

Victime d'une arnaque sur Internet ? Faites-nous part de votre témoignage



**Victime
arnaque
Internet
Faites-nous
de
part
témoignage**

**d'une
sur
? part
votre**

Vous êtes victime d'une arnaque ou d'un piratage sur Internet ? Votre témoignage nous permettra peut-être de vous aider.

Devant une explosion de cas d'arnaques et de piratages par Internet et des pouvoirs publics débordés par ce phénomène, nous avons souhaité apporter notre pierre à l'édifice.

Vous souhaitez nous faire part de votre témoignage, contactez-nous.

Vous devez nous communiquer les informations suivantes (tout message incomplet et correctement rédigé ne sera pas traité) :

- une présentation de vous (qui vous êtes, ce que vous faites dans la vie et quel type d'utilisateur informatique vous êtes) ;
- un déroulé chronologique et précis des faits (qui vous a contacté, comment et quand et les différents échanges qui se sont succédé, sans oublier l'ensemble des détails même s'ils vous semblent inutiles, date heure, prénom nom du ou des interlocuteurs, numéro, adresse e-mail, éventuellement numéros de téléphone) ;
- Ce que vous attendez comme aide (je souhaite que vous m'aidez en faisant la chose suivante :)
- Vos nom, prénom et coordonnées (ces informations resteront strictement confidentielles).

Contactez moi

Conservez précieusement toutes traces d'échanges avec l'auteur des actes malveillants.
Ils me seront peut-être utiles.



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.

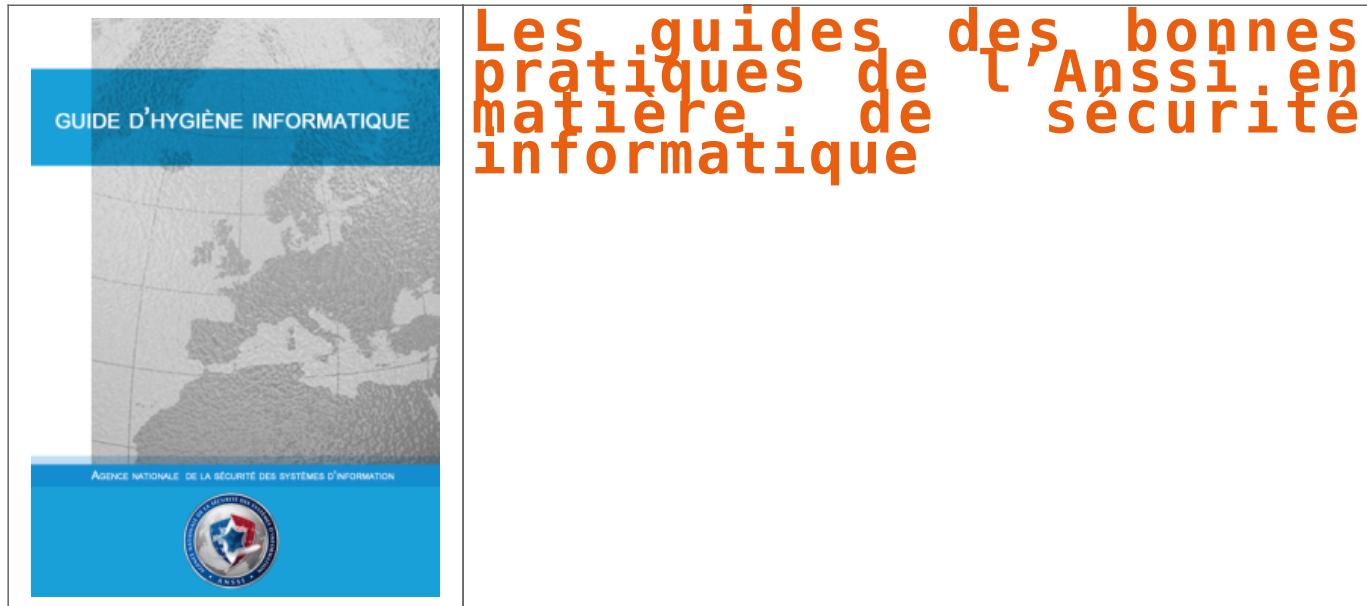


Consultant en Cybercriminalité et en Protection des Données Personnelles

[Contactez-nous](#)

Réagissez à cet article

Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique | Denis JACOPINI



Vous voulez éviter que le parc informatique soit utilisé pour affaiblir votre organisation ? L'un des guides publiés par l'ANSSI vous aidera à vous protéger.

