Le phishing, ça c'était avant : place aux fraudes au paiement par autorisation dans lesquelles on vous fait dire OK par téléphone

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

Interviewé par Atlantico, Denis JACOPINI nous parle d'une nouvelle forme de Phishing. Le APP (Authorised Push Payment Fraud – fraude au paiement par autorisation) serait une des techniques de fraude en forte croissance au Royaume Uni, et combinerait des techniques sophistiquées, au travers de SMS et d'appels, pour soutirer de l'argent aux victimes.

Le APP (Authorised Push Payment Fraud – fraude au paiement par autorisation) serait une des techniques de fraude en forte croissance au Royaume Uni, et combinerait des techniques sophistiquées, au travers de SMS et d'appels, pour soutirer de l'argent aux victimes. 19 370 cas auraient été répertoriés au Royaume Uni au cours de ces 6 derniers mois selon le daily mail. Quelles sont les techniques ici employées ? La France est-elle touchée ?
Denis Jacopini : Cette technique de fraude utilise de nombreux ingrédients de base :
• L'ingénierie sociale (pratique utilisant des techniques de manipulation psychologique afin d'aider ou nuire à autrui)
• L'usurpation (d'identité);
• Le passage en mode émotionnel par la peur ;
• L'interlocuteur est votre sauveur et est là pour vous aider.

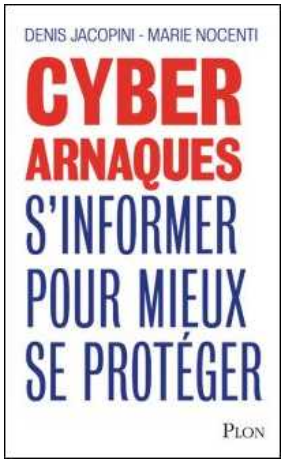
Dans le cas précis, nous avons aussi :
• L'usurpation du nom de la banque ;
• L'usurpation du numéro de téléphone de la banque ;
• Le passage en mode émotionnel de la victime basé sur la peur du piratage mais heureusement elle est en ligne avec un sauveur (baisse de la prudence, confiance aveugle…) ;
• La création d'une ambiance téléphonique de centre d'appel ;
• Un excellent comédien qui joue le rôle de l'employé de banque ;
• Une excellente connaissance des procédures internes des banques dont la banque usurpée.
En France, ce type d'arnaque n'est pas encore médiatisé. En effet, les banques n'aiment pas tellement communiquer sur leurs failles car :
• Ce n'est pas bon pour leur image ;
• Elles sont ensuite obligées de dépenser beaucoup pour corriger ;
• Elles préfèrent investir lorsque la fraude commence à leur coûter plus cher que les mesures de sécurité à mettre en place (gestion du risque).

Ces nouvelles techniques de fraude marquent elles une réelle professionnalisation de cette forme de criminalité ?
Denis Jacopini : Cette forme de criminalité existe depuis très longtemps et n'a pas attendu l'informatique et Internet pour se développer et se professionnaliser. Prétexter un gros risque et usurper l'identité des pompiers, des policiers, du plombier en utilisant leur costume, leur jargon, leur outils pour vous rassurer et reviennent ensuite pour mieux vous arnaquer ou vous cambrioler existe depuis que les escrocs existent.
Plus récemment, Gilbert Chikli Pionnier de l'arnaque au faux président, utilisait des techniques de manipulation psychologique et se servait de sa parfaite connaissance des procédures internes aux très grandes entreprises et sa maîtrise du langage juridique ou financier en fonction de l'identité de la personne usurpé pour obtenir de ses victimes des virements définitifs pour des sommes détournées de plusieurs dizaines de millions d'euros.
Chaque fois que des techniques d'arnaque ou d'escroquerie sont déjouées, décortiquées et dévoilées au grand jour, il y a des millions d'escrocs du dimanche vont analyser l'arnaque pour la reproduire et l'utiliser pour eux. Une fois que l'arnaque commence à être connue et de plus en plus de gens sont sensibilisés, les escrocs professionnels et utilisant leur génie à des fins illicites modifient leurs techniques pour toujours utiliser des moyens basés sur les ingrédients de base + des failles inexploitées utilisant ou non la technologie.
Comme les banques ont mis en place des mesures de sécurité utilisant l'internet, le SMS, le téléphone, les escrocs utilisent ces mêmes technologies en recherchant le moyen d'exploiter les failles qui ne seront jamais suffisamment protégées : Les failles du cerveau humain.

