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



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

[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"]

# Conservez une preuve en vue d'une plainte à la CNIL



Lorsque vous adressez une plainte en ligne à la CNIL, vous devez obligatoirement joindre une copie de vos démarches préalables auprès du site / responsable du fichier. Lorsque ces démarches s'effectuent depuis un site internet ou par sms, voici comment réaliser une « capture d'écran » selon le terminal que vous utilisez.

### Réaliser une capture d'écran depuis un ordinateur Depuis un PC

Réalisez une capture d'écran à l'aide de la touche « impr écran » en haut à droit de votre clavier (PC). Puis ouvrez un document (traitement de texte, paint ou courrier électronique) pour coller cette copie d'écran puis l'enregistrer.

#### Depuis un Mac

Pressez simultanément les touches Cmd + MAJUSCULE + 4. Ouvrez un document word, ou un courrier électronique pour le coller votre copie d'écran dans le corps de votre document ou de votre message, puis « enregistrer ».



Outre les outils et logiciels mis à disposition sur votre ordinateur, il existe des extensions gratuites (Screengrab, PageSaver...) à installer directement sur votre navigateur. Correctement paramétrées, celles-ci permettent de dater automatiquement une copie d'écran (page complète, visible ou sélection).

#### Cas d'utilisation :

un site internet dispose de deux mois pour répondre à votre demande d'opposition. Passé ce délai, vous pouvez solliciter la CNIL via une plainte en ligne. Il vous sera notamment demandé une capture d'écran justifiant votre démarche effectuée il y a plus de deux mois.

## Réaliser une capture d'écran sur Smartphone ou tablette

#### A partir d'un terminal Android

Appuyez simultanément sur le bouton Marche/Veille et sur « Volume bas ». Maintenez ces boutons enfoncés jusqu'à ce que vous soyez notifié par un son ou une petite animation.



#### A partir d'un terminal Apple (iPhone ou iPad)

Appuyer simultanément et de manière brève sur le bouton « Menu » (ou bouton Home au milieu de l'iPhone) et le bouton « Verrouillage » (ou bouton Power au dessus de l'iPhone).



#### A partir d'un terminal Windows Phone

Appuyez simultanément sur les boutons « Marche /veille » et « Volume + » pour prendre une photo de votre écran.

#### A partir d'un smartphone Samsung



Pressez en même temps sur le bouton « Home » et le bouton « Power » puis maintenez ces boutons enfoncés jusqu'à la capture d'écran

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité,

certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.









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

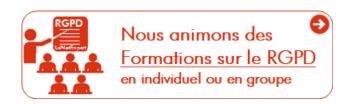
Contactez-nous

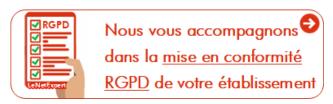
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une expérience d'une dizaine d'années dans la mise en conformité avec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

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

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

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





#### Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

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

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

Comment devenir DPO Délégué à la Protection des Données

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

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur

la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

Original de l'article mis en page : Conservez une preuve en vue d'une plainte à la CNIL | CNIL

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



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 ».

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

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

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

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

Source :

http://www.lexpress.fr/high-tech/securite-informatique-dirigea nts-formez-vos-salaries\_1660968.html

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





### Contacter Interpol en d'arnaque … une arnaque

casest

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 « arnacoeurs »

#### Le message :

je me nomme Gagne antoinette, suivez mon témoignage. Je suis Franco-Americaine residant en france et je me suis faire 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 parait-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 cote 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 se que j'ai fait sans arrière pensé 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 payait 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 probleme 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 çà.

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 touts 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

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

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



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

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

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

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances

similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître ! Commandez sur Fnac.fr https://www.youtube.com/watch?v=lDw3kI7ra2s

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

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj\_HKcbzRuvIPdu3FktA

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

Commandez sur Fnac.fr

Source : Denis JACOPINI

## 16% des entreprises victimes

# des Ransomwares. Réagissez!



Les ransomwares visent de plus en plus les entreprises françaises. Ce phénomène n'est pas près de s'arrêter au regard du business model très lucratif et de l'impunité juridique dont bénéficient les hackers.

Force est de constater que les hacker un plus d'un coup d'avance.

En effet, PC Cyborg, le premier Ransomware, date tout de même de 1989. Pourtant, depuis le temps, le phénomène n'ayant pas été pris au sérieux, il commence désormais à prendre une ampleur phénoménale.

