Un guide pour déjouer les cyber attaques | Denis JACOPINI

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

Les très petites et les moyennes entreprises (TPE et PME) seraient la cible de 77% des cyber attaques perpétrées en France

Un guide pour déjouer les cyber attaques

Plus de trois quarts des intrusions malveillantes par Internet visent des petites et moyennes entreprises. Le risque augmente et le coût des dégâts aussi.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI), en partenariat avec la CGPME (Confédération générale des petites et moyennes entreprises), a publié en début d'année un « Guide des bonnes pratiques de l'informatique » (http://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique).
Ce document de douze « recommandations » doit aider les petites entreprises à protéger leurs fichiers, déjouer les escroqueries financières, le sabotage de leurs sites de vente en ligne, surveiller leur image de marque sur les réseaux sociaux…

Comment se protéger des piratages ?
Premier conseil : le mot de passe. Le guide recommande d'en choisir un avec « 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance…) et ne figurant pas dans le dictionnaire ».
Deuxième élément important : configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible. Sinon, téléchargez les correctifs de sécurité disponibles.
Troisième point crucial, « éviter le Wi-Fi dans le cadre de l'entreprise », préconise le guide. Si vous souhaitez quand même en profiter, le WEP est à bannir absolument puisqu'un chiffrement de ce type peut être cassé en quelques minutes seulement. Il faudra donc lui préférer du WPA/WPA2 avec une clé suffisamment longue de « plus de 20 caractères de types différents ».
Enfin, le guide donne quelques conseils lorsque votre machine a un « comportement étrange », laissant penser à un piratage : « déconnectez la machine du réseau, pour stopper l'attaque. En revanche, maintenez là sous tension et ne la redémarrez pas, pour ne pas perdre d'informations utiles pour l'analyse de l'attaque ». Ensuite, prévenez le responsable informatique ou un prestataire compétent si besoin.

Les PME, premières cibles des cyber attaques
Si chacun a en tête l'exemple récent de Ryanair, délesté de 4,5 millions d'euros par des hackers chinois, ou de la chaîne TV5 monde privée de diffusion, les attaques par Internet ne sont pas réservées aux seules grandes entreprises. Les très petites et les moyennes entreprises (TPE et PME) seraient la cible de 77% des cyber attaques perpétrées en France, selon le Syntec, le syndicat de l'ingénierie et des services informatiques.

La raison est connue : les PME, qui travaillent souvent pour des grands comptes, détiennent des informations capitales, mais insuffisamment sécurisées, faute de moyens. Les hackers s'attaquent donc d'abord à ce « maillon faible ».

Des risques en hausse de 66%
Le 14 avril dernier, à la CCI de Bordeaux, lors d'une réunion d'information sur les « risques nouveaux et émergents » a été présentée une enquête réalisée en 2014 par Ipsos pour l'assureur Axa entreprises. Menée auprès de 500 dirigeants, elle a montré que, si les sociétés de 10 à 500 salariés placent l'environnement (pollution de l'air ou de l'eau) en tête de leurs risques, celui lié à Internet se situe immédiatement après.

Depuis 2009, le nombre d'incidents sur la toile de ce type augmente de 66% en moyenne par an, estime le cabinet d'audit PWC. Il a atteint le nombre de 117 339 attaques dans le monde en 2014. Le coût de la « réparation » et de la mise en place d'une meilleure protection augmente année après année et varie de quelques dizaines de milliers d'euros à plusieurs millions d'euros en fonction de la taille de l'entreprise et des dégâts. Et, il faut compter un délai de 30 à 40 jours pour un retour total à la normale.

Source : http://www.sudouest.fr/2015/05/07/un-guide-pour-aider-les-pme-a-dejouer-les-cyber-attaques-1914431-705.php
par Michel Monteil

5 conseils cyber pour vous protéger en vacances

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

Les attaques sur internet ne prennent pas de vacances, il faut être vigilant toute l'année. Protégez vos ordinateurs, installez un anti-virus et suivez nos conseils.

L'été bat son plein et chaque année les Français s'exposent sans le savoir à de nombreux cyber risques pendant les vacances. Norton by Symantec souligne l'importance de rester vigilant lorsque vous êtes connecté à internet et propose ci-dessous une liste de 6 conseils, utiles pour toute la famille :

En voyage, sur quel réseau WiFi se connecter en toute sécurité ?

