L’ABC des bonnes pratiques pour se protéger des Cyberattaques | Denis JACOPINI

Pour se prémunir des cyberattaques, la meilleure solution consiste à mettre en place quelques bonnes pratiques de base.

Encourager une gestion rigoureuse des mots de passe
Mettez en place des outils qui forcent les utilisateurs à choisir des mots de passe forts. Ceux-ci comprennent au moins huit caractères, des majuscules et des minuscules, des chiffres et des symboles du clavier (!, @, $, etc.), mais aucun mot entier. Ils doivent aussi être changés régulièrement, même si ça cause de la grogne.

Sensibiliser les employés
Souvent considérés comme la porte d'entrée des cybercriminels, les employés doivent être formés, par exemple au moyen de modules d'apprentissage vidéo, sur les risques d'attaques possibles et les différentes formes qu'elles peuvent prendre.

Effectuer régulièrement des tests
Une façon de vérifier si les campagnes de sensibilisation auprès des employés fonctionnent consiste à les tester en simulant, par exemple, l'envoi d'un courriel frauduleux. N'oubliez pas de l'envoyer aussi – et même surtout – à ceux qui occupent des postes stratégiques.

Limiter l'accès à l'information confidentielle
Ne donnez accès aux renseignements confidentiels qu'à ceux qui en ont réellement besoin dans l'entreprise.

Contrôler les processus de sécurité
Rien ne sert d'avoir des systèmes informatiques à la fine pointe si on ne les teste pas régulièrement. Il vaut mieux impartir la tâche à des experts si on ne possède pas les ressources nécessaires à l'interne. Les fournisseurs de solutions infonuagiques disposent d'une infrastructure de sécurité informatique qui peut bien souvent dépasser celle des entreprises.

Installer les mises à jour logicielles rapidement
Beaucoup d'attaques exploitent des vulnérabilités connues depuis plusieurs mois par les fournisseurs d'antivirus, qui d'ailleurs offrent déjà des correctifs pour les contrer. Prévoyez l'installation des mises à jour dans un délai optimal de 48 heures, ou d'au plus une semaine.

Source : https://www.lesaffaires.com/classements/les-500/cyberattaques-l-abc-des-bonnes-pratiques/579150

LeNetExpert a intégré la plateforme cybermalveillance.gouv.fr

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

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

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

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

LE NET EXPERT

:

• **SENSIBILISATION / FORMATIONS** :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• **MISE EN CONFORMITÉ RGPD / CNIL**

- **ÉTAT DES LIEUX RGPD** de vos traitements)
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Réagissez à cet article

Source : *Fiche rançongiciels (cryptolocker)*

Les emails et les sms comme moyens de preuve | Denis JACOPINI

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

Les emails et les sms comme moyens de preuve

Le courrier électronique vulgairement appelé « email » est devenu le moyen de communication le plus utilisé et par suite, le lieu de prédilection moderne pour les contenus illicites (propos racistes, photos à caractère pédophile, propos diffamatoires ou injurieux), l'instrument privilégié de fraudes informatiques au encore le moyen d'un manquement à des interdictions ou obligations (usage abusif de la messagerie électronique de l'entreprise) mais surtout le lieu où se trouve la preuve d'un grand nombre de faits ou actes juridiques (preuve de l'oublière, du consentement contractuel, des relations commerciales).
Depuis peu, la preuve par SMS a de plus en plus d'occasion à être employée en justice.
Ainsi, de manière très intéressante, le législateur et la jurisprudence ont fixé le contour de ces deux nouveaux moyens de preuve.

Nous envisagerons ci-après la situation dans laquelle une personne souhaiterait produire en justice un email ou un SMS qui a été reçu par un tiers et donc qui ne lui a pas été adressé personnellement.
En effet, la réception d'un email ou d'un SMS par cette personne lui permet de les produire en justice à condition de respecter le formalisme de constatation de ces moyens de preuve particuliers.

A cet égard, l'article 1316-1 du Code civil est clair :
« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».
Le fait qu'un courrier électronique puisse être utilisé comme mode de preuve ne fait dès lors pas de doute, à condition qu'il soit signé pour garantir l'intégrité de son contenu et l'identification de son auteur.

De plus, l'article 1316 du Code civil énonce :
« La preuve littérale, ou preuve écrit, résulte d'une suite de lettres, de caractères de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission ».