Initialement destinés aux professionnels de la sécurité informatique, les guides et recommandations de l'ANSSI constituent des bases méthodologiques utiles à tous. Vous trouverez sans peine votre chemin en utilisant les mots-clés, qu'un glossaire vous permet d'affiner, ou le menu thématique.

LISTE DES GUIDES DISPONIBLES

- Guide pour une formation sur la cybersécurité des systèmes industriels
- Profils de protection pour les systèmes industriels
- Sécuriser l'administration des systèmes d'information
- Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du rgs
- Recommandations pour le déploiement sécurisé du navigateur mozilla firefox sous windows
- Cryptographie – les règles du rgs
- Recommandations de sécurité concernant l'analyse des flux https
- Partir en mission avec son téléphone sa tablette ou son ordinateur portable
- Recommandations de sécurité relatives à active directory
- Recommandations pour le déploiement sécurisé du navigateur microsoft internet explorer
- l'homologation de sécurité en neuf étapes simples,
- bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,
- recommandations pour le déploiement sécurisé du navigateur google chrome sous windows,
- usage sécurisé d'(open)ssh,
- la cybersécurité des systèmes industriels,
- sécuriser une architecture de téléphonie sur ip,
- mettre en œuvre une politique de restrictions logicielles sous windows,
- prérequis à la mise en œuvre d'un système de journalisation,
- vulnérabilités 0-day, prévention et bonnes pratiques,
- le guide des bonnes pratiques de configuration de bgp,
- sécuriser son ordiphone,
- sécuriser un site web,
- sécuriser un environnement d'exécution java sous windows,
- définition d'une politique de pare-feu,
- sécuriser les accès wi-fi,
- sécuriser vos dispositifs de vidéoprotection,
- guide d'hygiène informatique,
- la sécurité des technologies sans contact pour le contrôle des accès physiques,
- recommandations de sécurité relatives à ipsec,
- la télé-assistance sécurisée,
- sécurité des systèmes de virtualisation,
- sécurité des mots de passe,
- définition d'une architecture de passerelle d'interconnexion sécurisée,
- ebios – expression des besoins et identification des objectifs de sécurité,
- la défense en profondeur appliquée aux systèmes d'information,
- externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques,
- archivage électronique... comment le sécuriser ?
- pssi – guide d'élaboration de politiques de sécurité des systèmes d'information,
- tdbssi – guide d'élaboration de tableaux de bord de sécurité des systèmes d'information,
- guide relatif à la maturité ssi,
- gissip – guide d'intégration de la sécurité des systèmes d'information dans les projets

Expert Informatique 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 protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/>

Comment éviter de se faire avoir par des e-mails de phishing



Phone security | Ervins Strauhmanis via Flickr CC License by

Comment
éviter
de se faire
avoir
par des
e-mails
de phishing

Toujours, toujours être sur ses gardes.

Ça n'arrive qu'aux autres, à ceux qui ne font pas attention, qui n'y connaissent rien, qui font n'importe quoi sur internet. Jusqu'au jour où ça nous arrive à nous. Ça, c'est se faire avoir par du phishing (du hameçonnage, en français), cette technique qui consiste à vous envoyer un e-mail en se faisant passer pour quelqu'un dans le seul but de vous faire cliquer sur un lien, et vous faire rentrer identifiants et mots de passe dans une nouvelle page vous les demandant.

À l'été 2014, on avait ainsi découvert que de nombreuses stars américaines s'étaient ainsi fait voler leur identifiant iCloud de cette façon, permettant aux pirates de collecter leurs photos privées, dont certaines ont ensuite fini par être partagées sur des forums. Même chose avec le piratage de l'adresse e-mail de John Podesta, l'ancien chef de campagne d'Hillary Clinton, lors de la dernière présidentielle américaine.