Sans solution sécurité et VPN ou sur un accès Wi-Fi ouvert, un internaute/mobinaute, ainsi que ses enfants, peuvent être confrontés à certains risques…

Enfants sur internet : rester vigilant même pendant les vacances

De nombreuses plateformes d'hébergement de contenu vidéos notamment permettent de configurer un contrôle parental, également, ne pas hésiter à prendre connaissance du contenu consulté par les plus jeunes.

Modifier régulièrement ses mots de passe

Il est d'importance critique d'avoir un mot de passe complexe ou d'utiliser un gestionnaire de mot de passe pour éviter d'être victime d'une usurpation d'identité. Le bon réflexe est donc de créer des mots de passe forts et uniques qui ne peuvent être facilement devinés, voire, d'utiliser un gestionnaire de mots de passe tel que Identity Safe de Norton…

Les logiciels et applications doivent toujours être à jour

Plusieurs menaces peuvent être contrées par de simples mises à jour de vos applications et appareils…

Effectuer une sauvegarde physique et dans le cloud de ses données.

Que ce soit le contenu qui reste à la maison ou le contenu apporté en vacances, le vol d'un appareil s'accompagne du vol des données qu'il contient – il est donc vital d'être en mesure de les récupérer rapidement.

Source : *Cyber sécurité : 5 conseils pour protéger toute la famille en vacances – Femme Actuelle*

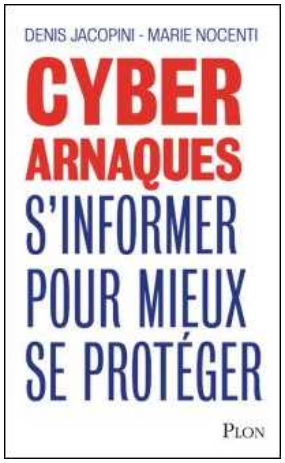
Autres conseils de Denis JACOPINI :

Et comme toujours, attention aux arnaques !

Apprenez à détecter de faux e-mails, de faux sites internet ou des sites internet piégés. Votre meilleur ennemi c'est vous, celui qui est imprudent, qui clique sans vérifier face à un e-mail qui vous fait peur ou qui vous annonce un cadeau…

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

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



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

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

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

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

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

Commandez sur Fnac.fr

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la 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

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 RISQUE

Un 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

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

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

---

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

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

Contenu de nos formations :

Le Règlement Général sur la Protection de Données (RGPD) entre en application le 25 mai 2018 et les entreprises ne s'y sont pas préparées. Or, elles sont toutes concernées, de l'indépendant aux plus grosses entreprises, et risqueront, en cas de manquement, des sanctions pouvant aller jusqu'à 4% de leur chiffre d'affaires. Au delà des amendes pouvant attendre plusieurs millions d'euros, c'est aussi la réputation des entreprises qui est en jeu. Quelle valeur lui donnez vous ? Serez-vous prêt à la perdre pour ne pas avoir fais les démarches dans les temps ?

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

Datadock 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 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 :

Nous animons des Formations sur le RGPD en individuel ou en groupe

Nous vous accompagnons dans la mise en conformité RGPD de votre établissement

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"]

Cybercriminalité : ne laissez pas les hackers faire la loi | Denis JACOPINI

Sécurité ne veut pas dire complexité. Il vaut mieux déployer des outils basiques, que pas d'outil du tout. Il faut également changer la façon d'appréhender la sécurité. Par exemple, le RSSI ne doit pas être une fin en soi, mais le point de départ pour avoir un plan d'action efficace et les solutions adéquates. Il va également faire le lien entre vulnérabilité des systèmes et impact sur le business.

La bataille du hacking est de plus en plus féroce, mais avec les bons outils et quelques bonnes pratiques les entreprises peuvent gagner la guerre contre la cybercriminalité

C'est une réalité, nous ne pouvons pas éviter les failles de sécurité. Les cybercriminels développent sans cesse de nouveaux outils pour déjouer les mesures de sécurité mises en place par les départements informatiques des entreprises. Certains hackers vont même jusqu'à communiquer publiquement des informations sur la manière de hacker des données, banalisant ces pratiques hautement dangereuses pour les entreprises.

