Mise en conformité RGPD : ce que les PME doivent faire

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

Entré en vigueur depuis le 25 mai 2018, le Règlement Général sur la Protection des Données a déjà commencé à bouleverser l'organisation globale des entreprises, quelle qu'en soit leur taille. Apparues complexes, ces nouvelles règles finissent par cacher une démarche qui s'avère finalement simple en respectant quelques étapes. Denis JACOPINI, notre Expert RGPD nous en dit plus.

LeNetExpert : Où en sont aujourd'hui la plupart des PME vis à vis de la démarche de mise en conformité RGPD ?
Denis JACOPINI : Avant de commencer l'animation d'une formation sur le RGPD, je demande toujours ce qu'on retenu les personnes ayant déjà assisté à des petits déjeuners, des déjeuners, dîners thématiques ou des Webinars sur ce thème.
Systématiquement elles me confient qu'elle n'ont retenu des informations sur leurs obligations, sur la complexité de la démarche mais pas sur la démarche concrète à réaliser.
Ce constat m'a permis de me conforter dans l'idée qu'il était important de construire le contenu de nos formations pour que les dirigeants de PME ou leurs futurs DPO (Data Protection Officer = en français Délégué à la Protection des Données) repartent à la fois en ayant compris l'intérêt de la démarche d'un tel règlement (et ils ont un intérêt direct) mais surtout avec de nombreux outils et des méthodes leur permettant une démarche de mise en conformité RGPD en toute autonomie.

LNE : Quelle sont les démarches que les PME devraient réaliser selon vous ?
Denis JACOPINI : Le 25 mai 2018, le règlement européen est entré en application. De nombreuses formalités auprès de la CNIL ont disparu mais en contrepartie, la responsabilité des organismes a été renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité. Ces démarches doivent être réalisées avec méthode et étapes.
La CNIL a mis à disposition de tout les organismes concernés par ces démarches un guide : RGPD : se préparer en 6 étapes.
Dans ce guide ont peut y trouver 6 étapes indispensables pour initier la démarche de mise en conformité :

1/ DÉSIGNER UN PILOTE
Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

2/ CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES
Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

3/ PRIORISER LES ACTIONS À MENER
Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

4/ GÉRER LES RISQUES
Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact relative à la protection des données (AIPD).

5/ ORGANISER LES PROCESSUS INTERNES
Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

6/ DOCUMENTER LA CONFORMITÉ
Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

LNE : Combien peut coûter à une PME ce type de démarche ?
Denis JACOPINI : Les établissements professionnels, associations et administrations doivent savoir qu'il n'y a aucune obligation de payer quoi que ce soit ou de faire appel à un professionnel. En effet, les organismes souhaitant entamer ou poursuivre leur démarche de mise en conformité peuvent réaliser eux même ces démarches. Le coût sera alors seulement lié au temps passé à réaliser cette démarche qui peut ne pas être négligeable selon la taille ou l'activité de votre structure. **Cette démarche peut donc être gratuite** pour un établissement qui aura choisi de se former de manière autodidacte ou **ou remboursée** en totalité si la formation que vous suivez est entièrement prise en charge par un organisme collecteur de la taxe formation.
En fait, le vrai prix dépend du contexte de départ, du volume d'éléments à améliorer et du temps consacré à la démarche de mise en conformité RGPD.

LNE : Quel type d'organisme accompagnez-vous dans leur démarche de mise en conformité ?
Denis JACOPINI : Tout organisme étant concerné, j'accompagne toute taille et tout type d'organisme. En fonction de la taille ou du secteur d'activité la démarche sera différente. Individuelle, de groupe, plus axée sur la formation, plus orientée sur l'accompagnement ou parfois encore, exclusivement basée sur la réalisation de la démarche de mise en conformité, nous nous adaptons à chaque organisme.

LNE : Comment bénéficier d'une démarche de mise en conformité gratuite ou pour avoir une formation prise en charge ?
La plupart des dirigeants savent aujourd'hui qu'ils peuvent demander la prise en charge de formations auprès de l'organisme auprès duquel ils versent leur taxe pour la formation professionnelle. Il vous suffit ensuite de nous formuler votre demande. Après quelques échanges, nous pouvons vous envoyer rapidement une proposition qu'il vous suffira de communiquer à votre organisme. Au terme de cette démarche administrative, un accompagnement personnalisé vous sera proposé afin de vous apprendre l'essentiel de la démarche et l'usage d'outils gratuits à mettre en oeuvre.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84 — Liberté • Égalité • Fraternité — RÉPUBLIQUE FRANÇAISE

Datadock — Organisme validé et référencé

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

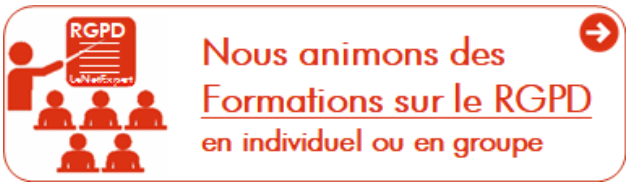
Contactez-nous

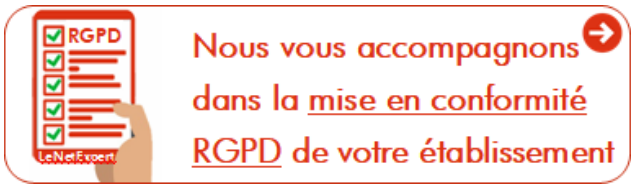
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

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

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

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





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles

en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

Source : RGPD : se préparer en 6 étapes

Vous pensez avoir reçu une arnaque à la mise en conformité RGPD ?
Signalez ou demandez notre avis sur signalements@lenetexpert.fr

Exemple de proposition douteuse de mise en conformité RGPD

CONTROLE
RGPD

Institution Européenne de la règlementation générale à la protection des données

000002962 - DD86.0015

[redacted]

Vos Références

Bulletin d'information du 25/03/2019
Région : Nouvelle-Aquitaine
Décret N° 2018-687 du 01 aout 2018
Numéro d'identifiant : RG-135010002962
Date limite de déclaration : 05/04/2019

Objet : Mise en conformité RGPD

Tél : 09 74 59 68 08
E-mail : contact@rgpd-registre.online

Madame, Monsieur,

La date du 25 Mai 2018 pour attester de la mise aux normes à la protection des données personnelles au sein de votre établissement (R.G.P.D) a été dépassée.

