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 »]

| Design | Language | Proceedings | Procedings | Procedings | Procedings | Proceedings | Proceedings | Procedings | Proceedings

- omment recommente um mail Traducteux : umment 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 :



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

• 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 ?

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

Six conseils pour éviter d'être victimes de phishing



Six conseils pour eyiter 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 clientéle...);
- 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.



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.

<u>VOUS ETES UN PARTICULIER. TPE/PUR OU UNE COLLECTIVITÉS TERRITORIALES ?</u>

Désormais, vous pouvez contacter le dispositif d'assistance aux victimes d'actes de cybermalveillance ; o;bermalveillance, gouv.fr (ette 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 étes un perceit et organismes competents proches de chez vous ; : cybermalveillance. ?

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

Pour information, Nous somes inscrits au programme cybermalveillance (DOUS. SOUNLATIEZ DROBALVEILLANCE, DOUS. F)

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

**WOUS SOUNLATIEZ DROBER PLAINTE : "
**OUS SOUNLATIEZ

Pour information, Nows somes inscrits au programme cybernalveillance.govv.fr

(e dispositif est aniné par le groupement d'intrêté public (EPJ) Action contre la cybernalveillance (ACMN).

(Aug. SOUNITE PIANTE PIAN

Utilisez Signal-Spam

VOUS SOMUNTEZ SIGNALEM (COTTEM UTILICITE 2

Utilisez le portail officiel de signalements de contenus illicites

VOUS NAZE DE SOUNÇON D'ATTANGE 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 dépose 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 spécialités dans le traitement judiciaire de la cybercriminalité :

Sous-Direction De LUTIE CONTRE LA CYBERCRIMINALITÉ (SDLC)
Service interministériel qui dépend de la Direction Centrale de la Police Judiciaire (DCP))
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 (DCLCTIC) 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 :
SOUL/OCLCTIC
101: rue des 3 Fontanotts

SOLCULIT 101, rue des 3 Fontanots 92 000 Nanterre Struces 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).

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:

Lontact : 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 POIs judiciaire de la Gendarmerie nationale, il regroupe l'ensemble des unités du PJGN qui traitent directement des et a Gendarmerie nationale.

Service à compétence judiciaire nationale, il regroupe l'ensemble des unités du PJGN qui traitent directement des tracherche, investigation, expertiss) 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 mendes par le réseau gendarmerie des enquêteurs numériques.

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

Contact :

SCRC/C3N

S. Boulevard de l'Hautil - TSA 36810

SSGR (CFCN) MOTIONS CEDEX

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

DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE (DGSI)

France Etat, secteurs prodejes, DIV

France de la Communication de

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

CYBER ARNAOUES S'INFORMER POLIR MIFLIX SE PROTÉGER

Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarmaques 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 arraques toujours plus sournoisement élabordés.

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

Plutôt que de présenter une longue liste d'arraques 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'arraques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivelse de recommains pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous métier sans risquer de vivre la fin trapique de ces histoires et d'en subir les conséquences parfois d'armatiques.

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

https://www.youtube.com/watch?v=lDxdkITra2s

https://www.youtube.c

https://youtu.be/usgl2zkR0917list=UUDHgj_HKCbzRuvIPdu3FktA
12/04/2018 Denis JACOPINI est invité sur Europe l à l'occasion de la sortie du Livre ("CHERAMMAQUES S'informer pour mieux se protéger"
Comment se Comment se auto



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 cyleverriainalité 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 protection des Données à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Franc. 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 ? 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]





Contactez-nous

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

DENIS JACOPINI - MARIE NOCENTI

GYBER ARNAQUES S'INFORMER POUR MIEUX SE PROTÉGER

PLON

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.

DENIS JACOPINI - MARIE NOCENTI

S'INFORME POUR MIEUX SE PROTÉGER

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 $\frac{1}{2}$ 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 INFORMATIONE
 - 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).

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



Mises en conformité RGPD;
 Accompagnement à la mise en place de DPO;
 Constitutions (at sensibilisations) à la

DPO;

formations

ct sensibilizations (4 sensibilizations) di
Coberctininalité (Autorisation et 92 se 0.0041 s.);

Audits Sécurité (ISO 27005) :

Expertises techniques et judiciaires ;

Recherche de preuves téléphones, disque durs, e-mails, contentieux, détoumement de clientéleu...)



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-mirrorl.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.

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, détoumements de clientèle...;
- Expertises de systèmes de vote électronique



Contactez-nous

Réagissez à cet article

Source : Petya : une échappatoire contre le ransomware agressif

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 :

 $\verb|http://www.itchannel.info/index.php/articles/157059/cyber-securite-menaces-plus-presentes-mais-collaborateurs-pas-formes. | the latest and the latest are also also as a superior of the latest and the latest are also as a superior of the latest are also as a superior$

GDPR compliance: Request for costing estimate















GDPR compliance: Request for costing estimate

You seem to express an interest in the GDPR (perhaps a little by obligation) and you want to tell us about a project. We thank you for your confidence.

Intervening on Data Protection missions since 2012, after having identified different types of expectations, we have adapted our offers so that they best neet your needs.