Si les principes du « secret des correspondances » et du respect à la vie privée interdisent la production en justice des emails et des SMS qui ne nous sont pas destinés (I), ce principe comporte cependant des exceptions légales et jurisprudentielles. (II)

I – Les principes du secret des correspondances et le respect de la vie privée comme limites à la preuve emails et SMS
Les juridictions veillent à ce que chaque partie administre la preuve dont elle a la charge de façon loyale.
Une jurisprudence constante considère la loyauté comme une condition d'admissibilité conditionnant la recevabilité de tout moyen de preuve (Cass. 3e civ., 15 janv. 1970).
Ainsi, les juges subordonnent, la recevabilité de la preuve au respect de règles ou principes tel que le respect de la vie privée ou le respect du secret des correspondances ou encore le respect des dispositions relatives aux données personnelles.
Le principe du secret appliqué à l'origine à la correspondance écrite s'est étendu à toute correspondance émise par la voie des télécommunications telle que les emails et les SMS.
L'article 1er de la loi n° 91-646 du 10 juillet 1991 dispose ainsi que :
« Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci ».

C'est une ordonnance de référé rendue par le Tribunal de grande instance de Paris le 27 janvier 2003 qui, pour la première fois, a consacré le principe du respect du secret des courriers électroniques (T. corr. Paris, 2 nov. 2000).
Ce principe a donc un caractère quasi absolu.

Ainsi, au civil, la preuve obtenue illicitement au moyen d'une violation du secret des correspondances est jugée irrecevable par les juges et peut être sanctionné pénalement le cas échéant.
Pour n'en convaincre, il suffit de constater le nombre important de dispositions légales sanctionnant la violation du secret de la correspondance.

L'article 226-15 du Code pénal dispose que :
« Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 € d'amende.
Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions ».

Par ailleurs, l'article323-1 alinéa 1er du Code pénal dispose que :
« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende ».
De plus de ces sanctions pénales, la victime d'une atteinte à la vie privée peut obtenir de son auteur des dommages et intérêts.

Outre la sanction pénale qui peut être lourde, une autre sanction est autrement plus lourde de conséquences pour l'auteur de la violation de correspondance : l'irrecevabilité de la preuve obtenue par violation du secret des correspondances. En effet, au civil, la preuve obtenue illicitement au moyen d'une violation du secret des correspondances est jugée irrecevable par les juges

II – Les tempéraments légaux et jurisprudentiels permettant la preuve en justice par emails ou SMS
Plus les années passent, plus les juges admettent la preuve par emails ou SMS.
Dans le cadre des procès pénaux, la chambre criminelle de la cour de cassation a jugé à plusieurs reprises que :
« aucune disposition légale ne permet aux juges répressifs d'écarter les moyens de preuve produits par les parties au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale, il leur appartient seulement d'en apprécier la valeur probante après les avoir soumis à la discussion contradictoire »
(Cass. crim., 13 oct. 2006).

Dans le cadre des procès en droit du travail, dans son célèbre arrêt Nikon, la chambre sociale de la cour de cassation a jugé que le respect de l'intimité de la vie privée du salarié interdit à l'employeur de prendre connaissance des emails personnels émis et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail (Cass. soc., 2 oct. 2001).

Le 17 mai 2005 la chambre sociale a limité ce principe général en jugeant que si « *l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé* », « *sauf risque ou événement particulier* »
(Cass. soc., 17 mai 2005).

La chambre sociale vient encore de préciser, dans un arrêt du 23 mai 2007 que :
« le respect de la vie personnelle du salarié ne constitue pas en lui-même un obstacle à l'application des dispositions de l'article 145 NCPC dès lors que le juge constate que les mesures qu'il ordonne procèdent d'un motif légitime et sont nécessaires à la protection des droits de la partie qui les a sollicités »
(Cass. soc., 23 mai 2007).

Par ailleurs, l'assistation jurisprudentielle de l'employeur au fournisseur de services Internet peut être intéressante car il pourra en résulter une obligation de conservation des données informatisées à la charge de l'employeur.

Ainsi, la Cour d'appel de Paris a jugé le 4 février 2005 que :
« en sa qualité non contractée de prestataire technique au sens de l'article 43-7 de la loi du 1er août 2000, la société BNP Paribas est tenue, en application de l'article 43-9 de ladite loi, d'une part, de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elle est prestataire et, d'autre part, à communiquer ces données sur réquisitions judiciaires »
(CA Paris, 14e ch., 4 fév. 2005).

Enfin, s'agissant des SMS un récent arrêt de la chambre sociale de la Cour de cassation vient de juger que l'utilisation d'un SMS comme mode de preuve est un procédé loyal recevable, par opposition à l'enregistrement d'une conversation téléphonique privée effectuée à l'insu de son auteur, car ce dernier ne peut ignorer que les messages sont enregistrés par l'appareil récepteur
(Cass. soc., 23 mai 2007).

