborateur constitue souvent un maillon faible de la sécurité du patrimoine informationnel qu'il faut donc s'efforcer de renforcer.
• Hiérarchiser vos documents et restreindre les accès;
• Ne pas avoir d'utilisateurs qui peuvent travailler sur leur ordinateur en mode administrateur;
• Crypter les informations les plus sensibles sur votre système informatique ou utiliser des containers cryptés;
• Utiliser toutes les consignes de sécurité relatives aux mails piégés, aux sites internet piégés et aux techniques d'ingénierie sociale risquant de donner un accès complet à votre ordinateur.
De plus, depuis le 6 janvier 1978, la loi Informatique et Libertés vous oblige, sauf si vous êtes un particulier, à protéger l'ensemble des données personnelles dont vous disposez (fichier client, contacts, fichiers fournisseurs, fichiers salariés, tableaux de congés…). Vous vous exposez à ce jour à une amende de 150 000 euros et 5 ans de prison. A compter du 24 mai 2018, l'amande pourra être portée jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial.
Pensez à anticiper ce risque en mettant en oeuvre des procédures visant à protéger les données personnelles que renferme votre système informatique et des moyens techniques destinés de vous protéger contre la fuite de données.

Que faire s'il est déjà trop tard ?
Vous pensez être espionné, épié 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. rechercher l'auteur de cet espionnage;
2. faire stopper l'acte de surveillance illicite;

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles
Contactez-nous

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

---

Ce qu'il faut savoir avant de se connecter sur du WiFi public | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Ce qu'il faut savoir avant de se connecter sur du WiFi public

Aéroports, hôtels, cafés… Le WiFi public est très utilisé, mais pas sans risque. 30 % des managers ont fait les frais d'un acte cybercriminel lors d'un voyage à l'étranger, selon Kaspersky Lab.

Spécialiste des solutions de sécurité informatique, Kaspersky Lab publie les résultats d'une enquête réalisée par l'agence Toluna auprès de 11 850 salariés, cadres et dirigeants dans 23 pays, sur leur utilisation de terminaux et Internet à l'étranger. Tous ont voyagé à l'international l'an dernier, à titre professionnel ou personnel. Premier constat : 82 % ont utilisé des services WiFi gratuits, mais non sécurisés (aucune authentification n'étant nécessaire pour établir une connexion réseau), depuis un aéroport, un hôtel, un café… Or, 18 % des répondants, et 30 % des managers, ont fait les frais d'un acte cybercriminel (malware, vol de données, usurpation d'identité…) lorsqu'ils étaient à l'étranger.

Droit ou devoir de déconnexion ?

« Les businessmen assument que leurs terminaux professionnels sont plus sûrs du fait de la sécurité intégrée », a souligné l'équipe de Kaspersky Lab dans un billet de blog. Et si cela n'est pas le cas, ils considèrent que ce n'est pas leur problème. Ainsi « un répondant sur quatre (et plus de la moitié des managers) pense qu'il est de la responsabilité de l'organisation, plutôt que de celle de la personne, de protéger les données. En effet, à leurs yeux, si les employeurs envoient du personnel à l'étranger, ils doivent accepter tous les risques de sécurité qui vont avec ».

Si des données sont perdues ou volées durant leur voyage, la plupart des managers seraient prêts à blâmer leur département informatique. Et ce pour ne pas avoir recommandé l'utilisation de moyens de protection comme un réseau privé virtuel (VPN), des connexions SSL ou encore la désactivation du partage de fichiers lors d'une connexion WiFi… Quant au droit à la déconnexion, lorsqu'il existe, il se pratique peu. Pour 59 % des dirigeants et 45 % des managers « intermédiaires », il y une attente de connexion quasi continue de la part de leur employeur.

