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



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

Chaque semaine, de nouveaux scandales éclatent comme, par exemple, le vol, il y a quelques jours, de milliers de photos intimes de stars américaines. Et cela nous concerne tous : « phishing », vol d'identité, harcèlement numérique, vols de compte bancaire : chaque seconde, 17 personnes sont victimes de cyber-escroqueries à travers le monde. Car Internet a créé une nouvelle génération d'escrocs 2.0. Leur butin s'élèverait l'année dernière à 400 milliards de dollars. Un chiffre en constante augmentation. Nous avons découvert les failles des nouvelles cartes bancaires NFC, sans contact. Désormais, les pickpockets n'ont plus besoin de mettre la main dans votre sac pour voler votre argent.

Nous allons vous raconter l'histoire de différentes victimes françaises. Celle de Laetitia, en proie au cyber-harcèlement, qui a failli mettre fin à ses jours. Stéphane, lui, pensait avoir rencontré l'amour sur la toile ; il était en fait entre les mains de brouteurs de Côte d'Ivoire. Nous avons remonté leurs traces à Abidjan.

Nous nous sommes également rendus en Roumanie dans une ville hors du commun que le FBI a surnommée Hacker-ville. Là-bas, une grande partie de la population vivrait des cyber-escroqueries. Certains escrocs ont accepté de nous rencontrer ; d'autres après avoir été arrêtés par les forces de l'ordre ont décidé de mettre leur génie informatique au service de la société.

Enfin, vous découvrirez que pour protéger leurs ados des dangers du web, des parents ont trouvé une solution radicale. Christophe est un papa espion : il contrôle les moindres faits et gestes de ses trois enfants. Grâce à une panoplie de logiciels et d'applications, il a accès à l'intégralité du contenu de leur téléphone et ordinateur. Internet est sans aucun doute la principale révolution de ces trente dernières années mais c'est peut-être aussi la fin de la vie privée.

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 (Symantec) 13,8 Milions de victimes Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

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

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source :

http://www.m6.fr/emission-zone_interdite/28-09-2014-vie_privee _en_danger_pourquoi_nous_sommes_tous_concernes/

Les 5 techniques de phishing les plus courantes | Denis JACOPINI



Le spam est aujourd'hui plus ume muisance qu'une réelle menace. En effet, les tentatives de vendre du viggra ou encore de recevoir l'héritage d'un riche prince d'une contrée éloignée ne font plus beaucoup de victimes. La majorité des solutions antispam bloquent ces emails et l'unique façon de les voir consiste à consulter votre dossier « courrier indésirable ». Toutefois, une menace bien plus sophistiquée et dangereuse atterrit dans votre boite de réception. Vous ciblant vous et vos employés. Comment of Simpleque vos employés en destructives de visit of simpleque vos employés en destructives de visit of simpleque vos employées de visit vos employées de visit de visit of simpleque vos employées de visit value ver sur sur la visit de visit vos employées de visit vente ver la visit vente de visit vente ver la visit vente de visit vente ver la visit vente ver la visit vente de visit vente ver la visit

L'impact du phishing one netroprise

Des milliers de phishing ont newyes quotidiennement (contre des millions pour le spam) par des organisations de cybercriminels ou des gouvernements étrangers (ou les deux quand ce dernier « soustraite »).

Cette menace n'est pas encore bien maîtrisée par la majorité des antispas et anti-virus sur le marché pour plusieurs raisons. Premièrement, le « faible » volume d'emails de phishing ne permet pas d'être détecté par la majorité des solutions reposant sur une base des signatures. Deux-elimement, l'emails elemble légitien et ne reprend pas les « codes » du spam.

Le phishing est une réétle menace pour les entreprises, car il y a deux façons d'être victime : voir sa marque usurpée ou tomber dans le piège quand on reçoit l'email.

Dans les deux cas, vuicil les 4 principaux dégâts que le phishing peut causer à voure entreprises.

Nuire à votre réputation si votre marque est utilisée pour duper des internautes. Bien souvent, vous ne savez même pas que votre marque est utilisée à des fins malicieuses.

Perte de données esniblées, de propriétes intelletuelles ou encore de secrets industriels.

Divulgation de vos données clients et partenaires.

Divulgation de vos données clients et partenaires.

Selon une étude de l'américain Verizon, 11% des récepteurs de phishing cliquent sur le lien!

Las 3 techniques de phishing les plus régandes

Pos si évident que cela à identifier. Tout le monde peut se laisser duper par manque de vigilance par un email de phishing, car celui ci semble légitime et original.

Pos si évident que cela à identifier. Tout le monde peut se laisser duper par manque de vigilance par un email de phishing, car celui ci semble légitime et original.

