4 conseils pour éviter les cyber-attaques pendant les soldes | Denis JACOPINI

4 conseils pour éviter les cyberattaques pendant les soldes

Période propice aux achats en ligne, les soldes sont aussi prisées par les cybercriminels. Tour d'horizon des mesures à prendre pour se prémunir d'une attaque informatique.

Les soldes d'hiver démarrent aujourd'hui. Période de forte activité, les e-commerçants vont voir leurs ventes augmenter et cela ne manquera pas d'attirer les cybercriminels en tout genre. A cette période, chaque année, les entreprises tout comme les particuliers sont la cible de nombreuses tentatives de piratage, cependant quelques conseils simples peuvent éviter aux particuliers les arnaques.

Pendant un mois les soldes représente un pic d'activité pour les sites d'achats en ligne. Début 2014, selon une étude de la Fevad (Fédération du e-commerce et de la vente à distance) et du CSA, 7 internautes sur 10 envisageaient de préparer ou de faire leurs achats en ligne pendant les soldes. Parmi eux, 26% envisageaient d'effectuer leurs achats via smartphones. L'occasion idéale pour les pirates informatiques en quête de nouvelles victimes !

Pour se prémunir de ces attaques, les internautes peuvent prendre quelques précautions simples mais pourtant essentielles :

- 1. Veiller à toujours avoir les dernières mises à jour de ses applications, de son système d'exploitation et des logiciels de sécurité. Des failles sont régulièrement enregistrées et les correctifs sont présents dans les mises à jour, mais encore faut-il les effectuer!
- 2. S'en tenir aux règles d'or : Ignorer ou bloquer les pop-ups, utiliser un mot de passe original et sécurisé (aux oubliettes le 0000 ou le 1234), commander sur des sites fiables et via des connexions sécurisées en https.
- 3. Eviter de cliquer sur les liens directement depuis un emailing :le phishing reste à la mode, et il est particulièrement efficace en période de soldes lorsque des dizaines d'emails vous propose leurs bons plans quotidiennement. Si une offre est pertinente : mieux vaut retaper l'adresse sur son navigateur afin d'éviter tout soucis.
- 4. Eviter les transactions depuis des réseaux Wi-Fi publics. La plupart des réseaux publics (gares, cafés, etc) ont un niveau de cryptage faible, et donc une moindre sécurité. Les informations bancaires pourraient atterrir dans les mains d'une tierce personne. Que l'on soit connecté depuis un ordinateur, une tablette, ou un mobile, mieux vaut donc se méfier des réseaux ouverts.

Autre point sensible : Les achats via smartphones et tablettes sont de plus en plus communs, mais il est important de se méfier lors de son shopping. En effet, ces terminaux font face à de nombreuses menaces et sont souvent moins bien sécurisés que les ordinateurs.

Ici aussi des règles d'or s'appliquent : ne pas télécharger d'applications gratuites et de propriétaires inconnus sur internet afin d'éviter les trojans, acheter et visualiser les comptes seulement via des applications propriétaires (celles de sa banque ou celles d'e-commerçants), supprimer l'historique de navigation, le cache et les cookies régulièrement afin de supprimer les données sensibles.

Après cette lecture, quel est votre avis ? Cliquez et laissez-nous un commentaire...

Source :

http://www.lesechos.fr/idees-debats/cercle/cercle-120665-4-conseils-pour-eviter-les-cyber-attaques-pendant-les-soldes-1080620.php

Formation RGPD pour devenir DPO de votre organisme — Prochaine formation les 17 18 et 19 septembre 2018 à Paris



Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection ontinale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité. Formation pour DPO « Je veux devenir le Délégué à la Protection des Données de mon établissement » : 2 jours (Mettez en place une démarche de mise en conformité RGPD) Conformité avec Le RGPD au sein de votre établissement. informatique <u>spécialisé en cybercriminalité et en RGPD (protection des Domnées à Caractère Personnel)</u>, consultant depuis 1996 et formateur depuis 1998. J'ai bientôt une expérience d'une dizaine active à la Protection des Domnées à Caractère Personnel. De formation d'abord technique, Correspondant ONIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des mateur, il n'est ainsi aissé d'expliquer le coté pragnatique de la démarché de nise en conformité avec le RGPD. Données, en tant que praticien de la mise en conformité et formatter, il n'est ainsi sies d'expliquer le coté promation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récement Délègué à la Protection des « Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. » Votre Prénom / NOM (obligatoire) Votre adresse de messagerie (obligatoire) Un numéro de téléphone (pour faciliter l'organisation) Yous souhaitez avoir des informations sur :

① - la formation « Comprendre le RGPD » : 1 jour

① - la formation » Le veux devenir Déléqué à la Protection des Données » 2 jours

② - la formation » Le mets en conformité mon établissement » 3+1 jours

② - la formation » Hise en conformité RGPD sur mesure »

② - un accompagnement personnalisé au RGPD aitez réserver une ou plusieurs place(s) à la formation : ras de date de preude pour i install. Face à une importante demande no formations et en accompagnements personnalisés ou individuels, nous avons momentamément interrompu l'organisation de formations de groupe. Nous sommes néammoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. Whétietze pas à nous faire par ted evos besoins et voyons ensemble si nous pouvons vous trouver une solution. Pas de date de prévue pour l'instant. Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons m Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution. Formation pour consultants : « J'accompagne mes clients dans leur mise en conformité avec le RGPD » Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néamonis à votre entière disposition si vous soubhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution. □Autre ville ou sujets souhaités en individuel (indiquez ci-dessous) Envoyer Nos formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre accepte. Si la formation était annulée (nombre de participants insuffisants ou en cas de force assjeure), votre accepte sera remboursé en intégralité dans les 3 jours (les chèques seront encaissés à partir du jour de la formation). En cas d'annulation de votre part mains de 48 heures avant la formation, l'accepte pourrain peus sêtre remboursé car de régler les fraits de rélavartion de salle et d'organisation, eux même non remboursables.