Il est évident qu'aujourd'hui aussi bien les entreprises que les états sont dépassés par ce phénomène. La liste des entreprises, parfois des OIV (Opérateurs d'importance Vitale) ou des OSE (Opérateur de Services Essentiels) ou des services publics touchés ne cesse de s'alourdir.

#### Que nous annonce le futur ?

Nos télévisions prises en otage par un ransomware (crypto virus ou programme informatique qui rend illisible vos données et inversera l'opération contre paiement d'une rançon, d'où le nom de crypto virus) pourrait bien arriver dans nos foyés dans les prochains mois. Notre auto, notre téléphone et bientôt nos maisons (serrures, lumières, fours, réfrigérateurs… n'importe quel objet connecté essentiel en définitive) pourraient bien nous demander un petit bitcoin en échange de son refonctionnement.

#### Que pouvons nous faire ?

Les entreprises doivent évoluer selon plusieurs axes :

- Reconsidérer la priorité consacrée à la sécurité informatique pour faire évoluer son infrastructure technique, organisationnelle, reconsidérer les conséquences en terme d'image ou de pérennité que pourraient entraîner une attaque informatique.
- Reconsidérer le personnel en charge du service informatique et former le responsable informatique à la sécurité ou mieux (ce que je recommande), utiliser les services d'un expert en cybersécurité ou en cybercriminalité en appui du service informatique.
- Responsabiliser les utilisateurs par une charte informatique complétée et présentée lors des cessions de sensibilisation.
- Sensibiliser (et former pour certains) les utilisateurs aux différents risques liés aux usages informatiques en partant des ransomwares, jusqu'aux différentes formes d'arnaques aux victimes dépouillées de plusieurs dizaines, centaines milliers d'euros voire des millions d'euros.

#### Et au niveau international ?

Il est évident que la tâche sera longue et fastidieuse mais il est à mon avis possible de combattre le phénomène en agissant sur plusieurs leviers.

Le voler législatif doit évoluer et s'adapter aux attaques informatiques internationales pour que les coopérations internationales puissent se passer sans délai.

Le volet coordination doit être couvert par une entité internationale qui pourrait devenir un point de contact aussi bien pour les autorités collectant les plaintes de victimes, pour les organismes faisant évoluer les instruments judiciaires, pour les éditeurs et constructeurs d'outils exposés au menaces.

[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 : Denis JACOPINI

Denis JACOPINI sur Sud Radio présente son livre « CYBERARNAQUES : S'informer pour mieux se protéger » et répond aux questions de Patrick ROGER



DENIS JACOPINI - MARIE NOCENTI

# GYBER ARNAQUES S'INFORMER POUR MIEUX SE PROTÉGER

Denis JACOPINI
sur Sud Radio
présente son
livre
« CYBERARNAQUES
: S'informer
pour mieux se
protéger » et
répond aux
questions de
Patrick ROGER

PLON

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

DENIS JACOPINI - MARIE NOCENTI

# **GYBER ARNAQUES**S'INFORMER POUR MIEUX SE PROTÉGER

PLON

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.

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



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

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

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

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances

similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître ! Commandez sur Fnac.fr https://www.youtube.com/watch?v=lDw3kI7ra2s

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

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj\_HKcbzRuvIPdu3FktA

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

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



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

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

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

#### Commandez sur Fnac.fr

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

# Si un courriel personnel n'est pas identifié comme tel, l'employeur peut-il l'examiner?



Si un courriel personnel n'est pas identifié comme tel, l'employeur peut-il l'examiner ?

Si le courriel n'est pas intitulé «Personnel», mais, par exemple, «félicitations pour la naissance de…» Il est évident que c'est personnel.

[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 : Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? — La Voix du Nord

# Une mairie peut-elle demander le numéro de sécurité sociale (NIR) des enfants en école primaire ? | Denis JACOPINI



Pour les inscriptions scolaires des enfants en école primaire (maternelle et élémentaire), les communes peuvent demander les informations suivantes :identité de l'enfant en âge scolaire :

- nom, prénoms, sexe, date et lieu de naissance, adresse ;identité et adresse du responsable légal ;
- profession du responsable légal ;
- classe de l'élève ;
- école fréquentée, s'il s'agit d'un établissement public,
- et date d'entrée dans cette école.

Les communes ne doivent pas enregistrer le numéro de sécurité sociale ni l'utiliser comme identifiant de l'élève.

Elles ne sont pas autorisées non plus à demander la copie de l'attestation de sécurité sociale.

En effet, cette information n'est d'aucune utilité pour les communes.Cette donnée ne peut pas non plus être collectée par l'école ou les instituteurs.

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.