Pos si évident que cela à identifier. Tout le monde peut se laisser duper par manque de vigilance par un email de phishing. Car celui ci semble légitime et original.

remplies. Le premier exemple de la série correspond à un phishing de masse, alors que les 4 suivants seront plus ciblés, reprenant l'art du Spear Phishing, qui nécessite des recherches avancées sur les cibles afin d'être crédible et de présenter l'autorité qui convient. Dans ces cas là, Alain sera le patron de Pierre, information facilement trouvable sur le site internet de la société.

1. Abus de confiance
Pierre reçoit un email lui demandant de confirmer un transfert d'argent. L'email contient un lien envoyant vers un site qui se présente comme celui de sa banque, mais en réalité il s'agit d'une copie, éditée, contrôlée et hébergée par des pirates. Une fois sur la page. Pierre entre normalement ses identifiants mais rien ne se passe et un message disant que le site est « temporairement indisponible » apparaît. Pierre étant très occupé, se dit qu'il s'en occupera plus tard. En attendant, il a envoyé ses codes d'accès aux pirates.

2. Fausse loterie
Plerre reçoit un email lui indiquant qu'il a gagné un prix. Habituellement Pierre n'y prête pas attention, car bien trop occupé. Toutefois, cette fois ci, l'email est envoyé par Alain, mentionnant une organisation caritative qu'ils soutiennent mutuellement. Pierre citique alors sur le lien, rien ne se passe à l'écran, mais un malware s'est installé sur son poste de travail.

. Mise à jour d'informations

derre reçoit un email d'Alain lui demandant de regarder le document en pièce jointe. Cé document contient un malvare. Pierre ne s'est rendu compte de rien, en ouvrant le document, tout semblait correct bien qu'incohérent par rapport à son travail. Résultat, le alvare enregistre tout ce que fait Pierre sur son poste (keylogger) depuis des mois, ce qui met en danger tout le Système d'Information de l'entreprise facilitant le vol de données.

Les attaques de phishing et spear phishing sont en augmentation, tant sur le nombre que sur leur niveau de sophistication. Si vos employés reçoivent ce type d'email il y a de forte chance qu'ils se fassent piéger.

Ou'est ce qui peut être fait pour protéger vos employés ?
Pour se protéger contre phishing, la majorité des entreprises se contentent de leur antispam et d'autres logiciels anti-virus ou de blocage des sites web. Toutefois, face à l'augmentation et à la sophistication des attaques, cette menace nécessite une protection dédiéc. Les solutions antispam et virus classiques ne sont plus suffisantes. Il reste la formation des employés, efficace mais trop peu utilisée et qui nécessite d'être réquilère.
Les organisations ont besoin de solutions dédiées à cette menace qu'est le phishing qui nécessite une analyse particulière pour être identifiée et bloquée. Les cybercriminels font évoluer leurs techniques rapidement mais la riposte technologique s'organise également, et certaines solutions anti-phishing sont désornais capables de bloquer tous les types de phishing et sur les phishing est d'inumain, et sur ce point le travail de formation et d'éducation reste énorme!

[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 (Symantec) 13,8 Milions de victimes 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 : Les 5 techniques de phishing les plus courantes | Programmez!

Mot de passe Wifi : trois

quarts des foyers français à la merci d'une attaque | Denis JACOPINI



Trois ménages français sur quatre ne protègent pas correctement leur borne wifi, rendant leurs ordinateurs, téléphones et tablettes accessibles aux pirates informatiques.

Près de trois ménages français sur quatre ne protègent pas correctement leur borne wifi domestique, rendant leurs ordinateurs, téléphones et autres équipements connectés aisément accessibles aux pirates informatiques, selon une étude publiée jeudi par l'éditeur de logiciels antivirus Avast Software.

D'après cette enquête, menée en novembre auprès de plus de 16 000 internautes français équipés d'un réseau wifi domestique, « la vaste majorité des routeurs (...) ne sont pas sécurisés ».

Mot de passe inexistant... ou évident

Les Français sont ainsi 10% à déclarer ne pas utiliser de mot de passe pour protéger leur réseau wifi et 24% à utiliser comme mot de passe « leur adresse, leur nom, leur numéro de téléphone, le nom de leur rue ou d'autres mots faciles à deviner ».

En outre, plus de la moitié des routeurs sont « mal sécurisés par défaut », avec des combinaisons de codes d'accès « beaucoup trop évidentes, telles que 'admin/admin' ou 'admin/motdepasse' », selon Avast.

Selon l'éditeur d'antivirus, 5% des bornes wifi françaises sont même « accessibles de l'extérieur » du domicile. Une proportion identique de sondés admet d'ailleurs avoir utilisé le réseau d'un de leurs voisins à son insu.