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



DÉSIGNATION N° DPO-15945





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

Contactez-nous

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

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

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





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

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

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

Comment devenir DPO Délégué à la Protection des Données

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

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

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

Source : Denis JACOPINI et Règlement européen : se préparer en 6 étapes

5 règles d'or pour les utilisateurs des réseaux sociaux | Denis JACOPINI



Le nombre total d'individus dans le monde est de 7,4 milliards. Fin 2015, Facebook a atteint les 1,59 millions d'utilisateurs. Avec une augmentation annuelle de 17%, le géant des réseaux sociaux est tout simplement trop important pour être ignoré. Ceci étant dit, c'est aussi vrai pour beaucoup d'autres réseaux sociaux

les 310 millions d'utilisateurs actifs par mois sur Twitter postent 347 222 fois en moyenne. Plusieurs d'entre eux tweetent plus d'une centaine de fois par jour, et nombreux sont ceux à tweeter une fois par jour. Plus de 40

millions de photos ont été partagées sur Instagram depuis son lancement, et plus de 80 millions de photos y sont publiées chaque jour. Ceci représente une énorme quantité de données : certaines importantes, d'autres intéressantes ou encore inutiles. Les réseaux sociaux, avec leurs propres tendances et leurs propres lois, fonctionnent comme une extension du monde réel, qui a un énorme impact sur nos v 1. N'alimentez pas les trolls Les trolls sur Internet sont des provocateur nos vies hors-ligne. Dans cet article, nous vous dévoilons quelques règles simples que chaque utilisateur de réseaux sociaux devrait garder en tête.

Les troils sur Internet sont des provocateurs qui se joignent à des conversations dans le but d'agacer les autres utilisateurs pour le « fun ». On peut trouver des troils n'importe où : sur les forums, les chats, et autres plateformes de communication en ligne. Les forums des nouveaux médias sont connus pour la participation élevée de troils. D'ailleurs, il y en a plein sur les réseaux sociaux. Comment devez-vous parler aux troils ? D'aucune façon ! Ignorez-les. Plusieurs personnes se font prendre au piège et engagent alors des débats houleux en essayant d'expliquer leur point de vue et passent une grande partie de

leur temps et de leur énergie en vain. Quelqu'un a toujours tort sur Internet. Ne perdez pas votre temps et votre énergie pour des trolls.



Si vous n'avez pas de chance, vous pourriez tomber sur un troll en quête de revanche, en spammant votre e-mail, ou même en essayant de ruiner votre vie. Par exemple, un couple américain a perdu du temps, de l'argent, leur travail et même détruit leur mariage en étant les victimes de cybercintimidation, se traduisant par des canulars téléphoniques (swatting) et autres formes d'harcèlement hors-ligne.

2. Ne postez pas ou ne partagez pas de contenu illégal

Les Emirats Arabes Unis et la Nouvelle Zélande disposent de lois qui punissent sévèrement les trolls et la cyberintimidation avec des sanctions allant de 35 000\$ à la prison.

Toutefois, vous pouvez écoper d'une amende ou même être confronté à des conséquences bien plus graves pour avoir posté, partagé du contenu ou toutes autres actions relatives dans bon nombre de pays. Par exemple, deux hommes ont été condamnés à quatre ans de prison après avoir créé une page facebook qui encourageait une eu Dengladeshe à eté envoyé en prison pour avoir plaisanté sur son souhait de voir le premier ministre mort. Par conséquent, mieux vaut être au courant des lois de chaque pays et de s'en souvenir au moment de publier ou partager sur Facebook ou Twitter.

3. Ne partagez pas des arnaques

Les fraudeurs piègent souvent les victimes avec des histoires choquantes telles que des bébés mourants, des chiots qui se noient, ou d'anciens combattants. De tels articles font le tour des réseaux sociaux en criant à l'aide. En réalité, ils sont déployés dans le but de voler de l'argent, de diffuser des malwares et des méthodes d'hameçonnage.



ollow

City News CityNews Toronto

_@CityNews

Consumers warned about online scam involving free puppieshttp://ow.ly/YAgcm 3:14 AM — 22 Feb 2016

2020 Retweets

99 likes

be tels articles génèrent beaucoup de partages, mais la majorité d'entre eux sont des arnaques. De vrais appels au secours proviennent en général de votre famille, amis, et amis de vos amis. Ayez toujours en tête que ce sont les pages officielles des entreprises qui mettent en place ce type d'aide et non pas des individus inconnus. C'est la raison pour laquelle il vaut ineux rester vigilant et vérifier chaque article avant de cliquer sur « aimer » ou « partager ». Pas envie de tous les contrôler un par un ? Ne prenez donc pas de risques pour vous et

vos amis.

