RGPD : Quelles actions sont à mettre en œuvre aujourd’hui pour assurer la mise en conformité des pratiques avec les nouvelles règles ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
		RGPD : Quelles actions sont à mettre en œuvre aujourd’hui pour assurer la mise en conformité des pratiques avec les nouvelles règles ?			

Le Règlement Général sur la Protection de Données (RGPD) est entré en application au 25 mai 2018 et <u>toutes les entreprises, administrations et associations</u> et leurs <u>sous-traitants</u> ne s'y sont toujours pas préparés. Or, <u>quelle que soit leur taille</u>, <u>elles sont toutes concernées</u> et risqueront, en cas de manquement, des sanctions financières jusqu'alors inégalées. Quelles actions sont à mettre en œuvre aujourd'hui pour assurer la mise en conformité des pratiques avec les nouvelles règles ?

Il importe d'auditer dès aujourd'hui les pratiques internes des différents services de l'entreprise (marketing, RH, IT…), mais également celles de ses partenaires.

Une étude des outils contractuels en place est également nécessaire, s'agissant en particulier des contrats avec les prestataires, des chartes internes, CGU, mentions d'information lors de la collecte des données… pour s'assurer de leur pertinence.

Une fois cet audit réalisé, les actions de mise en conformité seront identifiées et pourront être initiées : mise en place d'un registre, désignation d'un DPO, modification des contrats ou clauses contractuelles, sécurisation des traitements, refonte des CGU et formules d'information, etc.

Une cartographie des traitements et la mise au point d'un référentiel des finalités et des traitements permettront de comprendre l'état des pratiques, d'alimenter le suivi des formalités et les évolutions nécessaires, et d'établir l'existence de pratiques conformes et à jour au regard du RGPD en cas de contrôle des autorités.

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)

Réagissez à cet article

Source : *Le RGPD en 10 questions. Par François-Xavier Boulin, Avocat.*

63% des Français redoutent de donner des informations personnelles sur Internet | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	63% des Français redoutent de donner des informations personnelles sur Internet				

Selon une enquête réalisée par Dashlane et Opinionway, en France, au Royaume-Uni et aux États-Unis, les internautes français sont ceux qui se méfient le plus. 14% ne communiquent jamais leurs données personnelles, contre 4 % des Britanniques et 5% des Américains.

En fonction de leur identité culturelle, les internautes n'abordent pas la saisie des données personnelles sur la toile de la même manière. Selon un sondage Opinionway, réalisé en octobre 2015, les Français se montrent bien plus frileux que leurs homologues anglo-saxons: 63% d'entre eux avouent leur méfiance quand il s'agit de donner des informations personnelles sur le web contre 35 et 34% chez les Britanniques et les Américains. 14% des Français refusent de communiquer leurs informations personnelles, un chiffre qui tombe à 4 et 5% en Grande-Bretagne et aux États-Unis.
Quel que soit le pays, la donnée la plus sensible est le numéro de carte bancaire. Là encore, ce sont les Français qui arrivent en tête. 72% d'entre eux avouent leur crainte quand il s'agit de stocker cette information sur un site, contre 48% des Anglais et 41% des Américains.
Les critères qui rassurent ne sont pas les mêmes d'un pays à l'autre, selon l'enquête. Les Français se sentent en priorité protégés par le petit cadenas à côté de l'adresse qui indique une connexion sécurisée (68%), puis par l'assurance que les données ne seront pas transmises (36%). Les Britanniques et les Américains se fient, eux, à la marque ou au site Internet (53% et 47%).
En revanche, le mot de passe fait consensus. Il rime avec sécurité dans le cas de transactions pour 1/3 des Français, des Britanniques et des Américains.
Globalement, les internautes se posent beaucoup de questions quand il s'agit de payer en ligne. La vigilance reste de mise à l'égard de certains sites, de peur d'être piratés. 65% des Français évitent alors d'y utiliser leur carte. 66% des Britanniques et 70% des Américains s'abstiennent également.
Interrogés sur les systèmes sensés améliorer leur confiance, les participants se disent prêts à utiliser leur carte bancaire plus souvent, si l'utilisation une carte temporaire infalsifiable rend le piratage impossible. À cette condition, 70% des Français, 76% des Britanniques et 77% des Américains passeraient à l'acte. Autre critère jugé rassurant: une étape d'authentification supplémentaire (63% en France, 54% en Grande-Bretagne et 50% aux États-Unis).
Méthodologie : pour réaliser cette enquête, un échantillon représentatif a été constitué en fonction des critères de sexe, d'âge, de catégorie socioprofessionnelle en France, de catégorie sociale Esomar au Royaume-Uni et de revenus aux Etats-Unis. 1014 Français, 1004 Britanniques et 1009 Américains ont été soumis à un questionnaire en ligne sur système CAWI (Computer Assisted Web interview).