Un Français sur cinq a déjà été piraté

Le manque de sécurité des routeurs en fait « des points d'entrée très faciles d'accès pour les hackeurs, qui sont dès lors capables de pirater des millions de réseaux domestiques en France », a affirmé Vince Steckler, directeur général d'Avast, lors d'un point de presse.

Un Français sur cinq rapporte avoir déjà subi un piratage informatique, et 34% redoutent un vol d'informations personnelles ou de données bancaires et financières. Cependant, 42% sont persuadés que leur réseau domestique est suffisamment sûr.

Rappelons qu'un mot de passe, pour être le plus efficace possible, doit comporter des caractères aplha-numériques (lettres minuscules, majuscules, chiffres) et, si possible, des caractères spéciaux.

Et que les mots de passe les plus utilisés l'an dernier — et donc les plus faciles à « craquer » — étaient les suivants :

123456

password

12345678

qwerty

abc123

123456789

111111

1234567

iloveyou

123123

Admin

1234567890

Un conseil : évitez-les !

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

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été Les meilleurs conseils pour choisir vos mots de passe Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

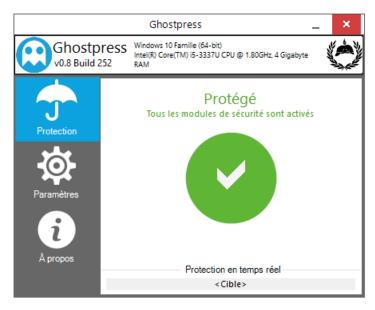
Source

http://www.ouest-france.fr/informatique-wifi-trois-quarts-desfoyers-francais-la-merci-dune-cyberattaque-3026280

Astuce : Un logiciel antiespions gratuit pour Windows | Denis JACOPINI



Ghostpress un logiciel anti-keylogger portable gratuit qui est en mesure de protéger votre ordinateur contre les logiciels espions.



Dans cet article, je vous présente **Ghostpress**, un logiciel anti-keylogger portable totalement gratuit qui est en mesure de protéger votre ordinateur des logiciels espions.

Mais qu'est-ce qu'un keylogger ?

En informatique, un keylogger (enregistreur de frappe) est un logiciel espion qui espionne l'utilisateur d'un ordinateur. Le but d'un tel outil est de s'introduire entre la frappe au clavier et l'apparition du caractère à l'écran. Cela permet à un pirate informatique de récupérer toutes les informations que vous avez tapez avec votre clavier comme un login et un mot de passe, une adresse, des informations bancaires etc. [Source]

Ghostpress

Ghostpress est un outil très simple d'utilisation et peu gourmand en ressource système. Il vous suffit simplement de le télécharger, puis de le lancer pour que tous les modules de sécurité soient activés. Ainsi, chaque actions que vous exécuterez sur l'ordinateur seront cachés des regards indiscrets.

Vous pouvez également désactiver temporairement le programme en cliquant sur le gros bouton vert et exécuter le programme automatiquement au démarrage de Windows en cochant une petite case dans les paramètres de l'outil.

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

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été Les meilleurs conseils pour choisir vos mots de passe Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ? Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Article original de @justgeekOriginal http://www.justgeek.fr/ghostpress-logiciel-anti-keylogger-wind ows-47093

10 conseils pour protéger sa vie privée sur Internet | Denis JACOPINI



Les données numériques que nous produisons sur Internet sont utilisées à notre insu à des fins publicitaires. Nos conseils pour protéger vos données personnelles

Le big data ou mégadonnées (J.O. n° 0193, 22 août 2014) désigne le volume exponentiel des données numériques et leur exploitation.

Tous producteurs de domnées
Les principaux acteurs du big data sont tout d'abord les États qui ont créé de multiples bases de données statistiques, mais aussi leurs services de renseignements (et tous leurs fichiers).
Vienment ensuite les acteurs du Web, les opérateurs des télécoms ou les grands de la distribution. Mais aussi chaque habitant de la planéte qui produit tous les jours une quantité importante de données : courriels, photos, vidéos, posts sur les blogs, achats en ligne.

adaptues a vos uesums, a vos uesums.

Cerner l'individu, tel est le but du marketino ciblé ! Grâce à lui. vous serez aidé dans vos achats, vos déplacements, dans la gestion de votre argent, dans le soin que vous prenez de votre santé.

Vos domnées personnelles aussi sont collectées par les applis mobiles.
3 applications sur 4 collectent les données personnelles contenues dans le téléphone : principalement la localisation, l'identifiant du téléphone et les données d'accès aux comptes personnels (sans que cela soit toujours justifié par la finalité de

Le droit à l'oubli pour effacer ses données sur le Web

Ces collectes de données ont conduit les individus à réclamer — légitimement — la possibilité de garder une forme de contrôle sur leurs usages futurs.

