Comment savoir si mon employeur a fait des déclarations à la CNIL ? | Denis JACOPINI

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

Comment savoir si mon employeur a fait des déclarations à la CNIL ?

Nous attirons votre attention sur le fait que cette information est modifiée par la mise en place du RGPD (Règlement Général sur la Protection des données). Plus d'informations ici : https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd Nous l'avons toutefois laissée accessible non pas par nostalgie mais à titre d'information.

Vous pouvez obtenir la liste des fichiers déclarés à la CNIL par votre employeur (vidéosurveillance, géolocalisation, recrutement, gestion du personnel, enregistrements des appels, etc.) en adressant une demande écrite à la CNIL. Précisez bien le nom de l'organisme concerné, son adresse postale et son numéro SIREN (il figure sur vos fiches de paye).

Adressez une demande à la CNIL

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)

Réagissez à cet article

Source : https://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=F5C86AFA2E4078840755E200A52C3452?name=Comment+savoir+si+mon+employeur+a+fait+des+d%C3%A9clarations+%C3%A0+la+CNIL+%3F&id=164

Guide des bonnes pratiques à adopter face aux risques numériques

Guide des bonnes pratiques à adopter face aux risques numériques

Issu des premiers constats réalisés par les référents de l'ANSSI en région, le guide d'élaboration en 8 points clés d'une charte d'utilisation des moyens informatiques et des outils numériques est une première réponse apportée aux PME et ETI.

Ce nouveau guide constitue le point de départ indispensable pour la mise en place ou de la réactualisation des bonnes pratiques à adopter face aux risques numériques.
S'il s'adresse avant tout aux PME et ETI, ce guide ne manquera pas également d'intéresser l'ensemble des organisations invariablement soumises aux mêmes problématiques.

PDF
Charte d'utilisation des moyens informatiques et des outils numériques
734.06 Ko

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Charte d'utilisation des moyens informatiques et des outils numériques – Le guide indispensable pour les PME et ETI | Agence nationale de la sécurité des systèmes d'information*

Un Employeur peut-il examiner

les messages échangés par ses employés sur leur téléphone professionnel ?

Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel ?

Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel ?

Dès lors que le téléphone du salarié est professionnel, l'employeur a ce droit, à moins d'avoir mentionné avant le message «personnel». Dans ce cas, l'employeur n'a plus le droit. Mais souvent, on n'oublie de l'écrire… »

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord*

Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ?

Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? #1

Un employeur peut-il consulter les courriels d'une messagerie professionnelle d'un de ses salariés ?

« L'employeur ne peut, hors présence du salarié, consulter ses messages sans son autorisation. Car, potentiellement, il pourrait y trouver des messages dits «personnels». Le principe, c'est qu'une messagerie ne peut pas être 100 % professionnelle. Quand on écrit un message à son conjoint pour le prévenir qu'on va être en retard par exemple. C'est donc toléré mais il ne faut pas en abuser. La seule condition pour l'employeur est dans le cas d'un danger grave : concurrence déloyale ou terrorisme. Mais, dans ce cas, cela nécessite la présence d'un huissier. »

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Connaissez-vous vos droits sur les données*

personnelles au travail (VRAI-FAUX) ? – La Voix du Nord

Comment se prémunir du phishing ? | Denis JACOPINI

Comment se prémunir du phishing ?

Le phishing, francisé sous le nom de „hameçonnage », est une méthode de fraude qui sévit sur le Web depuis 2005. Cette dernière permet de soutirer des données sensibles en exploitant les failles informatiques pour piéger les internautes.[popup show= »ALL »]

Un phénomène actuel omniprésent

L'actualité ne cesse d'en rapporter les méfaits :l'attaque de TV5 Monde, la création d'un phishing Google qui ressemble comme deux gouttes d'eau au célèbre moteur de recherche et l'élaboration d'une opération phishing pour s'évader d'une prison sont autant de phénomènes d'actualité qui démontrent que ce genre de fraude est de plus en plus perfectionné. Il est d'ailleurs estimé qu'un Internaute sur 10 se laisserait prendre au piège, c'est ce que révèle un article de Metronews. Afin de contrer ce phénomène,l'association Phishing-Initiative a été créée dans le but de protéger les internautes et de freiner les tentatives de phishing, toujours plus nombreuses.

