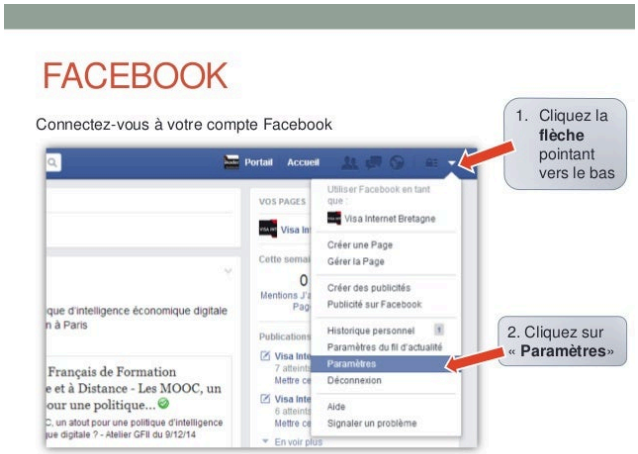
Facebook offre un outil de diagnostic pour se protéger des piratages de comptes | Denis JACOPINI

	Facebook offre un outil de diagnostic pour se protéger des piratages de comptes

Les membres de F18acebook peuvent désormais contrôler la sécurité de leur compte. Voici l'outil proposé par le réseau social pour prévenir le piratage des données personnelles.

Facebook n'est pas réputé pour la transparence de ses paramètres de confidentialité et de protection des données personnelles. A tel point qu'à de nombreuses reprises, les membres du réseau social se sont retrouvés perdus dans les options de partage leurs informations personnelles, mettant en danger la sécurité de leur compte Facebook. L'outil que vient de dévoiler Facebook va aider les utilisateurs à s'y retrouver. De manière simple et centralisée, Facebook permet à chacun de visualiser les réglages actifs sur son compte : niveau de confidentialité des informations partagées, applications connectées au compte, partage de localisation géographique, secret des messages échangés etc…
Le diagnostic de la sécurité des comptes se poursuit ensuite par le passage en revue des paramètres de protection : certaines applications inutilisées sont-elles encore actives, les alertes de connexion au compte sont-elles signalées par email, et l'utilisation du mot de passe du compte est-elle conforme aux usages? Avec cet outil, Facebook montre qu'il prend très au sérieux les menaces de piratage de compte de plus en plus pressantes, et invite ses membres à procéder à la vérification de leur compte Facebook dans les meilleurs délais.

A ce jour, le réglage des paramètres de sécurité dans FaceBook se fait dans le menu suivant :



Vous arriverez ensuite sur une liste de paramètres à modifier. Il faudra cliquer sur « Sécurité »

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.commentcamarche.net/news/5866867-piratage-de-compte-facebook-offre-un-outil-de-diagnostic

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

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

Cybercriminalité : ne laissez pas les hackers faire la loi

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.

Réagissez à cet article

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 ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique 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).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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

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

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

Contactez-nous

Source : http://www.lesechos.fr/idees-debats/cercle/cercle-119704-cybercriminalite-ne-laissez-pas-les-hackers-faire-la-

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

	Victime d’un prélèvement frauduleux sur votre compte bancaire ? Que faire ?

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

Consommateurs, exercez vos droits auprès de la CNIL | Denis JACOPINI

Consomateurs, exercez vos droits auprès de la CNIL

Participer à un concours, demander une carte de fidélité, remplir un formulaire sur internet, ou simplement poster sur les réseaux sociaux, nous transmettons très souvent des données personnelles à des organismes.