Article original de Ariane Beky

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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Les voyageurs daffaires ignorent les risques du WiFi public

---

Bases essentielles pour sécuriser son site web | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Bases essentielles pour sécuriser son site web

Il faut savoir qu'internet peut se révéler vulnérable. La sécurité d'un site n'est pas à prendre à la légère, c'est quelque chose de très compliqué qui requiert des connaissances techniques approfondies afin de pouvoir identifier les vulnérabilités et mettre en place les mesures de protection nécessaires.
La sécurité d'un site web est un enjeu crucial et essentiel pour tout administrateur système soucieux de préserver et protéger son site. Les hackers sont toujours à la recherche de nouvelles failles, mais de multiples solutions de sécurité s'offrent à vous de plus simples et de plus pointues qui vous permettront de lutter contre les pirates et les hackers et protéger son site internet.
Voici quelques simples conseils sous forme d'une liste de bonnes pratiques qu'un professionnel doit appliquer à la rigueur pour se défendre des attaques automatiques et **empêcher ceux qui visent votre site web d'y pénétrer** :

1. Veiller sur la mise à jour de votre site web

Il faut d'abord veiller à mettre à jour correctement le serveur web qui héberge le site. Si vous faites appel à un hébergeur professionnel, c'est son travail. Par contre, si vous héberger votre site vous-même c'est à vous de faire les mises à jour nécessaires. Ensuite, le système de gestion du site doit également être à jour, ainsi que toutes les applications qui jouent un rôle dans l'administration du site.
Certains systèmes de gestion de contenu comme WordPress permettent d'effectuer facilement les mises à jour automatiquement. Comme ils offrent aussi une quantité très importante de plugins dont certains peuvent présenter des failles flagrantes. Je vous conseille alors de **bien vous renseigner sur la qualité et l'efficacité d'un plugin avant de l'installer**.

2. S'assurer du sauvegarde et de la protection

N'oubliez jamais d'effectuer une sauvegarde régulière pour votre site web et aussi que pour toutes les autres informations. Sa fréquence dépendra de la fréquence de la mise à jour du site, c'est-à-dire que **vous devrez faire une sauvegarde de votre site à chaque fois que vous le mettez à jour**. Vous vous rendrez compte de la grande valeur de cette sauvegarde le jour où votre site sera piraté malgré les précautions que vous avez prises.
Enfin, vous devez protéger l'accès au serveur web pour éviter les tentatives d'attaque du site. Par exemple, l'authentification http et l'une des pratiques sur laquelle vous pouvez compter pour protéger votre serveur web.

3. Protéger les données sensibles

Lorsque vous collectez des données personnels, mots de passe, données financières, il faut veiller sur leur sécurité mieux que tout le reste. Il s'agit non seulement d'une obligation vis-à-vis de vos utilisateurs mais aussi d'une contrainte légale.
Il est indispensable que vous **chiffriez toutes les données stockées sur vos serveurs**. Il faut aussi chiffrer la connexion (SSL) pour éviter que des données soient interceptées lors de le communication entre l'utilisateur et votre site.
Vous devez faire des mots de passe l'objet d'un soin tout particulier pour assurer plus de sécurité, pour cela ils doivent être encryptés avant d'être stockés.
Comme vous devez aussi « hacher » les mots de passe avec un algorithme approprié comme «**bcrypt** » ou « **scrypt** » qui sont difficiles à être attaqués, et évitez les usuels MD5 et SHA1 qui sont plus vulnérables.

4. Vérifier la sécurité de votre hébergeur

C'est une astuce de sécurité d'ordre plus général, il est très important que votre hébergeur vous propose des versions plus récentes de Apache, MySQL et PHP. Renseignez-vous auprès de votre hébergeur ou utiliser un fichier PHP pour obtenir ces informations cruciales.