Et comme rien ne se perd sur la Toile, les citoyens sont de plus en plus nombreux à demander la création d'un droit à l'oubli, c'est-à-dire le moyen d'effacer ses données personnelles sur le Net. Ils sont soutenus par plusieurs institutions judiciaires.

Ainsi, pour la première fois, la Cour de justice de l'Union européenne a contraint, en mai 2014, Google à mettre en ligne un formulaire permettant à chacun de procéder à la suppression de ses données nominatives.

Pourtant, selon une étude réalisée par Reputation VIP en juin 2014, Google n'aurait satisfait que 36 % des demandes de suppression de données.

10 conseils pour protéger vos données personnelles
1. Maitriser son smartphone
Les applications installées sur le téléphone sont une mine d'or pour le marketing. Elles accumulent des informations sur nos comportements ou nos déplacements tout au long de la journée.
Pour éviter d'étre suivi à la trace, désactiver la géolocalisation par GPS dans les parametres de réglage (attention, cela interdit l'accès à certains services).
2. N'autoriser le partage de données (contacts, photos, vidéos) que lorsque c'est vraiment utile refuser dans les autres cass.
3. Bloquer les cookies
Sur son site, la Commission nationale de l'Informatique et des Libertés (Cnil) délivre plusieurs astuces pour échapper aux cookies, ces petits fichiers installés à l'insu de l'internaute lorsqu'on navigue sur le Web, et propose Cookieviz, un logiciel d'identification des cookies en temps réel.
Ces fichiers détectent et enrequistrent les achats, les sites consultés. dans le but de proposer de la publicité ciblée.

d'identification des cookies en temps réel.

Ces fichiers détectent et enregistrent les achats, les sites consultés. dans le but de proposer de la publicité ciblée.

On peut les refuser à l'entrée des sites, les bloquer (en configurant les paramètres du navigateur firefox, Internet Explorer_), activer la navigation privée et effacer l'historique.

4. Utiliser un serveur proxy et un pseudo

Un serveur proxy agit comme un intermédiaire entre le navigateur et Internet, cachant ainsi l'identité de l'utilisateur. Il en existe des dizaines que l'on peut télécharger gratuitement sur Internet puis installer sur son ordinateur : AnonymoX,
Privoxy, Squid.

Le but est de rendre son nom et/ou son prénom invisible sur Internet, les réseaux sociaux et dans les courriels.

Avec un pseudo, on peut s'abonner à des newsitetres, réaliser des achats en ligne ou accéder à des services sans délivrer d'informations personnelles.

5. Sécuriser son mot de passe

Choisir un mot de passe compliqué, c'est protéger ses données, un peu comme une porte blindée protégerait sa maison.

Il est préférable qu'il soit composé de chiffres et de lettres en minuscule et en majuscule. Il faut aussi soigner celui de sa boite mail.

6. Utiliser le réseau Tor

(hoisir un mot de passe compliqué, c'est protéger ses données, un peu comme une porte blindée protégeraits a maison.

Il est préférable qu'il soit composé de chiffres et de lettres en misuscule et en majuscule. Il faut aussi soigner celui de sa boite mail.

6. Utiliser le réseau Tor

Ce logiciel, l'éléchargeable sur Internet, permet de naviguer anonymement et son système de serveurs-relais empêche le suivi des données de l'utilisateur.

Ce système est utilisé par plus deux millions d'internautes, que ce soient des dissidents dans les pays où Internet est contrôlé, ou des journalistes ou des militaires, pour des raisons professionnelles.

7. Étre prudets sur les réseaux sociaux

La première précaution consiste à paramètrer ses comptes pour qu'ils soient privés, les paramètres par défaut rendant les comptes publics.

Puis à publier ses photos avec discermente, à bien choisir les amis avec lesquels on va les partager, à sélectionner les groupes que l'on rejoint.

8. Faire du tri

Trier ses followers (« suiveurs » ou « abonnés » sur les réseaux sociaux) avec des logiciels gratuits : Tuit Block sur Twitter; Privacy Fix sur Facebook, Linkedin et Google.

9. Vérilier réoultérement ce oui est toublié sur soi-même en taoant son non et son prénom dans les moteurs de recherche, essentiellement Google en France.