4. Pensez aux réactions des lecteurs

Vous avez probablement des collègues, des supérieurs et des clients parmi vos connections Facebook ou Instagram. Lorsque vous postulez pour un emploi, il est très probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines jettent un probable par exemple que les ressources humaines par le probable par exemple que les ressources humaines par le probable par exemple que les ressources humaines par le probable par exemple que les ressources humaines par le probable par exemple que les ressources humaines par le probable par exemple que les ressources humaines par le probable par exemple que les ressources humaines par le probable par exemple que les ressources humaines par le probable par exemple que les ressources humaines par le probable par exemple que les ressources humaines par le probable par exemple que le probable par exemple q

4. Penisez aux reactions des lecteurs vous avez probablement des supérieurs et des clients parmi vos connections Facebook ou Instagram. Lorsque vous postulez pour un emploi, il est très probable par exemple que les ressources humaines jettent un coup d'œil à votre profil sur les réseaux sociaux. Prenez en compte ce que vous voulez leur montrer, et plus important encore, ce que vous ne voulez pas.
Vous devez aussi réfléchir prudemment à ce que vous publiez sur les pages d'autres utilisateurs et sur des comptes publics tels que des entreprises ou des universités. Par exemple, en 2013, un homme originaire de Pennsylvanie a été renvoyé pour avoir «complimenté» une étudiante en ligne. Son commentaire n'aut rien de sexuelo ud "inapproprié, mais de toute évidence la mêre de la jeune fille n'avait pas apprécié. Un an auparavant, une professeure de Moses Lake, Washington, avait été virée parce qu'une femme qu'elle n'avait jamais rencontrée s'était plainte d'un de ces articles. Il s'agit de quelques exemples parmi tant d'autres qui prouvent qu'il vaut

nieux garder ses photos personnelles et ses articles pour des amis sûrs. Si vous avez besoin d'aide pour dissimuler vos articles privés des regards indiscrets, vous pouvez retrouver nos articles sur les paramètres de confidentialité de Facebook, Twitter, Instagram,LinkedIn, et Tumblr.

View image on Twitter



Kaspersky Lab ∏@kaspersky

Facebook privacy settings NOW https://kas.pr/3Wpw 8:13 PM - 26 Oct 2015

2525 Retweets

1313 likes

1313 likes

5. Ne dévoilez pas vos données publiques

De nombreux réseaux sociaux proposent d'« enregister » la géolocalisation lorsque vous prenez une photo, postez du contenu ou montrez les lieux que vous avez visités. Si vous êtes intéressé par un évènement, le réseaux social peut en informer vos amis au cas où ils voudraient vous accompagner.

Par défaut, tout le monde peut accéder à vos données, et les cybercriminels ont mille et une méthodes de s'en servir, ça peut aller de s'introduire dans votre maison jusqu'à voler votre identité numérique. C'est la raison pour laquelle nous vous recommandons vivement de dissimuler ce type des données à des personnes inconnues, à l'aide des paramètres de confidentialité de Facebook.

C'est aussi une bonne occasion pour que vous n'ajoutiez pas n'importe qui aveuglément : les gens envoient des demandes d'amis qui peuvent s'avérer être des bots, des trolls ou même des hackers. Même si Facebook vous informe que vous avez des dizaines of amis en commun, n'acceptez pas de demandes si vous n'êtes pas certain que ce soit des connaissances sûres.



- Formations et conférences en cybercriminalité
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Original de l'article mis en page : 5 règles d'or pour les utilisateurs des réseaux sociaux | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

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



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

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

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

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

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



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

Vous souhaitez rechercher des preuves dans un téléphone, un smartphone ou une tablette ?

Contactez-vous

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



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



Contactez-nous



RGPD : Vous voulez vous mettre en conformité ? Voici comment faire



Depuis le 25 mai 2015, le ROPO (Mèglement européen sur la Protection des Données) est applicable. De nombreuses formalités apprisés de la COLL ent dispare, de la consensable les conformatios est renforcée. Ils deivent désormais assurer une protection optimale des données à chaque instant et La mise en conformité est une démarche avant tout réglementaire. Elle doit d'abord commencer par un audit avec de nombreux référentiels relatifs à la protection des données à caractère personnel parfois précédée par une sensibilisation du Responsable de Traitement et de certains de ses salariés (la partie pédagogique de la démarche).

Ensuite, doit suivre la mise en conformité destrèa à améliorer l'évistant en vue de l'approcher le plus possible des règles.

Enfin, doivent suivre des contrôles réguliers compte tenu que les éléments tels que le contexte, les règles et les risques évoluent sans cesse. Vous souhaitez faire appel à un expert informatique qui vous accompagne dans la mise en conformité avec le RGPD de votre établissement ?

De om présente a Donis JACOPINI. De quis Expart en informatique assurement et <u>saticialiste</u>. En MEDI instruction des Données à Acractive Personnella Let. a cobercimisable. Convoltent despois 1906 en formation despois 1908, or la une experience depuis 2012 dans la misse en conformité avec la réglementation relative à la Protection des Données à Caractive Personnell. De formation d'abord technique, Correspondent Informatique et Limitative à la Protection des Données (DPO n'15845), en tant que praticion de la misse en conformité avec le REPOIX.

« Mon objectif est de mettre à disposition toute me expérience pour mettre en conformité votre établissement avec le REPOIX.

Vous souhaitez vous mettre en conformité avec le Règlement (UE) 2016/870 du parlement européen et du Conseil du 27 avril 2016 (dit 16070) et vous souhaitez vous faire accompagner. Au fil des années et depuis les mises en conformité avec la loi n' 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nous avons constaté que les mises en conformité devaient se dérouler (et encore à ce jour avec le RGDO) selon 3 phases principales :

1. * Assays de contexte e seu ve dérouler (et encore à ce jour avec le RGDO) selon 3 phases principales :

2. * Hiss en place da La conformité RGDO » avec amélioration des traitements et les mentres acceptables ou conformes. Ceci inclue dans bisen des cas l'enaltyse de risque;

3. * Suivi de l'évolution des traitements » en fonction de l'évolution des traitements et les mentres acceptables ou conformes. Ceci inclue dans bisen des cas l'enaltyse de risque;

3. * Suivi de l'évolution des traitements » en fonction de l'évolution des conformité RGDO » avec amélioration des l'évolution des traitements en vue de les rendre acceptables ou conformes. Ceci inclue dans bisen des cas l'enaltyse de risque;

3. * Suivi de l'évolution des traitements » en fonction de l'évolution des conformité RGDO dans le temps.