DÉSIGNATION N° DPO-15945





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

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de mise en conformité avec le RGPD.

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

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





#### Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

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

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

Comment devenir DPO Délégué à la Protection des Données

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

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

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

Source :

http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=2 3EEA0184FD81E5B5D9C191EA44B1EBD?name=Num%C3%A9ro+de+s%C3%A9curit%C3%A9+sociale+(NIR)+des+enfants+en+%C3%A9cole+primaire+%3A+une+mairie+peut-elle+le+demander+%3F&id=173

# La cybercriminalité, un vrai risque pour les administrations | Denis JACOPINI



Alors que le numérique fait désormais partie intégrante de nos vies personnelles et professionnelles, la sécurité est trop rarement prise en compte dans nos usages.

Les nouvelles technologies, omniprésentes, sont pourtant porteuses de nouveaux risques pesant lourdement sur les collectivités.

Par exemple, les données les plus sensibles (fichiers administrés ou membres, 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 informatiques. Une attaque informatique sur un système 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 se service et de l'image de la victime.

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

[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 : Denis JACOPINI

# Vol de données : cinq conseils pour se protéger contre les intrusions | Denis JACOPINI



Ransomware, chevaux de Troie et logiciels malveillants : les entreprises ne sont guère à l'abri des attaques de pirates qui représentent un grand risque pour leur sécurité. Mais contrairement aux idées préconçues, les menaces ne proviennent pas uniquement de l'extérieur. Les employés de l'entreprise peuvent ainsi mettre à profit les nombreuses possibilités qu'ils ont d'accéder aux systèmes de l'entreprise pour une utilisation frauduleuse des données, et cela sans beaucoup d'effort. Les organisations sont d'ailleurs rarement aussi bien protégées des attaques venant de l'interne que de celles extérieures.

Les cinq recommandations suivantes peuvent aider les entreprises à se protéger efficacement contre le vol de données par des employés.

1. Octroyer des droits d'accès différents
Pour protéger les données sensibles, il est nécessaire de donner aux employés travaillant dans différents départements des droits d'accès appropriés. Ainsi, le niveau de securité est determiné par le besoin de connaissances d'un projet : un employé n'a accès à certains documents et dossiers que si ceux-ci sont nécessaires pour effectuer une tâche qui tombe sous sa responsabilité. Ces divers cloisonnements mis en place au sein de l'entreprise sous la forme de « murailles de Chine » empêchent l'échange d'informations non nécessaire entre les différents départements, permettant de limiter la perte de données.

#### 2. Utiliser une double authentification forte

Afin de limiter tout risque, l'étape supplémentaire recommandée est une authentification à deux facteurs. Pour accéder au système, l'utilisateur doit, par exemple, non seulement entrer son mot de passe, mais aussi recevoir un SMS contenant un mot de passe unique, valable pour une seule session. Ainsi, il n'est pas possible d'accéder à l'information et aux données sensibles, même si le mot de passe a été volé.

#### 3. Durcir la protection des informations

Les fonctionnalités en terme de sécurité doivent inclure la protection des données. Le fournisseur ne devrait en aucun cas avoir accès aux fichiers et documents, par exemple. En outre, les droits des administrateurs doivent être limités aux informations pertinentes à leurs activités.

#### 4. Mettre en œuvre une gestion des droits d'information

Les technologies de gestion des droits d'information des documents sensibles peuvent contrôler et protéger contre le téléchargement non autorisé. Celles-ci assurent un contrôle efficace des documents même si les utilisateurs sont autorisés à accéder à l'information. Le filigrane empêche, en outre, une capture d'écran des informations. Il n'y a aucun risque de perte de données dans cet environnement protégé et elles ne tombent pas entre de mauvaises mains.

#### 5. Enregistrer toute modification

Pour éviter le vol de données par un employé de l'entreprise et de s'en rendre compte après coup, il est conseillé d'enregistrer tous les changements effectués afin que ceux-ci soient répertoriés dans un historique. Cela permet un flux d'informations toujours clair et transparent.

Sofia Rufin, Vice Présidente Régionale de Brainloop, commente la menace croissante que représentent les employés de l'entreprise dans le cadre de vols de données : « Nous avons observé au cours des dernières années, une augmentation du nombre des pertes de données dues à des failles en interne, les entreprises faisant encore trop souvent confiance à des standards de sécurité déficients. L'impact peut pourtant s'avérer désastreux sur l'image de l'entreprise, et les conséquences financières et légales peuvent menacer son développement économique… [Lire la suite]

[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 : Vol de données : cing conseils pour se protéger contre les intrusions — Global Security Mag Online