Comment reconnaître un mail frauduleux ?

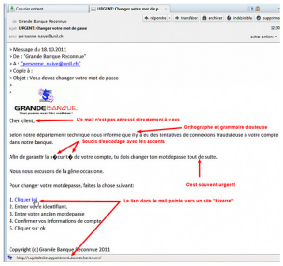
Comment repérer le vrai du faux ? Voici quelques méthodes qui permettent de voir si vous avez à faire à une tentative de phishing par e-mail :

• Votre e-mail semble provenir de votre banque et a l'air d'en être une copie originale, avec son logo et ses couleurs. Commencez par lire le message, si vous trouvez des erreurs d'orthographe ou des erreurs d'affichage, vous saurez qu'il ne s'agit alors que d'une pâle copie.

• Un message vous invite à vous rendre sur une page externe. Méfiance ! Avant de cliquer sur le lien, passez la souris sur le lien sans cliquer dessus. En bas à droite, vous découvrirez une URL « bizarre », qui n'a rien à voir avec l'entreprise.

• Le mail est trop insistant (dans le pire des cas, vous prédit une catastrophe) et vous demande expressément de donner vos codes bancaires et informations personnelles.

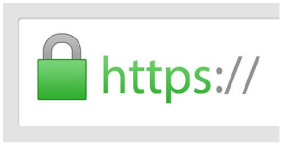
En voici un exemple type :



Flicker – phishing_exemple hameconnage pardownloasource.fr, CC BY 2.0, Certains Droits Réservés

Comment effectuer un paiement en ligne sécurisé ?

• Comment éviter la fraude et payer en toute sécurité quand vous faites vos achats en ligne ? Comment savoir s'il ne s'agit pas d'une tentative de phishing ? Vérifiez toujours lors de votre paiement que le site est sécurisé : l'URL débute par « https» et est accompagnée d'un petit cadenas, de cette façon :



Flickr – https par Sean MacEntee, CC BY 2.0, Certains Droits Réservés Et si vous ne souhaitez pas livrer vos coordonnées bancaires lors d'un achat en ligne, il existe des modes de paiements alternatifs qui ne nécessitent pas vos données bancaires. Pus sûrs, ils ne sont toutefois pas infaillibles :

• PayPal, que l'on ne présente plus, permet de la même manière d'acheter ou de vendre en ligne sans livrer le moindre code bancaire grâce à un compte virtuel qu'il est possible de remplir selon vos besoins. Si des systèmes tels que PayPal sont régulièrement confrontés à des tentatives de phishing (vigilance donc !), le fraudeur ne peut cependant remonter à votre compte en banque, ce qui vous offre une sécurité supplémentaire.

• La carte virtuelle prépayée autorise un paiement en ligne sécurisé puisqu'en aucun cas vous ne livrez vos coordonnées bancaires sur Internet. Pour comprendre comment cela fonctionne, vous pouvez vous fier aux instructions de Paysafecard.

• Concernant le m-paiement, soit le paiement par mobile, Apple Pay utilise les concepts de jetons de paiement et l'identification biométrique pour une protection optimale. Mais, malgré la technologie développée par Apple, des hackers ont réussi à mener une vaste fraude bancaire en volant des données bancaires et en les installant sur de nouveaux Iphone.

Quel que soit votre moyen de paiement en ligne, restez vigilants !

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

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire…

Source : https://www.globalsecuritymag.fr/Cybercriminalite-se-premunir-du,20150429,52544.html

---

Six conseils pour éviter d'être victimes de phishing

Six conseils pour éviter d'être victimes de phishing

Le phishing (e-mails frauduleux se faisant passer pour des marques de commerce ou de service avec l'intention de tromper le destinataire) est l'une des attaques les plus anciennes, mais aussi des plus rentable pour les cybercriminels.