Nous vous rappelons qu'à compter de cette date, les entreprises qui n'auront pas régularisé leur situation quant au nouveau règlement RGPD 2016/679 sur la protection des données, quelle que soit leur activité ou taille, sont passibles de sanctions pénales et financières pouvant s'élever jusqu'à 4% du Chiffre d'Affaire annuel de la société.

Pour information, le propriétaire ou l'exploitant d'un établissement traitant des données personnelles (Il peut donc s'agir du nom, prénom, de l'adresse physique ou d'une adresse e-mail mais aussi du numéro de sécurité sociale…) qui ne répond pas aux exigences de la législation sur le RGPD définies par la directive (UE) 2016/680 en date du 25 mai 2018, doit élaborer obligatoirement un rapport et une mise en place des protections des données avec documents justificatifs à l'appui en cas de contrôle.

Vous êtes invités à vous mettre en conformité sans délai.

Un service de traitement RGPD dédié à cette circonstance est disponible :

- Par téléphone : **09 74 59 68 08**
- Du lundi au jeudi de 9h00 à 18h00 sans interruption et le vendredi de 9h à 16h00.

Sylvain Blanchet
Gestionnaire RGPD

RAPPEL DE LA LOI

Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions pénales
(Chapitre VIII, article 83, alinéa 5)
Les violations des dispositions suivantes font l'objet d'amendes administratives pouvant s'élever jusqu'à 20 000 000 € ou 4 % du chiffre d'affaire annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.
Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions civiles
(Chapitre VIII, article 79 alinéa 1)
Sans préjudice de tout recours administratif ou extra judiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'une autorité de contrôle au titre de l'article 77, chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectuées en violation du présent règlement. Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. (Modifié par Loi n°2004-801 du 6 août 2004)

RÈGLEMENT GÉNÉRAL PROTECTION DONNÉES

MISE EN CONFORMITE
RELANCE

[redacted]

Numéro de dossier : [redacted]
Code contact : [redacted]
Date : 19/09/2018
Objet : Mise en conformité RGPD

Madame, Monsieur,

Nous vous rappelons qu'à compter du **25 mai 2018**, les entreprises qui n'auront pas régularisé leur situation quant au nouveau règlement **RGPD 2016/679** sur la protection des données, quelle que soit leur activité ou taille, sont passibles de sanctions pénales et financières pouvant s'élever jusqu'à **4%** du Chiffre d'Affaire annuel de la société.

Vous êtes invités à vous mettre en conformité sans délai.

Le Pôle administratif RGPD a mis en place un service d'assistance téléphonique centralisé, intégralement dédié à cette circonstance, disponible du lundi au vendredi de **09h00** à **18h00** au :

- Par téléphone : [redacted] (prix d'un appel local)

- En ligne : Remplir le questionnaire de pré diagnostic RGPD en ligne
[redacted]

Si vous avez déjà effectué votre rapport RGPD, merci de ne pas tenir compte de ce rappel.

