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

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

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

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

Contactez-nous

Réagissez à cet article

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

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.

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

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)

Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220

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

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

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

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

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

Commandez sur Fnac.fr

---

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

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

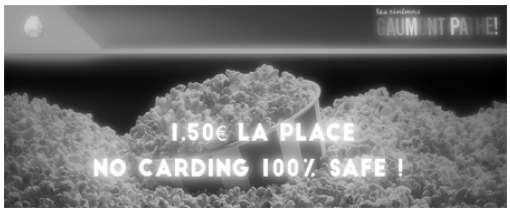
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

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

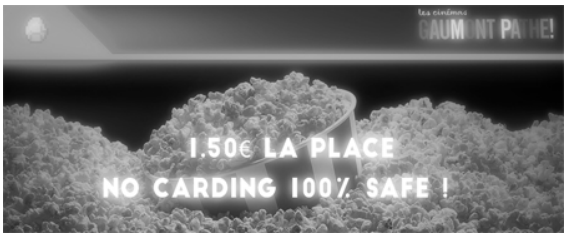


Place de ciné pas chère : une faille pour Gaumont Pathé ?

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*

Vidéoprotection / vidéosurveillance : combien de temps peuvent être conservées les images ? | Denis JACOPINI

Vidéoprotection / vidéosurveillance : combien de temps peuvent être conservées les images ?

La conservation des images ne doit pas dépasser 1 mois. En règle générale, conserver les images quelques jours permet d'effectuer les vérifications nécessaires en cas d'incident et de lancer d'éventuelles procédures disciplinaires ou pénales. Dans ce cas, les images sont extraites de l'installation et conservées pour la durée de la procédure.
Lorsque c'est techniquement possible, une durée maximale de conservation des images doit être paramétrée dans le système. Cette durée ne doit pas être fixée en fonction de la seule capacité technique de stockage des appareils.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique et en mise en conformité de vos déclarations à la CNIL.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

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

Source :
https://cnil.epticahosting.com/selfcnil/site/template.do?name=Vid%C3%A9oprotection%2Fvid%C3%A9osurveillance+%3A+combien+de+temps+peuvent+%C3%AAtre+conserv%C3%A9es+les+images+%3F&id=406

Le site Internet d’une mairie peut-il être contrôlé à distance par la Cnil ? | Denis JACOPINI

Le site Internet d’une mairie peut-il être contrôlé à distance par la Cnil ?

La réponse de Benjamin Vialle, agent au service des contrôles, Commission nationale de l'informatique et des libertés.
Oui. Depuis la loi du 17 mars 2014 relative à la consommation, la Commission nationale de l'informatique et des libertés (Cnil) a la possibilité de procéder à des contrôles en ligne, sur internet.
Ils permettent de constater à distance, depuis un ordinateur connecté à internet, des manquements à la loi informatique et libertés. Ces constatations sont relevées dans un procès-verbal adressé aux organismes concernés et leur seront opposables.

Téléservices
Des vérifications en ligne portant sur les téléservices relatifs aux demandes d'actes d'état civil ont été réalisées par la Cnil pour 33 communes. Le choix des communes s'est opéré selon un critère de représentativité : taille diverse, couleurs politiques différentes, répartition sur l'ensemble du territoire.
Trois principaux manquements à la loi informatique et libertés ont été constatés : un défaut de sécurisation de ces espaces (art. 34 loi informatique et libertés), un manque d'information des personnes (art. 32) et un défaut de formalité (art. 22).
30% des communes avaient mis en place un protocole HTTPS qui permet à l'usager une transmission sécurisée (car chiffrée) de ses données, entre son poste informatique et les serveurs de la commune. 10% des communes redirigent vers le site mon.service-public.fr, qui est correctement sécurisé.