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 ;

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

Contactez-nous

Source : http://www.boursorama.com/actualites/63-des-francais-redoutent-de-donner-des-informations-personnelles-sur-

Formation en cybercriminalité : Virus, arnaques et piratages informatiques, Solutions pour nos entreprises

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Formation en cybercriminalité : Virus, arnaques et piratages informatiques, Solutions pour nos entreprises				

Présentation

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

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

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

Objectif

Découvrez les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant d'enrayer ce phénomène.

Durée

1 journée

ou conférence de 2 heures.

Public concerné

Chefs d'entreprise, présidents d'associations, élus, décideurs, employés, agents, ….

Moyens pédagogiques

Vidéo projecteur et sonorisation souhaitée selon la taille de la salle.

Animateur

Denis JACOPINI

Expert Judiciaire en Informatique diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire. Spécialisé en Protection des données personnelles et certifié ISO 27005, il a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

Son métier : Aider les professionnels à se protéger des pirates informatiques, et à se mettre en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles.

Il intervient dans la France entière et à l'étranger pour former ou sensibiliser les décideurs, informaticiens et utilisateurs sur les techniques utilisées par les Pirates informatiques pour piéger leurs victimes et sur les obligations en matière de protection des données à caractère personnel.

Différentes interventions pour :

– Le **Conseil de l'Europe** ;

– Un **Centre d'Enseignement et de Recherche en Informatique** ;

– Le **Centre d'Etudes des Techniques Financières** et d'Ingénierie d'Aix en Provence ;

– Des **écoles d'avocats** ;

– Des **Compagnies d'Experts Judiciaires** ;

– De nombreux clubs ou associations de chefs d'entreprises dans la **France entière et à l'étranger** ;

– Le **Centre National de la Fonction Publique Territoriale** (CNFPT) pour des élus, des S.G. et des agents publics.

(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle – Numéro formateur : 93 84 03041 84)

Plus d'informations sur : 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 ;

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

Contactez-nous

Se mettre en conformité avec la CNIL – Oui mais comment ? | Denis JACOPINI

Se mettre en conformité avec la CNIL – Oui mais comment ?
Encore plus fort que la peur du gendarme, la peur d'avoir mauvaise réputation est la principale crainte des entreprises concernées par des actes illicites (C'est ce qui ressort d'une étude de PWC).

Des années pour la construire, une fraction de seconde pour la salir; Et si votre manque de respect des données personnelles de vos clients vous rattrapait..

Achats de Noël et hausse de la cybercriminalité : 4 conseils pour éviter d'être piraté | Denis JACOPINI

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

Achats de Noël et hausse de la cybercriminalité : 4 conseils pour éviter d'être piraté

La fin d’année arrive à grands pas et les français se sont déjà lancés dans la course aux cadeaux de Noël, notamment en ligne. Et cette frénésie de l’achat ne risque pas de s’atténuer puisqu’à partir du 6 janvier ce sera au tour des soldes d’hiver de prendre le relai. Les périodes d’achats massifs font le bonheur des e-commerçants… et des cybercriminels ! Tour d’horizon des mesures à prendre pour éviter une attaque informatique.

Les mois de décembre et janvier représentent une période de forte activité, les e-commerçants vont voir leurs ventes augmenter et cela ne manquera pas d’attirer les cybercriminels en tout genre. Chaque année à cette période, les tentatives de piratage envers les entreprises mais aussi les particuliers se multiplient.
L’essor du commerce en ligne, et également du commerce sur terminaux mobiles, constitue une aubaine pour les hackeurs. Pour se prémunir de ces attaques, les particuliers peuvent prendre quelques précautions simples mais pourtant essentielles :
1. Veiller à toujours avoir les dernières mises à jour de ses applications, de son système d’exploitation et des logiciels de sécurité.
Des failles sont régulièrement enregistrées par les acteurs du secteur, et les correctifs sont présents dans les mises à jour. Un logiciel non mis à jour risque fortement d’être vulnérable face à des failles pourtant déjà identifiées et corrigées.