Le phishing marche, souligne ainsi Wired, qui explique que 100.000 nouvelles attaques ont lieu chaque jour, et que quelques milliers réussissent. En septembre 2016, une étude allemande montrait qu'un étudiant interrogé sur deux pouvait se faire avoir par le message d'un inconnu. Alors pour éviter de se faire avoir, le magazine américain propose trois solutions.

1. Tout d'abord, **toujours réfléchir avant de cliquer**. «Si quelque chose a l'air bizarre, c'est que ça l'est probablement», et «vous devriez toujours être réticents à l'idée de télécharger les pièces jointes et de cliquer sur les liens, peu importe s'ils ont l'air innocent, ou la personne qui les a envoyés». En clair, toujours regarder l'origine de l'e-mail, et si quelque chose semble louche, ne pensez même pas à télécharger ou cliquer sur quoi que ce soit.

2. Ensuite, **scruter la source**. L'étape basique mais qu'on oublie si souvent. Pour être sûr que ce e-mail provient bien de Google, Yahoo!, ou de votre banque, vous devriez vraiment vérifier l'adresse qui vient de vous l'envoyer. Cela veut dire regarder dans l'URL de l'adresse si rien n'a l'air louche, ou si des caractères n'ont pas été remplacés par d'autres pour vous tromper (sur cette image par exemple, l'émetteur a ajouté un deuxième «l» à «paypal»). Si l'adresse e-mail est bien la bonne, mais que le test semble bizarre, vérifiez que c'est bien la bonne personne qui vient de vous l'envoyer, en tentant de la joindre par un autre canal.

3. Enfin, **préparer ses arrières**. En clair, faites comme si vous alliez vous faire avoir un jour ou un autre, et assurez-vous de limiter déjà les dégâts. «Cela veut dire prendre des précautions de cybersécurité standards, comme mettre en place une authentification à plusieurs facteurs (on vous a fait un tuto ici), utiliser un gestionnaire de mots de passe ou un autre système pour créer des mots de passe unique et aléatoires, et sauvegardez vos données.» Parce qu'au fond, le vrai e-mail faible dans toutes ces histoires se trouve entre la chaise et le clavier.

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 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 DGTIC 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](#)

Réagissez à cet article

Source : *Comment éviter de se faire avoir par des e-mails de phishing* | Slate.fr

Ne relayez pas les spams, canulars, chaînes de lettres... | Denis JACOPINI



Ne relayez pas les spams, canulars, chaînes de lettres...

Source

http://www.tahiti-infos.com/Clusir-Ne-relayez-pas-les-spams-ca-nulars-chaines-de-lettres_a121624.html

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits | Denis JACOPINI



Wi-Fi.
Attention
au
piratage
sur les
vrais et
faux
réseaux
gratuits

Ce sont les vacances mais nombre de touristes ne se séparent pas de leurs smartphones, tablettes ou ordinateurs portables. Et pour se connecter à l'internet, quoi de mieux qu'attraper un wi-fi gratuit. Une pratique qui peut se révéler très dangereuse. Des proies faciles pour les « sniffeurs » de données. Explications de Laurent Heslault, expert sécurité chez Symantec.

Vous êtes sur votre lieu de vacances et vous avez envie de vous connecter à l'internet. Pour consulter votre messagerie ou vos réseaux sociaux, envoyer des photos à vos proches, surfer sur le net ou consulter votre compte en banque ou faire une réservation.

Solution la plus simple : se connecter à un réseau Wi-Fi gratuit. Dans votre hôtel, camping, à la terrasse d'un café ou d'un restaurant... Les accès gratuits pullulent et se généralisent.