9. Weiltez a son e-repuration
Werifier réquitérement ce qui est publié sur soi-même en tapant son nom et son prénom dans les moteurs de recherche, essentiellement Google en France.
Adresser un courriel aux sites, blogs, moteurs de recherche pour faire supprimer les contenus qui portent atteinte à la vie privée.
10. Porter plainte
Si, après plusieurs demandes, vos données personnelles ne sont pas supprimées, il est possible d'adresser une plainte en ligne directement sur le site de la Cnil (sur cnil.fr).

[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 (Symantec) 13,8 Milions de victimes 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.

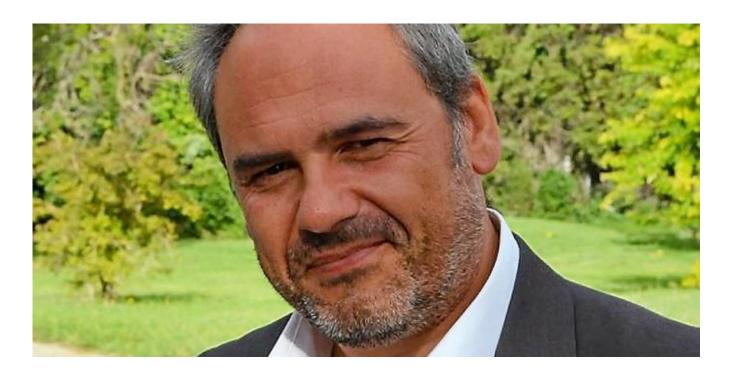
Commandez sur Fnac.fr

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

Auteur : Laurence Fritsch

Source :

http://www.dossierfamilial.com/10-conseils-pour-proteger-sa-vi

e-privee-sur-internet-21122.html

5 conseils pour combattre le piratage informatique



5 conseils pour combattre le piratage informatique

Pour beaucoup d'entre nous, acheter en ligne est devenu une habitude sans laquelle nous pouvons pas vivre. Les achats online simplifient notre quotidien car ils nous permettent de acheter des voyages, des vêtements, des cadeaux et aussi de faire nos courses alimentaires sans bouger ! Internet à changé notre système de vie et, aujourd'hui, presque tout peut s'acheter sur Internet.

Oui, il est beaucoup plus simple et confortable mais, au moment de payer, les doutes aflorent : comment garantir la sécurité d'une transaction pour pouvoir faire nos achats avoir la mouche à l'oreille ? Voici 5 conseils donnés pour le cabinet de sécurité ESET pour se prémunir contre les risques de piratage en ligne.

Vérifiez l'URL du site internet

Lorsque vous effectuez un paiement en ligne, l'URL doit impérativement commencer par « https:// ». Cela signifie que le site Internet est sécurisé. De plus, votre navigateur vous indiquera, au moyen d'un symbole en forme de cadenas, que la sécurité entre votre ordinateur et le site est bien établie. Doc, si vous n'êtes pas complètement sûrs du site dont vous êtes en train de mettre vos coordonnées, il vaut mieux faire demi-tour.

Faites vos achats que sur votre ordinateur personnel

À priori évident, **il ne faut pas profiter d'un réseau WiFi ouvert pour faire des achats et, non plus, sur un ordinateur que ne soit pas le vôtre**. Il est important de rappeler que quand vous fêtes ce type d'activité, vous apprêtez à transmettre des données sensibles, telles que votre numéro de carte bleue ou votre adresse personnelle.

Il est dès lors déconseillé d'utiliser un ordinateur public, ou même l'ordinateur d'un ami car vous ne connaissez pas si l'appareil est bien protégé. Il suffirait alors qu'un logiciel malveillant soit installé sur la machine pour que vos données privées soient récupérées par des cybercriminels.

Privilégiez les réseaux privés

On vient de le dire: les réseaux publics doivent, par essence, être faciles d'accès : c'est pourquoi ils sont le plus souvent dépourvus de toute protection. Si vous pouvez y accéder, un cybercriminel peut le faire aussi. On comprend donc facilement pourquoi il vaut mieux ne pas utiliser ce type de réseau pour effectuer un achat en ligne. Un hacker pourrait facilement accéder à votre ordinateur et à ce que vous y faites, et donc dérober sans difficulté votre numéro de carte bleue et autres données sensibles.

Évitez d'enregistrer vos données en ligne

Avec le développement d'intérêt et les services de pub sur la toile. De plus en plus de sites Internet vous proposent d'enregistrer vos coordonnées, numéro de carte bleue compris, afin que vous n'ayez pas à les saisir à nouveau à chaque achat.

C'est vrai que, si vous êtes des fous des achats en ligne, celle-ci est une fonctionnalité très pratique — surtout sur les sites sur lesquels vous achetez souvent, mais attention : si vous permettez au site Web de se rappeler de vos coordonnées, l'accès à votre compte doit absolument être protégé par un mot de passe fort pour éviter que ces données soient facilement récupérables par les cybercriminels. Voici quelques conseils pour créer un mot de passe efficace.

