

Conseils clé pour se protéger contre la cybercriminalité | Denis JACOPINI

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



#Conseils clé pour #se
protéger. contre la
#cybercriminalité

L'avis d'expert de Jean-Philippe Sanchez, Consultant Sécurité chez NetIQ France.

La cybercriminalité est souvent médiatisée lorsque d'énormes failles de sécurité sont révélées et que les dommages sont significatifs pour les entreprises touchées. L'attaque massive organisée par des pirates informatiques russes il y a quelques semaines à une échelle mondiale en est un très bel et marquant exemple, avec plus de 1,2 milliard de mots de passe volés.

Mais les hackers ne se limitent pas aux attaques massives, et des petites brèches de sécurité d'apparence anodines peuvent pourtant s'avérer avoir de lourdes conséquences, tant pour les grandes entreprises que pour les plus petites organisations possédant des données sensibles ou à forte valeur ajoutée.

Ne perdez pas votre temps à anticiper, sachez surtout détecter les failles et limiter les dégâts

La meilleure chose qu'un directeur informatique ou un responsable de la sécurité puisse faire pour protéger son entreprise est de comprendre et d'accepter l'impossibilité de maintenir les attaquants à l'écart. Tout le monde est tôt ou tard victime d'une faille de sécurité. Le plus important est de savoir dans quel délai vous la détecterez et dans quelle mesure vous pourrez limiter les dommages. Il convient de mettre l'accent sur la réduction du risque dans les domaines clés et la surveillance des événements au niveau du pare-feu pour détecter le plus rapidement possible l'intrusion d'un attaquant et la tentative de vol de données. Toute autre action ne reviendra qu'à reproduire des stratégies qui ont déjà montré leurs limites dans le passé, pour un coût encore plus élevé.

Ayez votre stratégie de sécurité sur l'identité et les données, et non plus l'infrastructure

Le mode de pensée centré sur le réseau et les appareils est de plus en plus délaissé en faveur d'une sécurité axée sur l'identité et les données.

Désormais, tenter de protéger l'infrastructure de l'entreprise n'apparaît plus comme une solution gagnante. Avec l'usage croissant de l'informatique mobile et du Cloud computing, cette tâche s'avère souvent trop complexe et n'est plus entièrement maîtrisée par le personnel informatique et de sécurité. En revanche, le personnel chargé de la sécurité réfléchit de plus en plus à la protection des données transférées d'un endroit à un autre, y compris dans le cloud, et à l'acquisition d'une meilleure connaissance de l'identité des individus qui ont accès à ces données. Néanmoins, suis-je certain de savoir qui accède actuellement à notre base de données de patients ? Est-il normal que ce salarié ouvre ce fichier de données clients ? Ces décisions sont de plus en plus complétées par l'introduction d'un contexte du type : dois-je permettre à ce salarié d'accéder à ces données sensibles alors qu'il est en vacances dans le Sud et qu'il se connecte depuis sa tablette dans un cybercafé ? Il s'agit là d'une façon plus intelligente (et efficace) d'appréhender les risques du comportement surveillé, en répondant aux problèmes de sécurité fondamentaux liés aux utilisateurs privilégiés, aux attaques internes et aux menaces persistantes avancées.

Ne misez pas tout sur la technologie, sensibilisez vos collaborateurs car ils sont les véhicules de vos données !

Il est toujours possible d'améliorer l'éducation – bien que je sois convaincu qu'il faille en changer le ton pour passer du « ne faites pas ceci » au « comme vous le ferez de toute façon, voici comment procéder pour éviter de prendre des risques ». Le pouvoir dans le monde de l'informatique professionnelle a changé de mains : il n'est plus dévolu au service IT autoritaire et centralisé, avec le personnel qui lui est associé, mais relève désormais des dirigeants de l'entreprise et des responsables métiers. Aujourd'hui plus que jamais, l'utilisateur de l'entreprise décide lui-même de la technologie à employer et de la façon de procéder. Dans ce contexte, l'éducation doit être recentrée sur les conseils et le choix de solutions sûres pour cesser de s'apparenter à une liste d'actions à éviter, qui sera de toute façon rarement respectée.