Expert en sécurité à Symantec, Laurent Heslault tire le signal d'alarme. « **Rien de plus simple que de pirater les données qui transitingent sur un réseau Wi-Fi gratuit** » assure-t-il. « **Par exemple, je m'installe à la terrasse d'un café et je crée un vrai faux point d'accès gratuit en empruntant le nom du café. Des gens vont s'y connecter et je n'ai plus qu'à récupérer toutes les données qui m'intéressent. Des mots de passe, des identifiants...** »

Des sniffeurs de données

Il exagère ? Non. « **L'expérience a été faite à la terrasse d'un café. Nous avons installé un logiciel qui permet de sniffer tous les appareils qui se branchaient sur le Wi-Fi. Ensuite, des complices, qui se faisaient passer pour des magiciens, allaient voir les gens en disant que par magie, ils avaient réussi à changer le code de leur téléphone ou leur image sur Facebook. Ils étaient étonnés !** » Rien de magique mais des logiciels de piratage qui se trouvent facilement sur le net.

Les données sur le Wi-Fi ne sont pas chiffrées

« **Les données qui transitingent sur le Wi-Fi ne sont pas chiffrées. Sauf quand vous vous connectez à un site sécurisé avec le protocole HTTPS. Donc ce sont des données faciles à intercepter.** » Danger sur les vrais faux points d'accès Wi-Fi mais aussi sur les vrais qui ne sont, dans la grande majorité des cas, pas chiffrés non plus. « **Par contre pas de problème pour une connexion 3G ou 4G qui sont chiffrées. Mais pour économiser leur forfait, les gens préfèrent se connecter au Wi-Fi** ».

Conseils

Alors quels conseils ? « **Ne jamais, sur un Wi-Fi public, entrer un mot de passe. D'autant que la plupart des internautes utilisent le même mot de passe pour tous leurs sites.** » En clair, limiter les dégâts en ne consultant que des sites qui ne demandent aucune identification.

Autre solution : protéger son smartphone ou sa tablette en y installent un logiciel qui va chiffrer toutes les données qui vont en sortir. Plusieurs types de logiciels existent dont le Wi-Fi Privacy de Norton qui est gratuit pendant 7 jours et peut s'installer sur des périphériques fonctionnant sous Ios et Androïd.

Article original de Samuel NOHRA.

Nous prodiguons une multitude d'autres conseils durant les formations que nous animons à destination des élus, chef d'entreprises, agents publics et salariés. [Consultez la liste de nos formations]



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.

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



5 règles
d'or pour
les utilisateurs
des réseaux
sociaux

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

Les 310 millions d'utilisateurs actifs par mois sur Twitter postent 347 222 fois en moyenne. Plusieurs d'entre eux tweetent plus d'une centaine de fois par jour, et nombreux sont ceux à tweeter une fois par jour. Plus de 40 millions de photos ont été partagées sur Instagram depuis son lancement, et plus de 80 millions de photos y sont publiées chaque jour.

Ceci représente une énorme quantité de données : certaines importantes, d'autres intéressantes ou encore inutiles. Les réseaux sociaux, avec leurs propres tendances et leurs propres lois, fonctionnent comme une extension du monde réel, qui a un énorme impact sur nos vies hors-ligne. Dans cet article, nous vous dévoilons quelques règles simples que chaque utilisateur de réseaux sociaux devrait garder en tête.

1. N'alimentez pas les trolls

Les trolls sur Internet sont des provocateurs qui se joignent à des conversations dans le but d'agacer les autres utilisateurs pour le « fun ». On peut trouver des trolls n'importe où : sur les forums, les chats, et autres plateformes de communication en ligne. Les forums des nouveaux médias sont connus pour la participation élevée de trolls. D'ailleurs, il y en a plein sur les réseaux sociaux.

Comment devez-vous parler aux trolls ? Daucune façon ! Ignorez-les. Plusieurs personnes se font prendre au piège et engagent alors des débats houleux en essayant d'expliquer leur point de vue et passent une grande partie de leur temps et leur énergie en vain. Quelqu'un a toujours tort sur Internet. Ne perdez pas votre temps et votre énergie pour des trolls.

[View image on Twitter](#)



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

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

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

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

3. Ne partagez pas des arnaques

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

[View image on Twitter](#)



Follow

 CityNews Toronto

[@CityNews](#)

Consumers warned about online scam involving free puppies <http://ow.ly/YAgm>

3:14 AM – 22 Feb 2016

*

*

2020 Retweets

*

*

99 Likes

De tels articles gènèrent beaucoup de partages, mais la majorité d'entre eux sont des arnaques. De vrais appels au secours proviennent en général de votre famille, amis, et amis de vos amis. Ayez toujours en tête que ce sont les pages officielles des entreprises qui mettent en place ce type d'aide et non pas des individus inconnus.