Dans le cadre des procédures de divorce, la Cour de cassation a admis la preuve par emails en rejetant l'argument selon lequel la production de courriels constituerait une atteinte au secret des correspondances et à la vie privée dans la mesure où le conjoint s'en serait emparé sans le consentement de l'autre. Elle a donc exclu que les emails puissent constituer un mode de preuve illicite réalisant une ingérence disproportionnée dans la vie privée non justifiée par l'intérêt de l'époux demandeur au divorce
(Cass. 1ère civ., 18 mai 2005).

Ainsi, l'absence de remise volontaire des documents ne fait pas présumer la fraude.
Encore plus récemment, la 1ère chambre civile de la cour de cassation vient de censurer un arrêt d'appel en jugeant, le 13 juin 2000, que :
« en matière de divorce, la preuve ne fait par tous moyens ; [et dès lors] … le juge ne peut écarter des débats un élément de preuve que s'il a été obtenu par violence ou fraude »
(Civ. 1ère, 17 juin 2000).

Les micromessages adressés par téléphone portable sont donc admis comme moyen de preuve de l'adultère quand bien même la lecture a été faite à l'insu de son destinataire et que cela constitue une atteinte grave à l'intimité de la personne, sauf à constater qu'ils ont été obtenus par violence ou par fraude.
Ne constitue ni une violence, ni une fraude, le fait de lire, à l'insu de son conjoint, les messages de son téléphone portable.

A la lecture de cette décision l'éminent Professeur de droit Jean Hauser fait la remarque suivante :
« conjoints infidèles, mettez votre journal intime au coffre, brûlez vos correspondances, ne perdez pas vos portables, effacez vos messages et vos images dès que reçues, codez vos ordinateurs, des oreilles ennemis vous écoutent et les spams et virus conjugaux sont les pires ! »
(RTD. Civ 2000, p. 514)

Pour conclure, la Cour de cassation a ouvert la voie à ces nouveaux moyens de preuve et laisse une large marge de manœuvre pour la découverte d'une telle preuve.

III – La preuve par email ou SMS liaitée par leur fiabilité technique
Lorsque l'e-mail produit à titre de preuve n'est pas signé, ce qui est souvent le cas dans les litiges, la question de la fiabilité technique se pose avec le plus d'acuité. Il en est ainsi dans les affaires en droit de la famille, en droit du travail et en droit pénal.
La personne soupçonnée d'avoir envoyé le mail litigieux pourra invoquer plusieurs types de défense pour mettre en doute la fiabilité d'un courriel.
Elle pourra tout d'abord prouver qu'elle n'était pas présente à son poste informatique à l'heure d'envoi du mail, ce qui n'est pas tâche facile.
En cas d'impossibilité d'apporter cette preuve, la personne pourra démontrer que d'autres personnes (époux, secrétaire, administrateur de réseau, tiers) ayant accès à son mot de passe auraient pu se connecter à son poste informatique et envoyer l'e-mail litigieux à partir de ce poste.
Si un mot de passe avait été mis en place, la personne soupçonnée pourra invoquer le fait que l'usurpateur a forcé son mot de passe et s'est introduit dans son poste informatique.
En effet, Eric Charton, dans un ouvrage intitulé Hacker's guide indique qu'« absolument tous les mots de passe créés par des logiciels fonctionnant sous Windows mais aussi sur Mac et sur des ordinateurs sous Linux peuvent être décodés par un contre-logiciel de décryptage spécialisé : il suffit de le trouver sur Internet, et il est souvent gratuit » (éd. CampusPress, 2003, p. 175).

Face à la production par l'employeur d'un e-mail envoyé par un salarié, le salarié peut invoquer le fait qu'un tiers (un pirate, le pirate suspecté étant souvent l'employeur ou l'administrateur réseau) ait pu envoyer cet e-mail du poste informatique du salarié en s'introduisant sur ce poste dans le but de confondre ce dernier.
Ne nième, dans un procès en divorce, l'époux qui ne voit opposer un mail extrêmement les manquements aux devoirs conjugaux, qu'il aurait envoyé, peut tenter de contester être l'auteur du mail (CA Paris, 11 fév. 2004).
En effet, il existe divers moyens afin de faire tomber la preuve par email ou par SMS, de sorte qu'il convient de s'armer d'un avocat spécialisé en la matière pour ne pas courir de risque dans le cadre de la procédure judiciaire en produisant une preuve viciée.