Thus, we can assist you in bringing your structure into compliance in several ways::

We can assist you to learn the essentials of European regulations relating to the Protection for Personal to a fast a compliance. Once the training is completed, you are independent but can always count on our support either in the form of personalized support:

At the end of this training, we will give you a certificate proving the implementation of a process to bring your establishment into compliance with the GDPR (General Data Protection Regulations). For information, we are referenced to the CNIL.

We carry out for you the audit which will highlight the points to be improved. At the end of this straining, we will give you a report proving the implementation of a concertions as part of your process to bring your establishment into compliance with the GDPR (General Data Protection Regulations).

At the end of this audit, we will give you a report proving the implementation of concertions as part of your process to bring your establishment into compliance with the GDPR (General Data Protection Regulations).

So you want to entrust all of your compliance?

In a perfectly complementary way with your IT service provider and possibly with your 'legal department, we can take care of the entire process of bringing your establishment into compliance with the GDPR (General Data Protection Regulation) and the various regulations required both to the needs of your structure in accordance with your strategy and your priorities, we would like you to answer these few questions:

Me guarantee extreme confidentiality on the information communicated. Persons authorized to consult this information are subject to profession Do not hesitate to communicate as many details as possible, this will allow us to better understand your expectations. Your First Name / NAME (required)
Your Organization / Company (required) Your email address (required) A telephone number (will not be used for commercial prospecting) You can write us a message directly in the free text area. However, if you want us to establish precise costing for you, we will need the information below. In order to better understand your request and establish a quote, please provide us with the information requested below and click on the "Send entered informations" button at the bottom of this page for us to receive it. You will receive an answer quickly. YOUR ACTIVITY Details about your activity :
Are you subject to professional secrecy? OYes⊕NoOI don't know OYes⊕NoOI don't know Does your activity depend on regulations?

If "Yes", which one or which ones? YOUR COMPUTER SYSTEM Can you describe the composition of your computer system. We would like, in the form of an enumeration, to know the equipment which has any access to personal data with for each device ALL the software (s) used and their function (s)

Examples:

- 1 WEB server with whiling software to bill my clients;

- 2 lestrops including:

> 1 with email software to correspond with clients and prospects - word processing for correspondence + billing software to bill my clients ...

> 1 with email software to correspond with clients and prospects - word processing for correspondence to the accounting for my company;

- 1 smartphone with email software to correspond with customers and prospects. Do you have one or more websites? OYes⊕NoOI don't know What is (are) this (thoses) website (s)? Do you have data in the Cloud? OYes⊕NoOI don't know Which cloud providers do you use? YOUR PERSONAL DATA PROCESSING

If you have already established it, could you provide us with the list of processing of personal data (even if it is incomplete)? SIZING YOUR BUSINESS Number of employees in your structure : How many of these employees use computer equipment ?

How many of these employees use computer equipment ?

umber of departments or departments ** in your structure (example: Commercial service, technical service ...) :

Please list the services or departments ** of your structure: SERVICE PROVIDERS & SUBCONTRACTORS Do you work with sub-contractors? OYes⊕NoOI don't know Do you work with sub-contractors?
Please list these subcontractors:

Do you work with service providers who work on your premises or in your agencies (even remotely)?

Please list these providers:

How many IT companies do you work with?
Please list these IT companies indicating the products or services for which they operate and possibly their country of establishment: OYes⊕NoOI don't know 0 YOUR SITUATION TOWARDS THE GDPR Does your establishment exchange data with foreign countries ?

If "Yes", with which country(ies)?

Have you already been made aware of the GDPR ?

Have people using IT equipment already been made aware of the GDPR ?

If you or your employees have not been made aware of the GDPR, would you like to undergo training ? OYes⊕NoOI don't know OYes@NoOI don't know The analysis of the data processing conditions in your professional premises or your professional premises is part of the compliance process. The analysis of the data processing conditions in your professional predicts on Do you have several offices, agencies etc. legally dependent on your establishment?

If "Yes", how much?

In which city (ies) (and country if not in France) do you or your employees work? o₩ We can support you in different ways We can support you an usireron ways.

A) We can teach you to become autonomous (training);

B) We can support you at the start and then help you become independent (support, audit + training);

C) We can choose to entrust us with the entire process of compliance (support);

D) We can accompany you in a personalized way (thank) you to detail your expectations).

What type of support do you want from us (A / B / C / D + details)? END OF QUESTIONNAIRE

If you wish, you can send us additional information such as:
- Emergency of your project:
Any additional information that you deem useful to allow us to better understand your project. Send entered informations $[block\ id="24086"\ title="Mentions\ légales\ formulaires"]$ ** = for example, commercial service, technical service, educational service, administrative and financial service ...

or send an email to rgpd[at]lenetexpert.fr

Denis JACOPINI is our Expert who will accompany you in your compliance with the GDPR.



n expert in sworn IT and specialized in GDPR (protection of Personal Data) and in cybercrime. Consultant since 1996 and trainer since 1998, I have experience since 2012 in compliance with the regulations rist technical training, CNIL Correspondent (CIL: Data Protection Correspondent) then recently Data Protection Officer (DPO n * 15845), as a compliance practitioner and trainer, I support you in all your procedurers for compliance with the CMPR. *

Why goal is to provide all my experience to bring your establishment into compliance with the GDPR. * Let me introduce myself: Denis JACOPINI. I am an expert in sworn IT and specialized in GDPR (protection of Perso relating to the Protection of Personal Data. First technical training, CNIL Correspondent (CIL: Data Protection

RGPD: Que se passe t-il si le 25 mai 2018 nous n'avons pas terminé notre mise en conformité?