Pôle Administratif RGPD
Le directeur régional

RAPPEL DE LA LOI

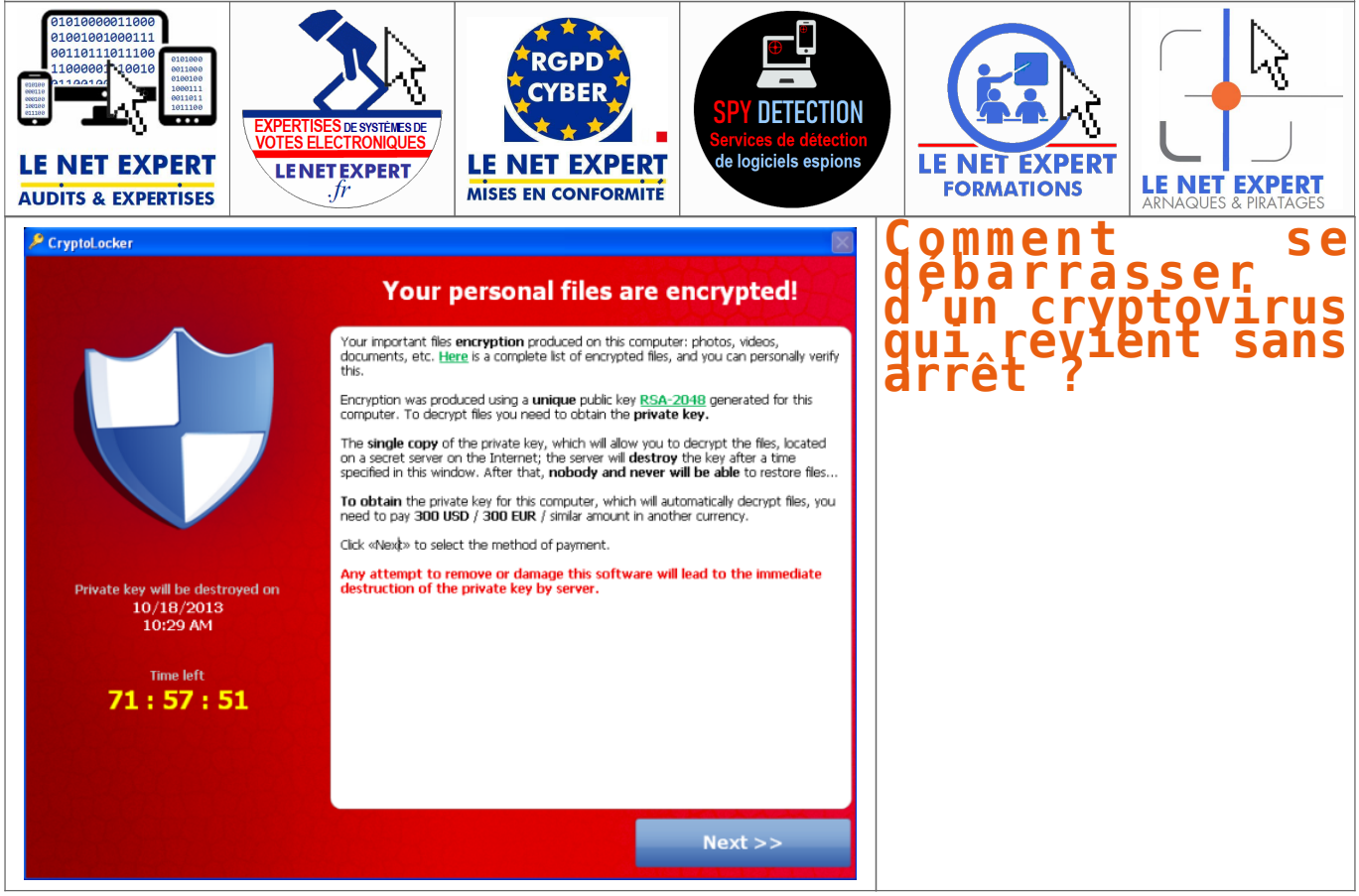
Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions pénales
(Chapitre VIII, article 83, alinea 5)
Les violations des dispositions suivantes font l'objet d'amendes administratives pouvant s'élever jusqu'à **20 000 000 EUR** ou **4 %** du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.
Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions civiles
(Chapitre VIII, article 79 alinea 1)
Sans préjudice de tout recours administratif ou extrajudiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'une autorité de contrôle au titre de l'article 77, chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du présent règlement.
Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
(Modifié par Loi n°2004-801 du 6 août 2004)
La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers. Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée.

[redacted] RGDP

Comment se débarrasser d'un cryptovirus qui revient sans

arrêt ?

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



Comment se débarrasser d'un cryptovirus qui revient sans arrêt ?

Vous vous êtes fait piéger par un Cryptovirus ? Après un bon nettoyage de l'ordinateur, vous avez réinstallé les fichiers perdus grâce à de précieuses sauvegardes. Cependant, quelques jours ou quelques semaines plus tard, vos fichiers sont à nouveau cryptés. Que faire ?

Que ça soit à la suite des nombreux défaçages de sites Internet (piratage du site Internet et changement de la page d'accueil) dont ont été victimes des dizaines de milliers de sites Internet en 2015 ou à la suite de vagues de virus cryptant la quasi totalité des données de votre ordinateur et vous demandant de payer une rançon pour continuer à les utiliser, nous avons été surpris par les mesures prises par le ou les informaticiens.
En effet, à la suite d'échanges avec ces pompiers informatiques afin de vérifier les mesures prises à la suite de l'attaque informatique, nous avons eu, et leurs clients également, la désagréable surprise que leurs actions se restreignaient à nettoyer le ou les postes infectés et restaurer la dernière sauvegarde. En d'autres termes, excepté pour ceux profitant de cette situation pour constater que leurs systèmes de sauvegardes parfois lourdement facturés ne fonctionnait pas ou ne sauvegardait pas tout, la quasi totalité des techniciens contactés nous ont confirmé que le grand changement dans leurs procédure à la suite d'une telle attaque de pirate, consistait à renforcer la vérification des procédures de sauvegarde !!!
Vous l'aurez compris, la conséquence évidente que si l'on ne soigne pas la cause du mal et qu'on ne fait qu'atténuer les effets, le mal reviendra.
Sauf à que ça vous plaise de passer votre temps de restaurer des données à chaque nouvelle attaque, il est peut-être temps de changer quelque chose.

En cas d'attaque par ransomware (cryptovirus), nous vous recommandons de vous former ou d'utiliser un spécialiste pour suivre les étapes suivantes (l'ordre peut être adapté en fonction de vos priorités) :

1. Payer ? nous ne recommandons pas ça car non seulement vous favorisez le développement de ces actes en récompensant les cybercriminels, mais également rien ne vous assure que vous pourrez récupérer l'utilisation de vos fichiers et enfin, même si vous payez et que vous en avez pour votre argent, il est fort probable que le même pirate ou un autre vous piège à nouveau.
2. Constatez et recueillez les preuves ;
3. Conservez les preuves soit pour une analyse ultérieure en vue de la recherche d'un antidote, soit pour une analyse approfondie de la technique utilisée par le pirate informatique, soit pour pouvoir porter plainte (si vous avez une assurance ou pour vous protéger si votre système informatique victime contamine d'autres systèmes informatique , ce qui vous rendraient responsable) ;
4. Éventuellement, portez plainte ;
5. Nettoyez votre système informatique de toutes traces du virus ;
6. Pour éviter qu'elle se reproduise, analysez avec précision l'attaque informatique afin de trouver la faille utilisée pour pénétrer votre système informatique en vue de sa réparation;
7. Restaurez les données pour pouvoir remettre en route son système informatique le plus rapidement possible ;
8. Recherchez la faille ;
9. Corrigez la faille ;
10. Recherchez d'autres failles ;
11. Par prévention, corrigez d'autres failles et augmentez vos mesures de sécurité ;
12. Contactez éventuellement les autorités compétentes (Police, Gendarmerie, OCLCTIC, BETFI, votre CERT, le CERTA, PHAROS…) ;

Denis JACOPINI, Expert Informatique assermenté, est spécialisé en cybercriminalité et en protection des données personnelles pourra vous accompagner pour chacune de ces étapes.
Contactez-nous
Vous êtes une société d'informatique démunie devant une situation spécifique, il n'y a aucun inconvénient à vous faire aider par un spécialiste en cybercriminalité. Nous pouvons également vous accompagner.