Ainsi, il sera dans certains cas opportun de solliciter les services d'un avocat afin d'obtenir, avant toute action, une ordonnance sur requête délivrée par le Président du tribunal de grande instance compétent ainsi que la présence d'un huissier associé, le cas échéant, par un expert en informatique pour procéder à des investigations afin de garantir la recevabilité juridique de ces éléments de preuve.

Je suis à votre disposition pour toute information ou action.
Cordialement,
Anthony Bem
Avocat à la Cour
106 rue de Richelieu – 75002 Paris
Tel : 01 40 26 21 01
Email : abem@cabinetbem.com
www.cabinetbem.com

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.legavox.fr/blog/maitre-anthony-bem/emails-comme-moyens-preuve-1185.htm#.VJ5rPoCA
Par Maitre Anthony BEM

Arnaques par mail (scam, phishing) : quelles précautions prendre ? | Denis JACOPINI

Arnaques par mail (scam, phishing) : quelles précautions prendre ?

Voici quelques règles simples à respecter pour éviter de communiquer des informations à des groupes criminels :
Ne communiquez jamais d'informations importantes (numéro de carte bancaire, mot de passe, etc.) en cliquant sur un lien reçu par courrier électronique ;
• Ne répondez jamais aux messages suspects : une banque ne vous demandera jamais de lui communiquer vos coordonnées bancaires par simple courriel. Et il est peu probable qu'un inconnu vous propose réellement de bénéficiez d'un héritage ;
• Partez toujours de la page d'accueil d'un site pour accéder aux autres pages, notamment celles où sont demandés des identifiants ;
• Quand vous êtes sur un site sécurisé, comme un site bancaire, vérifiez que le cryptage des données est activé : l'adresse du site doit commencer par « https:// » (et non « http:// ») avec un petit cadenas affiché sur la gauche ou en bas de votre navigateur ;
En cas de doute, prenez contact directement avec l'entreprise ou l'administration concernée par téléphone.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=574A69F22079A57A47EC87CD5F71F73C?name=Arnaques+par+mail+%28scam%2C+phishing%29+%3A+quelles+pr%C3%A9cautions+prendre+%3F&id=192

A quoi s'applique la loi « Informatique et Libertés ? | Denis JACOPINI

A quoi s'applique la loi « Informatique et Libertés » ?

REMARQUE :
Le contenu de cette page date d'avant l'entrée en viguruer du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 appelé aussi RGPD (Règlement Général sur la Protection des Données). au 19/07/2020, la loi Informatique & Libertés est toutefois toujours en vigueur et a été modifiée depuis le 25/05/2018. Le contenu de ce document reste toutefois valable.

La loi « Informatique et Libertés » s'applique :

• Aux fichiers, systèmes, dispositifs informatisés ou non ;
• Comportant des informations concernant des personnes physiques (nom, adresse, photos, identifiants divers, etc.) ;
• Mis en oeuvre par une personne physique ou morale installée en France ou exerçant une activité professionnelle ou associative en France.

La loi « Informatique et Libertés » ne s'applique pas :
• Aux fichiers ne comportant que des informations sur des personnes morales (sociétés, associations, établissement public), sans mention de leurs dirigeants ou actionnaires, personnes physiques ;
• Aux fichiers créés par des particuliers pour leur usage privé (répertoire personnel, etc.).

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en cybercriminalité et en déclarations à la CNIL, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=6C2979337DD5240A1A085F73F327AD22?name=La+loi+%22Informatique+et+Libert%C3%A9s%22%2C+elle+s%27applique+%C3%A0+quoi+%3F&id=491

Les bons réflexes face à la cybercriminalité | Denis JACOPINI

Les bons réflexes face à la cybercriminalité

Dans certains pays, la cybercriminalité est devenue une économie comme une autre. Difficile de lutter quand le sentiment d'impunité n'existe presque pas.
Période de Noël oblige, les cybercriminels aussi font leurs courses. Leur cible préférée… c'est vous !
Attention aux arnaques téléphoniques
Ah, les nouvelles technologies ! Elles sont tellement formidables qu'on ne peut plus s'en passer. Pour téléphoner, s'informer, se diriger et aussi faire ses achats… Internet ? Le plus grand marché du monde ! Et, comme sur tous les marchés, il y a aussi des voleurs, des pickpockets, des bonimenteurs… qui n'ont de limites que celles de leur imagination. Et elle est fertile.