2. S’en tenir aux règles d’or : ignorer ou bloquer les pop-ups ;
utiliser un mot de passe original et sécurisé contenant à la fois des majuscules, des chiffres et des caractères spéciaux, ne pas utiliser les mêmes identifiants sur plusieurs sites car le mot de passe pourrait être compromis ; commander sur des sites fiables et via des connexions sécurisées en https.

3. Eviter de cliquer sur les liens directement depuis un emailing :
le phishing est une technique de cyberattaque à la mode, et elle est particulièrement efficace en période de fin d’année – lorsque des dizaines d’emails propose quotidiennement aux internautes des bons plan pour Noël et pour les soldes. Si l’offre est alléchante, au lieu de cliquer directement sur le lien, mieux vaut effectuer une nouvelle recherche dans son navigateur et s’assurer qu’il s’agit du site réel.

4. Eviter les transactions depuis des réseaux Wi-Fi publics.
La plupart des réseaux publics (gares, cafés, etc) ont un niveau de cryptage faible, et donc une moindre sécurité. Les informations bancaires pourraient atterrir dans les mains d’une tierce personne. Que l’on soit connecté depuis un ordinateur, une tablette, ou un mobile, mieux vaut donc se méfier des réseaux ouverts.

Autre point sensible : les achats via smartphones et tablettes sont de plus en plus communs, mais il est important d’être encore plus vigilent depuis ces terminaux. En effet, ces terminaux font face à de nombreuses menaces et sont souvent moins bien sécurisés que les ordinateurs.
Ici aussi des règles d’or s’appliquent : ne pas télécharger d’applications gratuites de propriétaires inconnus afin d’éviter les trojans, acheter et visualiser les comptes bancaires seulement via des applications propriétaires (celles de sa banque ou celles d’e-commerçants de renom), mais aussi supprimer l’historique de navigation, le cache et les cookies régulièrement afin de supprimer les données sensibles.

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 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

Mise en conformité RGPD, formations et conférences Cybercriminalité et en protection des données personnelles, Expertises et Recherche de preuves

Denis JACOPINI est Expert en Cybercriminalité et en Protection des Données à Caractère Personnel.
Notre métier :

Animation de formations et de conférences

Cybercriminalité (virus, espions, piratages, fraudes, arnaques Internet)
Protection des Données à Caractère Personne (mise en

conformité avec la CNIL etle RGPD)
Audits sécurité, Expertises techniques et judiciaires

Audit sécurité (ISO 27005) ;
ID Swatting

Recherche de preuves (Investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
Expertises de systèmes de vote électronique ;

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

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?				

Vous vous retrouvez victime d'usurpation d'identité, quelqu'un s'est fait passer pour vous sur Facebook, twitter, viadeo, linkedin et vous voulez porter plainte. Sur quelle loi s'appuyer ?

Je ne suis pas avocat, cependant, une fois au commissariat de police ou en brigade de gendarmerie, il se peut que l'officier ne sache pas sur quelle loi et quel article s'appuyer. Sachez que s'il vous décourage de porter plainte sous le motif que c'est inutile dans la mesure ou le responsable de l'acte malveillant ne sera jamais retrouvé, il a tout de même l'obligation d'enregistrer la plainte que vous souhaitez déposer.

Pour vous aider, pour l'aider.
Selon la Loi LOPPSI 2 (LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure)
Article 226-4-1 du Code de Procédure Pénale : « Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.
Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. »
Voir cet article sur Légifrance :
www.legifrance.gouv.fr/affichCodeArticle.do;?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000023709201

Si par la suite vous souhaitez rechercher ou recueillir des preuves, afin de garantir leur recevabilité, notamment en matière d'intégrité du respect de la preuve, nous pouvons vous aider pour vous accompagner dans toutes ces démarches.
Contactez-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 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

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l’accès à ses outils informatiques ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Une entreprise peut-elle être condamnée pour défaut de sécurisation de l’accès à ses outils informatiques ?				

Nous attirons votre attention sur le fait que cette

information est modifiée par la mise en place du RGPD (Règlement Général sur la Protection des données). Plus d'informations ici : https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd Nous l'avons toutefois laissée accessible non pas par nostalgie mais à titre d'information.

Une entreprise peut être condamnée pour défaut de sécurisation de l’accès à ses outils informatiques ?