Remarque :
Certaines de ces étapes peuvent être longues et nécessiteront un accès à distance de votre installation.

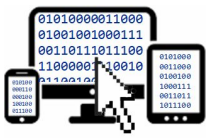
[block id="24761" title="Pied de page HAUT"]

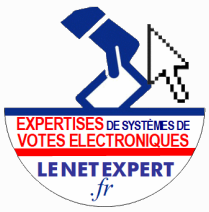
Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

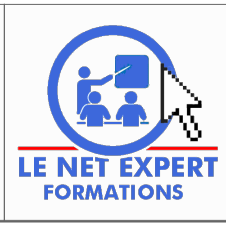
Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

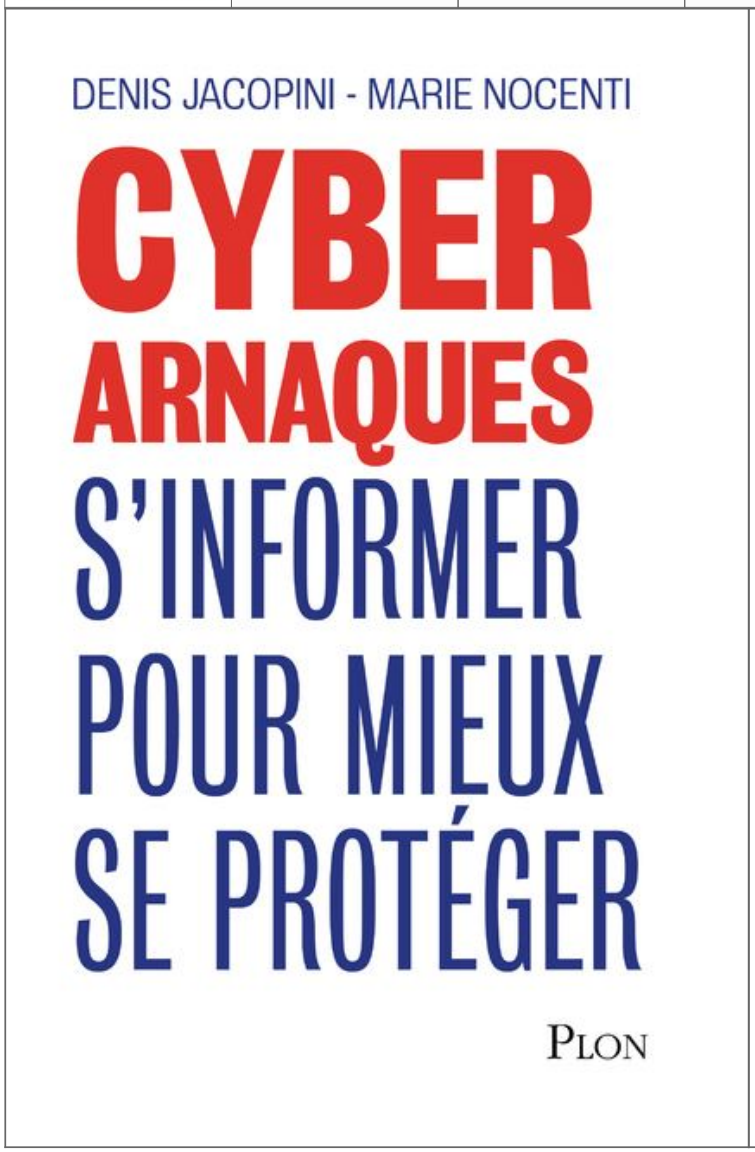
[block id="24760" title="Pied de page BAS"]

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







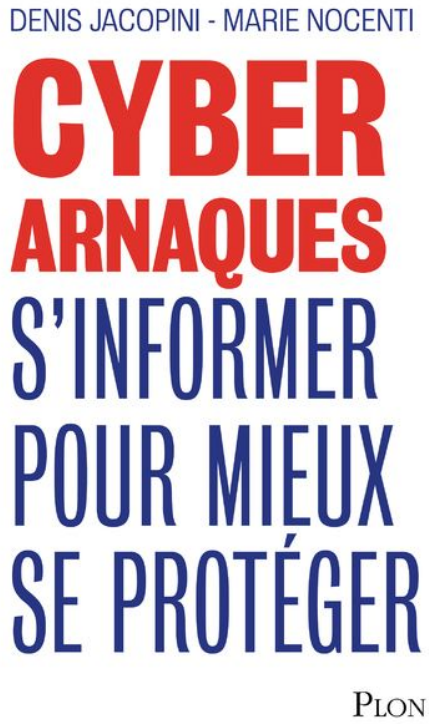


Comment détecter les arnaques sur Internet ? Denis JACOPINI vous en parle sur Europe 1 à l'occasion de la présentation de son livre « CYBERARNAQUES : S'informer pour mieux se protéger »

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

« Puisse cet ouvrage avoir de nombreux lecteurs ! Il ne devrait pas plaire aux arnaqueurs, car il est un réquisitoire contre leur perfidie et, sans aucun doute, une entrave à leur chiffre d'affaire. »
Général d'armée (2S) Watin- Augouard