Quels sont les réflexes à avoir pour éviter tout problème de ce type ?
Denis Jacopini : Le seul moyen que nous avons pour nous protéger est d'une part la prudence ultime en plus de la sensibilisation. Selon moi, les médias devraient signaler ce type d'arnaque afin de sensibiliser le plus grand nombre. Cependant, cette solution ne plait pas aux banques qui considèrent inutile de répandre la peur car cela risquerait d'écorcher de manière irréversible la confiance que nous avons mis des années à avoir envers les moyens de paiement électronique sur Internet.
A notre niveau, si j'ai un conseil à vous donner pour éviter tout problème de ce type, si vous vous trouvez dans une situation anormale qui vous est présenté par un interlocuteur, contactez directement l'établissement à l'origine de l'appel à partir des coordonnées dont vous disposez, et allez jusqu'au bout de la vérification AVANT de réaliser des opérations financières irréversibles et partagez le plus possible les cas d'arnaques.
Quand on sait à quoi ressemble le loup, on ne le fait pas rentrer dans sa bergerie. Par contre, s'il met un nouveau costume, le piège fonctionnera tant que ce nouveau costume ne sera pas connu du plus grand nombre. (d'où l'utilité de mon livre CYBERARNAQUES
https://www.amazon.fr/Cyberarnaques-Denis-JACOPINI/dp/2259264220

[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

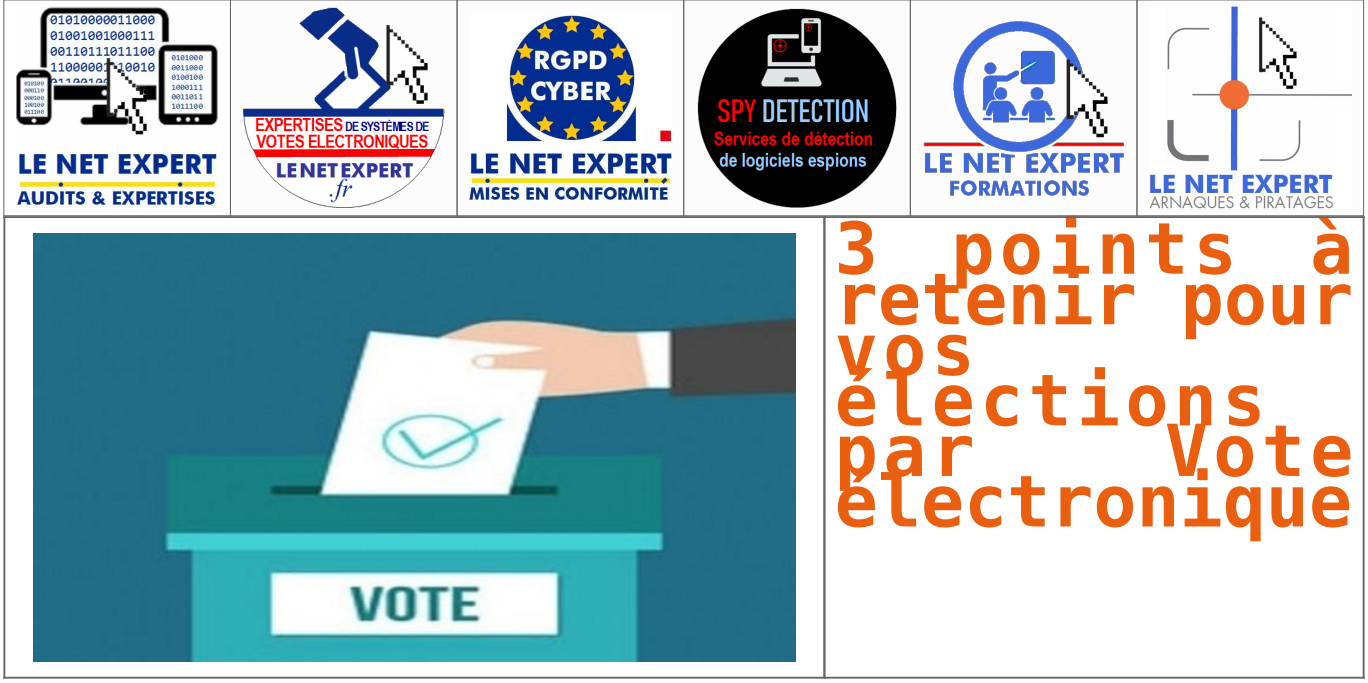
Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le 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 : *Le phishing, ça c'était avant : place aux fraudes au paiement par autorisation dans lesquelles on vous fait dire OK par téléphone | Atlantico.fr*