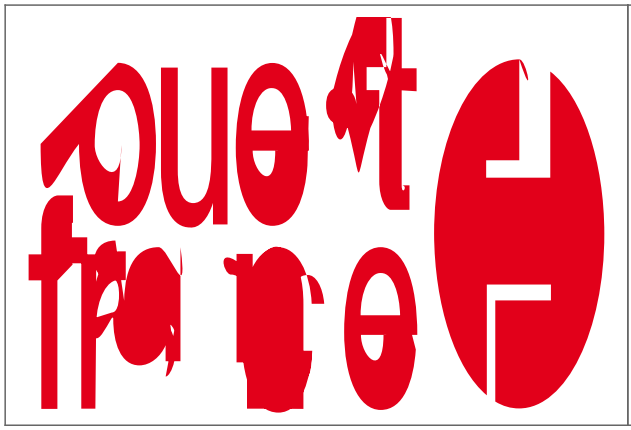
Grâce à la loi Informatique et Libertés, vous bénéficiez de droits spécifiques que vous pouvez – dans la plupart des cas – faire valoir vous-mêmes.

Droit d’accès
Droit de rectification
Droit d’opposition
Droit au déréférencement

Réagissez à cet article

Source : *Exercer vos droits – CNIL – Commission nationale de l’informatique et des libertés*

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

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)

Réagissez à cet article

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

RGPD dans les collectivités : Que faut-il mettre en oeuvre ?

Denis JACOPINI est Expert en Cybercriminalité et en Protection des Données à Caractère Personnel.
Notre métier :

Animation de formations et de conférences

Cybercriminalité (virus, espions, piratages, fraudes, arnaques Internet)
Protection des Données à Caractère Personne (mise en conformité avec la CNIL etle RGPD)
Audits sécurité, Expertises techniques et judiciaires

Audit sécurité (ISO 27005) ;
ID Swatting

Recherche de preuves (Investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
Expertises de systèmes de vote électronique ;

Formation en Cybercriminalité : Arnaques, virus et demandes

de rançons, Comment s’en protéger ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Formation en Cybercriminalité : Arnaques, virus et demandes de rançons, Comment s’en protéger ?				

Le contexte de l'Internet et l'ampleur du phénomène de la cybercriminalité, nous poussent à modifier nos comportements au quotidien.
Avons-nous raison d'avoir peur ? De quoi doit-on avoir peur ? Comment se protéger ?
Les réponses évidentes sont techniques, mais il n'en est pas moins vrai que des règles de bonnes pratiques et des attitudes responsables seront les clés permettant d'enrayer le phénomène.

OBJECTIF DE LA FORMATION EN CYBERCRIMINALITE :

La formation en cybercriminalité a pour but de créer des déclics chez les utilisateurs, mettre à jour les connaissances des informaticiens et faire prendre conscience aux chefs d'entreprises des risques en couvrant les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant d'enrayer le phénomène de la cybercriminalité.

PROGRAMME :

• Etat des lieux de la cybercriminalité en France et dans le monde;
• Les principaux cas de piratages et d'arnaques expliqués ;
• Les bonnes pratiques au quotidien pour limiter les risques ;
• Etude de vos témoignages, analyse de cas et solutions.
• PUBLIC CONCERNÉ : Utilisateurs, chefs d'entreprise, présidents d'associations, élus….

MOYENS PÉDAGOGIQUES :

• **Support de cours pour prise de notes**
• **Résumé remis en fin de cours.**
• **Vidéo projecteur et sonorisation souhaitée selon la taille de la salle.**

CONDITIONS D'ORGANISATION

• Formations individuelles ou en groupe
• Formations dispensées dans vos locaux ou organisées en salle de formation partout en France en fonction du nombre de stagiaires.

Téléchargez la fiche de présentation / Contactez-nous

QUI EST LE FORMATEUR ?