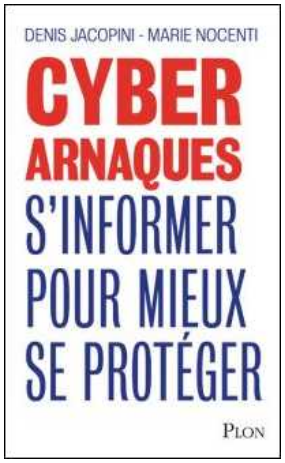
Commandez CYBERARNAQUES



Plutôt qu'un inventaire, Denis Jacopini, avec la collaboration de Marie Nocenti, a choisi de vous faire partager le quotidien de victimes d'Internet en se fondant sur des faits vécus, présentés sous forme de saynètes qui vous feront vivre ces arnaques en temps réel. Il donne ensuite de précieux conseils permettant de s'en prémunir. Si vous êtes confronté un jour à des circonstances similaires, vous aurez le réflexe de vous en protéger et en éviterez les conséquences parfois dramatiques… et coûteuses.
Un livre indispensable pour « surfer » en toute tranquillité !
Denis Jacopini est expert judiciaire en informatique, diplômé en cybercriminalité et en droit, sécurité de l'information et informatique légale à l'université de droit et science politique de Montpellier.
Témoin depuis plus de vingt ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus soigneusement élaborées, il apprend aux professionnels à se protéger des pirates informatiques.
Marie Nocenti est romancière.

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

Comment créer sa charte Informatique ? (ANSSI)

Comment créer sa charte Informatique ? (ANSSI)

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

1. L'OBJECTIF

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

2. DES DÉFINITIONS CLAIRES ET PRÉCISES

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

3. L'OBJET ET SA PORTÉE

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

4. LES USAGES

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

5. DÉFINIR LES DEVOIRS DE L'UTILISATEUR

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

6. LES MESURES DE CONTRÔLE

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

7. LES SANCTIONS

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

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

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

[Consultez le guide complet de l'ANSSI]

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

Mise en conformité RGPD. Attention aux arnaques…

En réaction à la fois aux très nombreuses inquiétudes qui me sont remontées au sujet de démarchages douteux d'organismes en apparence officiels (voir ci-dessous) vous informant de l'urgence de se mettre en conformité sous peine d'être passible d'une très forte amende et aux prix exorbitants pratiqués par de nombreux organismes, voici l'avis de notre Expert RGPD, Denis JACOPINI.

Vous pensez avoir reçu une arnaque à la mise en conformité RGPD ?

Signalez ou demandez notre avis sur signalements@lenetexpert.fr

LNE : Combien coûte une mise en conformité pour une entreprise de petite taille ?

Denis JACOPINI : Il me paraît déjà important de préciser que si quelqu'un vous a dit qu'il est conforme RGPD, il y a de très forte chance que soit il n'ait rien compris à la démarche RGPD, soit que ce soit un menteur. En effet, un organisme n'est pas conforme RGPD ou non conforme RGPD. J'ajouterai même que personne n'est conforme RGPD. Par contre, on doit parler de démarche de mise en conformité. Ainsi, soit un organisme a initié une démarche de mise en conformité, soit il n'a pas initié de démarche de mise en conformité.

Ensuite, les établissements professionnels, associations et administrations doivent savoir qu'il n'y a aucune obligation de payer quoi que ce soit ou de faire appel à un professionnel. En effet, les organismes souhaitant entamer ou poursuivre leur démarche de mise en conformité peuvent réaliser eux même ces démarches. Le coût sera alors seulement lié au temps passé à réaliser cette démarche qui peut ne pas être négligeable selon la taille ou l'activité de votre structure. **Cette démarche peut donc être gratuite** pour un établissement qui aura choisi de se former de manière autodidacte ou **peut être remboursée** en totalité si la formation que vous suivez est entièrement prise en charge par un organisme collecteur de la taxe formation.

En fait, le vrai prix dépend du contexte de départ, du volume d'éléments à améliorer et du temps consacré à la démarche de mise en conformité RGPD.

Quel type d'organisme accompagnez-vous dans leur démarche de mise en conformité ?

Tout organisme étant concerné, j'accompagne toute taille et tout type d'organisme. En fonction de la taille ou du secteur d'activité la démarche sera différente. Individuelle, de groupe, plus axée sur la formation, plus orientée sur l'accompagnement ou parfois encore, exclusivement basée sur la réalisation de la démarche de mise en conformité, nous nous adaptons à chaque organisme.

Comment bénéficier d'une démarche de mise en conformité gratuite ou pour avoir une formation prise en charge ?

La plupart des dirigeants savent aujourd'hui qu'ils peuvent demander la prise en charge de formations par l'organisme auprès duquel ils cotisent pour la taxe formation. Il suffit ensuite de nous formuler votre demande pour que nous vous envoyons une proposition qu'il vous suffira de communiquer à votre organisme. Au terme de cette démarche administrative, un accompagnement personnalisé vous sera proposé afin de vous apprendre l'essentiel de la démarche et l'usage d'outils gratuits à mettre en oeuvre.

Récemment, la CNIL vient de mettre en place une nouvelle formation en ligne ouverte à tous (MOOC) intitulée « L'atelier RGPD ». Elle est proposée aux professionnels pour leur permettre de découvrir ou mieux appréhender le RGPD. Il vous permet ainsi d'initier une mise en conformité dans votre organisme et de vous aider à la sensibilisation des opérationnels.