Dans ce contexte, les attaquants peuvent tenter et retenter de s'introduire dans les dispositifs de sécurité de l'entreprise et indiquer à leurs pairs ce qui a fonctionné ou non, jusqu'au jour où ils arriveront à leurs fins. Ce n'est, en effet, qu'une question de temps et de patience, des ressources qui font rarement défaut aux hackers.

Les RSSI : un point de départ et non une finalité en soi

Bien que les risques d'attaques cybercriminelles soient de plus en plus nombreux et les hackers de plus en plus doués pour détourner les systèmes de sécurité, il est toujours mieux d'avoir une politique de sécurité, même basique, que pas de protection du tout ! Cette affirmation semble évidente, mais aujourd'hui nombreuses sont les entreprises qui ne possèdent toujours aucune solution ou politique pour protéger leur organisation.

Embaucher un responsable de la sécurité informatique (SSI – Responsable de la Sécurité des Systèmes d'Information) représente déjà un grand pas pour une entreprise. Ce référent sécurité tranquillise les actionnaires et témoigne d'une réelle volonté de mettre la sécurité informatique dans la liste des priorités de l'entreprise.

Loin d'être une mesure suffisante en elle-même, cette mesure doit être la première brique pour poser les fondations d'un système de protection durable, résistant et évolutif. Les hackers tenteront, encore et encore, à chercher une faille de sécurité… jusqu'à ce qu'ils la trouvent ! Et tel est précisément le problème : une équipe de sécurité doit réussir chaque jour à maintenir les mauvais éléments à l'écart. Un attaquant, lui, ne doit réussir qu'une seule fois.

Traduire les problématiques techniques pour qu'elles parlent aux métiers

En réalité, les entreprises ont besoin d'un responsable de la sécurité qui soit capable de communiquer aussi bien sur l'impact économique que sur les implications des choix organisationnels en matière de sécurité et de technologie. Les responsables de la sécurité ont trop souvent tendance à se lancer dans des discussions hautement techniques et aborder des sujets difficiles à appréhender pour la plupart des dirigeants.

Pour accomplir leur mission et avoir un véritable impact sur l'activité, les responsables de la sécurité à tous les niveaux, soutenus par l'industrie de la sécurité, doivent être en mesure de transposer les conversations techniques sur les vulnérabilités du réseau en une discussion sur les coûts ou les opportunités pour l'entreprise proprement dite. Une fois ce pas franchi, l'entreprise peut prendre des décisions fondées concernant l'impact de ses choix.

Une nouvelle définition de la notion sécurité

Les outils proposés par les éditeurs assurent un certain degré de protection contre les pirates. Les solutions technologiques constituent le socle de la sécurité informatique en entreprise et se doivent donc d'être adaptées aux différents défis auxquels l'entreprise peut être potentiellement exposée. De nos jours, il ne s'agit cependant plus de s'attendre à ce que les logiciels soient des remèdes miracles contre les attaquants.

Il s'agit bel et bien d'améliorer les pratiques de sécurité et de permettre aux équipes qui en sont chargées de s'investir dans la mise en œuvre de procédures abouties. Aucun dispositif de sécurité n'est inviolable, c'est un fait. Il faut cependant se poser les bonnes questions, voire LA bonne question : « Parmi ce que nous surveillons déjà, que pouvons-nous utiliser pour réduire le risque à l'égard de notre activité ? »

Dans la plupart des cas, la clé réside dans une meilleure exploitation des outils existants et non dans l'acquisition de nouveaux outils, un message qui réjouira toujours le conseil d'administration. Le plus gros défi n'est pas nécessairement d'accroître la sécurité, mais de la rendre plus intelligente.

[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.lesechos.fr/idees-debats/cercle/cercle-119704-cybercriminalite-ne-laissez-pas-les-hackers-faire-la-loi-1072763.php

---

Victime d'un prélèvement frauduleux sur votre compte bancaire ? Que faire ? | Quelques conseils… | Denis JACOPINI

Malgré toutes les actions que nous menons pour vous former au risque en cybercriminalité ou tous les efforts pour vous sensibiliser, vous êtes victime d'une arnaque sur Internet. Alors, que faire ?

