

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-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-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-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-mailon 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, conteneurs, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRETF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

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

LeNetExpert a intégré la plateforme cybermalveillance.gouv.fr

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

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES <i>fr</i></p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
 <p>ACYMA</p>	<p>LeNetExpert a intégré la plateforme cybermalveillance.gouv.fr</p>				

Parce que les victimes doivent pouvoir compter sur des professionnels habitués à réagir face à des actes de piratage, des escroqueries ou vols de données etc., nous avons tenu à soutenir le projet cybermalveillance.gouv.fr. à mettant à leur disposition le meilleur de nos compétences.

2017 sera probablement l'année qui comptera le plus de victimes de rançongiciels. Les initiatives que l'on peut identifier sur le cyberspace ayant pour objectif de combattre ce fléau démontrent une réelle prise de conscience à toutes les strates de l'économie et de l'état. Vous trouverez ci-dessous un guide pdf spécialement fait pour vous aider à anticiper et à réagir face de telles menaces. Cette fiche réflexe est destinée à toutes les catégories de publics. Elle présente cette catégorie d'attaque informatique, les principales mesures à prendre pour s'en protéger, les actions à entreprendre lorsque l'on en est victime, ainsi que les infractions et sanctions pénales auxquelles s'exposent ceux qui les utilisent.



RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

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

LE NET EXPERT

:

- **SENSIBILISATION / FORMATIONS :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - AU RGPD
 - À LA FONCTION DE DPO
 - **MISE EN CONFORMITÉ RGPD / CNIL**
 - ÉTAT DES LIEUX RGPD de vos traitements
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - ORDINATEURS (**Photos / E-mails / Fichiers**)
 - TÉLÉPHONES (récupération de **Photos / SMS**)
 - SYSTÈMES NUMÉRIQUES
 - **EXPERTISES & AUDITS** (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - **SÉCURITÉ INFORMATIQUE**
 - SYSTÈMES DE **VOTES ÉLECTRONIQUES**
- Besoin d'un Expert ? contactez-nous**

Réagissez à cet article

Source : *Fiche rançongiciels (cryptolocker)*

Comment détecter e-mail malveillant

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES</p>	 <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITÉ</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES</p>	 <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITÉ</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
	Comment détecter e-mail malveillant				

Via votre messagerie ou votre boîte mail, certaines personnes malintentionnées tentent de mettre la main sur vos données personnelles en utilisant des techniques d’hameçonnage (phishing) ou d’escroquerie de type fraude 419 (scam) ! Ces techniques d’attaque évoluent constamment. Les conseils suivants vous aideront à déterminer si un message est légitime ou non.

Comment repérer une arnaque reçue dans votre messagerie ou votre boîte mail ?

• **Est-ce que le message/courriel vous est réellement destiné ?**

1. Généralement, les messages malveillants sont envoyés à destination d’un grand nombre de cibles, ils ne sont pas ou peu personnalisés.

2. Le message évoque un dossier, une facture, un thème qui ne vous parle pas ? Il s’agit certainement d’un courriel malveillant.

• **Attention aux expéditeurs inconnus** : soyez particulièrement vigilants sur les courriels provenant d’une adresse électronique que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact.

• **Soyez attentif au niveau de langage du courriel** : même si cela s’avère de moins en moins vrai, certains courriels malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d’orthographe ou des expressions inappropriées, c’est qu’il n’est pas l’œuvre d’un organisme crédible (banque, administration ...).

• **Vérifiez les liens dans le courriel** : avant de cliquer sur les éventuels liens, laissez votre souris dessus*. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime. Ne faites pas confiance aux noms de domaine du type impots.gouv.fr, impots.gouvfr.biz, infocaf.org au lieu de www.caf.fr.* *A noter : cette manipulation est impossible à effectuer depuis un écran de smartphone.*

• **Méfiez vous des demandes étranges** : posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n’a le droit de vous demander votre code carte bleue, vos codes d’accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d’une personne qui annonce faire partie de votre entourage.