Utilisiez un navigateur sécurisé

Même si le site sur lequel vous vous apprêtez à payer vous paraît fiable et que vous utilisez un réseau sécurisé, il se peut que des pirates informatiques parviennent à contourner les sécurités pour voler votre numéro de carte bleue. L'idéal est donc d'utiliser un navigateur sécurisé, comme celui inclut dans la solution ESET Internet Security. Grâce à cet outil, vos données sont cryptées directement entre le clavier et le navigateur, ce qui empêche toute possibilité de récupération de vos données bancaires.

Notre métier : Nous réalisons des audits sécurité, nous vous apprenons comment vous protéger des pirates informatiques et vous aidons à vous mettre en conformité avec le règlement Européen sur la protection des données personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur 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 réalise des audits et 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 \ d'informations \ d'informations \ d'information \$



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.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : 5 conseils pour combattre le piratage en ligne — Globb Security FR

Toujours sous Windows XP ? Vous êtes une menace pour la société



Windows XP ne bénéficie plus de correctif de sécurité depuis 2014 et représente par conséquent un risque. Les utilisateurs ont donc une responsabilité. Et si vous êtes un professionnel de l'IT avec des capacités de décision en entreprise, vous devriez être licencié pour maintenir l'usage d'XP.

La réaction à mon dernier article — « Pourquoi Windows doit mourir pour la troisième fois » — était considérable. Des centaines de milliers de personnes ont lu cet article, et nous avons eu des discussions très spirituelles, en effet.

Un tas d'entre vous l'a déclaré sans ambages : vous ne souhaitez pas mettre à niveau Windows XP. Vous êtes fâchés que Microsoft vous ait fait passer de XP à 7 et de 7 à 10. Vous êtes en colère de devoir en permanence mettre à jour le logiciel.

Une poignée d'entre vous a même suggéré de s'en prendre physiquement aux développeurs qui codent le logiciel vers lequel vous refusez de migrer…[lire la suite]

NOTRE MÉTIER:

- FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO
- EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES
- AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT
 - MISE EN CONFORMITE RGPD / FORMATION DPO

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, suivez nos formations ;

EXPERTISES TECHNIQUES: Dans le but de prouver un dysfonctionnement, de déposer ou vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense;

<u>COLLECTE & RECHERCHE DE PREUVES</u>: Nous mettrons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

<u>MISE EN CONFORMITÉ CNIL/RGPD</u>: Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons dans vos démarches de mise en conformité avec le RGPD (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous NOS FORMATIONS

: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles (Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005);
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

×

Source : Toujours sous Windows XP ? Vous êtes une menace pour la société — ZDNet

Formation pour DPO externe mutualisé et Délégués à la protection des données externalisé



Depuis 2012, nous accompagnons des établissement dans leur mise en conformité avec la réglementation sur les Données à Caractère Personnel.





Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant

Formation pour DPO externe ou Délégué à la ptotection des données externalisé : « <u>J'accompagne mes clients dans leur mise en conformité avec le RGPD</u> » : 3 jours + 1 jour d'accompagnement personnalisé (C'est le moment ou jamais de vendre des services « RGPD »)
Si votre objectif est avant tout de développer l'activité de mise en conformité avec le RGPD afin de <u>vendre cette prestation auprès de vos clients</u>, cette formation est faite sur-mesure pour vous en vous apportant l'ensemble des mesures et des cas qu'il est nécessaire de maîtriser pour que vos clients soient mis sur le chemin de la mise en

conformité. Vous êtes une société d'Informatique, un cabinet d'avocat, un cabinet d'expertise comptable, un consultant et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation se passe sur 3 jours en groupe plus une journée supplémentaire en individuel pour superviser la mise en place du RGPD dans votre établissement ou chez un de vos clients (frais liés au déplacement dans cet établissement en sus). Suivez LA formation qui vous apportera la plus grande autonomie dans la mise en conformité de tout notre catalogue.

Consultez les prochaines dates d'animation autour de chez vous ?



Je me présente : Denis JACOPINI. Je suis Expert de justice en informatique spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel), consultant depuis 1996 et formateur depuis 1998. J'ai bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à

formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre acompte. Si la formation était annulée (nombre de participants insuffisants ou en cas de force majeure), votre acompte sera remboursé en intégralité dans les 5 jours (les chèques seront encaissés à partir du jour de la formation). En cas d'annulation de votre part moins de 48 heures avant la formation, l'acompte pourra ne pas être remboursé car destiné à régler les frais de réservation de salle et d'organisation, eux même non remboursables.