Réagissez à cet article

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

Source

: <http://www.generation-nt.com/cybercriminalite-hacker-netiq-jean-philippe-sanchez-actualite-1905811.html>

Comment détecter les arnaques sur Internet ? Denis JACOPINI vous en parle sur Europe 1 à l'occasion de la présentation de son livre « CYBERARNAQUES : S'informer pour mieux se protéger »

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

x	<p>Comment détecter les arnaques sur Internet ? Denis JACOPINI vous en parle sur Europe 1 à l'occasion de la présentation de son livre « CYBERARNAQUES S'informer pour mieux se protéger »</p>					

Internet et les réseaux sociaux ont envahi notre quotidien, pour le meilleur mais aussi pour le pire... Qui n'a jamais reçu de propositions commerciales pour de célèbres marques de luxe à prix cassés, un email d'appel au secours d'un ami en vacances à l'autre bout du monde ayant besoin d'argent ou un mot des impôts informant qu'une somme substantielle reste à rembourser contre la communication de coordonnées bancaires ? La Toile est devenue en quelques années le champ d'action privilégié d'escrocs en tout genre à l'affût de notre manque de vigilance. Leur force ? Notre ignorance des dangers du Net et notre « naïveté » face aux offres trop alléchantes qui nous assaillent.

« Puisse cet ouvrage avoir de nombreux lecteurs ! Il ne devrait pas plaire aux arnaqueurs, car il est un réquisitoire contre leur perfidie et, sans aucun doute, une entrave à leur chiffre d'affaire. »

Général d'armée (2S) Watin- Augouard

Commandez CYBERARNAQUES



Plutôt qu'un inventaire, Denis Jacopini, avec la collaboration de Marie Nocenti, a choisi de vous faire partager le quotidien de victimes d'Internet en se fondant sur des faits vécus, présentés sous forme de saynètes qui vous feront vivre ces arnaques en temps réel. Il donne ensuite de précieux conseils permettant de s'en prémunir. Si vous êtes confronté un jour à des circonstances similaires, vous aurez le réflexe de vous en protéger et en éviterez les conséquences parfois dramatiques... et coûteuses.

Un livre indispensable pour « surfer » en toute tranquillité !

Denis Jacopini est expert judiciaire en informatique, diplômé en cybercriminalité et en droit, sécurité de l'information et informatique légale à l'université de droit et science politique de Montpellier.

Témoin depuis plus de vingt ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus soigneusement élaborées, il apprend aux professionnels à se protéger des pirates informatiques. Marie Nocenti est romancière.

Réagissez à cet article

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 : *Cyberarnaques S'informer pour mieux se protéger – broché – Denis Jacopini, MARIE NOCENTI – Achat Livre – Achat & prix | fnac*

Comment créer sa charte Informatique ? (ANSSI)

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Comment créer sa charte Informatique ? (ANSSI)				

L'ANSSI publie un guide pour accompagner les organisations dans l'élaboration d'une charte d'utilisation des moyens informatiques et des outils numériques. 8 points clés pour saisir l'opportunité d'accompagner efficacement la transition numérique des entreprises face à l'augmentation croissante de la menace.

1. L'OBJECTIF

La charte d'utilisation des moyens informatiques a pour finalité de contribuer à la préservation de la sécurité du système d'information de l'entité et fait de l'utilisateur un acteur essentiel à la réalisation de cet objectif...[lire la suite]

2. DES DÉFINITIONS CLAIRES ET PRÉCISES

Définir les termes clés du document permet de limiter leur interprétation juridique (administrateur, messagerie électronique, moyens d'authentification, système d'information, utilisateur, etc.)...[lire la suite]

3. L'OBJET ET SA PORTÉE

La charte doit rappeler ce sur quoi elle porte. Notamment, elle doit exprimer de manière explicite qu'elle a pour objet de préciser les droits et devoirs de l'utilisateur...[lire la suite]

4. LES USAGES

De nombreuses questions sont à envisager lorsque l'entité souhaite fixer les règles d'usage de son système d'information. L'entité met-elle à disposition une messagerie professionnelle ?...[lire la suite]

5. DÉFINIR LES DEVOIRS DE L'UTILISATEUR

Outre les obligations générales qu'il est bon de rappeler, les devoirs de l'utilisateur découlent directement des usages autorisés définis en amont...[lire la suite]