5. Créer votre site web avec Wix

Vous pouvez choisir des outils qui vont sécuriser votre site à votre place.
Pour ceux qui veulent se simplifier la vie et choisir une solution aussi sécurisé que pratique, il existe **Wix**. Lire la suite…

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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Bases essentielles pour sécuriser son site web | FunInformatique

Recommandations de la CNIL sur les mot de passe (Délibération n° 2017-012 du 19 janvier 2017)

Le mot de passe reste le moyen d'authentification le plus répandu. Alors que les compromissions de bases entières de mots de passe se multiplient, la CNIL a adopté une nouvelle recommandation sur les mots de passe. Elle fixe les mesures minimales à mettre en œuvre.

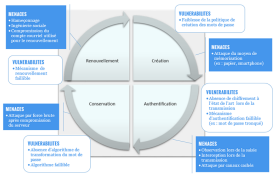
Recommandations de la CNIL sur les mot de passe (Délibération n° 2017-012 du 19 janvier 2017)

Le mot de passe reste le moyen d'authentification le plus répandu. Alors que les compromissions de bases entières de mots de passe se multiplient, la CNIL a adopté une nouvelle recommandation sur les mots de passe. Elle fixe les mesures minimales à mettre en œuvre.

Basée sur la gestion d'un secret, l'authentification par identifiant et mot de passe est un moyen simple et peu coûteux à déployer pour contrôler un accès.
Toutefois, cette méthode d'authentification présente un niveau de sécurité faible.
Ces dernières années, de nombreuses attaques informatiques ont entrainé la compromission de bases de données entières de comptes et des mots de passe associés. Ces fuites de données ont notamment contribué à enrichir les connaissances des attaquants en matière de mots de passe. Les risques de compromission des comptes associés à cette méthode d'authentification se sont fortement accrus et imposent une vigilance particulière.

Les risques liés à la gestion des mots de passe sont multiples et reposent notamment sur :
1. la simplicité du mot de passe ;
2. l'écoute sur le réseau afin de collecter les mots de passe transmis ;
3. la conservation en clair du mot de passe ;
4. la faiblesse des modalités de renouvellement du mot de passe en cas d'oubli (cas des questions « secrètes »).

Les principaux risques identifiés au cours du cycle de vie d'un mot de passe



Il n'existe pas de définition universelle d'un bon mot de passe, mais sa complexité et sa longueur permettent de diminuer le risque de réussite d'une attaque informatique qui consisterait à tester successivement de nombreux mots de passe (attaque dite en force brute). On considère que la longueur du mot de passe suffit pour résister aux attaques courantes à partir de 12 caractères. Lorsque la taille du mot de passe diminue, des mesures compensatoires doivent être prévues.

PHRASE2PASSE : UN OUTIL POUR ACCOMPAGNER LES UTILISATEURS

Pour aider les utilisateurs à choisir un mot de passe robuste et un moyen mnémotechnique, la CNIL a développé un outil pour générer un mot de passe à partir d'une phrase.
Le code de cet outil est disponible sous la forme d'une extension logicielle en javascript, afin que vous puissiez l'intégrer dans vos applications.
>Télécharger l'extension

Les exigences de la CNIL

1.

L'authentification par mot de passe : longueur, complexité, mesures complémentaires

Les exigences minimales de la CNIL en termes de taille et de complexité du mot de passe varient en fonction des mesures complémentaires mises en place pour fiabiliser le processus d'authentification : ainsi, si une authentification est basée exclusivement sur un mot de passe, cela implique a minima l'utilisation d'un mot de passe complexe d'au moins 12 caractères composé de majuscules de minuscules, de chiffres et de caractères spéciaux. Des mesures complémentaires à la saisie d'un mot de passe (restrictions, d'accès, collecte d'autres donnée, support détenu en propre par l'utilisateur) permettent de réduire la longueur et la complexité du mot de passe, car ces mesures permettent d'assurer un niveau de sécurité équivalent au mot de passe seul.
Le tableau ci-dessous fait état des 4 cas d'authentification par mot de passe identifiés par la CNIL dans sa recommandation