3 points à retenir pour vos élections par Vote électronique

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



EXPERTISES DE SYSTÈMES VOTES ÉLECTRONIQUES

EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES

- ACCOMPAGNEMENT AU CHOIX DES SOLUTIONS DE VOTE ÉLECTRONIQUE
- EXPERTISE PRÉALABLE AUX ELECTIONS
- PARTICIPATION AU SCELLEMENT DES URNES
- ACCOMPAGNEMENT PENDANT LE SCRUTIN
- PARTICIPATION AU DÉPOUILLEMENT DES URNES
- RAPPORT D'EXPERTISE PAR UN EXPERT INDÉPENDANT

Les décrets d'application de la Loi Travail continuent d'arriver en ce dernier mois de l'année 2016. L'ultime en date concerne le vote électronique (1). En tant que représentants du personnel, que vous soyez délégué du personnel ou membre du comité d'entreprise, vous vous demandez quelles sont les conditions à réunir pour recourir à ce type de dispositif. Vous souhaitez savoir quels sont les apports de la Loi Travail sur le vote électronique ; quel accord mettre en place et quelles garanties pour le système adopté ? Voici les 3 points essentiels à connaître à propos du vote électronique !

Avant la loi Travail, le vote électronique n'était possible que sous réserve d'avoir été prévu par un accord collectif. Mais est-ce toujours le cas ? Pour quelles élections peut-on recourir au vote électronique ? Quelles sont les garanties de régularité de ce vote ?

Les élections concernées par le vote électronique

Il est possible de recourir au **vote électronique** pour **deux élections** visées dans le décret du 5 décembre 2016 :

- les **délégués du personnel** ;
- les représentants du personnel au **comité d'entreprise**.

Sachez qu'il est d'ailleurs possible de combiner vote électronique et vote sous enveloppe, à condition que l'acte qui autorise le recours au vote électronique n'exclue pas cette possibilité *(2)*.

Les modalités du vote électronique

La mise en place du vote électronique est soumise à quelques formalités préalables. Ce recours doit être prévu dans un **accord de groupe** ou un **accord d'entreprise** (2).
Désormais, à défaut d'accord collectif, **l'employeur** peut **décider unilatéralement** de recourir au vote électronique *(2)*. C'est la nouveauté inscrite dans ce décret d'application de la loi travail.
Sachez aussi que le **protocole d'accord préélectoral**, qui doit être négocié entre l'employeur et les organisations syndicales représentatives, doit mentionner l'accord collectif ou la décision de l'employeur de recourir au vote électronique.

Quel est le contenu du protocole d'accord préélectoral ?
Lors de la négociation de ce protocole, il faudra tenir compte des contraintes techniques posées par ce vote particulier. En effet, comme tout dispositif électronique, des garanties doivent être prises pour assurer la **régularité du vote** et sa **confidentialité**.
A ce titre, le code du travail établit un **cahier des charges** à respecter :

- des **fichiers distincts** dans l'urne : il doit y avoir deux fichiers qui doivent être bien séparés. Le premier « **Fichier des électeurs** » doit permettre l'authentification des électeurs. Le second fichier nommé « **Contenu de l'urne électronique** » détaillera lui les clés de chiffrement et de déchiffrement, ainsi que le contenu de l'urne. Ce fichier n'est **consultable que par les personnes en charge de la gestion et de la maintenance du système de vote** *(3)*.
- le système de vote doit pouvoir être **scellé** pendant toute la durée du scrutin *(4)*.
- une **expertise indépendante** doit être réalisée **avant le scrutin***(5)* par un **expert indépendant** mandaté par l'employeur.
- une **assistance technique** doit être mise en place par l'employeur pour veiller au bon fonctionnement du système et intervenir en cas de besoin *(6)*. Des tests doivent être effectués sur le matériel avant le déroulement du vote.

Les garanties prévues pour la régularité du vote

Le vote électronique doit présenter certaines garanties indispensables à sa régularité :

- le **respect du cahier des charges** prévu par la loi.

Il est mentionné dans l'accord collectif ou la décision unilatérale de l'employeur de recourir au vote électronique.
Par ailleurs, **chaque salarié** doit avoir **accès à ce cahier des charges** selon le décret du 5 décembre 2016 *(2)*. Il peut être mis à leur disposition via l'intranet de l'entreprise ou consultable dans les locaux de l'entreprise.