6. LES MESURES DE CONTRÔLE

Les mesures de contrôle que l'entité peut mettre en place peuvent être étendues, pourvu qu'elles aient fait l'objet d'une information préalable des utilisateurs (via la charte) et qu'elles soient conformes au droit en vigueur...[lire la suite]

7. LES SANCTIONS

La charte informatique étant un document de portée juridique, elle permettra de fonder les sanctions à l'encontre d'un utilisateur qui ne l'aurait pas respectée. Il est impératif de prévoir une échelle des sanctions disciplinaires...[lire la suite]

8. S'ASSURER DE L'OPPOSABILITÉ DE LA CHARTE

L'opposabilité de la charte nécessite également son acceptation par les utilisateurs (signature de la charte ou annexe au contrat de travail)...[lire la suite]

[Consultez le guide complet de l'ANSSI]

Réagissez à cet article

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 ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

Quel sont nos principales activités ?

▪ **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique 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).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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



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



[Contactez-nous](#)



Source : Charte d'utilisation des moyens informatiques et des outils numériques – Le guide indispensable pour les PME et ETI | Agence nationale de la sécurité des systèmes d'information

Notre avis sur le choix des logiciels de sécurité | Denis JACOPINI

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



Denis JACOPINI



SPAM : GARE AUX ARNAQUES !

LES PRINCIPALES ARNAQUES DU MOMENT

LCI

vous informe

Notre avis sur le choix des logiciels de sécurité



Réagissez à cet article

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 ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD) et à se protéger des pirates informatiques.**

Quel sont nos principales activités ?

- **RGPD**
 - FORMATION AU RGPD
 - FORMATION DE DPO
 - AUDITS RGPD

- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
 - FORMATIONS / SENSIBILISATION D'UTILISATEURS
 - RECHERCHE DE PREUVES

- **EXPERTISES**
 - EXPERTISES PRIVÉES
 - EXPERTISES DE VOTES ÉLECTRONIQUES
 - EXPERTISES JUDICIAIRES
 - RECHERCHE DE PREUVES
 - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique 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).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme. Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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



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



[Contactez-nous](#)



1.

http://assiste.com.free.fr/p/abc/a/pirates_informatiques.html

2.

<http://www.imprimer-dematerialiser.fr/la-cybercriminalite-2015-en-8-chiffres>

Cybercriminalité, prenez les devants pour vous protéger !

| Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Cybercriminalité, prenez les devants pour vous protéger !				

Depuis le début de l'année, nous constatons une nouvelle vague de cybercriminalité ciblant les TPE PME. Ces attaques de type « rançongiciel » s'appuient essentiellement sur le programme malveillant CTB-Locker. Que faire si cela vous arrive ? Wooxo vous livre quelques conseils pour se prémunir de telles attaques...Que faire en cas de survenance d'une telle attaque ?

Si vous ou l'un de vos clients fait l'objet d'une telle attaque, nous recommandons de déconnecter immédiatement du réseau et d'éteindre les machines identifiées comme compromises.

L'objectif est de bloquer la poursuite du chiffrement et la destruction des documents partagés.

Recherchez et supprimez tous les messages similaires dans les boîtes de messagerie des utilisateurs et procéder à une réinstallation complète du poste et la restauration d'une sauvegarde réputée saine des données de l'utilisateur ou du serveur.

Que faire pour se prémunir ?

Les anti-virus sont de moins en moins efficaces pour contrer ces attaques devenues très sophistiquées. Ils vous informeront que votre poste est infecté mais il sera trop tard.

A titre préventif, nous recommandons d'effectuer des sauvegardes saines et fréquentes des systèmes et des données (postes de travail, serveurs mais aussi ordinateurs portables itinérants), de vérifier qu'elles se sont correctement déroulées et de conserver un minimum de 3 versions pour chaque document sauvegardé.

Les sauvegardes doivent impérativement être stockées sur des supports de données isolés du réseau et des serveurs d'exploitation.

Réagissez à cet article

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)

Tous les combien doit-on changer son mot de passe ? | Denis JACOPINI

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



Denis JACOPINI



Tous les combien
doit-on changer
son mot de passe
?

Est-il vraiment utile de changer un mot de passe très régulièrement, comme le demandent de nombreuses entreprises ou conditions d'utilisations de certains services en ligne ? Ne vaut-il pas mieux se concentrer sur un bon code, suffisamment long ?