	Exemple d'utilisation	Longueur minimum	Composition du mot de passe	Mesures complémentaires
Mot de passe seul	FORUM, BLOG	12	• majuscules • minuscules • chiffres • caractères spéciaux	Conseiller l'utilisateur sur un bon mot de passe
Avec restriction d'accès (le plus répandu)	SITES DE E-COMMERCE, COMPTE D'ENTREPRISE, WEBMAIL	8	Au moins 3 des 4 types suivants : • majuscules • minuscules • chiffres • caractères spéciaux	Blocage des tentatives multiples : (exemples) • Temporisation d'accès au compte après plusieurs échecs • « Capcha » • Verrouillage du compte après 10 échecs
Avec information complémentaire	BANQUE EN LIGNE	5	Chiffres et/ou lettres	Blocage des tentatives multiples **+** • Information complémentaire communiquée en propre d'une taille d'au moins 7 caractères (ex : identifiant dédié au service) **ou** • Identification du terminal de l'usager (ex : adresse IP, adresse MAC…)
Avec matériel détenu par la personne	CARTE BANCAIRE OU TÉLÉPHONE	4	Chiffres	Matériel détenu en propre par la personne (ex : carte SIM, carte bancaire, certificat) + Blocage au bout de 3 tentatives échouées

Dans tous les cas,
le mot de passe ne doit pas être communiqué à l'utilisateur en clair par courrier électronique.
Ces exigences sont des règles minimales. Le contrôle d'accès peut devoir reposer sur des règles plus robustes selon les risques auxquels le système est exposé.

2.

Sécurisation de l'authentification

Quelles que soient les mesures mises en place, la fonction d'authentification doit être sûre :
• elle utilise un algorithme public réputé fort ;
• sa mise en œuvre logicielle est exempte de vulnérabilité connue.
Lorsque l'authentification n'a pas lieu en local, l'identité du serveur doit être contrôlée au moyen d'un certificat d'authentification de serveur et le canal de communication entre le serveur authentifié et le client doit être chiffré à l'aide d'une fonction de chiffrement sûre. La sécurité des clés privées doit être assurée.

3.

La conservation des mots de passe

Le mot de passe ne doit jamais être stocké en clair. Il doit être transformé au moyen d'une fonction cryptographique non-réversible et sûre, intégrant l'utilisation d'un sel ou d'une clé.
Le sel ou la clé doit être généré au moyen d'un générateur de nombre pseudo-aléatoires cryptographiquement sûr (il utilise un algorithme public réputé fort et sa mise en œuvre logicielle est exempte de vulnérabilité connue). Il ne doit pas être stocké dans le même espace de stockage que l'élément de vérification du mot de passe.

4.

Le renouvellement du mot de passe

Renouvellement périodique

Le responsable de traitement veille à imposer un renouvellement du mot de passe selon une périodicité pertinente et raisonnable, qui dépend notamment de la complexité imposée du mot de passe, des données traitées et des risques auxquels il est exposé.
La personne concernée doit être en mesure de changer elle-même son mot de passe. Dans ce cas, les règles afférentes à la création de mots de passe s'appliquent.

Renouvellement sur demande

À la demande de la personne concernée, par exemple en cas d'oubli, le responsable de traitement met en œuvre une procédure de renouvellement du mot de passe.
Si ce renouvellement nécessite l'intervention d'un administrateur, un mot de passe temporaire est attribué à la personne concernée, le changement du mot de passe attribué temporairement lui est imposé lors de sa première connexion.
Si ce renouvellement intervient de manière automatique : le mot de passe ne doit pas être transmis en clair. L'utilisateur doit être redirigé vers une interface dont la validité ne doit pas excéder 24 heures, lui permettant de saisir un nouveau mot de passe, et ne permettre qu'un seul renouvellement.
Si le renouvellement fait intervenir un ou plusieurs éléments supplémentaires (numéro de téléphone, adresse postale…) :
• ces éléments ne doivent pas être conservés dans le même espace de stockage que l'élément de vérification du mot de passe ; sinon, ils doivent être conservés sous forme chiffrée à l'aide d'un algorithme public réputé fort, et la sécurité de la clé de chiffrement doit être assurée ;
• afin de prévenir les tentatives d'usurpation s'appuyant sur le changement de ces éléments, la personne doit être immédiatement informée de leur changement.