Une attestation de suivi sera délivrée dans le Mooc à tout participant ayant parcouru la totalité des contenus et ayant répondu correctement à 80 % des questions par module…[lire la suite]

Vous pensez avoir reçu une arnaque à la mise en conformité RGPD ?
Signalez ou demandez notre avis sur signalements@lenetexpert.fr

Exemple de proposition faisant l'objet de nombreux doutes de la part de nos lecteurs :

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

MISE EN CONFORMITE
RELANCE

[redacted]

Numéro de dossier : [redacted]
Code contact : [redacted]
Date : 19/09/2018
Objet : Mise en conformité RGPD

Madame, Monsieur,

Nous vous rappelons qu'à compter du **25 mai 2018**, les entreprises qui n'auront pas régularisé leur situation quant au nouveau règlement **RGPD 2016/679** sur la protection des données, quelle que soit leur activité ou taille, sont passibles de sanctions pénales et financières pouvant s'élever jusqu'à **4%** du Chiffre d'Affaire annuel de la société.

Vous êtes invités à vous mettre en conformité sans délai.

Le Pôle administratif RGPD a mis en place un service d'assistance téléphonique centralisé, intégralement dédié à cette circonstance, disponible du lundi au vendredi de **09h00** à **18h00** au :

- Par téléphone : [redacted] (prix d'un appel local)

- En ligne : Remplir le questionnaire de pré diagnostic RGPD en ligne

[redacted]

Si vous avez déjà effectué votre rapport RGPD, merci de ne pas tenir compte de ce rappel.

Pôle Administratif RGPD
Le directeur régional

RAPPEL DE LA LOI

Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions pénales
(Chapitre VIII, article 83, alinea 5)
Les violations des dispositions suivantes font l'objet d'amendes administratives pouvant s'élever jusqu'à **20 000 000 EUR** ou **4 %** du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.
Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions civiles
(Chapitre VIII, article 79 alinea 1)
Sans préjudice de tout recours administratif ou extrajudiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'une autorité de contrôle au titre de l'article 77, chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du présent règlement.
Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
(Modifié par Loi n°2004-801 du 6 août 2004)
La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers. Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée.

[redacted] RGDP

CONTROLE
RGPD

Institution Européenne de la règlementation générale à la protection des données

000002962 - DD86.0015

[redacted]

Vos Références

Bulletin d'information du 25/03/2019
Région : Nouvelle-Aquitaine
Décret N° 2018-687 du 01 aout 2018
Numéro d'identifiant : RG-135010002962
Date limite de déclaration : 05/04/2019

Objet : Mise en conformité RGPD

Tél : 09 74 59 68 08
E-mail : contact@rgpd-registre.online

Madame, Monsieur,

La date du 25 Mai 2018 pour attester de la mise aux normes à la protection des données personnelles au sein de votre établissement (R.G.P.D) a été dépassée.

Nous vous rappelons qu'à compter de cette date, les entreprises qui n'auront pas régularisé leur situation quant au nouveau règlement RGPD 2016/679 sur la protection des données, quelle que soit leur activité ou taille, sont passibles de sanctions pénales et financières pouvant s'élever jusqu'à 4% du Chiffre d'Affaire annuel de la société.

Pour information, le propriétaire ou l'exploitant d'un établissement traitant des données personnelles (Il peut donc s'agir du nom, prénom, de l'adresse physique ou d'une adresse e-mail mais aussi du numéro de sécurité sociale…) qui ne répond pas aux exigences de la législation sur le RGPD définies par la directive (UE) 2016/680 en date du 25 mai 2018, doit élaborer obligatoirement un rapport et une mise en place des protections des données avec documents justificatifs à l'appui en cas de contrôle.

Vous êtes invités à vous mettre en conformité sans délai.

Un service de traitement RGPD dédié à cette circonstance est disponible :

- Par téléphone : **09 74 59 68 08**
- Du lundi au jeudi de 9h00 à 18h00 sans interruption et le vendredi de 9h à 16h00.

Sylvain Blanchet
Gestionnaire RGPD

RAPPEL DE LA LOI

Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions pénales
(Chapitre VIII, article 83, alinéa 5)
Les violations des dispositions suivantes font l'objet d'amendes administratives pouvant s'élever jusqu'à 20 000 000 € ou 4 % du chiffre d'affaire annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.
Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions civiles
(Chapitre VIII, article 79 alinéa 1)
Sans préjudice de tout recours administratif ou extra judiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'une autorité de contrôle au titre de l'article 77, chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectuées en violation du présent règlement. Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. (Modifié par Loi n°2004-801 du 6 août 2004)

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

REÇU LE
- 3 DEC. 2018

RGPD FRANCE

Numéro de dossier : 31674145300013

Date : Le 30/11/2018

Objet : Mise en conformité Loi RGPD

993 / **5664**

[redacted]

Madame, Monsieur,

Votre établissement ne semble pas être en conformité dans la démarche de normalisation de la protection des données RGPD (Règlement général sur la protection des données)
Toutes les entreprises européennes doivent entreprendre leurs démarches de mise en conformité relatives au RGPD.

La date de mise en application est fixée au 25 mai 2018, tout établissement en non-conformité est passible de sanctions financières et pénales prévues par le règlement n°2016/679 ainsi que les articles 226-16à226-24 du Code pénal.

La démarche de mise en conformité permet de suspendre cette sanction.

Nous vous invitons à vous régulariser dès à présent :

- Par téléphone : **09.70.73.45.58**
- Du lundi au jeudi (9h00 - 18h00)
- Le vendredi (9h00 - 13h00)

Informations importantes :

Le bureau de traitement a mis en place une assistance téléphonique pour vous aider à la prise en charge de votre dossier. Sont concernées par cette obligation toutes entreprises qui collectent, conservent et/ou à utilisent des données à caractère personnel de citoyens de l'Union Européenne. L'absence de démarche RGPD expose les établissements à une amende de 4% du chiffre d'affaire annuel.

A NOTER QUE LES SOCIÉTÉS RÉCALCITRANTES À SE CONFORMER AU RGPD RISQUENT UNE SANCTION PÉNALE DE 300.000€ ET DE 5 ANS D'EMPRISONNEMENT.