Dans le guide « Recommandations de sécurité relatives aux mots de passe », l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) conseille :

« Les mots de passe doivent avoir une date de validité maximale. A partir de cette date l'utilisateur ne doit plus pouvoir s'authentifier sur le système si le mot de passe n'a pas été changé. Ceci permet de s'assurer qu'un mot de passe découvert par un utilisateur mal intentionné, ne sera pas utilisable indéfiniment dans le temps. »

En plus de conseiller de changer par un mot de passe complexe non lié à notre identité pour chaque service et chaque site Internet le mot de passe par défaut ou initialement communiqué, la durée de renouvellement de mot de passe recommandée dans ce guide est de 90 jours.

La CNIL recommande quant à elle :

« Le responsable de traitement veille à imposer un renouvellement du mot de passe selon une périodicité pertinente et raisonnable, qui dépend notamment de la complexité imposée du mot de passe, des données traitées et des risques auxquels il est exposé.»

Concrètement, tous les combien de temps devons nous changer de mot de passe.

En raison de la difficulté à retenir un nombre élevé de mots de passe complexes, il a été remarqué que si nous obligeons les utilisateurs à changer de mot de passe plusieurs fois par an, ces derniers finissent par employer des mots de passe plus faibles mais plus faciles à retenir. En effet, il a été constaté qu'imposer les utilisateurs de changer trop souvent de mot de passe complexe les amenait à choisir un mot de passe « proche » d'un choix précédent par exemple en incrémentant un chiffre en fin du mot de passe précédent (1, 2, 3, 4,...)

En attendant que les informaticiens imposent couramment aux utilisateurs l'identification à double facteur et des services de traçabilité pour l'ensemble des usages quotidiens et principalement ceux qui concernent des données dans le Cloud (messagerie électronique comprise), en attendant que soient répandues des mesures de sécurité améliorées rendant ainsi moins essentiel l'utilisation de mots de passe complexes et différents pour chaque service par l'usage de « tokens » sous forme de porte clés, cartes à puces, ou applications mobiles d'authentification, il me semble aujourd'hui prudent d'adapter la fréquence de renouvellement des mots de passe au contexte.

Ainsi, tout en vous conseillant de bien respecter l'utilisation de mots de passe complexes et différents pour chaque service et vous recommandant fortement que vos mots de passe « utilisateurs » ne soient connus de personne, pas même de votre informaticien parfois imprudent sans le savoir, je vous recommande de changer immédiatement de mot de passe lorsque :

- Vous constatez quelque chose d'anormal associé à votre compte ;
- Vous perdez ou lorsque vous est volé un appareil dans lequel ont été cochés l'enregistrement des mots de passe réseau ou dans les navigateurs ;
- Le fournisseur de service vous avertit s'être fait pirater son système informatique (encore faut-il qu'il l'ait équipé de sondes de détection d'intrusion et de détecteurs de fuites de données).

Pour faciliter l'usage de mots de passe différents et complexes, vous pouvez utiliser un gestionnaire de mots de passe, sorte de coffre-fort numérique dans lequel sont enfermés et fortement sécurisés les différents mots de passe longs et complexes auto-générés que vous n'aurez plus besoin de connaître. KeePass 2.0 est l'un de ces coffres-forts de mots de passe qui a obtenu la CSPN (Certification de Sécurité de Premier Niveau) de la part de l'ANSSI.

Réagissez à cet article

Est-il vraiment utile de changer un mot de passe très régulièrement, comme le demandent de nombreuses entreprises ou conditions d'utilisations de certains services en ligne ? Ne vaut-il pas mieux se concentrer sur un bon code, suffisamment long ?

Dans le guide « Recommandations de sécurité relatives aux mots de passe », l'ANSSI (Agence Nationale de la Sécurité des Système d'Information) conseille :

« Les mots de passe doivent avoir une date de validité maximale. A partir de cette date l'utilisateur ne doit plus pouvoir s'authentifier sur le système si le mot de passe n'a pas été changé. Ceci permet de s'assurer qu'un mot de passe découvert par un utilisateur mal intentionné, ne sera pas utilisable indéfiniment dans le temps. »

En plus de conseiller de changer par un mot de passe complexe non lié à notre identité pour chaque service et chaque site Internet le mot de passe par défaut ou initialement communiqué, la durée de renouvellement de mot de passe recommandée dans ce guide est de 90 jours.