C'est la raison pour laquelle il vaut mieux rester vigilant et vérifier chaque article avant de cliquer sur « aimer » ou « partager ». Pas envie de tous les contrôler un par un ? Ne prenez donc pas de risques pour vous et vos amis.

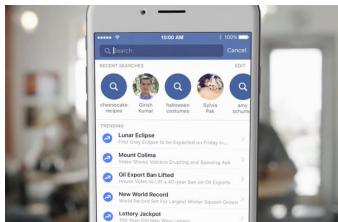
4. Pensez aux réactions des lecteurs

Vous avez probablement des collègues, des supérieurs et des clients parmi vos connections Facebook ou Instagram. Lorsque vous postulez pour un emploi, il est très probable par exemple que les ressources humaines jettent un coup d'œil à votre profil sur les réseaux sociaux. Prenez en compte ce que vous voulez leur montrer, et plus important encore, ce que vous ne voulez pas.

Vous devez également être prudent lorsque vous publiez sur les pages d'autres utilisateurs et sur des comptes publics tels que des entreprises ou des universités. Par exemple, en 2013, un homme originaire de Pennsylvanie a été renvoyé pour avoir « complimenté » une étudiante en ligne. Son commentaire n'avait rien de sexuel ou d'inapproprié, mais de toute évidence la mère de la jeune fille n'avait pas apprécié. Un an auparavant, une professeure de Moses Lake, Washington, avait été virée parce qu'une femme qu'elle n'avait jamais rencontrée s'était plainte d'un de ces articles. Il s'agit de quelques exemples parmi tant d'autres qui prouvent qu'il vaut mieux garder ses photos personnelles et ses articles pour des amis sûrs.

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

[View image on Twitter](#)



Follow

 Kaspersky Lab

[@Kaspersky](#)

Check your Facebook privacy settings NOW <https://kas.pr/3Wpw>

8:13 PM – 26 Oct 2015

*

*

2525 Retweets

*

*

1313 likes

5. Ne dévoilez pas vos données publiques

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

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

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

Article original de John Snow



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

- Expertise technique : virus, espions, pratiques, logiciels malveillants, infections et défaillances (Investigations téléphones, disques durs, e-mails, conteneurs, débrouillages de clients...);
- Expertise de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.I. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

 **Le Net Expert**
INFORMATIQUE

[Contacter-nous](#)

Réagissez à cet article

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

Spécial Phishing 1/3 : Quelle est la technique des pirates informatiques ?



On vous incite à communiquer des informations importantes ?

Ne tombez pas dans le piège.

1. Vous recevez un courriel piégé

Le courriel suspect vous invite à :

- cliquer sur une pièce-jointe ou un lien piégés
- communiquer des informations personnelles

2. L'attaquant se fait passer pour une personne ou un tiers de confiance

L'attaquant est alors en mesure de :

- prendre le contrôle de votre système
- faire usage de vos informations

3. Impact de l'attaque

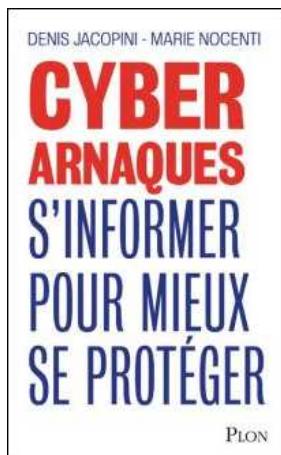
- Intégrité
- Authenticité
- Disponibilité
- Confidentialité

Motivations principales

- Atteinte à l'image
- Appât du gain
- Nuisance
- Revendication
- Espionnage
- Sabotage

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

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



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

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

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

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

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

Commandez sur Fnac.fr

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

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

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

Commandez sur Fnac.fr

Source : ANSSI – *On vous incite à communiquer des informations importantes ? Ne tombez pas dans le piège.*

« Bloctel », la nouvelle

« liste rouge » contre les spams téléphoniques | Denis JACOPINI

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



Denis JACOPINI
vous informe
LCI

« Bloctel » la nouvelle « liste rouge » contre les spams téléphoniques

Invitation par SMS à télécharger une vidéo, demande de rappel d'un correspondant inconnu, démarchage pour une cuisine, des fenêtres en PVC ou des panneaux solaires... Tout possesseur d'un téléphone mobile a déjà dû faire face à ces nombreuses sollicitations, plus ou moins intrusives.