Pour chacume des phases, nous vous laissons une totale liberté et vous choisissez si vous souhaiter :

• * Faire > (nous vous apprenons et vous poursuiver le maintem de la size en conformité tout en apparent étour en systement en conformité ou de la value de la size en conformité tout en apparent s'equitrement un rapport des actions réalisens pour de la conformité de votre établissement en totale autonomie et vous établissons régulairement un rapport des actions réalisées opposable à un contrôle de la CNIL).

Denandez un devis avec le formulaire ci-dessous

Part. Cast. and. inselect approach. A fair. Assau accossors. A since mass A fair.

1. Use formation of use journed poor vox assessible as a MSPO : A proposed to MSPO is a cqu'il fast avoir pour bies démarrer »;

2. Use formation de deux jours pour les futurs ou actuels DFO : A be veux devenir le Délégéé à la Protection des Données de mon établissement »;

3. Use formation une' jours pour les tratures ou actuels DFO : A be veux devenir le Délégéé à la Protection des Données de mon établissement »;

3. Use formation une' jours pour les tratures ou actuels approache à actue no conformité uver le REFD ».

Afin de vous communiquer une indication du coût d'un tel accompagnement, nous aurons besoin d'éléments sur votre structure : Durée dépendant de la taille, de l'activité et des ressources de votre établissement

Nous vous garantissons une confidentialité extrême sur les informations communiquées. Les personnes habilitées à consulter ces informations sont soumises au secret professionnel.

N'hésitez pas à nous communiquer le plus de détails possibles, ceci nous permettra de mieux connaître vos attentes.

Votre Prénom / NOM (obligatoire)

Votre Organisme / Société (obligatoire)

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (ne sera pas utilisé pour le démarchage)

Vous pouvez nous écrire directement un message dans la zone de texte libre. Méanmoins, si vous souhaitez que nous vous établissions un chiffrage précis, nous aurons besoin des informations ci-dessous.

Afin de mieux comprendre votre demande et vous établir un devis, merci de nous communiquer les informations demandées ci-dessous et cliquez sur le bouton "Envoyer les informations saisies" en bas de cette page pour que nous les recevions. Une réponse vous parviendra rapidement.

VOTRE ACTIVITÉ

Détails sur votre activité : Étes-vous soumis au secret professionnel ? Votre activité dépend-elle d'une réglementation ? Si "Oui", laquelle ou lesquelles ?

O0ui⊕NonOJe ne sais pas O0ui⊕NonOJe ne sais pas

vous nous décrire la composition de votre système informatique. Hous souhaiterions, sous forme d'énumération, connaître les équipements qui en quelconque accès à des données à caractère personnel avec pour chacun des appareils 7005 le(s) legicial(s) utilisé(s) et leur(s) fonction(s

ypscome annumenaque, mous sommateranes, sous torme d'énumeration, consaitre les equipments qui ont un quelconque accès à des données à caractère personnel avec pour chacun des appareils TOUS le(s)

- serveur MEB avec site Internet pour faire commattre non activité;
- l'ordinateur fixe vec ogiciel de fracturation pour facturer mas clients;
- l'addinateur fixe vec ogiciel de fracturation pour facturer mas clients.
- l'avec logiciel de massagerie électronique pour corresponders evec des clients et des prospects traitsement de testes pour la correspondence » logiciel de facturation pour facturer mes clients.
- l'avec logiciel de messagerie électronique pour corresponders de commandation de commandation de la structure ;
- santiphone avec logiciel de messagerie électronique pour corresponder avec des clients et des prospects.

- i smartphonne avec logiciel de messag Avez-vous nou plusieurs sites Internet ? Quel(s) est(sont) ce(s) site(s) Internet ? Avez-vous des données dans le Cloud ? Quel(s) fournisseur(s) de Cloud(s) utilisez-vous ?

O0ui⊕NonOJe ne sais pas

VOS TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL
Si vous avez déjà établi la liste des traitements de données à caractères personnels, pourriez-vous nous en communiquer la liste (même incomplète) ?

DDENSIONMENT DE VOTRE STRUCTURE

Nombre de salariés de votre structure :

Parmi ces salariés, combiem utilisent un équipment informatique ?

Nombre de services** dans votre structure (ecemple : Service commercial, service technique...) :

Merci d'émounter les services** de votre structure :

O0ui⊕NonOJe ne sais pas

Merci d'énumérer ces sou-i-traiants :

Travaillez-vous avuc des pretataires qui interviencent dans vos locaux ou dans vos agences ?

Merci d'énumérer ces prestaires :

Avec combien de sociétés d'informatique travaillez-vous ?

Merci d'énumérer ces sociétés d'informatique en indiquant les produits ou services pour lesqueis elles interviennent et eventuellement leur pays :

VOTRE SITUATION VIS-À-VIS DU RGPO
Votre établissement échange t-il des données avec l'étranger ?
Si oui, avec munifolome ?

Oʻʻui⊕NonOJe ne sais pas Oʻʻui⊕NonOJe ne sais pas Oʻʻui⊕NonOJe ne sais pas

Si oui, avec quel(s) pays ?
Arez-vous déjà été sensibilisé au RAPO ?
Les personnes utilisant un équipement infornatique on-telles déjà été sensibilisées au RAPO ?
Si vous ou vos collaborateurs n'ont pas été sensibilisés au RAPO, souhuitez-vous suivre une fornation ?

L'analyse des conditions de traitements de données dans votre local professionnel ou vos locaux professionnels fait parti
Disposez-vous de plusieurs bureaux, agences etc. dépendant jurisiquement de votre établissement ?

"Oul", combair "Oul", com

O0ui⊕Non

Nous pourons vous accompagner de différentes manières.