• **L’adresse de messagerie source n’est pas un critère fiable** : une adresse de messagerie provenant d’un ami, de votre entreprise, d’un collaborateur peut facilement être usurpée. Seule une investigation poussée permet de confirmer ou non la source d’un courrier électronique. Si ce message semble provenir d’un ami – par exemple pour récupérer l’accès à son compte – contactez-le sur un autre canal pour vous assurer qu’il s’agit bien de lui !

Comment réagir ?

Si vous avez un doute sur un message reçu, il y a de fortes chances que celui-ci ne soit pas légitime :

- N’ouvrez surtout pas les pièces jointes et ne répondez-pas;
- Si l’escroquerie que vous souhaitez signaler vous est parvenue par un spam (pourriel), rendez-vous sur www.signal-spam.fr;
- Supprimez le message puis videz la corbeille;
- S’il s’agit de votre compte de messagerie professionnel : transférez-le au service informatique et au responsable de la sécurité des systèmes d’information de votre entreprise pour vérification. Attendez leur réponse avant de supprimer le courrier électronique.

Comment s’en prémunir ?

- Utilisez un logiciel de filtre anti-pourriel ou activez l’option d’avertissement contre le filoutage présent sur la plupart des navigateurs.
- Installez un anti-virus et mettez-le à jour.
- Désactivez le volet de prévisualisation des messages.
- Lisez vos messages en mode de texte brut.

Si vous êtes victime d’une escroquerie en ligne ?

Signalez les escroqueries auprès du site www.internet-signalement.gouv.fr, la plateforme d’harmonisation, d’analyse de recoupement et d’orientation des signalements. **Pour s’informer sur les escroqueries** ou pour signaler un site internet ou un courriel d’escroqueries, un vol de coordonnées bancaires ou une tentative d’hameçonnage : contacter Info Escroqueries au 0811 02 02 17 (prix d’un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile) – Du lundi au vendredi de 9h à 18h

Rendez-vous sur cybermalveillance.gouv.fr , la plateforme nationale d’assistance aux victimes d’actes de cybermalveillance. Que vous soyez un particulier, une entreprise ou une administration, retrouvez :

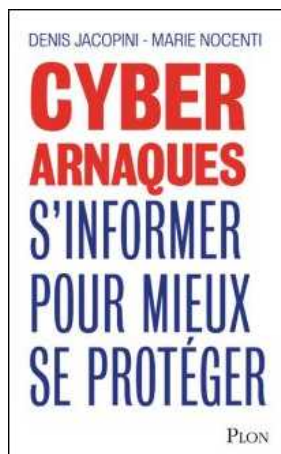
- des conseils / vidéos pour sensibiliser votre entourage professionnel ou personnel,
- des services de proximité en cas de dommages causés par une attaque informatique.

...[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 cyberarnaqes 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'arnaqes 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'arnaqes 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 : *Phishing : détecter un message malveillant* | CNIL

Piratage de votre boîte mail,

quelles peuvent être les
conséquences sur votre vie
personnelle

	Piratage de votre boîte mail, quelles peuvent être les conséquences sur votre vie personnelle
-----------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------

Votre boîte mail est souvent la clé qui permet d'accéder ou de vous inscrire aux services en ligne. Raison de plus pour la sécuriser au maximum !



Pour votre boîte mail : un mot de passe solide

Vous devez utiliser un mot de passe propre et unique pour vous connecter à votre webmail et surtout ne pas l'utiliser pour un autre compte.

Pourquoi c'est important ?

Utiliser le même mot de passe pour votre compte de messagerie et votre compte de réseau social est une pratique risquée. Si votre fournisseur de réseau social est victime d'une fuite de données comprenant vos moyens d'authentification, une personne mal intentionnée pourrait les utiliser pour non seulement accéder à votre compte de réseau social mais aussi pour accéder à votre messagerie.