Denis JACOPINI est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire et a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.
Il anime dans toute le France et à l'étranger des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles.
A ce titre, il intervient régulièrement sur différents médias et sur La Chaine d'Info LCI pour vulgariser les sujets d'actualité en rapport avec ces thèmes.
Spécialisé en protection des données personnelles, il accompagne les établissements dans leur mise en conformité CNIL en les accompagnant dans la mise en place d'un Correspondant Informatique et Libertés (CIL).
Enfin, il intervient en Master II dans un centre d'Enseignement et de Recherche en Informatique, en Master Lutte contre la Criminalité Financière et Organisée, au Centre National de la Fonction Publique Territoriale et anime le blog LeNetExpert.fr sur lequel il partage et publie de très nombreuses informations sur ses thèmes de prédilection.
Denis JACOPINI peut facilement être contacté sur :
http://www.leNetExpert.fr/contact

Réagissez à cet article

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

Arnaque à la webcam : des conseils pour bien réagir – Denis JACOPINI

	#Arnaque à la webcam : des conseils pour bien réagir

Alors que les arnaques à la webcam se multiplient et touchent chaque années des milliers de victimes, la CNIL publie un guide de ces pratiques.

Pour chaque situation particulière, l'arnaque semble se dérouler à peu près de la même façon : la victime se rend la plupart du temps sur un site de rencontre, et entame la conversation avec une jeune femme ou un jeune homme au physique plutôt attrayant. La victime se voit alors proposer de continuer la conversation par Webcam, et s'exécute. Le cyber-escroc fait une capture d'écran, et menace de diffuser la vidéo ou les images de cet échange sur le compte Facebook d'un proche ou sur un site de partage de vidéos, si la personne ne lui remet pas la somme de 200 euros sous 24/48h.
Afin de faire face à cette situation, la Commission nationale de l'informatique et des libertés (CNIL) a publié une fiche pratique, destinée à informer et accompagner les victimes de ces cyber escrocs. Il y est notamment indiqué :
• qu'il ne faut surtout pas répondre aux tentatives de chantage du cyber-escroc ;
• qu'il convient d'alerter les autorités compétentes, via la plateforme du Ministère de l'intérieur ;
• qu'il faut demander au site de dépublier le contenu gênant ;
Rappelons que des sociétés, spécialisées dans l'effacement des contenus gênants, existent. De plus, et depuis un arrêt rendu par la Cour de justice de l'Union européenne, les internautes peuvent saisir les moteurs de recherche d'une demande de déréférencement d'un contenu associé à leur nom et prénom.

Quel réflexe adopter ?
1. **Ne répondez surtout pas à un cyber-escroc**
Soyez parfaitement hermétique à toute tentative de chantage : ne communiquez aucune donnée personnelle, ne versez surtout pas d'argent quel que soit la somme demandée.
2. **Verrouillez immédiatement vos comptes sociaux**
Paramétrez vos comptes sociaux professionnels et vos comptes Facebook de manière à ce que le malfaiteur n'associe pas votre nom à une liste d'amis / de contacts. Ne rendez accessible votre profil Facebook qu'auprès de vos amis de confiance. Enfin, ne publiez rien de personnel sur votre mur. Des personnes mal intentionnées peuvent détourner ces informations à d'autres fins. Notre page Facebook délivre quelques conseils pour bien paramétrer vos comptes.
3. **Alertez les autorités via la plateforme du Ministère de l'Intérieur**
Effectuez des captures d'écran justifiant votre situation (messages reçus, contenus à effacer …). Voir la fiche pratique
4. **Signalez directement l'escroquerie sur la plateforme www.internet-signalement.gouv.fr**
Renseignez-vous via le service Info Escroqueries au 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile ; Du lundi au vendredi de 9h à 18h)
5. **Parlez-en à une personne de confiance**
La violence des termes employés par l'escroc et le risque d'exposition de votre vie privée peuvent être vécus comme un traumatisme. Il est conseillé d'en parler avec une personne de confiance.Vous êtes mineur ? Des télé-conseillers sont gratuitement à votre écoute au 0800 200 000 de 9h à 19h en semaine. Voir le site Net écoute
6. **Informez vos amis de l'escroquerie**
Veillez à informer discrètement les personnes susceptibles d'être sollicitées par le cyber-escroc en mentionnant sobrement que vous êtes victime d'une escroquerie en ligne et qu'il ne faut ni ouvrir, ni partager, ni répondre à une éventuelle sollicitation provenant d'un inconnu.
7. **Effectuez régulièrement des recherches à votre nom**
Vous pouvez par exemple programmer une alerte à votre nom qui vous enverra un message sur votre webmail dès qu'un contenu associé à votre nom est mis en ligne. Certains services existent ici ou là.**Si la vidéo a été diffusée …**
8. **Demandez systématiquement au site de dépublier le contenu gênant**
Exemple : si la vidéo a été mise en ligne sur Youtube : demandez à Youtube de supprimer cette vidéo. Si le site ne répond pas à votre demande sous deux mois, adressez vous à la CNIL en suivant la procédure de notre formulaire de plainte en ligne.
9. **En parallèle, demandez au moteur de recherche de déréférencer le contenu en cause**
Depuis un récent arrêt de la cour de justice européenne, les internautes peuvent saisir les moteurs de recherche d'une demande de déréférencement d'un contenu associé à leurs nom et prénom.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
formateur n°93 84 03041 84