A) Mous pourons vous accompagner de différentes manières.

B) Nous pouvons vous accompagner au début puis vous aider à devenir autonome ensuite (accompagnement, audit + formation);

C) Yous pouver choisir de nous confare la testilait de la démarché emis en conformate (accompagnement);

D) Nous pouvers vous accompagnement soulaite de la formation de maise en conformate (accompagnement);

Ouel type d'accompagnement soulaite vous de notre pare (AdVICA - décalis);

Ouel type d'accompagnement soulaite vous de notre pare (AdVICA - décalis);

Si vous le souhaitez, vous pouver nous communiquer des informations complémentaire telles que :

- Nombre d'agences au total (qui dépendent de l'établissement principal = qui n'ont pas leur propre numéro SIRET);

- Nombre d'agences au totals (qui dépendent de l'établissement principal = qui n'ont pas leur propre numéro SIRET);

- Nombre d'agences au total qui nt pas leur propre numéro SIRET;

- Nombre d'agences que votre structure a en France;

- Ungence de votre projet;

- Toute information complémentaire que vous juperez utile pour nous permettre de mieux connaître votre projet.

Envoyer les informations saisies

[block id="24086" title="Mentions légales formulaires"]

* = Données à Caractère Personnel
de commercial, Service technique, Service pédagogique, Serv

ervice administratif et financier.

ou bien, envoyez un e-mail à ropd[a-ro-ba-sellene

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









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

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de mise en conformité avec le RGPD.

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

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





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

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

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

Comment devenir DPO Délégué à la Protection des Données

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

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles

en 6 étapes

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

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

Source : Denis JACOPINI

Attaques informatiques : Comment s'en protéger ?



Attaques informatiques : Comment s'en protéger ? Les cyberattaques se faisant de plus en plus nombreuses et sévères, les entreprises doivent apprendre à s'en protéger. Pour cela, les directions juridiques et de l'informatique peuvent s'appuyer sur l'expertise de la police judiciaire et des experts en data protection.

Tous les quinze jours en moyenne, une attaque sévère — où des données sont exfiltrées — est découverte. Face à ce constat, le tribunal de commerce de Paris a réuni quatre tables rondes d'experts de la sécurité informatique, des représentants de la police judiciaire et des experts-comptables fin juin pour examiner les solutions de protection dont disposent les données qu'ils utilisent et partagent, les formatique des représentants de la police judiciaire et des experts-comptables fin juin pour examiner les solutions de protection dont disposent les données qu'ils utilisent et partagent, les formatiques des décirités : les utilisateurs, car ce sont eux qui choisissent les données qu'ils utilisent et partagent, les formatiques des décirités et l'ensdément d'un data cettre conseillé.

Prévention

reventum.

All est difficile d'apir lorsque l'attaque a déjà en lieu », précise Sylvie Sanchis, chef de la Befti (1) de la police judiciaire de Paris. Le moyen le plus efficace dont disposent les entreprises pour se protéger est donc la prévention. Il faut avant tout investir dans la sécurité informatique. Si certaines sociétés sont réticentes en raison du coût, il est important de rappeler qu'il sera toujours moindre que celui engendré par une attaque.

les modes opératoire

Less modes opératoires d'ediffration des données se diversifient et se sophistiquent au fil des années. Certains se veuelent discrets afin que l'entreprise me preme commissance de l'attaque que très tardivement, d'autres relievent du chantage ou de la demande de rasquor.

L'attaque peut veuir d'un mait qui, à son ouverture, télécterpreu nu vivrus sur l'ordinanteur de l'employe, les données peuternis de l'employe que aprendir à se s'inni (annaque aprendir). Quant aux monomeres, il s'aguit de l'aquitele naturellant se prettant de nançuner l'entreprise pour garvenir à se s'inni (annaque aprendir). Quant aux monomeres, l'aguit de l'aquitele naturellant se prettant de nançuner l'entreprise pour garvenir à sonnées. Bonn ce cas, Anne Souvira, changée de sission aux questions l'entreprise pour garvenir de service sonnées. Sonnées comme comme avoir aux monomeres, l'aguit de l'aquitele de prettain de la change de sission aux questions de l'aquite de l'aprendir de

L'importance de porter plainte

La réaction à adopter, la plus rapide possible, fait partie de la sécurité informatique : « C'est un travail de réflexion en amont qui permettra d'adopter la bonne stratégie », selon Ciryl Piat, lieutenant-colonel de la gendarmerie metionale. Suite à une cyber-attaque, la plupart des entreprises sont réticentes à porter plainte, par peur d'une mauvaise réputation ou par scepticisse vis-à-vis de la rétlet utilité de cette procédure. Alice Cherif, chef de la section « cybercrimanité » du parquet de Paris, précise que la plainte présente l'avantage d'identifier les éléments d'inventantain » de l'inventantain » de la financia de l'avantage d'identifier et partie une manure procédure. Alice Cherif, chef de la section « cybercrimanité » du parquet de Paris, précise que la plainte présente l'avantage d'identifier les éléments d'inventantain » de l'inventantain » de l'inventantain

L'utilité du cloud

L'une des façons de sécuriser ses domées est de les confier à un tiers spécialiste qui les stockera en ligne sur un cloud. « Il s'agit d'un système complexe commecté sur Internet, où les domnées sont stockées sur des disques durs physiques situés dans des salles d'hébergement, les fameux data centers », explique Julien Levrard, chef de projet sécurité chez OWM. Le cloud rend l'accès plus difficile aux malfaiteurs d'autant qu'ils ignorent la localisation de la domnée. Vigilance et prévention : les malitres mots en matière de cybercriminalité.