De plus, une fois l'accès à votre messagerie obtenu, il deviendra possible de voir la liste des messages d'inscriptions à vos comptes sur différents sites (si vous ne les avez pas supprimés de votre boîte). Il sera ainsi possible de connaître certains de vos identifiants de compte et d'utiliser la fonction d'oubli de mots de passe pour en prendre le contrôle.

Cette absence de sécurité ou l'utilisation d'un mot de passe faible vous expose à des risques :

- Usurpation de votre boîte mail pour piéger votre liste de contacts ;
- Ajout d'une redirection de mail (souvent indétectable après la compromission d'une boîte mail) : vos emails continuent de fuiter malgré tout changement de mot de passe ultérieur...
- Connexion du pirate à vos sites et applications tierces ;
- Utilisation de vos coordonnées bancaires pour payer ;
- Usurpation d'identité grâce aux données collectées dans votre boîte mail ;
- Demande de rançon suite à des données compromettantes retrouvées dans votre boîte mail ;
- ...

[CONSEIL] – En parallèle d'un bon mot de passe :

- Il est déconseillé d'utiliser sa boîte mail en tant qu'espace de stockage, notamment pour les données qui peuvent vous paraître sensibles et notamment, les bulletins de paie, les justificatifs d'identité envoyés qui peuvent notamment contenir votre adresse postale personnelle, ou les mots de passe échangés en clair. Attention également aux photos qui permettent de vous ré-identifier sur des sites de réseaux sociaux et donnent la possibilité à une personne malveillante de se créer une fausse identité.
- Il convient de supprimer les emails reçus, envoyés ou enregistrés en tant que brouillon qui paraissent avoir une importance particulière ou de chiffrer les documents que vous mettez en pièce jointe.
- Enfin pour protéger votre identité, il est recommandé d'utiliser une boîte mail sous pseudonyme pour l'inscription à des services que vous jugez intrusifs, ou particulièrement sensibles (site de jeux concours, site de rencontre ...).

L'initiative

haveibeenpwned est un site conçu par Troy Int, informaticien indépendant. Il recense tous les mails compromis à l'occasion de fuite de données massive. L'utilisateur n'a qu'à entrer son email pour savoir s'il figure dans une base de données piratée et si ses mots de passes sont potentiellement entre les mains de personnes malveillantes.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous accompagner dans vos démarches de mise en conformité avec la réglementation Européenne relative à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <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 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](#)

Réagissez à cet article

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

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES <i>fr</i></p>	 <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
		<h2>Formation RGPD : l'essentiel sur le règlement Européen pour la protection des Données Personnelles</h2>			

Contenu de nos formations :

Le Règlement Général sur la Protection des Données (RGPD) entre en application le 25 mai 2018 et les entreprises ne s'y sont pas préparées. Or, elles sont toutes concernées, de l'indépendant aux plus grosses entreprises, et risqueront, en cas de manquement, des sanctions pouvant aller jusqu'à 4% de leur chiffre d'affaires. Au delà des amendes pouvant attendre plusieurs millions d'euros, c'est aussi la réputation des entreprises qui est en jeu. Quelle valeur lui donnez-vous ? Serez-vous prêt à la perdre pour ne pas avoir fait les démarches dans les temps ?

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.



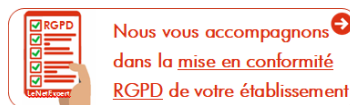
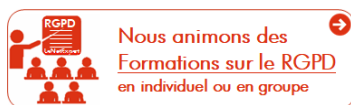
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

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)

Rançongiciel et hameçonnage : quelle démarche entreprendre si vous êtes la cible d'une cyberattaque ?



Rançongiciel
et
hameçonnage
: quelle
démarche
entreprendre
si vous êtes
la cible
d'une
cyberattaque
?

Les ordinateurs contiennent des documents privés et données confidentielles (renseignements personnels, identifiants bancaires, codes secrets) qui peuvent être convoités par une tierce personne mal intentionnée. En cas de cyberattaque, il est important de savoir réagir vite pour se protéger d'une utilisation frauduleuse de vos données personnelles. Nous expliquons ici les principales cybermenaces qui planent sur les internautes, les recommandations de sécurité pour s'en prémunir et, surtout, comment agir si vous êtes la victime d'un cybercriminel.