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









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

Contactez-nous

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

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

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

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





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

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

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

Comment devenir DPO Délégué à la Protection des Données

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

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles

en 6 étapes

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

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

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

Pendant les vacances continuez à protéger vos données personnelles



Le sutilisateurs sont de plus en plus concernés par le sort de leurs données. Potentiellement victimes, ils doivent prendre plus de temps pour consulter les pages de politique de confidentialité. Qu'en est-il de ces utilisateurs finaux ? Sont-ils acteurs de la sécurité en ligne de leurs données ? Il n'est pas inutile de rappeler certains points.

• Les dangers du Wi-fi public

Lorsque vous rejoignez un réseau Wi-Fi public ouvert à votre café préféré, vous pouvez obtenir plus qu'un expresso. Vous pourriez potentiellement être victime d'un vol d'informations. En outre, un pirate peut avoir créé un faux réseau Wi-Fi qui semble réel (avec un nom similaire par exemple). L'utilisation d'un VPN est donc fortement recommandée.

• Les dangers des applications

Les applications sur votre smartphone peuvent vous espionner. Soyez très prudent lorsque vous sélectionnez des applications. Jetez un œil aux fonctionnalités dictées par le développeur. Maximisez les paramètres de confidentialité autant que possible.

• Les dangers des médias sociaux

Évitez les quiz Facebook qui peuvent relever toutes vos données (Cambridge Analytica). Minimisez les informations que vous partagez sur les réseaux sociaux. N'acceptez pas les demandes de personnes que vous ne connaissez pas.

Tout le monde peut prétendre être quelqu'un d'autre en ligne — prenez des mesures supplémentaires pour assurer votre sécurité et celle de votre famille. En conclusion, n'hésitez pas à vous référer à des conseils, guides, vidéos de la part des professionnels du secteur et autres associations, sans oublier le site de la CNIL et ses guides qui fournissent de bons conseils et recommandations.

[Lire l'article complet sur LaTrinune.fr]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été Les meilleurs conseils pour choisir vos mots de passe Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ? Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : Vous attendez tout du RGPD pour protéger vos données en ligne. Pas si vite !

Comment retrouver l'auteur d'un e-mail ou d'un post ? | Denis JACOPINI





Comment retrouver l'auteur d'un, e-mail ou d'un post ?

Victime d'usurpation d'identité, d'insultes ou de propos diffamatoires, vous désirez retrouver l'auteur d'un e-mail ou d'un post sur un forum ou sur un réseau social ? Les conseils de Denis JACOPINI, expert informatique assermenté.

1. RETROUVER L'AUTEUR D'UN EMAIL

1.1 Les envois d'e-mail

Tout comme un courrier postal sans système de sécurité tel le Recommandé avec Accusé de Réception, l'envoi d'un e-mail ne garanti pas sa réception par le destinataire désiré.

Il devient ainsi aisé de contester la réception d'un e-mail et quand bien même il a été prouvé qu'un email a été reçu et lu, rien ne peut attester qu'il a bien été consulté par la bonne personne. Pour parer à ses failles, il existe des solutions rarement utilisées d'envoi sécurisés par des tiers de confiance pouvant attester la récupération d'un e-mail par une personne identifiée et des procédés de cryptages/décryptages permettant de rendre consultable l'email par le détenteur d'une clé unique.

Sachez que la notion d'accusé de réception n'est pas universelle et dépendant de la compatibilité éventuelle être les logiciels de messagerie de l'expéditeur et du destinataire.

En conclusion, après l'envoi d'un e-mail qui n'utilise pas de procédé de traçabilité, il n'y a pas d'outil permet de confirmer la lecture de l'e-mail par une personne précise. Les outils de traçabilité standards communément rencontrés dans les solutions d'e-mailing, utilisent généralement une petite image spécifique, invisible stockée sur un serveur qui, une fois affichée sur le logiciel de messagerie du destinataire, horodate et mémorise l'adresse IP de l'accès et les paramètres du destinataire ayant affiché l'image.

1.2 La réception d'emails

Lorsque le destinataire d'un e-mail prend connaissance de son message, il est mis en forme par son logiciel de messagerie électronique. Les e-mails peuvent être reçus au format « texte » ou au format « html » avec des mises en forme esthétiquement intéressantes et peuvent contenir ou non une ou plusieurs pièces jointes.

Cependant, chaque e-mail reçu répond à un format spécifique

Un courrier électronique est composé de deux parties : les entêtes et le corps du message, séparés par une ligne vide. Les entêtes stockent les informations contextuelles : qui envoie le message, à qui, avec quel objet, ou encore à quelle date. Le corps du message est quant à lui encodé sous forme de texte, ou de parties multiples (par exemple un texte et des images).