Sur la base de « plus des gens le reçoivent, meilleure est la probabilité que quelqu'un tombe dans le piège » ces campagnes frauduleuses dont le seul but est le vol de données personnelles et financières, ont beaucoup évolué dans les dernières années. Et, en plus, **au cours du premier trimestre de 2016 les cas de spam avec des pièces jointes malveillantes, ils n'ont pas cessé d'augmenter**.
Il y a quelques années, il était facile de distinguer ces e-mails entrant dans la boîte de réception car ils avaient des fautes d'orthographe, des conceptions plutôt anciens… qui nous fassent au moins nous méfier. D'autres viennent directement comme spam, ou comme un courrier indésirable. Mais maintenant, **ils ont évolué**. Bon nombre de ces campagnes utilisent des courriels parfaitement conçus: avec le logo, les couleurs et l'apparence de la marque qui sont en train de supplanter.

Mais le fait que, heureusement, ils ne donnent pas des coups au dictionnaire, signifie que ces emails sont beaucoup plus difficiles à détecter comme frauduleux. Cependant, **il y a un certain nombre de précautions que nous pouvons prendre pour éviter de devenir une victime de ces e-mails malveillants.** Check Point propose ces conseils que nous devons mettre en pratique pour les détecter au début, ou presque:
1. **Surveillez les e-mails qui viennent de marques célèbres.** Le site OpenPhish rassemble les marques les plus utilisées par les cybercriminels pour mener à bien leurs attaques de phishing. **Parmi eux, Apple, Google et Paypal figurent dans le top dix des plus touchés par ce type de campagne**. Les raisons sont évidentes: ils sont extrêmement populaires, il est donc plus susceptible de réussir à usurper l'identité des victimes potentielles.
2. **Vérifiez l'expéditeur du message. Les emails officiels sont toujours envoyés avec le domaine de la marque, par exemple @paypal.com.** Les cybercriminels peuvent mettre le nom de marque, mais ils ne peuvent jamais utiliser le domaine réel.
3. **Fautes d'orthographe.** Nous venons de dire que les cybercriminelles ont beaucoup amélioré en ce sens mais **ils restent toujours quelques erreurs de basse**, souvent en raison de mauvaises traductions.
4. **Hyperliens.** Les liens qui sont envoyés par le biais de ces e-mails sont clairement frauduleux. Une fois que vous y accédez normalement **ils conduisent à des formes où ils volent les données**. Donc, lorsque vous accédez à un site Web qui n'a pas le protocole HTTPS, vous devenez une victime.
5. **« Cher utilisateur ».** Il faut tenir en compte que **les entreprises traitent leurs clients par leur nom et prénom** mais les cybercriminels envoient des e-mails en masse, impersonnelles.
6. **Urgence.** Dans de nombreux e-mails de ce type, **il y a généralement un sentiment d'urgence pour donner nos données personnelles**: le compte est fermé, vous perdrez de l'argent, votre colis sera envoyé sont des exemples.
7. **Attention aux pièces jointes.** Des entreprises n'envoient jamais des pièces jointes dans leurs e-mails. **Évitez d'ouvrir ces documents**, sauf si vous êtes très sûr de l'expéditeur.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : Six conseils pour éviter d’être victimes de phishing – Globb Security FR

Victime de piratage ? Les bons réflexes à avoir

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Victime de piratage ? Les bons réflexes à avoir				

Sur Internet, nul n'est à l'abri d'une action malveillante ou de messages non sollicités. Les éléments suivants vous aideront à avoir les bons réflexes.

VOUS ETES UN PARTICULIER, TPE/PME OU UNE COLLECTIVITÉS TERRITORIALES ?

Désormais, vous pouvez contacter le dispositif d'assistance aux victimes d'actes de cybermalveillance : cybermalveillance.gouv.fr Cette plateforme est le résultat d'un programme gouvernemental assumant un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès de la population française. Vous êtes un particulier, une entreprise ou une collectivité territoriale et vous pensez être victime d'un acte de cybermalveillance ?