Vous avez constaté un débit frauduleux sur votre compte bancaire ?
Les raisons peuvent être multiples. Carte bancaire copiés, votre numéro de carte bancaire généré aléatoirement, numéros de votre carte bancaire interceptés, virus ou logiciel d'espionnage informatique etc.

1) Tout d'abord, faites le plus vite possible opposition sur votre CB

en appelant le service interbancaire des cartes perdues ou volées qui est disponible 7 jours sur 7 au 08 92 705 705 (0,34€/min). Cela permettra d'éviter d'autres prélèvements frauduleux.

2) Contactez votre conseiller bancaire
pour lui expliquer l'arnaque dont vous avez été victime pour récupérer votre argent. La banque devrait vous proposer de vous rembourser sans délai. Si vous rencontrez des difficultés pour vous faire entendre, évoquez l'article de loi suivant :
L'Article L133-18 du code monétaire et financier précise :
» En cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L. 133-24, le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de l'opération non autorisée et, le cas échéant, rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. Le payeur et son prestataire de services de paiement peuvent décider contractuellement d'une indemnité complémentaire «

3) Portez plainte au commissariat ou à la gendarmerie la plus proche.
Le Défenseur des droits a pu constater que les policiers incitent les plaignants à ne déposer qu'une main courante, et non une plainte.
– La main courante est simplement déclarative; elle n'implique pas que la justice soit informée, ni qu'une investigation soit lancée; elle pourra seulement être versée à l'instruction si une procédure judiciaire a lieu.
– La plainte, en revanche, suppose une transmission au procureur de la République qui décide des suites à y donner.
Il est vrai que si les escrocs sont à l'autre bout du monde, il y a peu de chance que la police de notre pays réussisse à mettre un terme à leurs agissements… mais déposez plainte ! Ainsi votre cas sera connu des services de Police et cela pourra vous prémunir contre d'éventuelles complications suite à l'arnaque que vous avez subie. En effet les escrocs pourraient profiter des données qu'ils ont pour multiplier leurs méfaits. En portant plainte, vous montrez à la police que vous êtes bien une victime et que vous en subissez les conséquences.
Enregistrer votre plaine est une obligation des services de Police ou de Gendarmerie en vertu de l'article 15-3 du code de procédure pénale et de la Charte de l'accueil du public et de l'assistance aux victimes.
Ils sont censés enregistrer une plainte dès que la demande est émise, quels que soient le lieu où a été commise l'infraction et le lieu de résidence de la victime, et sans que cette dernière ait besoin d'apporter pour cela un quelconque élément de preuve (certificat médical, devis, etc).
Munissez-vous de tous les renseignements suivants :
• une pièce d'identité ;
• votre relevé bancaire sur lequel figure(nt) le (ou les) paiement(s) contesté(s);
• les coordonnées de votre banque;
• les références de votre carte bancaire;
• tout autre renseignement pouvant aider à l'identification de l'escroc.
Suite à ce dépôt de plainte, une enquête sera ouverte et transmise au procureur de la République.

4) Vous pouvez aussi appeler « Info Escroqueries »
N'oubliez pas le numéro « Info Escroqueries » 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile) à utiliser si à la base, vous avez été la cible d'un e-mail frauduleux ou d'une escroquerie.

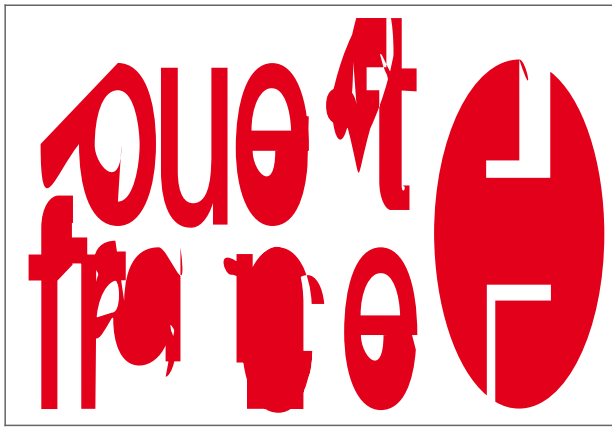
5) Rechercher l'origine de l'escroquerie
Une fois les actions précédentes réalisées, afin d'éviter que le problème ne se reproduise, il est indispensable d'identifier l'origine du prélèvement frauduleux.
Par exemple, si votre système informatique s'est fait pirater, l'arnaque se reproduira.
Pour cela, contactez un expert informatique spécialisé en cybercriminalité.