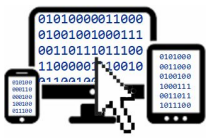
Les courriels. Les faux courriels grossiers, bourrés de fautes d'orthographe, censés émaner d'opérateurs institutionnels, font aujourd'hui figure de dinosaures. Mais ceux qui les ont remplacés poursuivent le même objectif : vous extorquer vos coordonnées personnelles et bancaires. A la mode en ce moment, les faux courriels terroristes qui font croire que les destinataires n'auront la vie sauve qu'en finançant leur cause.
Les logiciels. Dans le même ordre d'idée, les « rançongiciels » poursuivent le même but en bloquant purement et simplement votre ordinateur et réclament une rançon. Il ne faut, bien évidemment, jamais payer. Idem quand une fenêtre apparaît, indiquant que votre ordinateur est bloqué et que vous devez acquitter une amende, une clé de déchiffrement…
Les petites annonces. Qu'elles soient affichées gratuites comme dans le cas de dons d'animaux par exemple (méfiez-vous des frais d'envoi ou de douane), qu'il s'agisse d'annonces d'offres d'emploi (si on vous propose de réceptionner des colis, prudence) ou réservées aux particuliers, toutes les annonces sont susceptibles de n'être que miroir aux alouettes. Méfiez-vous systématiquement de tout paiement qui vous serait demandé via Western Union, Ukash, MoneyPak…

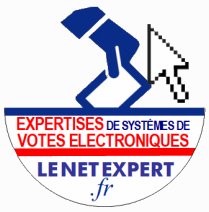
Six conseils pour éviter les pièges
1. Se méfier des offres trop alléchantes, prendre son temps et ne pas agir dans l'urgence.
2. Ne jamais envoyer ses coordonnées de cartes bancaires ou ses coupons de cartes prépayées par courriel.
3. Ne jamais expédier un colis avant que l'argent soit bien viré sur votre compte bancaire ou PayPal.
4. Être vigilant avec les demandes provenant de l'étranger quand on ne dispose que d'un contact par courriel.
5. Rechercher le courriel de son interlocuteur sur un moteur de recherche pour vérifier son identité.
6. En cas de publication d'une annonce, masquer les informations qui pourraient être utilisées pour usurper une identité.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lanouvellerepublique.fr/Loir-et-Cher/Actualite/Faits-divers-justice/n/Contenus/Articles/2014/12/24/Les-bons-reflexes-face-a-la-cybercriminalite-2164937

Comment détecter e-mail malveillant





Comment détecter e-mail malveillant

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

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

• **Est-ce que le message/courriel vous est réellement destiné ?**
1. Généralement, les messages malveillants sont envoyés à destination d'un grand nombre de cibles, ils ne sont pas ou peu personnalisés.
2. Le message évoque un dossier, une facture, un thème qui ne vous parle pas ? Il s'agit certainement d'un courriel malveillant.
• **Attention aux expéditeurs inconnus** : soyez particulièrement vigilants sur les courriels provenant d'une adresse électronique que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact.
• **Soyez attentif au niveau de langage du courriel** : même si cela s'avère de moins en moins vrai, certains courriels malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées, c'est qu'il n'est pas l'œuvre d'un organisme crédible (banque, administration …).
• **Vérifiez les liens dans le courriel** : avant de cliquer sur les éventuels liens, laissez votre souris dessus*. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime. Ne faites pas confiance aux noms de domaine du type impots.gouvv.fr, impots.gouvfr.biz, infocaf.org au lieu de www.caf.fr.* *A noter : cette manipulation est impossible à effectuer depuis un écran de smartphone.*
• **Méfiez vous des demandes étranges** : posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n'a le droit de vous demander votre code carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.
• **L'adresse de messagerie source n'est pas un critère fiable** : une adresse de messagerie provenant d'un ami, de votre entreprise, d'un collaborateur peut facilement être usurpée. Seule une investigation poussée permet de confirmer ou non la source d'un courrier électronique. Si ce message semble provenir d'un ami – par exemple pour récupérer l'accès à son compte – contactez-le sur un autre canal pour vous assurer qu'il s'agit bien de lui !

Comment réagir ?

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

Comment s'en prémunir ?

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

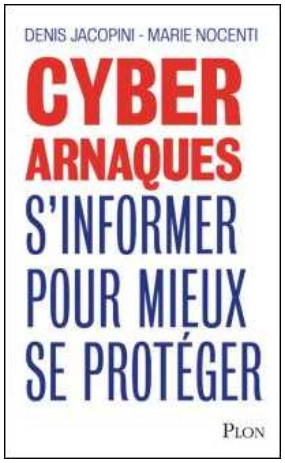
Si vous êtes victime d'une escroquerie en ligne ?