La plateforme en ligne du dispositif est là pour vous mettre en relation avec les spécialistes et organismes compétents proches de chez vous ; : cybermalveillance.gouv.fr

Pour information, Nous sommes inscrits au programme cybermalveillance.gouv.fr

Ce dispositif est animé par le groupement d'intérêt public (GIP) Action contre la cybermalveillance (ACYMA) et porté par une démarche interministérielle.

VOUS SOUHAITEZ PORTER PLAINTE ?

Rapprochez du commissariat ou de la brigade de Gendarmerie les plus proches du lieu de l'infraction. Facilitez le travail de l'agent de Police ou de Gendarmerie auprès de qui vous déposerez plainte.

• **Victime de VIRUS – CRYPTOVIRUS – LOGICIEL ESPION** : Portez plainte pour l'infraction suivante : Atteintes aux Systèmes de Traitement Automatisé de Données (S.T.A.D.) sanctionnées par les articles L.323-1 et suivants du Code pénal ;

• **UTILISATION ILLICITE DE VOS DONNÉES PERSONNELLES** : Vous devez saisir la CNIL sur les motifs d'atteintes aux droits de la personne liés aux fichiers ou traitement informatiques (art. 226-16 à 226-24 du Code pénal / Loi 78-17 du 6 janvier 1978 dite « informatique et liberté » modifiée par la loi 2004-801 du 6 aout 2004) ;

• **USURPATION D'IDENTITÉ** : Portez plainte sur ce motif en apportant les preuves (captures d'écran, e-mails, mieux encore un constat d'huissier) ;

• **MENACES** : Déposez plainte sur le motif d'atteintes aux personnes en apportant toutes les preuves (les témoignages ou attestations sont très souvent insuffisants) ;

• **PHISHING / FAUSSE LOTERIE / UTILISATON FRAUDULEUSE DE CB** : Déposez plainte pour Escroquerie ; Une plateforme téléphonique spécialisée existe : « Info-escroqueries » : 0811 02 02 17

• **ATTEINTE AUX MINEURS** : Déposez plainte sur le fondement de l'article 227-23 du Code pénal ;

QUE DEVIENDRA MA PLAINTE EN CAS D'ATTAQUE POUR RANSOMWARE (CRYPTO-VIRUS) ?

Depuis la loi du 03 juin 2016, la section F1 spécialisée cyber du parquet de Paris jouit d'une compétence nationale concurrente. Une circulaire du Ministère de la Justice du 10 mai 2017 ordonne aux parquets locaux de se dessaisir systématiquement au profit du parquet de Paris en cas de plainte pour ransomware.

La politique du parquet de Paris est de systématiquement saisir:

– la DCPJ (OCLCTIC) pour les victimes en zone police

– la DGGN (SCRC/C3N) pour les victimes en zone gendarmerie

En bref:

-la plainte peut être déposée n'importe où, mais prioritairement auprès de l'unité de police/gendarmerie territorialement compétente et avec laquelle la victime a l'habitude de traiter pour tout type d'infraction

– une fois déposée, la plainte sera transmise par l'unité de police/gendarmerie au parquet local, qui la transmettra immédiatement au parquet de Paris, qui saisira pour enquête la DCPJ (OCLCTIC) ou la DGGN (SCRC/C3N) en fonction de la zone de la victime

NB: La mission de la DCPJ (OCLCTIC) et de la DGGN (SCRC/C3N) est de conduire les enquêtes judiciaires pour identifier et interpeller les auteurs. Notre mission n'est en aucun cas de faire de la remédiation et de la gestion de crise SSI. Cette mission de remédiation / gestion de crise SSI est de la compétence:

– pour les OIV (opérateurs d'infrastructures vitales) et les administrations: ANSSI

– pour les entreprises non OIV: de leur propre compétence (elles peuvent faire appel à des prestataires privés en SSI)

VOUS RECEVEZ DES MESSAGES NON SOLLICITÉS ?

Utilisez Signal-Spam

VOUS SOUHAITEZ SIGNALER UN CONTENU ILLICITE ?

Utilisez le portail officiel de signalements de contenus illicites

VOUS AVEZ DES SOUPÇON D'ATTAQUE INFORMATIQUE ?