Une entreprise peut être sanctionnée par la CNIL, par exemple, si l’organisme juge que les mots de passe sont peu sécurisants : les noms des employés, inchangés depuis quelques années. Avec les nouvelles réglementations européennes entrées en vigueur en 2018, les amendes peuvent s’élever à 20 millions d’euros voire 4% du chiffre d’affaires mondial…

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)

Réagissez à cet article

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

Comment supprimer une informations gênante sur Internet ? | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Comment supprimer une information gênante sur Internet ?				

Victime d'usurpation d'identité, d'insultes ou de propos diffamatoires, vous désirez faire disparaître une information compromettante d'Internet ? Il est temps d'agir sur votre e-réputation. Les conseils de Denis JACOPINI, expert informatique assermenté.

1 Où supprimer

Nous pouvons considérer plusieurs niveaux de suppression :
– Au niveau des supports (sites Internet) stockant les informations à supprimer vers lesquels pointent les outils permettant de trouver l'information ;
– Au niveau des outils permettant de trouver les informations ;
– Au niveau des supports ayant une copie des informations à supprimer vers lesquels pourraient pointer les outils permettant de trouver l'information ;
–

Supprimer la totalité des informations ne peut être garanti

En effet, les actions menées sur Internet par les utilisateurs sont Internationales. En 2016, dans le monde, nous comptons un peu plus de 3,3 milliards d'internaute et un peu plus d'un milliard de sites Internet. C'est autant d'utilisateurs susceptibles d'enregistrer une information dans leur ordinateur ou la diffuser sur Internet, sur un blog ou un forum dans le plus grand secret.
A ce jour, les seuls moyens à notre disposition pour trouver de l'information sur Internet sont :
• soit de connaître l'url (Uniform Resource Locator) utilisées pour identifier les pages et les sites web (par exemple : https://www.lenetexpert.fr/contacter-denis-jacopini-expert-judiciaire-en-informatique-correspondant-cnil-cil/)
• soit on passe par des outils permettant de rechercher de l'information (ex : http://www.google.fr et on recherche « Contacter Denis JACOPINI »)
• soit on passe par des outils spécialisés dans la recherche d'information qui vont scruter dans différents type de services Web (annuaires, réseaux sociaux, espaces de partage, de microblogage…)
Nous sommes en mesure de vous apporter ce service ?
N'hésitez pas à nous contacter

1.1 Suppression d'informations à une adresse précise

Prendre contact avec le responsable du site Internet ou le propriétaire du compte contenant l'information est la première étape que nous recommandons.
Par exemple, si une information fausse ou compromettante est constatée à l'adresse suivante : https://www.lenetexpert.fr/contacter-denis-jacopini-expert-judiciaire-en-informatique-correspondant-cnil-cil, le plus simple est de contacter la personne en charge du site internet racine soit http://www.lenetexpert.fr en expliquant la raison de notre demande de suppression d'informations
Retrouver la personne responsable du contenu du site Internet peut s'avérer simple (dans le meilleur des cas, le site dispose d'une rubrique « Contact » ou « contactez-nous », ou bien d'une rubrique « Mentions légale » contenant un numéro SIREN, SIRET, l'identité d'un « responsable de la publication »…) ou parfois compliquée (aucune rubrique précédemment citée n'est présente). Il sera alors nécessaire de trouver les coordonnées de la personne en charge de l'hébergement du site internet en question par d'autres moyens en fonctions des informations pouvant être trouvées sur le site Internet ou sur des sites proposant des services de « Whois », répertoriant les informations administratives et techniques relatives au noms de domaines.
Enfin, vous pouvez aussi contacter le responsable d'un site internet en recherchant le nom du site, de la marque ou du service dans des annuaires internet, des moteurs de recherche ou sur des réseaux sociaux ou d'anciennes versions du site internet.
Notez toutefois qu'en France, tous les sites internet édités à titre professionnel ont l'obligation de créer une rubrique « mentions légales » dans laquelle vous pourrez peut-être aussi trouver un numéro SIREN ou SIRET si le site Internet appartient à un professionnel ou une association déclarée à l'INSEE.
Nous sommes en mesure de vous apporter ce service ?
N'hésitez pas à nous contacter