Espace non sécurisé
Cependant, plus de 60% des communes contrôlées ne sécurisaient pas l'espace dédié à la dématérialisation des demandes d'actes d'état civil. Au titre de ses missions, la Cnil doit contrôler les conditions dans lesquelles les fichiers sont créés et utilisés.
Ce nouveau pouvoir de contrôle en ligne crée les conditions juridiques qui permettent d'adapter la mission de la Cnil de protection des données personnelles au développement numérique.

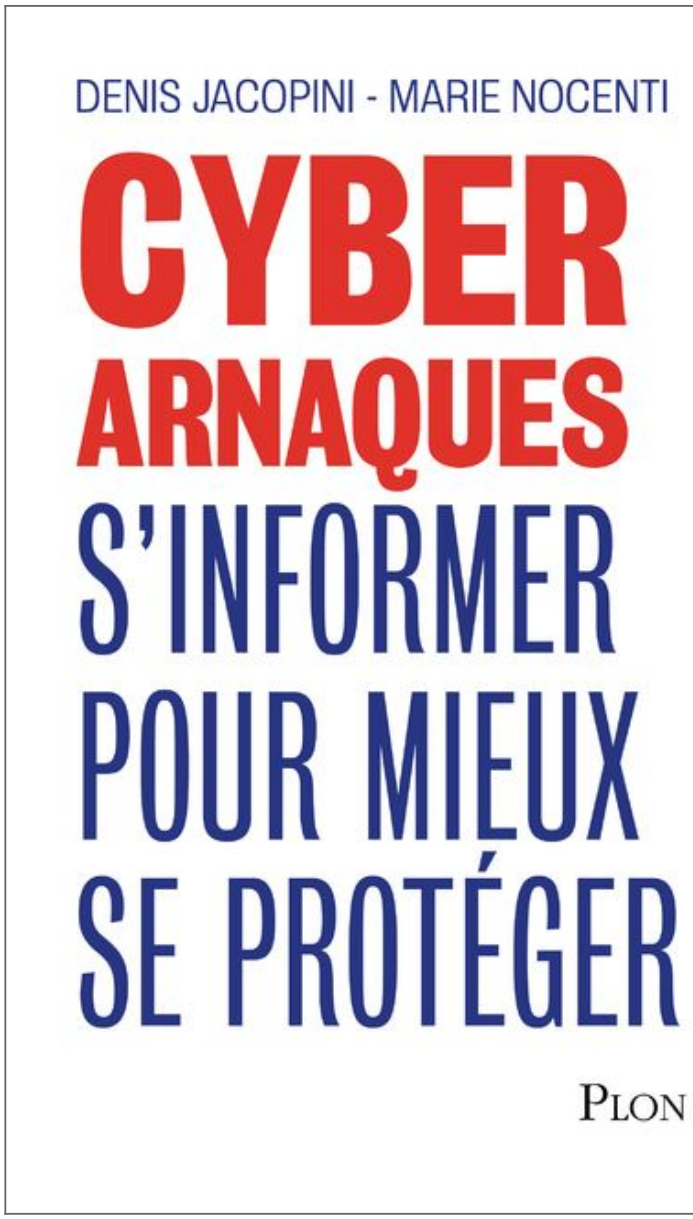
Source :
http://www.courrierdesmaires.fr/51195/le-site-de-la-mairie-peut-il-etre-controle-a-distance-par-la-cnil/

Utilisation juridique des documents numériques . Peuvent-ils constituer une preuve ? | Denis JACOPINI

Depuis 2000, la validité comme preuve juridique des documents numériques est reconnue , au même titre que la preuve écrite sur papier et ce à condition de pouvoir justifier de son authenticité et de son intégrité.

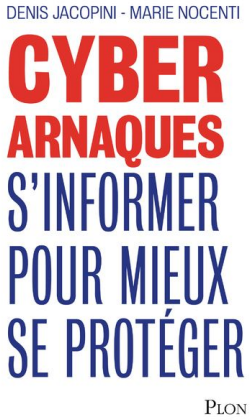
Comment obtenir ces deux conditions pour pouvoir utiliser en justice un document numérique ?