Les recommandations de sécurité pour se protéger des cyber-escrocs

Selon l'ANSII (agence nationale de la sécurité des systèmes d'information), il vous est fortement conseillé de respecter **quelques règles simples pour vous protéger contre les cyberattaques**. Effectuer des sauvegardes régulières de vos fichiers importants sur des supports de stockage amovibles (CD, clé USB, disque dur externe). Mettre à jour régulièrement les principaux logiciels de vos appareils numériques (ex : Windows, antivirus, lecteur PDF, navigateur, etc.) en privilégiant leur mise à jour automatique. Ne pas avoir une confiance aveugle dans le nom de l'expéditeur de l'email. En cas de doute, n'hésitez pas à contacter directement l'expéditeur par un autre moyen de communication. Se méfier de courriel type « hameçonnage ciblé » qui vous propose un contenu personnalisé pour mieux tromper votre vigilance. Ne pas ouvrir les pièces jointes et ne pas suivre les liens des messages électroniques douteux (fautes d'orthographe, caractères accentués, nom des pièces jointes trop succinct). Ne jamais répondre à une demande d'information confidentielle par courriel.

En cas de cyber-attaque, il faut immédiatement déconnecter du réseau tout appareil susceptible d'être infecté et alerter au plus vite le responsable de sécurité ou le service informatique. Dans le cadre d'un rançongiciel, il est primordial de **ne pas payer la rançon**, car il n'est nullement garanti que la victime récupère la clé de déchiffrement qui lui permettra de récupérer l'accès à ses données personnelles.

Comment réagir si vous êtes victime d'un rançongiciel ou d'hameçonnage ?

Vous devez vous rendre dans un **commissariat de police** ou une **brigade de gendarmerie** pour **déposer plainte**, ou bien **adresser un courrier au Procureur de la République** auprès du **Tribunal de Grande Instance compétent**.

Pour mener correctement l'enquête, il faudra **fournir les renseignements suivants**.

- Les références du (ou des) transfert(s) d'argent effectué(s).
- Les informations de la (ou des) personne(s) contactée(s) : pseudos utilisés, adresse de messagerie ou adresse postale, numéros de téléphone, fax, copie des courriels...
- Le numéro complet de la carte bancaire ayant servi au paiement, la référence de votre banque et de votre compte, et la copie du relevé de compte bancaire où apparaît le débit frauduleux.
- Tout autre renseignement utile à l'identification du cyber-escroc.

Vous pouvez également **utiliser la plateforme de signalement Pharos** ou le numéro de téléphone dédié : 0811 02 02 17 pour signaler les faits dont vous avez été victime. La suite de l'enquête sera prise en charge par des services spécialisés...[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 ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons 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 ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons 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 (Règlement 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](#)

Réagissez à cet article

Source : *Rançongiciel et hameçonnage : quelle démarche entreprendre si vous êtes la cible d'une cyberattaque ?*

Formation en Cybercriminalité : Arnaques, virus et demandes de rançons, Comment s'en protéger ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITE</p>	 <p>LE NET EXPERT SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
		<p>Formation en Cybercriminalité : Arnaques, virus et demandes de rançons, Comment s'en protéger ?</p>			

Le contexte de l'Internet et l'ampleur du phénomène de la cybercriminalité, nous poussent à modifier nos comportements au quotidien.

Avons-nous raison d'avoir peur ? De quoi doit-on avoir peur ? Comment se protéger ?

Les réponses évidentes sont techniques, mais il n'en est pas moins vrai que des règles de bonnes pratiques et des attitudes responsables seront les clés permettant d'enrayer le phénomène.

OBJECTIF DE LA FORMATION EN CYBERCRIMINALITE :

La formation en cybercriminalité a pour but de créer des déclics chez les utilisateurs, mettre à jour les connaissances des informaticiens et faire prendre conscience aux chefs d'entreprises des risques en couvrant les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant d'enrayer le phénomène de la cybercriminalité.