Message
Aujourd'hui 13:22



Info message
vocal. Vous avez
une notification
vocale disponible.
Cliquez pour
l'écouter : [http://
allo-mms.com/](http://allo-mms.com/)

Depuis le 1er juin, les particuliers qui le désirent peuvent inscrire gratuitement leurs numéros (fixe et portable) sur la liste d'opposition au démarchage téléphonique « Bloctel » (bloctel.gouv.fr), mise en place par l'Etat.

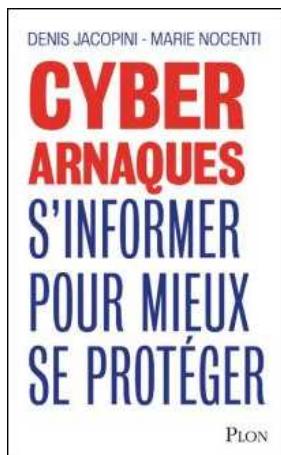
Elle va remplacer la liste « Pacitel » créée en 2011, à l'initiative du gouvernement, par la Fédération française des télécoms. Cette dernière regroupe les principaux opérateurs (hors Free). Contrairement à Pacitel, l'ensemble des entreprises de démarchage auront obligation de se conformer à cette nouvelle liste Bloctel, sous peine d'amende allant jusqu'à 75 000 euros. Ils devront chaque mois retirer de leurs bases de données les numéros de téléphone inscrits sur la liste.

LA MAJORITÉ DES DÉMARCHAGES SE FAIT DEPUIS L'ÉTRANGER

Martine Pinville, secrétaire d'Etat en charge du commerce, qui a pris la succession de Carole Delga, à l'origine de l'entrée en vigueur de ce système, se dit « confiante » dans le succès de cette plate-forme. Mais elle précise que si un démarchage abusif est constaté, « il faudra à ce moment-là relever le numéro de téléphone et, si possible, le nom de la société qui a appelé, afin de nous le signaler sur Bloctel ou à la DGCCRF. Nous ferons les poursuites nécessaires ». Difficile toutefois d'identifier un numéro bien souvent masqué. L'autre écueil réside dans le fait que la majorité des démarchages se fait depuis l'étranger... [Lire la suite]

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

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



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

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

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

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

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

Commandez sur Fnac.fr

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

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

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

Commandez sur Fnac.fr

Source : « *Bloctel* », la nouvelle « liste rouge » contre les spams téléphoniques

Victime d'une fraude sur

votre carte de paiement ?
L'état met à votre
disposition une nouvelle
plateforme : Percev@l

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

 LE NET EXPERT AUDITS & EXPERTISES	 LENETEXPERT fr EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES	 LE NET EXPERT MISES EN CONFORMITÉ	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATION	 LE NET EXPERT ARNAQUES & PIRATAGES
Denis JACOPINI 		Victime d'une fraude sur votre carte de paiement L'état met à votre disposition une nouvelle plateforme : Percev@l			

Depuis quelques jours, un nouveau téléservice est disponible sur service-public.fr. Il permet aux victimes de fraude à leur carte de paiement de se signaler auprès des autorités.