(1) Brigade d'enquête sur les fraudes aux technologies de de l'informatio



Original de l'article mis en page : Cybercriminalité : comment se protéger ? — Magazine Decideurs

Quelques préconisations sur la géolocalisation des personnes vulnérables | Denis JACOPINI



Ouelques préconisations sur la géolocalisation des personnes vulnérables Les particuliers. les établissements hospitaliers ou médico-sociaux peuvent aujourd'hui utiliser des appareils de suivi électroniques (bracelets. boîtiers. etc.) pour assurer la sécurité de

- Afin de respecter les droits de ces personnes, la CNIL a fait les recommandations suivantes :
 Recueillir si possible l'accord de la personne concernée ou celui de ses représentants légaux ou de ses proches. La personne doit au minimum être informée ;
- Les appareils doivent pouvoir être désactivés et réactivés par les personnes concernées, lorsque celles-ci sont en possession de leurs moyens ;
- · La procédure de gestion des alertes doit être précisée dans un protocole ;
- Privilégier les systèmes qui laissent à la personne concernée l'initiative de la demande d'assistance, plutôt qu'une su
- S'appuyer sur une évaluation personnalisée des risques et non sur une logique de prévention collective. La géolocalisation ne doit pas être utilisée systématiquement pour toutes les personnes âgées ou tous les enfants accueillis dans un établissement.

Avant de faire le choix d'utiliser ce type d'appareil, une évaluation collégiale et pluridisciplinaire doit donc être menée par l'équipe qui prend en charge la personne vulnérable.

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 ?

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

Un avis ? Laissez-nous un commentaire !

S o u r c e
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=9DCFCE66E3DC38F485EA18F87E1E023F?name=G%C3%A9olocalisation+des+personnes+vuln%C3%A9rables+%3A+les+pr%C3%A9conisations+de+la+CNIL&id=299

Usurpation d'identité, propos diffamatoires, concurrence déloyale, atteintes E-réputation Nous pouvons vous aider | Denis JACOPINI



Victime de la cybercriminalité: Quelqu'un vous #insulte sur Internet (propos diffamatoires), se fait passer pour vous (usurpation d'identité sur Facebook, Twitter, viadeo, linkedin, instagram, par e-mail), ou diffuse certaines de vos informations confidentielles, vous pouvez rapidement devenir victime d'une atteinte à votre e-réputation.

confidentielles, vous pouvez rapidement devenir victime d'une atteinte à votre e-réputation.

Pour initier une action vers la personne malveillante en direction soit d'une arrangement à l'amiable ou d'une action judiciaire, vous devez constituer un dossier avec un maximum d'éléments prouvant la légitimité de votre action.

Denis JACOPINI, Expert Informatique assermenté et spécialisé en protection des données personnelles et en cybercriminalité a rassemblé dans ce document quelques actions qui devront être menées et est en mesure de vous conseiller et de vous accomplians vos démans vos démanches.

Nous pouvons classer les atteintes à la e-réputation en 3 grandes catégories :

a) Attaintes à la vie privée (par exemple en diffusant ou divulguant des informations personnelles ou confidentielles)
b) Délaigrements, injures, propos diffamatoires, citations hors contextes et médisances
c) Usurpation d'identité
Lors qu'un expert est contacté pour une mission sur un de ces sujets, un constat d'huissier peut éventuellement avoir été demandé, notamment pour constater les faits reprochés. Sans constat, l'expert devra se baser soit sur les informations ou doci
que lui communiquera la victime (avec pour issue une vérification de l'exactitude ou de l'intégrité des informations) ou bien procédera à un constat des faits lors de sa mission.

Plusieurs types d'informations peuvent être soumises à l'expert : Expertiser un e-mail, un post sur un forum, un réseau social ou bien des informations apparaissant sur des supports tels qu'un moteur de recherche, annuaire Internet ou bien un site Internet se fait d'abord en analysant le contexte, puis en réalisant

Expertise d'E-mails En l'absence de pro-fff

Expertise d'E-mails

B. l'absence de procédés de signature électronique garantissant l'intégrité absolue d'un e-mail et de procédé de traçabilité pouvant garantir l'envoi et la distribution dans la boite destinataire d'un e-mail, et, étant quasiment systématiquement dans l'impossibilité de pouvoir expertiser le système informatique à la fois de l'expéditeur et du destinataire, l'expert est souvent blen démuni pour prouver l'absence de fraude dans un « change électronique.

Les prenaires informations à roi relever sont blen évidement la « date de l'e-mail », « l'identité du un des correspondants» mais aussi une information qui apporte une véracité supplémentaire au mail incriss précédement cau mail incriss précédement plant de l'e-mail se pueunt certs event informations insissions précédement relevées, mais également avoir des informations sur les serveurs source, destination et intermédiaires impluyés dans l'échange electronique. (LA FONCTION D'AFFICIAMED DE L'ENTER D'UN BHAIL FAIT PANTED DE LA PURPANT DES LOGICIELS DE MESSAGENTE!

La dérariare information privant être fort utile consiste à rechercher des informations sur les serveurs source, destination et informations sur les serveurs apporter des éléments persentant à l'avocat d'emagaer auprès de la personne à qui l'atteint à la e-réputation est reprochée une demande de réparation à l'amiable ou par voie judiciaire.

Avec les éléments recueillis permettre des éléments persenter une requête à un juge, laquelle permettra à l'expert d'obtenir d'autres éléments reclueilles permettant à l'avocat d'emagaer auprès de la personne à qui l'atteint à la e-réputation est reprochée une demande de réparation à l'amiable ou par voie judiciaire.

Lire notre dossier au sujet des signatures éléctroniques.

Lire notre dossier au sujet des signatures électroniques http://www.lenetexpert.fr/dossier-du-mois-j-inju-2041-lutilisation-juridique-documents-numeriques-lere-dematerialisation-outrance/ Expertise de post sur forum ou sur les réseaux sociaux ?