La CNIL recommande quant à elle :

« Le responsable de traitement veille à imposer un renouvellement du mot de passe selon une périodicité pertinente et raisonnable, qui dépend notamment de la complexité imposée du mot de passe, des données traitées et des risques auxquels il est exposé.»

Concrètement, tous les combien de temps devons nous changer de mot de passe.

En raison de la difficulté à retenir un nombre élevé de mots de passe complexes, il été remarqué que si nous obligions les utilisateurs à changer de mot de passe plusieurs fois par an, ces derniers finissaient par employer des mots de passe plus faibles mais plus faciles à retenir. En effet, il a été constaté qu'imposer les utilisateurs de changer trop souvent de mot de passe complexe les amenait à choisir un mot de passe « proche » d'un choix précédent par exemple en incrémentant un chiffre en fin du mot de passe précédent (1, 2, 3, 4,...)

En attendant que les informaticiens imposent couramment aux utilisateurs l'identification à double facteur et des services de traçabilité pour l'ensemble des usages quotidiens et principalement ceux qui concernent des données dans le Cloud (messagerie électronique comprise), en patientant que soient répandues des mesures de sécurité améliorées rendant ainsi moins essentiel l'utilisation de mots de passe complexes et différents pour chaque service par l'usage de « tokens » sous forme de porte clés, cartes à puces, ou applications mobiles d'authentification, il me semble aujourd'hui prudent d'adapter la fréquence de renouvellement des mots de passe au contexte.

Ainsi, tout en vous conseillant de bien respecter l'utilisation de mots de passe complexes et différents pour chaque service et vous recommandant fortement que vos mots de passe « utilisateurs » ne soient connus de personne, pas même de votre informaticien parfois imprudent sans le savoir, je vous recommande de changer immédiatement de mot de passe lorsque :

- Vous constatez quelque chose d'anormal associé à votre compte ;
- Vous perdez ou lorsque vous est volé un appareil dans lequel ont été cochés l'enregistrement des mots de passe réseau ou dans les navigateurs ;
- Le fournisseur de service vous avertit s'être fait pirater son système informatique (encore faut-il qu'il l'ait équipé de sondes de détection d'intrusion et de détecteurs de fuites de données).

Pour faciliter l'usage de mots de passe différents et complexes, vous pouvez utiliser un gestionnaire de mots de passe, sorte de coffre-fort numérique dans lequel sont enfermés et fortement sécurisés les différents mots de passe longs et complexes auto-générés que vous n'aurez plus besoin de connaître. KeePass 2.0 est l'un de ces coffres-forts de mots de passe qui a obtenu la CSPN (Certification de Sécurité de Premier Niveau) de la part de l'ANSSI.

Réagissez à cet article

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)

Formation informatique cybercriminalité : Virus, arnaques et piratages informatiques, risques et solutions pour nos entreprises | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Formation informatique cybercriminalité : Virus, arnaques et piratages informatiques, risques et solutions pour nos entreprises				

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

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. Par exemple, les données les plus sensibles (fichiers clients, contrats, projets en cours...) peuvent être dérobées par des attaquants informatiques ou récupérées en cas de perte ou vol d'un ordiphone (smartphone), d'une tablette, d'un ordinateur portable. La sécurité informatique est aussi une priorité pour la bonne marche des systèmes industriels (création et fourniture d'électricité, distribution d'eau...). Une attaque informatique sur un système de commande industriel peut causer la perte de contrôle, l'arrêt ou la dégradation des installations.

Ces incidents s'accompagnent souvent de sévères répercussions en termes de sécurité, de pertes économiques et financières et de dégradation de l'image de l'entreprise.

Ces dangers peuvent néanmoins être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses et faciles à mettre en oeuvre dans l'entreprise.

Suivez cette formation :

- **si vous êtes chefs d'entreprises, responsables d'agences, président d'associations, que vous soyez indépendant ;**
- **si vous souhaitez sensibiliser vos salariés, seul maillon faible sur lequel votre service informatique (probablement peu pédagogue) ne peut rien faire ;**
- **si vous souhaitez mettre en place une charte informatique et vous souhaitez qu'elle soit mieux comprise et mieux acceptée par vos salariés ;**
- **si vous souhaitez vous mettre en conformité avec la CNIL, cette formation est le premier pas vers une compréhension des risques informatiques.**

Plus d'information sur les formations que nous proposons :

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

Réagissez à cet article

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 ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

Quel sont nos principales activités ?