Consultez la note d'information *Les bons réflexes en cas d'intrusion sur un système d'information* sur le site du CERT-FR

La Police et la Gendarmerie nationale ont toutes deux mis en place un réseau territorial d'enquêteurs spécialisés en cybercriminalité répartis par zones de compétence. Les Investigateurs en CyberCriminalité (ICC/Police) et les N-TECH (Gendarmerie) sont présents dans les services territoriaux de vos régions.

Si vous êtes victime d'infractions mentionnées ci-dessus, vous pouvez directement déposer plainte auprès de leurs services ou bien adresser un courrier au Procureur de la République près le Tribunal de Grande Instance compétent.

Pour information, en fonction du type d'infraction, des services sont spécialisés dans le traitement judiciaire de la cybercriminalité :

SOUS-DIRECTION DE LUTTE CONTRE LA CYBERCRIMINALITÉ (SDLC)

Service interministériel qui dépend de la Direction Centrale de la Police Judiciaire (DCPJ)

Cette Sous-Direction reprend les missions traditionnelles de l'Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication (OCLCTIC) auxquelles doit être ajoutée une plateforme de signalement et d'orientation technique et judiciaire.

Infractions traitées : piratages, fraudes aux moyens de paiement, téléphonie et escroqueries sur Internet.

Contact :

SDLC/OCLCTIC

101, rue des 3 Fontanots

92 000 Nanterre

Site Internet

Services de signalements en ligne de contenus illégaux sur l'Internet

Plateforme téléphonique « Info-escroqueries » : 0811 02 02 17

BRIGADE D'ENQUÊTE SUR LES FRAUDES AUX TECHNOLOGIES DE L'INFORMATION (BEFTI)

Paris et petite couronne – Particuliers & PME

La BEFTI dépend de la Direction Régionale de la Police Judiciaire de Paris (DRPJ-PARIS).

Composée de groupes d'enquêtes spécialisés et d'un centre d'assistances techniques, cette brigade est compétente pour les investigations relatives aux actes de piratage sur Paris et ses trois départements limitrophes (92, 93 et 94).

Contact :

BEFTI

122-126 rue du Château des Rentiers

75 013 Paris

Site Internet

CENTRE DE LUTTE CONTRE LES CRIMINALITÉS NUMÉRIQUES (C3N) DU SERVICE CENTRAL DU RENSEIGNEMENT CRIMINEL (SCRC) DE LA GENDARMERIE NATIONALE

France – Particuliers & organismes

Ce centre dépend du Pôle judiciaire de la Gendarmerie nationale.

Service à compétence judiciaire nationale, il regroupe l'ensemble des unités du PJGN qui traitent directement de questions (formation, veille et recherche, investigation, expertise) en rapport avec la criminalité et les analyses numériques (Département Informatique-Electronique de l'IRCGN). Il assure également l'animation et la coordination au niveau national de l'ensemble des enquêtes menées par le réseau gendarmerie des enquêteurs numériques.

Domaine de compétence: atteintes aux STAD, infractions visant les personnes et les biens.

Contact :

SCRC/C3N

5, Boulevard de l'Hautil – TSA 36810

95037 CERGY PONTOISE CEDEX

contact : cyber[at]gendarmerie.interieur.gouv.fr

DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE (DGSI)

France – État, secteurs protégés, OIV

La DGSI dépend du Ministère de l'Intérieur.

Créée en mai 2014 à la suite de la DCRI (Direction Centrale du Renseignement Intérieur), cette direction générale en poursuit les missions de protection des intérêts fondamentaux de la Nation.

Infractions traitées : actes de piratage ciblant les réseaux d'État, les établissements composés de Zones à Régime Restrictif et les Opérateurs d'Importance Vitale.

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.