1.2 Suppression d'informations dans les outils de recherche

–
Supprimer une information sur un site Internet n'a pas d'action directe et immédiate sur le contenu des annuaires et des moteurs de recherche. Cependant, supprimer une information sur un site Internet peut avoir des actions à posteriori comme c'est le cas pour les moteurs de recherche, tels que Google, qui disposent de Bots (par exemple les robots GoogleBot) qui scrutent le contenu des sites Internet et le contenu derrière leurs liens, à la recherche de toute modification, ajout ou suppression d »informations.
Supprimer une information sur un site Internet peut ainsi avoir pour effet de supprimer l'information dans l'index de recherche du moteur de recherche mais ceci sera sans garantie en terme de réalisation ou de délai.
Cependant, si le préjudice porte sur la présence sur Internet d'une information compromettante, il ne faut pas perdre de vue qu'un internaute lambda recherche sur Internet dans la quasi totalité des cas en passant par un moteur de recherche.
Notez qu'en France, le moteur de recherche Google est utilisé dans plus de 93% des cas et draine chaque mois un plus de 40 millions de recherches, Bing est utilisé dans un peu plus de 4% des cas et Yahoo dans un peu plus de 2% des cas. Cela laisse très peu de place (moins de 1%) aux autres moyens utilisés pour rechercher de l'information sur Internet.
[illegible]
De plus, une étude de Advanced Web Ranking de février 2015 nous informe que sur la première page de google, le premier résultat récoltera 33% des clics, le second résultat 15,6% des clics, le troisième résultat 10% des clics, le 4ème résultat 7% des clics, le 5ème résultat, 6% des clics, les 5 derniers résultats récoltant seulement 4% des clics.
Il est donc facile de remarquer que 75% des consultations seront réalisées sur la 1ère page. Les liens présents sur la seconde page des résultats de Google récolteront 5% des clics.
Ainsi, plus de 80% des recherches ne concernant que les deux premières pages de Google et ces habitudes de consultation étant quasiment similaires sur appareils mobiles et sur d'autres moteurs de recherche,
compte tenu qu'il sera impossible d'agir sur tous les annuaires, tous les moteurs de recherche et tous les sites Internet,
compte tenu que du coup, les prétendants à l'existence numérique concentrent leurs efforts pour être présents sur ces outils de recherche,
compte tenu que ne pas y être présent sur ces outils de recherche revient à ne tout simplement pas avoir d'existence numérique,
alors, concentrer ses efforts pour disparaître des 3 premières pages des 3 principaux moteurs de recherches sur Internet permettra de faire disparaître 98% des informations indésirables.
A la suite d'une plainte déposée en 2010 auprès de l'Agence espagnole de protection des données, dans son Arrêt du 13 mai 2014, la Cour de Justice de l'Union Européenne accorde aux individus le droit de s'opposer au traitement de leurs données personnelles.
À la suite de cette décision, Google a publié un formulaire en ligne le 31 mai 2014 permettant à chaque citoyen européen de demander le déréférencement des liens qui apparaissent dans une recherche associée à leur nom, tout en prenant en compte l'intérêt prépondérant du public à avoir accès à l'information.
Le mercredi 16 juillet 2014, le moteur de recherche Bing a mis à disposition son formulaire de demande de blocage des résultats de recherches sur Bing en Europe et en décembre de cette même année, Yahoo a mis à disposition son formulaire.

Nous sommes en mesure de vous apporter ce service ?
N'hésitez pas à nous contacter
–