▪ **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS
- RECHERCHE DE PREUVES

▪ **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique 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).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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



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



[Contactez-nous](#)



Escroqueries aux Faux Ordres de Virements Internationaux (FOVI)

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





Escroqueries aux Faux Ordres de Virements Internationaux (FOVI)

La Direction Zonale de la Sécurité Intérieure à Bordeaux vous informe d'une évolution dans le mode opératoire pour les Faux Ordres de Virements Internationaux (FOVI).

Les escroqueries aux Faux Ordres de Virements Internationaux ont représenté un préjudice estimé à 550 millions d'euros depuis leur apparition début 2010. A ce jour, trois modes opératoires existent : le faux président, la prise à distance du poste de travail et le changement de relevé d'identité bancaire (RIB).

Depuis septembre 2016, il a été observé un changement de mode opératoire relatif au changement de RIB.

Pour rappel, ce mode opératoire est utilisé dans le cadre du paiement d'un loyer ou d'une facture en instance dans la société ciblée. Dans ces deux cas, un individu se présente comme un responsable du fournisseur et contacte par téléphone, puis par mail, le service comptabilité de l'entreprise ciblée en l'informant d'un changement de domiciliation bancaire.

Afin de rassurer l'entreprise ciblée et de transmettre les nouvelles coordonnées bancaires, les escrocs utilisent désormais le site Internet LA POSTE pour créer un compte leur permettant d'utiliser le service payant de la lettre recommandée en ligne. Créé sous une fausse identité, ce compte leur permet de régler des envois postaux et ainsi de faire parvenir à l'entreprise ciblée un courrier matérialisé, distribué par LA POSTE et remis en main propre au destinataire, contenant les coordonnées bancaires gérées par les escrocs.

Face à cette nouvelle menace, une vigilance accrue est de mise. Nous vous encourageons à diffuser ce message auprès des personnes concernées de votre société.

Flash Ingérence n°22 (mars 2016) relatif aux Faux Ordres de Virements Internationaux (FOVI)

...[lire la suite]

Réagissez à cet article

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, twitter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à se mettre en conformité avec la réglementation numérique (dont le RGPD) et à se protéger des pirates informatiques.

Quel sont nos principales activités ?

- **RGPD**

- FORMATION AU RGPD

- FORMATION DE DPO

- AUDITS RGPD

- MISE EN CONFORMITÉ RGPD

- ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES

- EXPERTISES DE VOTES ÉLECTRONIQUES

- EXPERTISES JUDICIAIRES

- RECHERCHE DE PREUVES

- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique 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).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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



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

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

Contactez-nous



Original de l'article mis en page : Alerte #Cybersécurité :
Escroquerie aux Faux Ordres de Virements Internationaux (FOVI)
| Pôle Numérique CCI Bordeaux Gironde

Est-ce utile de former les salariés à la sécurité informatique ? | Denis JACOPINI

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



Est-ce utile de
former les salariés à
la sécurité
informatique ?

L'avènement du big data et de la mobilité modifient en profondeur l'utilisation des outils informatiques. Le chef d'entreprise doit donc adapter ses méthodes de management, pour éviter les débordements.

Le bon usage des outils est aujourd'hui un sujet de grande importance au sein des entreprises. Si bien que les dirigeants doivent adapter leurs techniques managériales.

Une simple clé USB branchée sur son ordinateur de bureau ou une pièce jointe malveillante ouverte sans précaution peuvent s'avérer catastrophiques pour les entreprises. Au travail, l'usage des outils informatiques doit être encadré. Au dirigeant de prendre ses responsabilités et d'expliquer à ses employés que l'on n'utilise pas un ordinateur au travail comme on le ferait à la maison. Une règle primordiale pour s'assurer du bon fonctionnement et de la sécurité des données de l'entreprise.