L'expertise préalable par un expert indépendant.
Tout le système et le matériel de vote doit avoir été examiné par un expert rémunéré par l'employeur.
Il s'assure de l'existence de la **décision unilatérale de l'employeur** ou de l'**accord collectif** autorisant le recours au vote électronique.
Il doit s'assurer également des modalités garantissant la **confidentialité** et la **sécurité du dispositif** : l'existence des deux fichiers séparés concernant les électeurs et le contenu de l'urne, l'exclusivité de l'accès aux données électroniques par les gestionnaires du système, le caractère hermétique et scellé du matériel.
Il rédigera un **rapport** sur ces points. Ce dernier doit être tenu **à la disposition de la CNIL** *(7)*.

La déclaration à la CNIL.
Comme tout dispositif électronique et de stockage informatique de données, le vote électronique doit faire l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés *(8)*.
A ce titre, la CNIL a fait une recommandation relative à la sécurité des systèmes de vote électronique.
Lire la recommandation de la CNIL

Les **organisations syndicales représentatives de salariés** doivent être **informées de l'accomplissement de cette formalité** déclarative auprès de la CNIL.

Les résultats du vote.
Si l'acte qui autorise le recours au vote électronique n'a pas exclu le vote sous enveloppe à bulletin secret, sachez qu'il ne sera pas possible d'obtenir des premiers résultats pendant le scrutin. En effet, le récent décret précise bien qu'**aucun résultat partiel n'est accessible pendant le déroulement du vote.** L'ouverture des enveloppes ne pourra être faite qu'après la clôture du vote électronique *(9)*.

(1) Décret n°2016-1676 du 5 décembre 2016 relatif au vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise
(2) Articles R2314-8 et R2324-4 du Code du travail
(3) Article R2324-6 du Code du travail
(4) Article R2324-7 du Code du travail
(5) Article R2324-8 du Code du travail
(6) Article R2324-9 du Code du travail
(7) Articles R2314-12 et R2324-8 du Code du travail
(8) Articles R2314-14 et R2324-10 du Code du travail
(9) Articles R2314-19 et R2324-15 du Code du travail

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

A Lire aussi :
Nouveautés dans l’organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L’Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage

d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :

- Expert en Informatique **assermenté et indépendant** ;
- **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
- ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
- qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
- et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes

électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Article original de Juritravail : Vote électronique : les 3 points à retenir !

Un guide pour aider les entreprises face à Facebook ou Twitter | Denis JACOPINI

Un guide pour aider les entreprises face à #Facebook ou #Twitter

Le Medef a édité un guide pour informer les entreprises des risques liés aux #réseaux sociaux et des mesures à prendre.

Facebook, Twitter, LinkedIn, Viadeo: les réseaux sociaux n'ont plus secret pour des millions de Français. Les entreprises, elles, ne sont pas forcément à l'aise avec la question. Ces outils, qui sont souvent à la limite des sphères privées et publiques, induisent de nouveaux risques pour les sociétés: se faire dénigrer sur la Toile, se faire usurper son identité, ou voir des salariés, par des conversations sur les réseaux professionnels livrer, sans s'en rendre compte, des informations confidentielles. Pour aider les chefs d'entreprise, le Medef vient d'éditer un guide sur le sujet, intitulé «réseaux sociaux et entreprises, quels enjeux juridiques». Le petit livret est très didactique puisque le premier chapitre consiste à expliquer… ce qu'est un réseau social.

«On s'est rendu compte que les entreprises avaient en la matière des pratiques très différentes. Certaines encouragent leurs salariés à communiquer sur les réseaux sociaux, mais sans fixer aucun cadre. Dans d'autres, la communication est beaucoup plus contrôlée. Certaines ont déjà mené des actions de sensibilisation auprès de leurs salariés, dont une avec une pièce de théâtre», explique-t-on au Medef, où un groupe de travail avait été constitué pour rédiger le guide. D'après une étude du cabinet Proskauer, la manière forte est aussi de mise. 29% des 120 grandes entreprises internationales interrogées ont bloqué l'accès à Twitter, Facebook et autres réseaux sur le lieu de travail, et 27% en contrôlent l'utilisation. A vrai dire, ce sont les PME qui sont le plus «en retard»: elles n'ont souvent pas le temps de se pencher sur la question, ni les moyens de monter des cellules de veille. Le guide est donc là pour les sensibiliser.