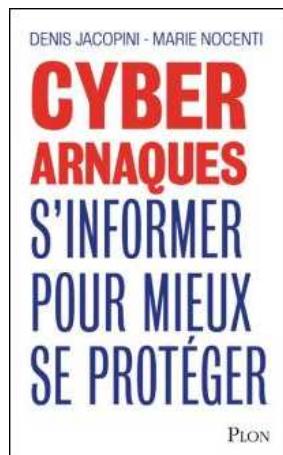
Un tel service était nécessaire et attendu depuis longtemps. En effet, la fraude aux cartes de paiement a lieu essentiellement sur Internet aujourd’hui (à plus de 70% selon les statistiques publiées par l’Observatoire de la sécurité des moyens de paiement). Cela veut dire que le lieu où se commet réellement l’infraction n’a en général aucun rapport avec l’endroit où se trouve la victime. De surcroît, c’est le cumul des informations provenant des nombreuses victimes qui permettra d’identifier les fraudeurs et leur mode opératoire et facilitera la coopération internationale (plus facile si on peut identifier un préjudice conséquent lié aux mêmes auteurs).

Lorsqu’on constate un paiement frauduleux avec son numéro de carte bancaire (en consultant son relevé de compte en ligne, ou encore en étant prévenu par sa banque ou son prestataire de paiement), les opérations suivantes peuvent maintenant être réalisées par les victimes:

- Mettre sa carte en opposition en contact son organisme de paiement (en général par un simple appel téléphonique)
 - Réaliser son signalement sur le téléservice Percev@l (on le retrouve simplement sur le site service-public.fr en cherchant Percev@l ou « fraude carte bancaire »)
 - Transmettre le récépissé fourni par Percev@l à sa banque pour faciliter les opérations de remboursement
- [lire la suite]

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

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



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

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

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

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

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

Commandez sur Fnac.fr

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

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

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

Commandez sur [Fnac.fr](https://www.fnac.fr)

Source : *Percev@l – plateforme de signalement des fraudes aux cartes de paiement – est ouverte! – Investigation & transformation numériques*

Le phishing, ça c'était avant : place aux fraudes au paiement par autorisation dans lesquelles on vous fait dire OK par téléphone

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



LE NET EXPERT
AUDITS & EXPERTISES

EXPERTISES DE SYSTÈMES DE
VOTES ÉLECTRONIQUES
LENETEXPERT
.fr

RGPD
CYBER

LE NET EXPERT
MISES EN CONFORMITÉ

SPY DETECTION
Services de détection
de logiciels espions

LE NET EXPERT
FORMATIONS

LE NET EXPERT
ARNAQUES & PIRATAGES

Le phishing, ça c'était :
ayant place aux
fraudes au
paiement par
autorisation
dans lesquelles
on vous fait
dire OK par
téléphone

Interviewé par Atlantico, Denis JACOPINI nous parle d'une nouvelle forme de Phishing. Le APP (Authorised Push Payment Fraud – fraude au paiement par autorisation) serait une des techniques de fraude en forte croissance au Royaume Uni, et combinerait des techniques sophistiquées, au travers de SMS et d'appels, pour soutirer de l'argent aux victimes.

Le APP (Authorised Push Payment Fraud – fraude au paiement par autorisation) serait une des techniques de fraude en forte croissance au Royaume Uni, et combinerait des techniques sophistiquées, au travers de SMS et d'appels, pour soutirer de l'argent aux victimes. 19 370 cas auraient été répertoriés au Royaume Uni au cours de ces 6 derniers mois selon le daily mail. Quelles sont les techniques ici employées ? La France est-elle touchée ?

Denis Jacopini : Cette technique de fraude utilise de nombreux ingrédients de base :

- L'ingénierie sociale (pratique utilisant des techniques de manipulation psychologique afin d'aider ou nuire à autrui)
- L'usurpation (d'identité) ;
- Le passage en mode émotionnel par la peur ;
- L'interlocuteur est votre sauveur et est là pour vous aider.

Dans le cas précis, nous avons aussi :

- L'usurpation du nom de la banque ;
- L'usurpation du numéro de téléphone de la banque ;
- Le passage en mode émotionnel de la victime basé sur la peur du piratage mais heureusement elle est en ligne avec un sauveur (baisse de la prudence, confiance aveugle...) ;
- La création d'une ambiance téléphonique de centre d'appel ;
- Un excellent comédien qui joue le rôle de l'employé de banque ;
- Une excellente connaissance des procédures internes des banques dont la banque usurpée.