2 Comment supprimer

2.1 En résumé, pour supprimer une information sur un site Internet à une adresse précise :

A) Aller sur le site Internet et rentrer en contact avec le site Internet ou avec le responsable de la publication
– rubrique « Contact », « Contactez-nous » ou similaire ;
– rubrique « Mentions légales » ou similaire ;
B) Rechercher le représentant légal de l'activité professionnelle associée au site Internet à partir de son numéro SIREN ou SIRET (liste non exhaustive)
– www.infogreffe.fr
– www.societe.com
– www.europages.com
– www.hoovers.com
C) Rechercher la personne en charge de l'hébergement de l'information avec des outils de Whois (liste non exhaustive)
– www.afnic.fr/fr/produits-et-services/services/whois/
– www.gandi.net/whois?lang=fr
– www.whois-raynette.fr/
– http://whois.domaintools.com
D) Rechercher la personne en charge de l'hébergement de l'information sur les réseaux sociaux (liste non exhaustive)
– plus.google.com
– www.facebook.com
– www.twitter.com
– www.linkedin.com
– www.viadeo.com
E) Rechercher la personne en charge de l'hébergement de l'information dans les annuaires et les moteurs de recherche (liste non exhaustive)
– www.google.com
– www.google.fr
– www.bing.com
– www.yahoo.com
– www.yahoo.fr
F) Rechercher d'anciennes versions du site Internet qui pourraient contenir des informations par la suite supprimées
– http://archive.org/web (Wayback machine)
Nous sommes en mesure de vous apporter ce service ?
N'hésitez pas à nous contacter
Si l'information à supprimer est personnelle, en France, vous disposiez d'un droit d'accès, de modification ou de suppression à cette information (Article 34 et suivants de la Loi Informatique et Libertés du 6 janvier 1978).
La CNIL met à votre disposition un générateur de courrier (https://www.cnil.fr/modeles/courrier) destiné à vous aider à faire exercer vos droits auprès des responsables de sites Internet.
Exemple de courrier :
Conformément à l'article 40 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, je vous prie de [objet_de_la_demande]
Vous voudrez bien m'adresser copie de l'enregistrement ainsi modifié.
Je vous rappelle que vous disposez d'un délai maximal de deux mois suivant la réception de ce courrier pour répondre à ma demande, conformément à l'article 94 du décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée.
Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.
Si l'information à supprimer fait l'objet d'une demande de suppression judiciaire, l'Expert informatique désigné pour réaliser cette mission pourra directement contacter le responsable du site internet pour lui communiquer l'ordonnance justifiant son action et demander le retrait pur et simple de le'information.
En cas de difficulté, remontez la au juge en charge du suivi de votre affaire.
Enfin, si vous n'arriver pas à trouver ou à contacter une personne en charge du site Internet contenant l'information à supprimer, vous avez la possibilité de signaler un acte d'injure ou de diffamation sur le site Internet du ministère de l'Intérieur : http://www.internet-signalement.gouv.fr ou saisir une juridiction de proximité (https://www.service-public.fr/particuliers/vosdroits/F1785).

2.2 En résumé, pour supprimer une information dans les 3 moteurs de recherche les plus utilisés en France :

A) Google : Accéder au formulaire de demande de suppression de résultats de recherche au titre de la législation européenne en matière de protection des données :
https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=fr
B) Bing : Accéder au formulaire de de demande de blocage des résultats de recherches sur Bing en Europe
https://www.bing.com/webmaster/tools/eu-privacy-request
C) Yahoo :
https://fr.aide.yahoo.com/kb/search/Demande-de-blocage-de-r%C3%A9sultats-de-recherche-sur-Yahoo-Search–Formulaire-pour-r%C3%A9sidents-europ%C3%A9ens-sln24378.html
D) Une technique appelée le Flooding consiste à produire beaucoup de contenus et de liens pour apparaître dans les premiers résultats et de faire passer le contenu incriminé sur les pages moins consultées.

Nous sommes en mesure de vous apporter ce service ?
N'hésitez pas à nous contacter

2.3 Si vous pouvez modifier le contenu des pages Web du site Internet :

A) Supprimez les fichier sou les dossiers contenant l'information
B) Modifiez la ou les pages d'index ou d'accueil en rajoutant dans l'entête « <meta name= »robots » content= »noindex » /> »
C) Par le biais d'un fichier .htaccess vous pouvez aussi rendre privé et protégé par mot de passe l'accès à un dossier
Nous sommes en mesure de vous apporter ce service ?
N'hésitez pas à nous contacter
Bien évidemment cette liste de conseils pas exhaustive et n'attend que vos avis et commentaires pour l'enrichir

---

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 ;

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

Contactez-nous

Etude et publication de Denis JACOPINI
LIENS SOURCES
Utilisation des moteurs de recherche en France

http://www.journaldunet.com/ebusiness/le-net/1087481-parts-de-marche-des-moteurs-de-recherche-en-france/
Taux de clic en fonction de la position dans les résultats
http://www.mathiasp.fr/blog/seo/quel-est-le-taux-de-clic-en-fonction-des-positions-dans-google/544

Attaques informatiques : comment les repérer ? | Denis JACOPINI

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

Attaques informatiques : comment les repérer ?

Une entreprise met souvent plusieurs mois avant de s'apercevoir qu'elle est victime d'une attaque informatique. Certains signes doivent néanmoins l'alerter.