Responsabiliser les employés

« Au-delà de la formation des salariés, je préfère la notion de responsabilisation, nuance Philippe Soullier, dirigeant chez Valtus. Il y a un degré de confiance à donner. Chez nous par exemple, je ne vois aucun souci à ce qu'un employé consulte son mail personnel ou son compte Facebook. C'est un fait, nous sommes dans une époque où se développe une certaine confusion entre le temps de travail et la vie personnelle. Mais à partir du moment où le travail est correctement effectué, je n'y vois pas d'inconvénient. »

Les salariés disposent d'un certain degré de liberté, mais des limites sont fixées. « Sur la navigation, nous fermons évidemment l'accès à certains sites internet. Nos services informatiques bloquent par exemple la consultation des sites à caractère pornographique ». Outre cet exemple évident, la confiance joue à plein. « Nous disons aux salariés: 'c'est votre outil de travail, prenez-en soin !' », assure Philippe Soullier. Une stratégie managériale confortée par le fait que les salariés ne sortent pas de l'école: « Ils ne sont pas forcément technophiles et prennent moins de risques avec leurs outils professionnels que la 'génération Facebook' », admet Philippe Soullier.

Inciter à la prudence

Du côté de l'Anssi, l'Agence nationale de sécurité informatique, on aimerait voir se développer des « chartes de bonne conduite » dans les petites structures. « Ce travail commence par le haut de la chaîne. Les dirigeants doivent se montrer eux-mêmes irréprochables, sinon le message ne passe pas. Un dirigeant doit accepter de s'entendre dire non par un administrateur, précise Vincent Strubel, sous-directeur expertise au sein de l'agence. Il faut rester simple, pragmatique. On explique par exemple que l'on ne doit pas importer sa musique ou ses photos sur l'ordinateur de travail, que l'on ne réutilise pas constamment les mêmes mots de passe et qu'il ne faut surtout pas cliquer sur un lien quelque peu douteux. » Attention aussi aux connexions wifi dans les cafés lorsque la mobilité est de mise dans l'entreprise. « Il faut faire preuve de prudence dans toutes les situations », insiste-t-il.

La question du bon usage des outils informatiques est intimement liée aux enjeux de sécurité. Toujours chez Valtus: « Nos employés travaillent avec des entreprises. Ils reviennent chez nous en possession de données potentiellement sensibles. Ils doivent absolument comprendre que ce n'est pas parce que l'on peut en discuter au bureau que nos échanges ont un caractère public », raconte Philippe Soullier.

L'utilisation des adresses e-mail personnelles, le contenu même des messages doivent donc être maniés avec vigilance. Une précaution appuyée par Jan Villeminot, employé au service informatique de l'entreprise Intersec: « Les pirates informatiques savent parfaitement que la première faille d'une entreprise, c'est l'humain ».

Réagissez à cet article

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 ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

Quel sont nos principales activités ?

▪ **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique 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).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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



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



[Contactez-nous](#)



Source

http://www.lexpress.fr/high-tech/securite-informatique-dirigeants-formez-vos-salaries_1660968.html

Contacter Interpol en cas d'arnaque ... est une arnaque | Denis JACOPINI

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



Denis JACOPINI



vous informe

Contacter Interpol en cas d'arnaque ... est une arnaque

L'e-mail se présente d'abord comme un témoignage de victime s'étant faite arnaquer par un escroc. Cette dernière vous communique ensuite les coordonnées du contact chez Interpol présenté comme son sauveur.

Nous venons ce matin de recevoir un e-mail intitulé : « **Je suis victime d'une arnaque de rencontre et une personne ayant venu a mon aide suivez mon témoignage** » .

Au travers d'un long message, la victime explique s'être faite arnaquer de plusieurs dizaines de milliers d'euros par un personnage indélicat lui ayant fait croire à l'amour inespéré. Accroc à l'être aimé, la victime déclare l'avoir aidé financièrement à plusieurs reprises.

Une fois le pot aux roses découvert, malgré qu'il fut trop tard pour que la victime puisse récupérer son argent, elle réussit tout de même l'exploit de se sortir de ce piège grâce à un Inspecteur général sauveur

Plein de bonne volonté, la victime souhaite même vous faire partager son tuyau en partageant avec vous les coordonnées de ce contact chez Interpol.

Une fois de plus, il s'agit d'une arnaque visant aussi à vous réclamer de l'argent pour récupérer votre argent !!!