PROGRAMME :

- Etat des lieux de la cybercriminalité en France et dans le monde;
- Les principaux cas de piratages et d'arnaques expliqués ;
- Les bonnes pratiques au quotidien pour limiter les risques ;
- Etude de vos témoignages, analyse de cas et solutions.
- PUBLIC CONCERNÉ : Utilisateurs, chefs d'entreprise, présidents d'associations, élus....

MOYENS PÉDAGOGIQUES :

- Support de cours pour prise de notes
- Résumé remis en fin de cours.
- Vidéo projecteur et sonorisation souhaitée selon la taille de la salle.

CONDITIONS D'ORGANISATION

- Formations individuelles ou en groupe
- Formations dispensées dans vos locaux ou organisées en salle de formation partout en France en fonction du nombre de stagiaires.

Téléchargez la fiche de présentation / Contactez-nous

QUI EST LE FORMATEUR ?

Denis JACOPINI est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire et a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

Il anime dans toute la France et à l'étranger des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles.

A ce titre, il intervient régulièrement sur différents médias et sur La Chaîne d'Info LCI pour vulgariser les sujets d'actualité en rapport avec ces thèmes.

Spécialisé en protection des données personnelles, il accompagne les établissements dans leur mise en conformité CNIL en les accompagnant dans la mise en place d'un Correspondant Informatique et Libertés (CIL).

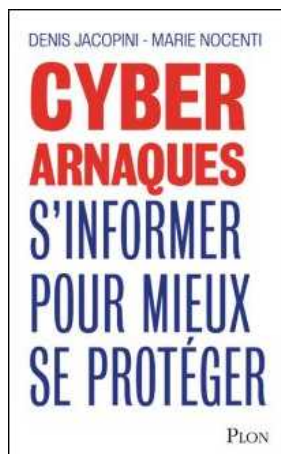
Enfin, il intervient en Master II dans un centre d'Enseignement et de Recherche en Informatique, en Master Lutte contre la Criminalité Financière et Organisée, au Centre National de la Fonction Publique Territoriale et anime le blog LeNetExpert.fr sur lequel il partage et publie de très nombreuses informations sur ses thèmes de prédilection.

Denis JACOPINI peut facilement être contacté sur :

<http://www.leNetExpert.fr/contact>

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 cyberarnaqes 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'arnaqes 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'arnaqes 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://www.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](https://www.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)

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					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LENETEXPERT.fr</p>	 <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITE</p>	 <p>LE NET EXPERT SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
<p>Denis JACOPINI</p>  <p>vous informe</p>		<p>Victime d'une fraude sur votre carte de paiement ? L'état met à votre disposition une nouvelle plateforme : Percev@l</p>			

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).

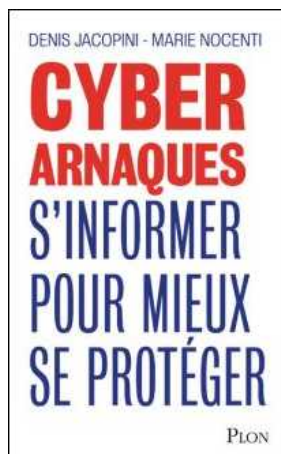
Lorsqu'on constate un paiement frauduleux avec son numéro de carte bancaire (en consultant son relevé de compte en ligne, ou encore en étant prévenu par sa banque ou son prestataire de paiement), les opérations suivantes peuvent maintenant être réalisées par les victimes:

- 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]

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 cyberarnaqes 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'arnaqes 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'arnaqes 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://www.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](https://www.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

Comment protéger son site internet des pirates informatiques ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LENETEXPERT.fr</p>	 <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
			<p>Comment protéger son site internet des pirates informatiques ?</p>		

Il n'y a rien de plus stressant que de se faire hacker ou pirater un compte. Cependant, les criminels virtuels ne s'attaquent pas seulement à votre identité, ils prennent votre argent ou même la source de vos revenus. Ici, cette source ce sont les commerces en ligne et les sites web de vente. Que faire pour y remédier ?