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

Rendez-vous sur cybermalveillance.gouv.fr , la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance. Que vous soyez un particulier, une entreprise ou une administration, retrouvez :
• des conseils / vidéos pour sensibiliser votre entourage professionnel ou personnel,
• des services de proximité en cas de dommages causés par une attaque informatique.
…[lire la suite]

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

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



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les 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 Milions de victimes de la 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

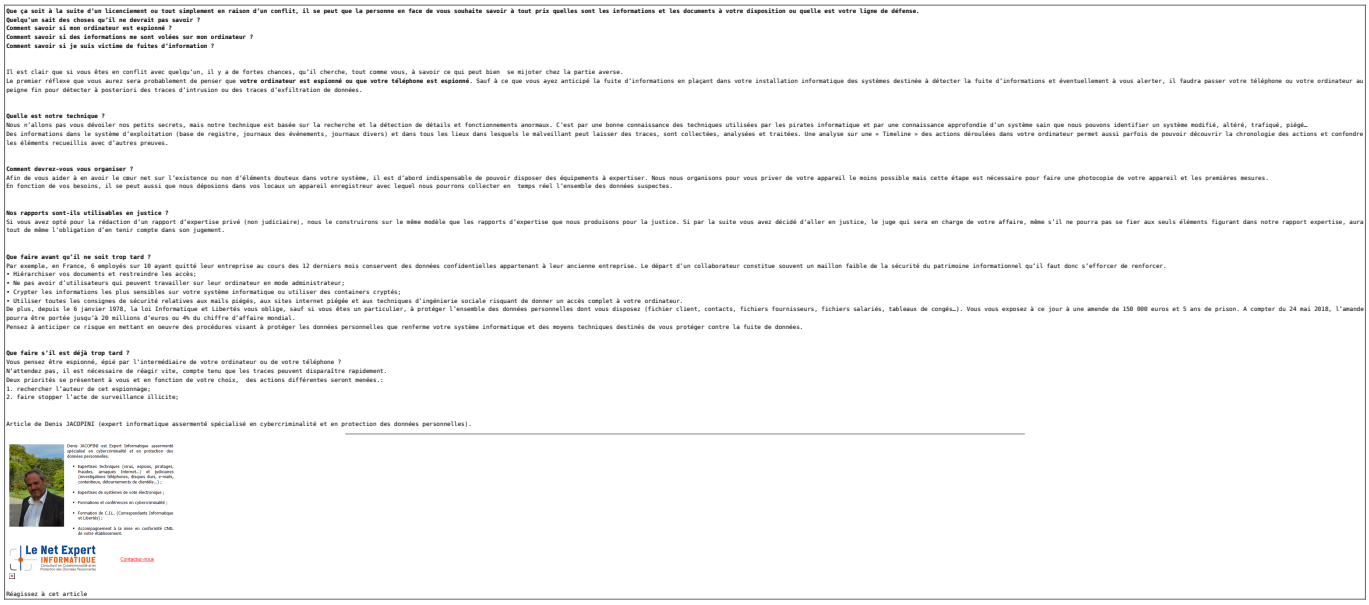
Source : *Phishing : détecter un message malveillant | CNIL*

Mon ordinateur ou mon

téléphone est-il espionné ? Des informations me sont-elles volées ? | Denis JACOPINI

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

Mon ordinateur ou mon téléphone est-il espionné ? Des informations me sont-elles volées ?



Que ça soit à la suite d'un licenciement ou tout simplement en raison d'un conflit, il se peut que la personne en face de vous souhaite savoir à tout prix quelles sont les informations et les documents à votre disposition ou quelle est votre ligne de défense.
Quelqu'un sait des choses qu'il ne devrait pas savoir ?
Comment savoir si mon ordinateur est espionné ?
Comment savoir si des informations ne sont volées sur mon ordinateur ?
Comment savoir si je suis victime de fuites d'information ?

Il est clair que si vous êtes en conflit avec quelqu'un, il y a de fortes chances, qu'il cherche, tout comme vous, à savoir ce qui peut bien se mijoter chez la partie averse.
Le premier réflexe que vous aurez sera probablement de penser que **votre ordinateur est espionné ou que votre téléphone est espionné**. Sauf à ce que vous ayez anticipé la fuite d'informations en plaçant dans votre installation informatique des systèmes destinée à détecter la fuite d'informations et éventuellement à vous alerter, il faudra passer votre téléphone ou votre ordinateur au peigne fin pour détecter à posteriori des traces d'intrusion ou des traces d'exfiltration de données.