N'utilisez pas les coordonnées de ces « arnaceurs »

Le message :

je me nomme Gagne antoinette, suivez mon témoignage. Je suis Franco-Américaine résidant en France et je me suis faite arnaquer par une personne que j'ai rencontrée sur un site de rencontres (Meetic). Nous avons parlé par skype pendant quelques mois, il montrait sa photo (très bel homme) mais a dit qu'il ne savait pas comment faire fonctionner une webcam, je n'ai donc jamais vu son vrai visage. Il se prétendait Italien d'origine vivant en Alsace. Avocat de formation, il a quitté son pays suite à un divorce et mésentente avec sa famille. Et paraît-il beaucoup qu'il a beaucoup d'euros dans un compte en Suisse, il m'a même envoyé un site de la banque avec son numéro de compte et un mot de passe afin que je vois ses comptes. Il m'a dit de détruire le mot de passe par la suite. Après plus d'un mois de conversation soutenue pendant lesquelles il parlait d'amour, il a dit partir pour l'Afrique pour acheter de l'or, en Côte d'Ivoire plus précisément. Rendu en Afrique il m'a contactée pour me dire que tout allait mal et qu'il s'était fait confisquer son passeport. Il avait besoin d'argent pour payer une taxe sur les produits qu'il a achetés. Il m'a demandé de lui porter un coup de main et je me que j'ai fait sans arrière pensée par envois successifs par western union pour payer différentes choses. Je les lui ai fait parvenir par Western Union une somme de 75.000€ car j'ai été idiote, j'ai vraiment cru en son histoire. Ensuite il a dit être malade dans un hôpital à Abidjan en Côte d'Ivoire et ne pas avoir d'assurance pour la chirurgie. Il me demandait encore plus de dollars. Il m'a envoyé une facture de la clinique (fausse bien sûr) par internet. Ensuite, comme ces gens avaient mon numéro de téléphone, ils ont commencé à me harceler pour me faire payer disant qu'il allait mourir si je ne payais pas plus. J'ai senti l'arnaque et je lui ai dit que c'est de l'arnaque. Il m'a appelé jusqu'à 10 fois la même nuit pour pleurer au téléphone me disant qu'il était amoureux de moi et qu'il ne pouvait pas croire que je le traitais ainsi, lui qui croyait en Dieu, comment pouvais-je le traiter d'escroc sans scrupules. Les appels continuaient jour et nuit, tantôt d'un soit disant médecin, Philipps duchez, une autre fois d'une personne de la banque etc... C'est alors que j'ai téléphoné à l'interpol de France Lyon pour faire une plainte. mais heureusement j'ai expliqué ce problème tous le problème a interpol du Lyon qui ma fait prendre contact avec un Inspecteur General de police Interpol du nom de Leroux Richard qui depuis l'Afrique qui coordonnais des actions avec l'interpol de la France Lyon et le regroupement du CDEAO pour un remboursement immédiat. Et grâce à lui et Dieu on ma remboursé la totalité de mes 75.000€ qu'on m'avait arnaquer environ y suivi des frais de dedommagements, J'ai bien eu de la chance car j'ai échappée belle a cette crise. À partir de ce instant j'ai dès lors reprise confiance en moi et ne cherche plus d'embrouille sur les sites de rencontre parce qu'il n'y a pas de vérité en tout ça.

Alors si vous avez été arnaqué sur la toile d'une : grosse somme d'argent, d'achats non conformes à la photo, de virement bancaire, de chantage sur le net, de faux maraboutage et faux compte, paypal, de fausses histoire d'amour pour soutirer de l'argent, de vente de voiture, de gay et lesbienne et de faux tirage a la loterie etc...., si vous le contacté, il trouvera facilement vos escroc et une fois qu'ils seront arrêtés grace a leur systeme WALO WALO car j'ai suivi vraiment leurs instructions et sa a marché pour moi. Je remercie beaucoup L'inspecteur de police Leroux Richard sans lui je serais sans doute à la rue car j'avais épuisée toutes mes économies pour ses voleurs. Pour tous ceux ou celles qui ont été dans le même cas comme moi voici l'adresse email de L'inspecteur de police Leroux Richard.

Emails : celluleinterpolmondial@rocketmail.com / policeinterpolmondial@live.fr

Cordialement a vous

Réagissez à cet article

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 : Denis JACOPINI