La première précaution quand il s'agit de se protéger contre le piratage ? Mettre un plug-in de sécurité sur votre CMS. La deuxième précaution consiste à changer les droits de vos fichiers. Néanmoins, cette option n'est pas sans difficulté, car certains hébergeurs refusent ce genre de modification. Une autre astuce serait de sauvegarder régulièrement vos données pour pouvoir l'effacer en cas de piratages afin de ne laisser aucune trace de ce dernier. Dans le cas contraire, il est fort possible que vous perdiez votre crédibilité auprès de vos internautes et clients.

Pour conclure, le piratage est un sujet et un fléau courant actuellement, qu'il est toutefois possible de contrôler. Par contre, les pirates ne s'arrêtent jamais. Ils peuvent revenir pour hacker votre site ou votre serveur : une mise à jour constante de votre système de protection est donc de mise...[lire la suite]

Conseil de Denis JACOPINI :

Nous remarquons de nombreux piratages causés par une relation physique ou logique avec votre Système Informatique d'entreprise. Une autre recommandation consiste en plus de les héberger sur des machines différentes, à utiliser des identifiants et des mots de passe évidemment complexes mais aussi différents non seulement pour chacun de services du site Internet mais surtout des autres éléments de votre Système Informatique.

[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 : *Piratage informatique : comment protéger son site internet ?*

Wifi gratuit: Attention à vos données personnelles !





Wifi
gratuit:
Attention, à
vos données
personnelles
!

Les utilisateurs de réseaux de wifi du monde entier ne sont pas à l'abri du danger. D'après une enquête réalisée par Norton by Symantec, la grande majorité des internautes de l'Hexagone adoptent des comportements dangereux pour leur sécurité comme pour leur confidentialité.

Les Français parmi les mauvais élèves

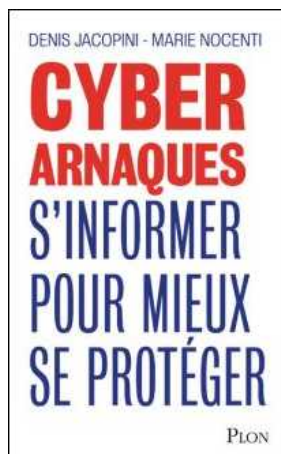
Un sondage a été réalisé par Norton by Symantec sur un échantillon de 1 000 personnes environ dans chacun des 15 pays supervisés, dont la France et les Etats-Unis. L'enquête a tenté de mettre en avant les dangers d'une **connexion à des réseaux de wifi gratuit**. Il a été révélé que les internautes prennent de très gros risques pour leur sécurité et leur confidentialité par le biais du troc connexion-information. Ce dernier se manifeste sous plusieurs formes : adresse email à fournir, coordonnées, géolocalisation à accepter ou encore publicité à voir. Selon l'étude, la quasi-totalité des internautes de l'Hexagone (87%) ne cesse de multiplier les comportements dangereux pour leur sécurité comme pour leur confidentialité.

Les comportements dangereux des mobinautes

L'étude a mis en avant le comportement des internautes du monde entier. Ainsi, 43% des sondés sont impatients de se connecter à peine installés au restaurant, au café, à l'hôtel, dans un magasin ou même chez un ami. Plus encore, l'envie est si pressante que 25% avouent avoir déjà tenté de se connecter sans la permission du propriétaire du réseau. Les 7% ont déjà tenté de pirater ou deviner le mot de passe (7%), rapporte *LCI*. Pour avoir une bonne **connexion**, 55% des personnes enquêtées accepteraient de fournir n'importe quelle information...[lire la suite]

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 cyberarnaqes 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'arnaqes 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'arnaqes 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 :
<http://www.linfo.re/magazine/high-tech/722259-wifi-gratuit-halte-a-vos-donnees-personnelles> »>Wifi gratuit: attention à vos données personnelles! – LINFO.re – Magazine, High-Tech