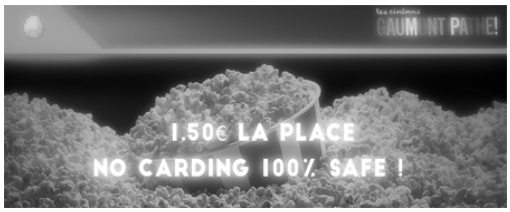
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

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 : *En cas d’incident | Agence nationale de la sécurité des systèmes d’information*

Place de ciné pas chère : une faille pour Gaumont Pathé ? | Denis JACOPINI

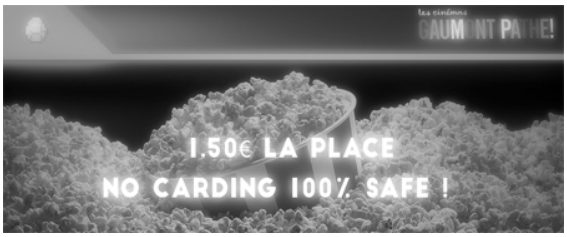


Place de ciné pas chère : une faille pour Gaumont Pathé ?

Place de ciné pas chère ? Bluff, escroquerie ou piratage informatique ? Une boutique du black market francophone propose de payer ses places de cinéma 5 fois moins chères que le prix initial. Une possibilité pirate qui ne viserait que les cinémas Pathé Gaumont !

Les amateurs de cinémas ne me contrediront pas, le cinéma est devenu un petit luxe loin d'être négligeable dans un budget. Même si des cartes de réductions existent, cela fait rarement la sortie cinéma (deux adultes, deux enfants) à moins de 50€ (si on rajoute quelques friandises), et à la condition ou la séance n'est pas en 3D, ce qui fait gonfler la note. Bref, tout le monde n'a pas la chance d'aller au cinéma deux fois par semaine. Bilan, ce qui est mon cas, les cartes de réduction sont un bon moyen d'assouvir son plaisir de salle obscure. D'autres internautes, beaucoup plus malhonnêtes, n'hésitent pas à revendre des entrées à un prix défiant toutes concurrences.

Place de ciné pas chère ?



Dans une boutique du black market francophone, je suis tombé sur une publicité annonçant proposer des places de cinéma à 1,5€/2€. Des places ne pouvant être utilisées que dans les cinémas Gaumont Pathé! Le président des cinémas Pathé, Jérôme Seydoux et Nicolas Seydoux, président de Gaumont (Grand Père et Oncle respectifs de la dernière James Bond Girl, Léa Seydoux) auraient-ils décidé de faire des réductions aussi inattendues qu'impossibles ? Malheureusement pour les cinéphiles, ce n'est pas le cas.Il semble que le vendeur derrière cette proposition alléchante de Place de ciné pas chère a trouvé une méthode pour escroquer l'entreprise. « ***J'ai des places de cinéma gratuites et illimitées valables dans tous les Pathé de France,*** indique ce commerçant. ***Ces places ne sont pas cardées*** [comprenez acquises avec des données bancaires piratées, NDR], ***juste ma tête***« . Le vendeur indique ne pas vouloir donner plus d'informations sur sa méthode. Une technique qu'il utiliserait depuis deux ans « ***pour moi et mes amis et qu'il n'est jamais rien arrivé***« . D'après ce que j'ai pu constater, le pirate semble être capable de générer des codes « invitation ». Le pirate a même créé un shop (boutique automatisée) qui permet d'acquérir autant de place que le black marketeur est capable de générer contre la somme demandée. Paiement en bitcoins… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Place de ciné pas chère : une faille pour Gaumont Pathé ? – ZATAZ*

Cyberarnaques S’informer pour mieux se protéger – Denis Jacopini, Marie Nocenti | fnac

	Cyberarnaques S’informer pour mieux se protéger

Internet et les réseaux sociaux ont envahi notre quotidien, pour le meilleur mais aussi pour le pire… Qui n'a jamais reçu de propositions commerciales pour de célèbres marques de luxe à prix cassés, un email d'appel au secours d'un ami en vacances à l'autre bout du monde ayant besoin d'argent ou un mot des impôts informant qu'une somme substantielle reste à rembourser contre la communication de coordonnées bancaires ? La Toile est devenue en quelques années le champ d'action privilégié d'escrocs en tout genre à l'affût de notre manque de vigilance. Leur force ? Notre ignorance des dangers du Net et notre « naïveté » face aux offres trop alléchantes qui nous assaillent.