Ex forums ou les réseaux sociaux pevennt être aussit les dépositaires malgré deux d'échanges ayant pour conséquence l'atteinte à la réputation d'une victime.

Les forums ou les réseaux sociaux pevennt être aussit les dépositaires malgré deux d'échanges ayant pour conséquence l'atteinte à la réputation d'une victime.

Les presières informations à relever sont bien évidement la « date du message » et « l'identité de l'auteur ». (LOFUNES DECANN DATEE, DOSE SOURCE, ECANNES AVEC LE FOURNISSEUR DU SERVICE)

D'autres éléments peuvent nous auter à identifier l'auteur physique d'un message par recoupement d'informations recueillies sur literent ou dans d'autres sites d'échanges tels que des indices dans les propos ou des informations dans les images utilisées (recherche sur Google, Social Mention, Samepoint, Mention met, Alerti, Youscesi, Sprout Social, «Cairn.com, zen-reputation com.).

Tout comme avec les éléments permettant d'identifier l'auteur didition d'un evail. ('expert pour apporter des éléments permettant d'identifier l'auteur des faits permettant ainsi d'engager seul ou au travers d'un l'avocat, auprès de la personne à qui l'atteinte à la e-réputation est reprochée une demande de réparation à l'amable ou par voie judiciaire.

L'atteints recueille permettent, par voie judiciaire, de présenter une requête à un juge, tapautie permettra d'autres éléments techniques relatives à l'échange.

Remarque : En cas de difficulté de faire retirer l'information à l'origine de l'atteinte à la E-réputation, la technique du Flooding peut être utilisée. Elle consiste à noyer l'information par une profusion d'information au contenu cette fois maîtrisé et

Intelligement choisi.

Expertise d'informations sur des annuaires ou de sites Internet

Lorsque des contenus portant atteinte à l'E-réputation se trouvent sur des sites Internet, la procédure consiste à identifier le responsable du contenu portant atteinte à la réputation de la victime. Le point d'entrée pour avoir des infor au nom de domaine est principalement le bureau d'enregistrement pouvant nous renseigner sur les coordonnées des différents contacts.

Nous pouvons faciliement nous trouver confrontés à plusieurs contacts:

**Le contact qui a déposé le nom de domaine.

**Contact qui a déposé le nom de domaine.

Nous pouvons facilement mous trouver confrontés à plusieurs contacts :
le contact qui a réglé le nom de domaine
celui qui a réglé l'hébergement
celui qui a réglé l'hébergement
celui qui a réglé l'hébergement
celui qui a mis en ligne l'sinformation incrisinée
celui qui a mis en ligne l'sinformation incrisinée
celui qui a mis en ligne l'sinformation concernée
(Ecci peut représenter autant de contacts pouvant être impliqués ou non dans notre expertise.
Le point d'entrée pour avoir des informations sur ces contacts est principalement le bureau d'enregistrement (registrar en anglais) est une société ou une association gérant la réservation de noms de domaine Internet).
Nous pouvons avoir plus d'information sur les différents contacts relatifs à un non de domaine (propriétaire, contact administratif, contact technique) en utilisant la fonction « whois » proposé par les bureaux d'enregistrement ou sur https://www.fusin.cet.
Voici quelques exemples de registres avec les domaines de premier niveau qu'ils maintiennent :
Verisign, Inc. : .com; .net; .come
Public Interest Régistry et Afilias : .org;
Afilias : .info;
CIRA : .ca;
DEMIC: .de;
DEMIC: .de;
Requevel : .di;
AFILIS : .finfo;
CIRA : .ca;
CELICA : .ca :

http://whois.domaintools.com

* http://www.stowaruovsca.com/ Down.informalist. Down.informalist. Down.informalist. Down.informalist. Down.informalist. Down.informalist. Tributiarist. Statistics. Tributiarist. Tribu nonymat d'un particulier (personne physique), titulaire d'un nom de domaine enregistré sous diffusion restreinte (le nom et les coordonnées du

Enfin, il peut être parfois utile de retrouver le contenu d'un site internet à une date antérieure.

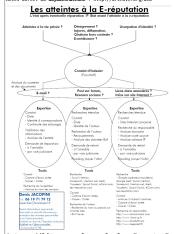
Enting, it peut etre part loss titze de recrouver te concenie du miscre de date anterieure. Am de date anterieure.

Pour cela, il existe un outil perpésentant les arrivies d'Internet : Internet Archive.

L'Internet Archive, ou IA est un organisme à but non Lucratif consacré à l'archivage du Web et situé dans le Presidio de San Francisco, en Californie. Le projet sert aussi de bibliothèque numérique. Ces archives électroniques sont constituées de cliché instantanés (copie de pages prises à différents moments) d'Internet, de logiciels, de films, de livres et d'enregistrements audio.

Site Internet de Internet Archive : https://archive.org

: http://archive.org/web Accès direct au WayBackMachine



Autres délits pour lesquels les Experts Informatiques peuvent être contactés:

Le cybersquatting

Le cybersquatting

Le cybersquatting, aussi appelé cybersquattage, est une pratique consistant à enregistrer un nom de domaine correspondant à une marque, avec l'intention de le revendre ensuite à l'ayant droit, d'altérer sa visibilité ou de profiter de sa notoriété.

Parmal les buts recherchés par les cybersquatteurs nous avons:

- Spéculation au nom de domaina un nom de domaina un mon de domaine au nom de domaine un mon de domaine de l'ayant-droit, pour que celui-ci achète le nom de domaine au cybersquatteur à un tarif élevé.