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 plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI

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 RISQUE

Un 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

Rançongiciel et hameçonnage : quelle démarche entreprendre si vous êtes la cible d’une cyberattaque ?

Rançongiciel et hameçonnage : quelle démarche entreprendre si vous êtes la cible d’une cyberattaque ?

Les ordinateurs contiennent des documents privés et données confidentielles (renseignements personnels, identifiants bancaires, codes secrets) qui peuvent être convoités par une tierce personne mal intentionnée. En cas de cyberattaque, il est important de savoir réagir vite pour se protéger d'une utilisation frauduleuse de vos données personnelles. Nous expliquons ici les principales cybermenaces qui planent sur les internautes, les recommandations de sécurité pour s'en prémunir et, surtout, comment agir si vous êtes la victime d'un cybercriminel.

Les recommandations de sécurité pour se protéger des cyber-escrocs

Selon l'**ANSII** (agence nationale de la sécurité des systèmes d'information), il vous est fortement conseillé de respecter **quelques règles simples pour vous protéger contre les cyberattaques**. Effectuer des sauvegardes régulières de vos fichiers importants sur des supports de stockage amovibles (CD, clé USB, disque dur externe). Mettre à jour régulièrement les principaux logiciels de vos appareils numériques (ex : Windows, antivirus, lecteur PDF, navigateur, etc.) en privilégiant leur mise à jour automatique. Ne pas avoir une confiance aveugle dans le nom de l'expéditeur de l'email. En cas de doute, n'hésitez pas à contacter directement l'expéditeur par un autre moyen de communication. Se méfier de courriel type « hameçonnage ciblé » qui vous propose un contenu personnalisé pour mieux tromper votre vigilance. Ne pas ouvrir les pièces jointes et ne pas suivre les liens des messages électroniques douteux (fautes d'orthographe, caractères accentués, nom des pièces jointes trop succinct). Ne jamais répondre à une demande d'information confidentielle par courriel.

En cas de cyber-attaque, il faut immédiatement déconnecter du réseau tout appareil susceptible d'être infecté et alerter au plus vite le responsable de sécurité ou le service informatique. Dans le cadre d'un rançongiciel, il est primordial de **ne pas payer la rançon**, car il n'est nullement garanti que la victime récupère la clé de déchiffrement qui lui permettra de récupérer l'accès à ses données personnelles.

Comment réagir si vous êtes victime d'un rançongiciel ou d'hameçonnage ?

Vous devez vous rendre dans un **commissariat de police** ou une **brigade de gendarmerie** pour **déposer plainte**, ou bien **adresser un courrier au Procureur de la République** auprès du **Tribunal de Grande Instance compétent**.

Pour mener correctement l'enquête, il faudra **fournir les renseignements suivants**.

• Les références du (ou des) transfert(s) d'argent effectué(s).

• Les informations de la (ou des) personne(s) contactée(s) : pseudos utilisés, adresse de messagerie ou adresse postale, numéros de téléphone, fax, copie des courriels…

• Le numéro complet de la carte bancaire ayant servi au paiement, la référence de votre banque et de votre compte, et la copie du relevé de compte bancaire où apparaît le débit frauduleux.

• Tout autre renseignement utile à l'identification du cyber-escroc.

Vous pouvez également **utiliser la plateforme de signalement Pharos** ou le numéro de téléphone dédié : 0811 02 02 17 pour signaler les faits dont vous avez été victime. La suite de l'enquête sera prise en charge par des services spécialisés…[lire la suite]

NOTRE MÉTIER :

• FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO

• EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES

• AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT

• MISE EN CONFORMITE RGPD / FORMATION DPO

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, suivez nos formations ;

EXPERTISES TECHNIQUES : Dans le but de prouver un dysfonctionnement, de déposer ou vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettrons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons dans vos démarches de mise en conformité avec le RGPD (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

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

(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)

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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Rançongiciel et hameçonnage : quelle démarche entreprendre si vous êtes la cible d’une cyberattaque ?*