Pierre Bellini

DEPARTEMENT DE MISE EN CONFORMITE RGDP
Tel: 09.70.73.45.58

Siret 83901203600019

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84 — Liberté • Égalité • Fraternité — RÉPUBLIQUE FRANÇAISE

Datadock — Organisme validé et référencé

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

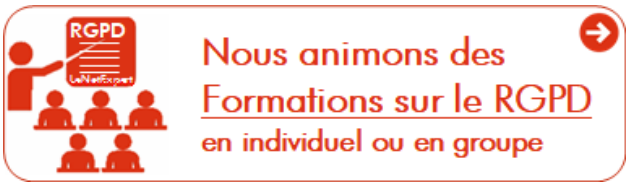
Contactez-nous

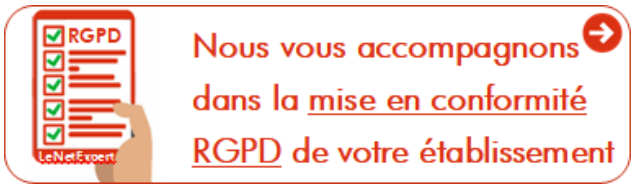
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

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

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

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





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles

en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

Source : *La CNIL lance sa formation en ligne sur le RGPD ouverte à tous | CNIL*

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

[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"]

1. http://assiste.com.free.fr/p/abc/a/pirates_informatiques.html
2. http://www.imprimer-dematerialiser.fr/la-cybercriminalite-2015-en-8-chiffres

---

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

Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
LE NET EXPERT AUDITS & EXPERTISES	EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES LE NET EXPERT .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

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

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

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

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

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

La CNIL recommande quant à elle :

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

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

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

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

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

• Vous constatez quelque chose d'anormal associé à votre compte ;

• Vous perdez ou lorsque vous est volé un appareil dans lequel ont été cochés l'enregistrement des mots de passe réseau ou dans les navigateurs ;

• Le fournisseur de service vous avertit s'être fait pirater son système informatique (encore faut-il qu'il l'ait équipé de sondes de détection d'intrusion et de détecteurs de fuites de données).

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

Réagissez à cet article

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

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

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

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

La CNIL recommande quant à elle :

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

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

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

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

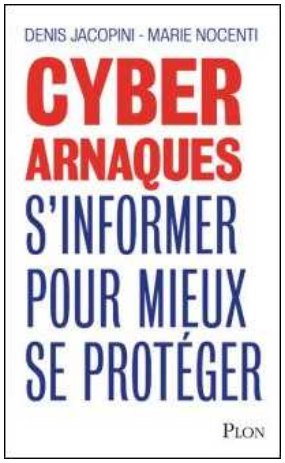
Ainsi, tout en vous conseillant de bien respecter l'utilisation de mots de passe complexes et différents pour chaque service et vous recommandant fortement que vos mots de passe « utilisateurs » ne soient connus de personne, pas même de votre informaticien parfois imprudent sans le savoir, je vous recommande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

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

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

[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

Les meilleurs conseils pour choisir vos mots de passe |

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 LE NET EXPERT .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 meilleurs conseils pour choisir vos mots de passe

A l'occasion de la Journée du Mot de Passe, les meilleurs conseils aux utilisateurs pour éviter que leurs codes secrets ne soient découverts.

Le 5 mai était la Journée Mondiale du Mot de Passe. Une idée marketing lancée par des éditeurs de solution de sécurité informatique. Pour marquer cette date d'une pierre blanche, plusieurs éditeurs ont analysé les habitudes des utilisateurs. Avast Software par exemple propose des recommandations pour créer et protéger des mots de passe indéchiffrables.

Créer des mots de passe fiables et les modifier fréquemment

Une actualité ponctuée d'histoires comme celles de la faille d'Ashley Madison, le site de rencontres extra-conjugales, démontre que les gens n'utilisent pas correctement leurs mots de passe. Les utilisateurs ne créent pas de codes assez fiables et il est certain qu'ils ne les changent pas régulièrement – même face au risque de voir leurs données sensibles et leurs potentielles frasques exposées, ou leur mariage brisé. Les utilisateurs créent des mots de passe facilement déchiffrables souvent par manque d'information ou par paresse, en témoigne la liste des codes les plus souvent utilisés compilée par les chercheurs.

Dans le top 10 :

1. 123456
2. 123456789
3. password
4. 101
5. 12345678
6. 12345
7. Password1
8. qwerty
9. 1234
10. 111111

Cette liste comprend les mots de passe les plus simples, tels que 123456, password, et qwerty. D'autres se retrouvent plus bas dans la liste comme iloveyou (#19) ou trustno1 (#57) – une ironie pour un code figurant dans la liste des mots de passe les plus populaires. « ***Certains pensent qu'une liste de mots de passe seuls qui fuite en ligne n'est pas un problème – cependant, environ 50 % de ces mots de passe étaient associés à une adresse mail,*** déclare le chercheur d'Avast Michal Salat. ***Nous savons que les gens utilisent les mêmes combinaisons de mails et de mots de passe pour différents comptes. C'est pourquoi si un hacker connait le mot de passe de votre profil Ashley Madison, il connaitra également celui de votre Facebook, Amazon, eBay, etc.*** »

Comment créer des mots de passe fiables ?

Il n'y a pas de meilleure occasion que le 5 mai pour commencer à changer ses habitudes et protéger ses codes. Voici quelques conseils pour garder un mot de passe fiable et sécurisé. Je vais être honnete avec vous, si vous ne prenez pas 5 minutes pour réfléchir à votre sécurité et à la bonne gestion de vos précieux, passez votre chemin !