Exemple d'entête d'un message ayant comme seul texte affiché pour le destinataire :

```
Objet : Bonjour !
Message :
Boniour David.
Tiens-moi au courant pour la réunion.
L'entête contiendra :
Received: from 31.121.118.45 (EHLO serveur.fr)
 by mta1007.mail.ukl.yahoo.com with SMTP; Fri, 21 Sep 2012 21:31:16 +0000
Received: by serveur.fr (Postfix, from userid 106)
  id 3DF2F15A0CD; Fri, 21 Sep 2012 23:31:16 +0200 (CEST)
From: "Thomas"
To: david@yahoo.fr
Subject: Bonjour!
Date: Fri, 21 Sep 2012 23:31:16 +0200
MIME-Version: 1.0
Content-Transfer-Encoding: 8bit
Content-Type: text/plain; charset=iso-8859-1
X-Mailer: Mozilla Thunderbird
Message-Id:
```

Bonjour David,

Tiens-moi au courant pour la réunion.

Thomas

L'analyse de l'entête nous permet d'avoir la date et l'heure d'envoi (attention aux indications de fuseau horaire), l'adresse IP et le nom de domaine du serveur expéditeur, l'ID de l'e-mail sur le serveur expéditeur

Remarque :

Un échange d'e-mails (minimum envoi + réponse) permettra plus facilement d'apporter la preuve de que le destinataire a bien reçu le message électronique puisqu'il y répond…

A la suite d'une usurpation d'identité, d'une arnaque, d'un dénigrement, d'injures, de médisence ou de propos diffamatoires, vous pouvez souhaiter retrouver l'expéditeur d'un e-mail :

- A) Constat éventuel par Procès Verbal d'Huissier de l'e-mail ;
- B) Analyse des éventuels échanges d'e-mails
- C) Analyse par un Expert Informatique de l'entête de l'email afin d'extraire la date, l'heure, l'adresse IP et le nom de domaine du serveur d'expédition de l 'e-mail ;
- D) Rechercher le propriétaire d'une adresse IP avec l'outil www.ripe.net ou http://network-tools.com ;
- E) Plages d'adresses IP attribuées par opérateurs sur la page http://www.nirsoft.net/countryip/fr.html ;
- F) Contact éventuel des fournisseur d'accès à Internet pour retrouver l'abonné à Internet à partir de l'adresse IP (ordonnance d'un Juge).

2. RETROUVER L'AUTEUR D'UN POST SUR UN FORUM

A la suite d'une arnaque, d'un dénigrement, d'injures, de médisance ou de propos diffamatoires, vous pouvez chercher des traces de l'auteur dans des forums ou réseaux sociaux. Vous aurez alors des traces de ses posts, souvent bien insuffisants pour remonter jusqu'à l'auteur malveillant.

Pourtant, quelques pistes peuvent être exploitées :

- A) Constat éventuel par Procès Verbal d'Huissier du post avec horodatage.
- B) L'auteur peut utiliser des éléments permettant de retrouver son identité (par exemple, son pseudo est peut-être utilisé sur plusieurs sites et l'identification peut être tentée par recoupement d'informations…)
- C) Rechercher d'autres traces du pseudo dans d'autres sites (Social Mention, Samepoint, Mention.net, Alerti, Youseemii.fr, Webmii, Sprout social, eCaim.com, zen-reputation);
- D) L'analyse de données Exif permet d'avoir des renseignements supplémentaires (par exemple : ExifViewer) ;
- E) Si une demande de retrait par voie amiable des informations par l'auteur n'aboutit pas, vous avez la possibilité de signaler un acte d'injure ou de diffamation sur le site Internet du ministère de l'Intérieur : http://www.internet-signalement.gouv.fr ou saisir une juridiction de proximité (https://www.service-public.fr/particuliers/vosdroits/F1785) ;
- F) Comme pour un contenu dans un moteur de recherche, on peut essayer d'utiliser le Flooding pour envoyer le post dans des pages de résultat lointaines.

Bien évidemment cette liste de conseils pas exhaustive et n'attend que vos avis et commentaires pour l'enrichir

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 (Symantec) 13,8 Milions de victimes 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

Etude et publication de Denis JACOPINI LIENS SOURCES

Utilisation des moteurs de recherche en France

http://www.journaldunet.com/ebusiness/le-net/1087481-parts-de-marche-des-moteurs-de-recherche-en-france/

Taux de clic en fonction de la position dans les résultats http://www.mathiasp.fr/blog/seo/quel-est-le-taux-de-clic-en-fonction-des-positions-dans-google/544