Réagissez à cet article

Sources : http://www.net-iris.fr/veille-juridique/actualite/34611/arnaque-a-la-webcam-la-cnil-donne-des-conseils-pour-bien-reagir.php

http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/reagir-en-cas-de-chantage-a-la-webcam

Vie privée en danger : pourquoi nous sommes tous concernés | Denis JACOPINI

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

Vie privée en danger : pourquoi nous sommes tous concernés

Est-il possible de rentrer chez nous, d'écouter nos conversations et de s'immiscer dans notre intimité sans y être invité ? Nous avons découvert qu'il suffit pour cela d'une simple connexion Internet. Ordinateur, téléphone portable, réseaux sociaux et même cartes bancaires : désormais nous sommes en permanence connectés les uns aux autres. Mais nos informations personnelles sont-elles réellement bien protégées ? Pas si sûr…

Chaque semaine, de nouveaux scandales éclatent comme, par exemple, le vol, il y a quelques jours, de milliers de photos intimes de stars américaines. Et cela nous concerne tous : « phishing », vol d'identité, harcèlement numérique, vols de compte bancaire : chaque seconde, 17 personnes sont victimes de cyber-escroqueries à travers le monde. Car Internet a créé une nouvelle génération d'escrocs 2.0. Leur butin s'élèverait l'année dernière à 400 milliards de dollars. Un chiffre en constante augmentation. Nous avons découvert les failles des nouvelles cartes bancaires NFC, sans contact. Désormais, les pickpockets n'ont plus besoin de mettre la main dans votre sac pour voler votre argent.
Nous allons vous raconter l'histoire de différentes victimes françaises. Celle de Laetitia, en proie au cyber-harcèlement, qui a failli mettre fin à ses jours. Stéphane, lui, pensait avoir rencontré l'amour sur la toile ; il était en fait entre les mains de brouteurs de Côte d'Ivoire. Nous avons remonté leurs traces à Abidjan.

Nous nous sommes également rendus en Roumanie dans une ville hors du commun que le FBI a surnommée Hacker-ville. Là-bas, une grande partie de la population vivrait des cyber-escroqueries. Certains escrocs ont accepté de nous rencontrer ; d'autres après avoir été arrêtés par les forces de l'ordre ont décidé de mettre leur génie informatique au service de la société.
Enfin, vous découvrirez que pour protéger leurs ados des dangers du web, des parents ont trouvé une solution radicale. Christophe est un papa espion : il contrôle les moindres faits et gestes de ses trois enfants. Grâce à une panoplie de logiciels et d'applications, il a accès à l'intégralité du contenu de leur téléphone et ordinateur. Internet est sans aucun doute la principale révolution de ces trente dernières années mais c'est peut-être aussi la fin de la vie privée.

Réagissez à cet article

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

Source : http://www.m6.fr/emission-zone_interdite/28-09-2014-vie_privee_en_danger_pourquoi_nous_sommes_tous_concernes/