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).

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

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

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

Contactez-nous

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*

L’absence de formalité auprès de la CNIL, lorsqu’elle est obligatoire, peut constituer une infraction pénale | Nous pouvons vous aider à vous mettre en conformité | Denis JACOPINI

	L’absence de formalité auprès de la CNIL, lorsqu’elle est obligatoire, peut constituer une infraction pénale	Nous pouvons vous aider à vous mettre en conformité

L’absence de formalité auprès de la CNIL, lorsqu’elle est obligatoire, peut constituer une infraction pénale.

Art. 226-16 de la Loi Informatique et Libertés
Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu’aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d’emprisonnement et de 300 000 € d’amende.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l’ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l’hygiène informatique.

Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

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

Source : Denis JACOPINI
Illustration : http://claudinelepage.eu/?p=8261

Cyber-Sécurité : des menaces de plus en plus présentes, mais des collaborateurs pas assez formés | Le Net Expert Informatique

	La Cyber-Sécurité de plus en plus menacante, mais des collaborateurs pas assez formés

Les entreprises ont encore trop souvent tendance à sous-estimer le #risque lié au manque de formation de leurs équipes (hors services informatiques) à la cybersécurité. La preuve…

Une enquête réalisée par Intel Security montre que si les collaborateurs de la DSI restent les plus #exposés aux cyberattaques (26 % au niveau européen contre 33 % en France, ce taux étant le plus élevé), les équipes commerciales et les managers (top et middle management) le sont aujourd'hui de plus en plus. En France, 18 % des commerciaux, 17 % du middle management et 14 % des dirigeants sont des #cibles potentielles. Viennent ensuite les personnels d'accueil (5 % en France, taux identique à la moyenne européenne), et le service client (seulement 7 % en France, contre 15 % au niveau européen).
Or ces types de personnel restent tous #mal formés à la sécurité informatique. Le risque est particulièrement fort au niveau des équipes commerciales avec 78 % de professionnels non formés et 75 % des personnels d'accueil. Ces taux descendent un peu pour le top management (65 % de non formés) et pour les équipes du service client (68 %). Côté middle management, la moitié est formée (51 % en France, 46 % au niveau européen).
L'enquête souligne également qu'au-delà des attaques ciblant les personnes non averties via leurs navigateurs avec des liens corrompus, les #attaques de réseaux, les #attaques furtives, les #techniques évasives et les #attaques SSL constituent une menace croissante pour les entreprises. On en recense plus de 83 millions par trimestre. Pour les contrer, les professionnels informatiques français réévaluent la stratégie de sécurité en moyenne tous les huit mois, en ligne avec les pratiques des autres pays européens sondés. 21 % mettent par ailleurs à jour leur système de sécurité moins d'une fois par an (contre 30 % en moyenne au niveau européen). Et 72 % d'entre eux (et 74 % en moyenne en Europe) sont persuadés que leur système de sécurité pourra contrer ces nouvelles générations de cyberattaques.
Or, ils se trompent. Les #attaques DDoS par exemple. Conçues pour créer une panne de réseau et permettre aux hackers de détourner l'attention de l'entreprise, tandis qu'ils se faufilent dans son système et volent des données, elles ne sont pas vraiment prises au sérieux (malgré leur augmentation +165% et leur dangerosité), puisque seuls 20 % des professionnels informatiques français estiment qu'elles constituent la principale menace pour le réseau de leur entreprise.
Au final, il existe un profond décalage entre l'évolution des attaques et la perception qu'en ont les entreprises qui ne peuvent plus négliger la formation de leurs équipes non IT.

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

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

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

Source :
http://www.itchannel.info/index.php/articles/157059/cyber-securite-menaces-plus-plus-presentes-mais-collaborateurs-pas-formes.html