Domus tutissimum cuique refugium atque receptaculum sit

· Créer des mots de passe longs et complexes. Il suffit de reprendre une phrase d'un livre que vous aimez. N'oubliez pas d'y placer quelques chiffres, majuscules et signes de ponctuations.
· Utiliser un mot de passe différent pour chaque compte. Lors de les conférences, je fais sortir les clés des participants. Une clé pour chaque porte (voiture, boite aux lettres, maison, bureau…). En informatique, il faut la même régle pour ses mots de passe.
· Ne pas partager ses mots de passe. C'est peut-être une proposition idiote au premier abord, mais combien de fois, lors d'ateliers que je propose dans les écoles, j'entends le public m'expliquer avoir partager avec son ami, son voisin… sa clé wifi !
· Changer ses mots de passe régulièrement. Pour mon cas, il change tous les 35 jours. Je ne suis pas à l'abris du vol d'une base de données dans les boutiques, sites… que j'utilise.
· Utiliser un gestionnaire de mot de passe pour mémoriser ses mots de passe ? Je suis totalement contre. Il en existe beaucoup. Mais faire confiance à un outil dont on ne maîtrise ni le code, ni la sécurité, me parait dangereux. Beaucoup d'utilisateurs y trouvent un confort. L'ensemble de vos mots de passe sont regroupés dans une solution informatique qui chiffre les données. Un seul mot de passe est requis pour utiliser n'importe quel compte sauvegardé. Bref, vaut mieux ne pas perdre ce précieux cerbére !

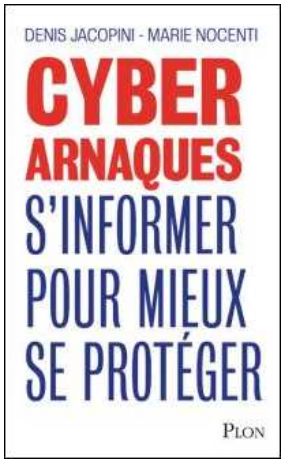
· Verrouiller son matériel avec un mot de passe. Les systèmes existent. utilisez les. Je croise bien trop d'ordinateur s'ouvrant d'une simple pression sur la touche « Entrée ».
· Activer la double-authentification ou l'authentification forte. Indispensable aide. Téléphone portable, sites Internet, Facebook, Twitter… La double authentification renforce l'accès à vos espaces. En cas de perte, vol, piratage de votre précieux. Sans la double authentification, impossible d'accèder à vos données.

De son côté TeamViewer rappele aussi qu'il est déconseillé de fournir des informations personnelles identifiables : Utiliser plusieurs mots de passe forts peut impliquer quelques difficultés de mémorisation. Aussi, afin de s'en souvenir plus facilement, beaucoup d'utilisateurs emploient en guise de mot de passe des noms et des dates qui ont une signification personnelle. Les cyber-délinquants peuvent cependant exploiter des informations accessibles publiquement et des comptes de réseaux sociaux pour trouver ces informations et s'en servir pour deviner les mots de passe… [Lire la suite]

D'autres bons conseils pour gérer vos mots de passe sur disponibles le site de l'ANSSI ou de la CNIL.

[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 : *Générer un mot de passe indéchiffrable, possible ? – Data Security BreachData Security Breach*

Escroqueries aux Faux Ordres

de Virements Internationaux (FOVI)

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

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

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

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

Pour rappel, ce mode opératoire est utilisé dans le cadre du paiement d'un loyer ou d'une facture en instance dans la société ciblée. Dans ces deux cas, un individu se présente comme un responsable du fournisseur et contacte par téléphone, puis par mail, le service comptabilité de l'entreprise ciblée en l'informant d'un changement de domiciliation bancaire.
Afin de rassurer l'entreprise ciblée et de transmettre les nouvelles coordonnées bancaires, **les escrocs utilisent désormais le site Internet LA POSTE pour créer un compte leur permettant d'utiliser le service payant de la lettre recommandée en ligne**. Créé sous une fausse identité, ce compte leur permet de régler des envois postaux et ainsi de faire parvenir à l'entreprise ciblée un courrier matérialisé, distribué par LA POSTE et remis en main propre au destinataire, contenant les coordonnées bancaires gérées par les escrocs.
Face à cette nouvelle menace, une vigilance accrue est de mise. Nous vous encourageons à diffuser ce message auprès des personnes concernées de votre société.

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

…[lire la suite]

[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"]

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

---

Conservez une preuve en vue d’une plainte à la CNIL

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

Réaliser une capture d'écran depuis un ordinateur

Depuis un PC

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

Depuis un Mac

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

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

Cas d'utilisation :

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

Réaliser une capture d'écran sur Smartphone ou tablette

A partir d'un terminal Android

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

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

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

A partir d'un terminal Windows Phone

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

A partir d'un smartphone Samsung

.

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

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

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

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Datadock
Organisme validé et référencé

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

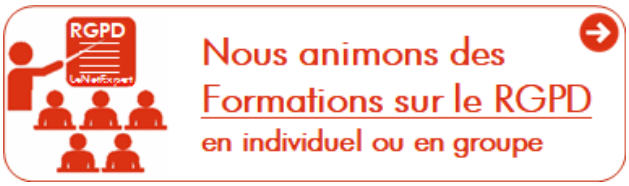
Contactez-nous

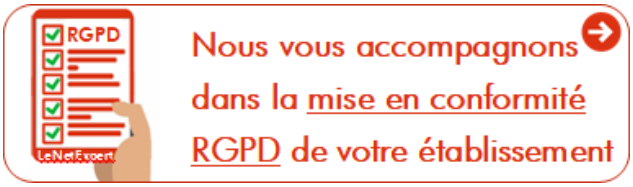
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité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

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

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

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





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur

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

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

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