RGPD : Que se passe t-il si le 25 mai 2018 nous n'avons pas terminé notre mise en conformité ? Le Net Expert : Denis JACOPINI, vous êtes spécialisé dans l'accompagnement des PME dans la mise en conformité avec le RGPD depuis plusieurs années. Que se passe t-il si le 25 mai 2018 nous n'avons α νε ειπίπε votre mise en conformité avec le RGPD ou pire, vous venez à peine de l'initier pour votre entreprise, association ou administration, stricto sensu, en tant que responsable de traitement pénalement responsable, vous devenez amendable et les sanctions encourues, forcément pécuniaires selon les cas, pourraient être accompagnées de peines de prison comme le précise l'article 226-17 du Code pénal. Ainsi, le Règlement sera « obligatoire dans tous ses éléments et directement applicable dans tout État membre », dont la France dès le 25 mai 2018, et puisqu'il s'agit d'un règlement, celui-ci Ainsi, le Règlement sera « obligatoire dans tous ses éléments et directement applicable dans tout État membre », dont la France dès le 25 mai 2018, et puisqu'il s'agit d'un règlement, celui-ci entrera directement en vigueur, sans nécessiter de législation de transposition.

En réalité, avant que soient engagées des sanctions à votre encontre, vous serez contacté par la CNIL, laquelle vous demandera certainement de justifier les mesures prises à l'égard du Règlement Européen. Il est clair qu'au plus vous faites preuve de négligence, de mauvaise foi et de résistance, les sanctions risquées se rapprocheront du maximum à savoir la plus grande valeur entre 4% de votre chiffre d'affaire mondial ou 20 millions d'euros.

Si par contre, vous avez entamé une démarche de mise en conformité à savoir au minimum commencé à suivre une formation, désigné officiellement une personne (interne ou externe à votre entreprise) à cette démarche réglementaire et même si vous en êtes seulement au stade où vous avez commencé à établir la liste de vos traitements avec les risques inhérents à la vie privée et aux libertés fondamentales des propriétaires des données à caractère personnel et si possible vous avez commencé à mettre en place des mesures correctives, vous montrerez ainsi à l'autorité administrative indépendante de contrôle du bon respect de la réglementation relative à la protection des données à caractère personnel (la CNIL en France) que vous avez pris en compte cette démarche dans votre de contrôle du bon respect de la réglementation relative à la protection des données à caractère personnel (la CNIL en France) que vous avez pris en compte cette démarche dans votre de vous avez pris en compte cette démarche dans votre de vous avez pris en compte cette démarche dans votre de vous avez prise en compte cette démarche dans votre de vous avez prise en compte cette démarche dans votre de vous avez prise de vous avez prise en compte cette démarche dans votre de vous avez prise en compte cette démarche dans votre de vous avez prise organisation, pris au sérieux des défaillance en matière juridique ou technique de votre organisation et que des améliorations sont en cours. L'ensemble des démarches accomplies même après le 25 mai 2018 joueront en votre faveur en anéantissant les risques de sanction, bien évidemment à condition que vous ne fassiez aucune victime en cas de fuite de données avant. Consultez la liste de nos formations et services sur le RGPD Besoin d'un accompagnement pour vous mettre en conformité avec le RGPD ? ? Besoin d'une formation pour apprendre à vous mettre en conformité avec le RGPD ? A Lire aussi : Mise en conformité RGPD : Mode d'emploi Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles 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 Le RGPD, règlement européen de protection des données. Comment devenir DPO ? 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) Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel. Par des actions de formation, de sensibilisation ou d'audits 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 : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles **Le Net Expert** INFORMATIQUE Contactez-nous Cybersécurité & Conformité

Source : Denis JACOPINI (Expert Informatique spécialisé RGPD)

Comment déjouer les arnaques aux distributeurs automatiques de billets (DAB)



Comment
déjouer les
arnaques aux
distributeurs
automatiques
de billets
(DAB) ?

Déjouer les escroqueries au DAB et adopter les bons gestes pour s'en prémunir, par la brigade des fraudes aux moyens de paiement

<u>Denis JACOPINI :</u>

Parce que nous considérons que notre connaissance des risques et le premier rempart contre les pirates, nos avons souhaité partager avec vous cette vidéo.

N'hésitez pas à nous contacter pour l'organisation de sessions de formations ou de conférences de sensibilisation aux risques informatiques, pour apprendre à vous protéger des pirates, des arnaques et limiter ainsi votre exposition à ces pièges.

Plus d'informations sur

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

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

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



- Audits RGPI
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- 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



Réagissez à cet article