- Page parking

Le nom de domaine contient des liens sponsorisés qui rapportent des revenus au cybersquatteur. Idéalement, les liens sponsorisés sont en rapport avec le thème de la marque parasitée.

num de domaine contación de contrefaçon, le cybersquatteur reprenant les repères visuels de la boutique nom de domaine pointe vers une boutique vendant généralement des produits similaires au commerçant dont la marque est cybersquattée. Il s'agit souvent de produits de contrefaçon, le cybersquatteur reprenant les repères visuels de la boutique nom de domaine pointe vers une boutique vendant généralement des produits similaires au commerçant dont la marque est cybersquattée. Il s'agit souvent de produits de contrefaçon, le cybersquatteur reprenant les repères visuels de la boutique officielle. Cette pratique s'apparente au phishing car il s'agit de piéger le consommateur en usurpant l'identité d'un tiers.

Nuisance à la marque site fait passer un message péjoratif ou dénigrant à l'égard de la marque.

Le site fait passer un message péjoratif ou dénigrant à l'égard de la marque.

Les actions possibles contre le cybersquattage.

En France, le cybersquattage riset pas passible de sanctions pénales, seules des actions civiles sont envisageables.

Les actions les plus courantes concernent en atteinte à une marque (propriété intellectuelle) ou encore parasitisme. Des actions peuvent respectivement être portées devant le tribunal de grande instance (TGI) ou le tribunal de commerce dans le cas di
conflit entre commerçants.

Procédure extrajudiciaire :

Procedure extrajuniciaire:
Les organismes qui gérent les noms de domaines (registres) et les parties prenantes (titulaire du nom de domaine et ayant-droit sur la marque) étant souvent de nationalités multiples d'une part, et les procédures judiciaires étant longues et couteuses d'autre part, l'ICANNI a mis au point une procédure extrajudiciaire permettant au plaignant de recourir devant le registre pour récupérer un nom de domaine : la procédure UDRP.
Cette procédure est payante et la décision et à la discriction du registre. Une décision judiciaire ultérieure prévoudre cpendant sur la décision suit ou UDRP.

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 ul a 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

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...
Source : http://www.metronews.fr/info/paris-on-refuse-de-lui-louer-un-appartement-a-cause-de-son-profil-internet/modC!uUpMqgL3WsBnc/

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



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

Toutes les fausses applications découvertes par ESET et détectées grâce à ESET Mobile Security (application lockscreen nommée « Pokémon GO Ultimate » et les applications scareware

« Guide & Cheats for Pokémon GO » et « Install Pokemongo ») ne sont plus disponibles sur Google Play. Elles ont été retirées de l'app Store suite à l'alerte donnée par ESET. Même si ces fausses applications ne sont pas restées longtemps sur le Google Play, elles ont généré quelques milliers de téléchargements. L'application « Pokémon GO Ultimate », a piégé entre 500 et 1.000 victimes, « The Guide & Cheats for Pokémon GO » en a atteint entre 100 et 50.000 téléchargements.

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

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

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

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

Conseils des experts en sécurité ESET pour les afficionados de Pokémon GO :

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

Conseils de Denis JACOPINI

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



Article original de ESET



Denis JACOPINI est Expert Informatique assermente spécialisé en cybercriminalité et en protection des

- Expertises techniques (virus, espions, piratages fraudes, arnaques Internet...) et judiciaire (investigations téléphones, disques durs, e-mails
- Expertises de systèmes de vote électronique
- Formations et conférences en cybercriminalit
- Formation de C.I.L. (Correspondants Informatique
 of Libertée)
- Accompagnement à la mise en conformité CNI de votre établissement.



Contactez-nous

Demande de Devis pour un audit RGPD





Demande de Devis pour un audit RGPD

April 12 M (W) (W) page upon 1 / folia to the cold (page A) and the cold (page A) and the cold (page A) and the cold (page A) (W) (page A)			
The states of contract a state of the state			
The state of the s			
Section 1.			
tion can permission an confidentialist orbits not in toleration conscipts. In present initialists a consist on information unit vanion as somety permissioned.			
Enterly act that delegand by the delegand to print any and the appointment and the app			
N AND LANGUAGE REPORT			
State Strategies was the promotion of strategies			
No paradiant and in the final and a stage of the final and the final and a stage of the final and th			
WE AREA COLORIDAD COLORIDA			
	NOT A STATE OF THE PARTY OF THE		1
	Milled of our will be delicated in a second of the second	******	
The state of the s			
	b. It made impossible describerage part describerage part describerage de la propertie y largered de completation par france la regil la malignatura de la propertie de describera de describera de la propertie describerages part descripadar de des describera de des properties. Basis de la describeration de la properties de la		
	And could be distinct that is that I take I	*.*.*	
	No case and appropriate to their act translation as advance a contract parameter, purpose and activity of contract to the company of		
	Ballot de altra fondam de la fo	#	
	Transfer and the first facilities of	#1919 - 111 F	
	Material State of State (State of the State of S		
	The Financial and problems is a problem on a financial and the second of		
	THE STATE OF THE PARTY OF THE P		
	To be, and setting to the strong of		
	Visited, and selected pairs 1 Annual parameter and recognition and the selection an	*****	
	Visign as continue as horizontale as because due unto two professional and those professional and gallet as to desire as the professional and gallet as to desire as the desire as the professional and applicate professional and	•	
	The procedure country of the control of the country		
	Fig. 10 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1		
_			
* - Maria B. Collection Maria B. Collectio			

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



DÉSIGNATION N° DPO-15945





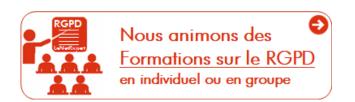
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

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

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

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





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

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

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

Comment devenir DPO Délégué à la Protection des Données

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

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

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

Source : Denis JACOPINI