Quelle est notre technique ?
Nous n'allons pas vous dévoiler nos petits secrets, mais notre technique est basée sur la recherche et la détection de détails et fonctionnements anormaux. C'est par une bonne connaissance des techniques utilisées par les pirates informatique et par une connaissance approfondie d'un système sain que nous pouvons identifier un système modifié, altéré, trafiqué, piégé…
Des informations dans le système d'exploitation (base de registre, journaux des événements, journaux divers) et dans tous les lieux dans lesquels le malveillant peut laisser des traces, sont collectées, analysées et traitées. Une analyse sur une « Timeline » des actions déroulées dans votre ordinateur permet aussi parfois de pouvoir découvrir la chronologie des actions et confondre les éléments recueillis avec d'autres preuves.

Comment devrez-vous vous organiser ?
Afin de vous aider à en avoir le cœur net sur l'existence ou non d'éléments douteux dans votre système, il est d'abord indispensable de pouvoir disposer des équipements à expertiser. Nous nous organisons pour vous priver de votre appareil le moins possible mais cette étape est nécessaire pour faire une photocopie de votre appareil et les premières mesures.
En fonction de vos besoins, il se peut aussi que nous déposions dans vos locaux un appareil enregistreur avec lequel nous pourrons collecter en temps réel l'ensemble des données suspectes.

Nos rapports sont-ils utilisables en justice ?
Si vous avez opté pour la rédaction d'un rapport d'expertise privé (non judiciaire), nous le construirons sur le même modèle que les rapports d'expertise que nous produisons pour la justice. Si par la suite vous avez décidé d'aller en justice, le juge qui sera en charge de votre affaire, même s'il ne pourra pas se fier aux seuls éléments figurant dans notre rapport expertise, aura tout de même l'obligation d'en tenir compte dans son jugement.

Que faire avant qu'il ne soit trop tard ?
Par exemple, en France, 6 employés sur 10 ayant quitté leur entreprise au cours des 12 derniers mois conservent des données confidentielles appartenant à leur ancienne entreprise. Le départ d'un collaborateur constitue souvent un maillon faible de la sécurité du patrimoine informationnel qu'il faut donc s'efforcer de renforcer.
• Hiérarchiser vos documents et restreindre les accès;
• Ne pas avoir d'utilisateurs qui peuvent travailler sur leur ordinateur en mode administrateur;
• Crypter les informations les plus sensibles sur votre système informatique ou utiliser des containers cryptés;
• Utiliser toutes les consignes de sécurité relatives aux mails piégés, aux sites internet piégés et aux techniques d'ingénierie sociale risquant de donner un accès complet à votre ordinateur.
De plus, depuis le 6 janvier 1978, la loi Informatique et Libertés vous oblige, sauf si vous êtes un particulier, à protéger l'ensemble des données personnelles dont vous disposez (fichier client, contacts, fichiers fournisseurs, fichiers salariés, tableaux de congés…). Vous vous exposez à ce jour à une amende de 150 000 euros et 5 ans de prison. A compter du 24 mai 2018, l'amande pourra être portée jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial.
Pensez à anticiper ce risque en mettant en œuvre des procédures visant à protéger les données personnelles que renferme votre système informatique et des moyens techniques destinés de vous protéger contre la fuite de données.

Que faire s'il est déjà trop tard ?
Vous pensez être espionné, épié par l'intermédiaire de votre ordinateur ou de votre téléphone ?
N'attendez pas, il est nécessaire de réagir vite, compte tenu que les traces peuvent disparaître rapidement.
Deux priorités se présentent à vous et en fonction de votre choix, des actions différentes seront menées.:
1. rechercher l'auteur de cet espionnage;
2. faire stopper l'acte de surveillance illicite;

Article de Denis JACOPINI (expert informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles).

Réagissez à cet article

Original de l'article mis en page : Comment se protéger contre la fuite d'informations avec le départ des collaborateurs ? — Lexsi Security Hub

---

Les bonnes pratiques contre les Cyberattaques | Denis JACOPINI

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

LE NET EXPERT AUDITS & EXPERTISES | EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES LENETEXPERT.fr | RGPD CYBER LE NET EXPERT MISES EN CONFORMITÉ | SPY DETECTION Services de détection de logiciels espions | LE NET EXPERT FORMATIONS | LE NET EXPERT ARNAQUES & PIRATAGES

Les bonnes pratiques contre les Cyberattaques

Pour se prémunir des cyberattaques, la meilleure solution consiste à mettre en place quelques bonnes pratiques de base.

Encourager une gestion rigoureuse des mots de passe
Mettez en place des outils qui forcent les utilisateurs à choisir des mots de passe forts. Ceux-ci comprennent au moins huit caractères, des majuscules et des minuscules, des chiffres et des symboles du clavier (!, @, $, etc.), mais aucun mot entier. Ils doivent aussi être changés régulièrement, même si ça cause de la grogne.