Plutôt qu'un inventaire, Denis Jacopini, avec la collaboration de Marie Nocenti, a choisi de vous faire partager le quotidien de victimes d'Internet en se fondant sur des faits vécus, présentés sous forme de saynètes qui vous feront vivre ces arnaques en temps réel. Il donne ensuite de précieux conseils permettant de s'en prémunir. Si vous êtes confronté un jour à des circonstances similaires, vous aurez le réflexe de vous en protéger et en éviterez les conséquences parfois dramatiques… et coûteuses.
Un livre indispensable pour « surfer » en toute tranquillité !
Denis Jacopini est expert judiciaire en informatique, diplômé en cybercriminalité et en droit, sécurité de l'information et informatique légale à l'université de droit et science politique de Montpellier.
Témoin depuis plus de vingt ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus soigneusement élaborées, il apprend aux professionnels à se protéger des pirates informatiques.
Marie Nocenti est romancière.
Commandez CYBERARNAQUES sur le site de la FNAC (disponible à partir du 29/03/2018)

LE NET EXPERT
• ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)
- **ANALYSE DE VOTRE ACTIVITÉ**
- **CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES**
- **IDENTIFICATION DES RISQUES**
- **ANALYSE DE RISQUE (PIA / DPIA)**
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
• FORMATIONS / SENSIBILISATION :
- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**
• RECHERCHE DE PREUVES (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES
• EXPERTISES & **AUDITS** (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous
Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Réagissez à cet article

Source : *Cyberarnaques S'informer pour mieux se protéger – broché – Denis Jacopini, MARIE NOCENTI – Achat Livre – Achat & prix | fnac*

Victime du ransomware Petya ? Décryptez gratuitement les fichiers | Denis JACOPINI

Victime du ransomware Petya ? Décryptez gratuitement les fichiers

Il est possible de récupérer gratuitement ses fichiers après une infection par le ransomware Petya. Pas forcément simple à mettre en œuvre, une méthode a vu le jour.

Petya bloque totalement l'ordinateur. Pour cela, il écrase le Master Boot Record du disque dur et chiffre la Master File Table sur les partitions NTFS (système de fichiers de Windows). Cette MFT contient les informations sur tous les fichiers et leur répartition.
La procédure malveillante laisse croire à une vérification du disque dur après un plantage et un redémarrage. La victime aura au final droit à une tête de mort en caractères ASCII et une demande de rançon (0,9 bitcoin) pour espérer récupérer ses fichiers et déchiffrer le disque dur prétendument chiffré avec un algorithme dit de niveau militaire.
Un bon samaritain (@leostone) a mis en ligne un outil pour se dépêtrer de Petya (https://petya-pay-no-ransom-mirror1.herokuapp.com) sans devoir payer une rançon. La procédure nécessite de récupérer des données d'un disque dur affecté pour obtenir une clé de déchiffrement promise en quelques secondes. Manifestement, il était simplement question d'un encodage en Base64.
Pour BleepingComputer.com, l'expert en sécurité informatique Lawrence Abrams a confirmé la validité de l'outil. Chercheur en sécurité chez Emisoft, Fabian Wosar a de son côté développé un outil Petya Sector Extractor (http://download.bleepingcomputer.com/fabian-wosar/PetyaExtractor.zip) permettant d'extraire facilement les données à fournir à l'outil de Leostone.
Bien évidemment, le disque dur infecté doit être connecté à un autre ordinateur afin de pouvoir y accéder (extraire les données pour l'outil de Leostone). Une fois la clé de déchiffrement obtenue, il est à replacer dans l'ordinateur d'origine et il faudra saisir la clé sur l'écran affiché par Petya.
L'existence de cette faille pour se débarrasser de Petya sans payer de rançon sera nécessairement portée à la connaissance de l'auteur du ransomware. Le code du nuisible pourrait dès lors être prochainement modifié en fonction.

Source : *Petya : une échappatoire contre le ransomware agressif*