Deux cent jours, c'est en moyenne le temps nécessaire à une entreprise pour découvrir qu'elle a été victime d'une attaque informatique. Et encore, à condition qu'elle le découvre. A cela s'ajoute le temps de réparation, qui est presque aussi long. Pourquoi une telle durée ? Parce qu'au fil des années, les attaques se sont sophistiquées et les objectifs des pirates ont évolué.

S'il y a dix ou quinze ans, les hackers voulaient absolument montrer leurs exploits, ils sont aujourd'hui plus discrets. Le but n'est plus de « faire un coup » mais de récupérer des données personnelles, financières ou d'endommager subrepticement un système sans que la victime s'en aperçoive immédiatement.

C'est pourquoi, si certaines attaques peuvent être assez rapidement perceptibles comme les dénis de service (la saturation du système qui devient inopérant), la plupart des menaces restent ignorées des utilisateurs. Ce qui peut être extrêmement dommageable puisque pendant cette période, l'entreprise risque de se faire voler ses secrets industriels et surtout peut donner accès, involontairement, aux systèmes de ses fournisseurs ou de ses donneurs d'ordre : « En général, ce sont des tiers qui détectent les attaques.

Les grands comptes, qui ont les outils pour faire cette surveillance, remarquent des anomalies chez leurs sous-traitants » souligne Jérôme Billois, directeur du pôle Cyber-sécurité chez Solucom.

Mais comment, lorsque l'on est une PME, que l'on n'a pas d'expert en interne, déceler une attaque informatique et la distinguer par exemple d'une panne de machines ou de réseau ?

Pour Gérôme Billois, la première parade est la vigilance. « Il faut sensibiliser les utilisateurs et remonter les comportements anormaux » explique l'expert.

Des anomalies qui peuvent être protéiformes, pas toujours synonymes d'attaques, mais qu'il convient de vérifier : ralentissement soudain du poste de travail ; ordinateur qui doit fréquemment être redémarré ; taux d'activité inhabituel des sites Web avec des accès fréquents aux bases de données… « Il faut être attentif au système d'information, voir si les volumes de données sont cohérents et regarder les destinations », rappelle Gerôme Billois. Autres éléments à surveiller : le nombre et l'activité des comptes autorisés à administrer le système. « Les pirates, parfois, se créent un compte administrateur. Or, s'il y en a plus que le nombre initialement autorisé, cela peut être le signe d'une intrusion. Il faut également regarder les heures où ces comptes ont été actifs, les comptes malveillants agissant plutôt en dehors des heures habituelles de travail. Mais attention, précise Gérôme Billois, si l'on mène une telle surveillance, il faut que cela soit mentionné dans la charte informatique et signalé à la Commission nationale informatique et libertés (Cnil) via une déclaration simplifiée. »

L'entreprise sera également attentive au rapport que lui envoie son anti-virus, car, même si celui-ci n'arrête pas toutes les attaques, il demeure le premier rempart. Il faut vérifier que sur tous les postes, les antivirus sont bien activés, sachant que certains utilisateurs n'hésitent pas à désactiver ces solutions accusées de ralentir les opérations ou d'empêcher le téléchargement de logiciels. Les Smartphones et les tablettes, particulièrement ceux qui fonctionnent sous le système Androïd, peuvent être aussi attaqués. Il existe en effet de nombreuses (fausses) applications dont l'objectif est de récupérer des données ou de faire payer l'utilisateur : « Il faut se méfier quand l'application demande des droits élevés alors qu'elle n'en a pas besoin. Par exemple, une application de bureautique qui va requérir de la géolocalisation. »

Heureusement, les entreprises, même les plus petites, disposent d'une palette d'outils pour se protéger. Outre l'antivirus, elles ont la possibilité d'acquérir des systèmes de détection d'intrusion (IDS) qui écoutent le trafic réseau de manière furtive, afin de repérer des activités anormales ou suspectes. « Elles peuvent également avoir une approche pro-active et souscrire auprès de prestataires spécialisés des services qui vont faire la surveillance interne de leur système d'information », précise Gérôme Billois. Mais la première protection (comme le principal risque) reste l'humain. « Il faut bien gérer le départ des employés, surtout s'ils sont partis en mauvais termes ». Et ne pas oublier de faire régulièrement les mises à jour des logiciels de sécurité et de vérifier, via la solution d'administration de système, que tout fonctionne correctement.

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 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 : http://www.leparisien.fr/economie/business/attaques-informatiques-comment-les-reperer-07-12-2015-5348215.php