En France, ce type d'arnaque n'est pas encore médiatisé. En effet, les banques n'aiment pas tellement communiquer sur leurs failles car :

- Ce n'est pas bon pour leur image ;
- Elles sont ensuite obligées de dépenser beaucoup pour corriger ;
- Elles préfèrent investir lorsque la fraude commence à leur coûter plus cher que les mesures de sécurité à mettre en place (gestion du risque).

Ces nouvelles techniques de fraude marquent elles une réelle professionnalisation de cette forme de criminalité ?

Denis Jacopini : Cette forme de criminalité existe depuis très longtemps et n'a pas attendu l'informatique et Internet pour se développer et se professionnaliser. Prétexter un gros risque et usurper l'identité des pompiers, des policiers, du plombier en utilisant leur costume, leur jargon, leur outils pour vous rassurer et reviennent ensuite pour mieux vous arnaquer ou vous cambrioler existe depuis que les escrocs existent.

Plus récemment, Gilbert Chikli Pionnier de l'arnaque au faux président, utilisait des techniques de manipulation psychologique et se servait de sa parfaite connaissance des procédures internes aux très grandes entreprises et sa maîtrise du langage juridique ou financier en fonction de l'identité de la personne usurpé pour obtenir de ses victimes des virements définitifs pour des sommes détournées de plusieurs dizaines de millions d'euros.

Chaque fois que des techniques d'arnaque ou d'escroquerie sont déjouées, décortiquées et dévoilées au grand jour, il y a des millions d'escrocs du dimanche vont analyser l'arnaque pour la reproduire et l'utiliser pour eux. Une fois que l'arnaque commence à être connue et de plus en plus de gens sont sensibilisés, les escrocs professionnels et utilisant leur génie à des fins illicites modifient leurs techniques pour toujours utiliser des moyens basés sur les ingrédients de base + des failles inexploitées utilisant ou non la technologie.

Comme les banques ont mis en place des mesures de sécurité utilisant l'internet, le SMS, le téléphone, les escrocs utilisent ces mêmes technologies en recherchant le moyen d'exploiter les failles qui ne seront jamais suffisamment protégées : Les failles du cerveau humain.

Quels sont les réflexes à avoir pour éviter tout problème de ce type ?

Denis Jacopini : Le seul moyen que nous avons pour nous protéger est d'une part la prudence ultime en plus de la sensibilisation. Selon moi, les médias devraient signaler ce type d'arnaque afin de sensibiliser le plus grand nombre. Cependant, cette solution ne plait pas aux banques qui considèrent inutile de répandre la peur car cela risquerait d'écarter de manière irréversible la confiance que nous avons mis des années à avoir envers les moyens de paiement électronique sur Internet.

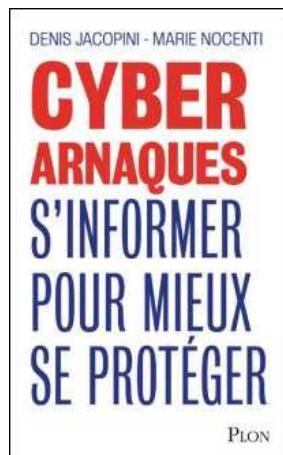
A notre niveau, si j'ai un conseil à vous donner pour éviter tout problème de ce type, si vous vous trouvez dans une situation anormale qui vous est présenté par un interlocuteur, contactez directement l'établissement à l'origine de l'appel à partir des coordonnées dont vous disposez, et allez jusqu'au bout de la vérification AVANT de réaliser des opérations financières irréversibles et partagez le plus possible les cas d'arnaques.

Quand on sait à quoi ressemble le loup, on ne le fait pas rentrer dans sa bergerie. Par contre, s'il met un nouveau costume, le piège fonctionnera tant que ce nouveau costume ne sera pas connu du plus grand nombre. (d'où l'utilité de mon livre CYBERARNAQUES ☺

<https://www.amazon.fr/Cyberarnaques-Denis-JACOPINI/dp/2259264220>

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

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



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

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

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

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

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

Commandez sur Fnac.fr

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

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

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

Commandez sur Fnac.fr

Source : *Le phishing, ça c'était avant : place aux fraudes au paiement par autorisation dans lesquelles on vous fait dire OK par téléphone* | Atlantico.fr