Que faire en cas de risque de compromission du mot de passe ?

Si un responsable de traitement de données détecte une violation de données en rapport avec le mot de passe d'une personne,
• Le responsable de traitement doit notifier la personne concernée, dans un délai n'excédant pas 72 heures ;
• Il doit imposer à l'utilisateur concerné le changement de son mot de passe lors de sa prochaine connexion ;
• Il doit lui recommander de veiller à changer ses mots de passe d'autres services dans l'hypothèse où il aurait utilisé le même mot de passe pour ceux-ci.
Faites-nous par de vos remarques
Les professionnels sont invités à remonter à la CNIL les difficultés de mise en œuvre que pourrait poser l'application de cette recommandation. Cette recommandation pourra faire l'objet de révisions et de mises à jour.

Texte officiel

> Délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe
…[lire la suite]

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 de formation, de sensibilisation ou d'audits 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 DIRTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

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 mêle 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 connections 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Denis JACOPINI interviewé par une journaliste de Ouest France | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

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

Est-ce utile de protéger la WebCam et le microphone de son ordinateur avec de l'adhésif ? | Denis JACOPINI

Est-ce utile de protéger la WebCam et le microphone de son ordinateur avec de l'adhésif ?

Cela peut sembler absurde, mais c'est une mesure de précaution élémentaire, probablement conseillée par la direction en charge de la sécurité de Facebook, sur tous les ordinateurs portables susceptibles d'être attaqués.

En 2013, des chercheurs en sécurité informatique de l'université John Hopkins, aux Etats-Unis, avaient démontré qu'il était possible de prendre le contrôle des webcams des Mac, ce qui est aussi chose fréquente sur les PC.
La firme Symantec avait même alerté, la même année, sur ce qu'elle désignait comme des « creepwares »,« Certaines personnes mettent un morceau d'adhésif sur la webcam de leur portable, peut-être vous-mêmes le faites. Sont-elles trop prudentes, paranoïaques, un peu étranges ? (…)
Beaucoup d'entre nous ont entendu des histoires de gens qui étaient espionnés sur leur ordinateur (…). Mais ces histoires sont-elles vraies et les précautions prises par des gens en apparence paranoïaques sont elles justifiées ? Malheureusement la réponse est oui », écrivait alors Symantec. L'éditeur a même publié une vidéo de prévention :
Source Numerama

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

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

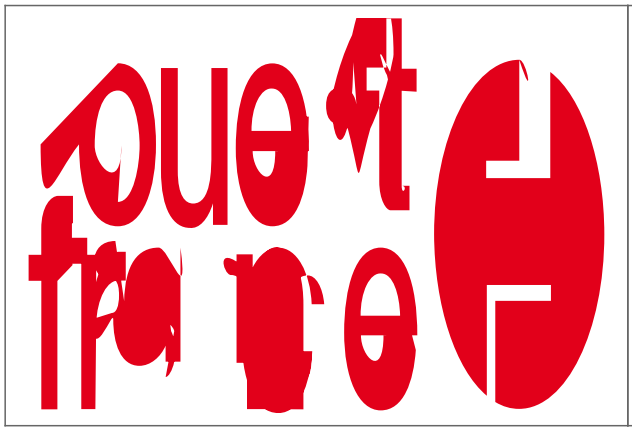
Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

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

Original de l'article mis en page : Pourquoi Mark Zuckerberg met du scotch sur la webcam et le micro de son Mac – Tech – Numerama

---

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



Comment se connecter 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) ;
• 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 mêle 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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article