Sensibiliser les employés
Souvent considérés comme la porte d'entrée des cybercriminels, les employés doivent être formés, par exemple au moyen de modules d'apprentissage vidéo, sur les risques d'attaques possibles et les différentes formes qu'elles peuvent prendre.

Effectuer régulièrement des tests
Une façon de vérifier si les campagnes de sensibilisation auprès des employés fonctionnent consiste à les tester en simulant, par exemple, l'envoi d'un courriel frauduleux. N'oubliez pas de l'envoyer aussi – et même surtout – à ceux qui occupent des postes stratégiques.

Limiter l'accès à l'information confidentielle
Ne donnez accès aux renseignements confidentiels qu'à ceux qui en ont réellement besoin dans l'entreprise.

Contrôler les processus de sécurité
Rien ne sert d'avoir des systèmes informatiques à la fine pointe si on ne les teste pas régulièrement. Il vaut mieux impartir la tâche à des experts si on ne possède pas les ressources nécessaires à l'interne. Les fournisseurs de solutions infonuagiques disposent d'une infrastructure de sécurité informatique qui peut bien souvent dépasser celle des entreprises.

Installer les mises à jour logicielles rapidement
Beaucoup d'attaques exploitent des vulnérabilités connues depuis plusieurs mois par les fournisseurs d'antivirus, qui d'ailleurs offrent déjà des correctifs pour les contrer. Prévoyez l'installation des mises à jour dans un délai optimal de 48 heures, ou d'au plus une semaine.

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

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

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

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

Attaques informatiques : comment les repérer ?

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

Source : http://www.lesaffaires.com/dossier/gestion-des-risques/cyberattaques-toutes-les-bonnes-pratiques/579165

Comment bien sécuriser ses e-mails ? | Denis JACOPINI

Peut-on encore se passer de l'e mail dans le cadre de nos activités professionnelles ? Je ne le crois pas. Il est pratique et instantané. Cependant, peu sécurisé en standard, sans précautions, il pourrait bien vous attirer des ennuis.

Selon une étude récente de SilverSky, Email Security Habits Survey Report, 53 % des employés ont déjà reçu des données sensibles d'entreprise non cryptées par e mail ou en pièces jointes, que 21 % des employés déclarent envoyer des données sensibles sans les chiffrer et que 22 % des entreprises sont concernées chaque année par la #perte de données via e-mail.

Inquiétant vous direz-vous ? Catastrophique quand on sait que tout détenteur de données à caractère personnel est tenu à la sécurisation de ces données, conformément à la loi informatique et libertés, encadrée par la CNIL.
Et c'est encore pire quand on prend en compte les informations soumises au secret professionnel ou revêtues de confidentialité que nous échangeons quotidiennement… (plus de 100 milliards d'e-mails sont échangées chaque jour…)
Un des derniers incidents en date : la récente #divulgation des numéros de passeport de 31 leaders mondiaux…
Malgré l'évolution du contexte législatif il est bien étonnant que les entreprises ne soient pas plus nombreuses à choisir de sécuriser leurs échanges par e-mail.

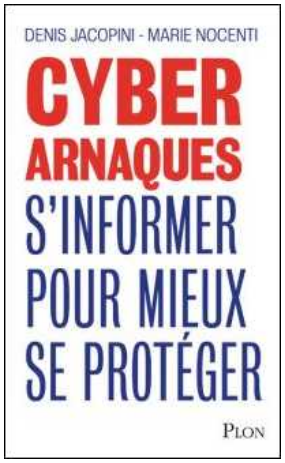
Des solutions ?
Oui, heureusement, et je vais partager avec vous mes conseils :
Mettez en place des procédés de signature numérique et le chiffrement des e-mails garantissent la confidentialité d'un message.
Vous éviterez ainsi que des données sensibles ne tombent dans de mauvaises mains.
Avantage pour le destinataire : l'assurance de l'identité réelle de l'expéditeur de l'e-mail et que le contenu du message n'a pas été modifié après son envoi.
L'utilisation simultanée de ces procédés vous permettront ainsi de répondre à un besoin de Confidentialité (par le chiffrement) et un besoin d'Intégrité (par la signature électronique).

Enfin, aucun de ces deux procédés vous assurera une protection contre la fuite d'informations ou de données confidentielles à votre insu. POur cela, nous vous recommandons d'utiliser des système de « Protection contre la fuite des données » ou de « Data Leak Protection ».*

Plus d'info sur la confidentialité des e-mails ici

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

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



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

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

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

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

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

Commandez sur Fnac.fr

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

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la 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