Sur ces réseaux, les règles de droit classique – code du travail, code civil, code de la propriété intellectuelle etc… – s'appliquent. Mais il existe également des dispositifs spécifiques. Et tout cela s'entremêle. Le poids d'une charte sur l'utilisation des réseaux sociaux par les salariés ne sera pas le même si cette charte est inscrite dans le règlement intérieur, ou pas. Les salariés ont le droit de parler sur les réseaux de l'organisation et du fonctionnement de l'entreprise, à condition que leurs propos ne soient pas injurieux. L'entreprise elle-même doit évidemment respecter les règles de droit à l'image lorsqu'elle publie sur ces réseaux. Bref, un guide n'est pas de trop dans ce maquis!

Lien pour télécharger le guide

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

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

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

Les meilleurs conseils pour choisir vos mots de passe

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

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

Attaques informatiques : comment les repérer ?

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

Source : http://www.lefigaro.fr/conjoncture/2014/09/11/20002-20140911ARTFIG00296-un-guide-pour-aider-les-entreprises-face-a-facebook-ou-twitter.php

---

Conseils pour assurer la sécurité numérique des nomades | Denis JACOPINI

Même lorsqu'il s'aventure dans le vaste cybermonde, le collaborateur nomade doit avoir accès aux ressources internes de l'entreprise. Il représente alors un danger. Comment se protéger ? Quelques conseils de Gérard Peliks, expert et enseignant en sécurité de l'information.

#Identification et authentification fortes de l'utilisateur
Ce n'est pas l'outil qui doit être tracé, mais l'individu qui s'en sert. « Il s'agit d'identifier et d'authentifier, avec la plus grande attention, l'ayant-droit aux ressources de l'organisation », indique Gérard Peliks, expert et enseignant en sécurité de l'information. Première étape : l'identifiant ou login. Seconde phase : l'authentifiant, autrement dit la preuve de l'identité de l'utilisateur. « Le plus fiable est la combinaison de deux paramètres : ce que l'on a (par exemple une calculatrice, un token usb…) et ce que l'on sait (un code pin). En attendant les solutions de biométrie multimodale… », précise Gérard Peliks.

#Intégrité et confidentialité des transactions
Les échanges entre l'organisation et le collaborateur nomade doivent être sécurisés dans leur confidentialité et leur intégrité. « Il s'agit de créer un tunnel chiffrant dont les deux extrémités sont mutuellement identifiées », souligne Gérard Peliks. Les virtual private networks (VPN) ou réseaux privés virtuels (RPV) garantissent la confidentialité des données transmises, donc vulnérables, sur Internet. La signature électronique peut en garantir l'intégrité. Ce qu'on appelle le protocole de « tunnellisation » ou d'encapsulation consiste à chiffrer les transmissions entre le poste nomade et l'Intranet de l'organisation.

#Chiffrement des données sur disque
En cas de perte ou de vol d'un PC, ou d'un téléphone portable, la confidentialité des informations contenues n'est plus assurée, si elles sont stockées en clair. « On ne perd pas seulement l'objet, mais des données, avec tout ce que cela peut entraîner comme risque d'image, de réputation et même de conséquences juridiques », pointe Gérard Peliks. Tout l'enjeu est donc de rendre illisibles les informations contenues dans l'appareil, si on ne possède pas les clefs pour les déchiffrer. « Le chiffrement de fichiers, de partitions, voire même de l'intégralité du disque, permet de sécuriser les contenus sensibles », explique-t-il.

#Destruction des fichiers
Quand il s'agit d'éliminer un fichier, la touche « delete » et le vidage de la corbeille ne détruisent rien mais se contentent de cacher le document. Et des outils de récupération permettent de pister les anciennes données. Pour effacer définitivement, ou « massicoter » les contenus, il convient d'utiliser des méthodes de suppression sécurisée. « En utilisant des utilitaires de destruction, on s'assure que les fichiers sont réellement passés à la « déchiqueteuse », préservant ainsi leur confidentialité », indique Gérard Peliks.

#Sensibilisation des collaborateurs
Dans un contexte de dématérialisation généralisée, tous les collaborateurs sont potentiellement amenés à travailler un jour en mode nomade, ou avec des collègues en télétravail. D'où l'importance de sensibiliser l'ensemble des collaborateurs de l'organisation aux processus de sécurité. « Dès le début de la collaboration, mais aussi tout au long de la vie du collaborateur dans l'organisation, les règles de sécurité et de confidentialité doivent être rappelées », insiste Gérard Peliks. En plus de faire signer une charte sur l'utilisation du réseau, l'organisation doit communiquer sur les conséquences juridiques de tout manquement au règlement intérieur.

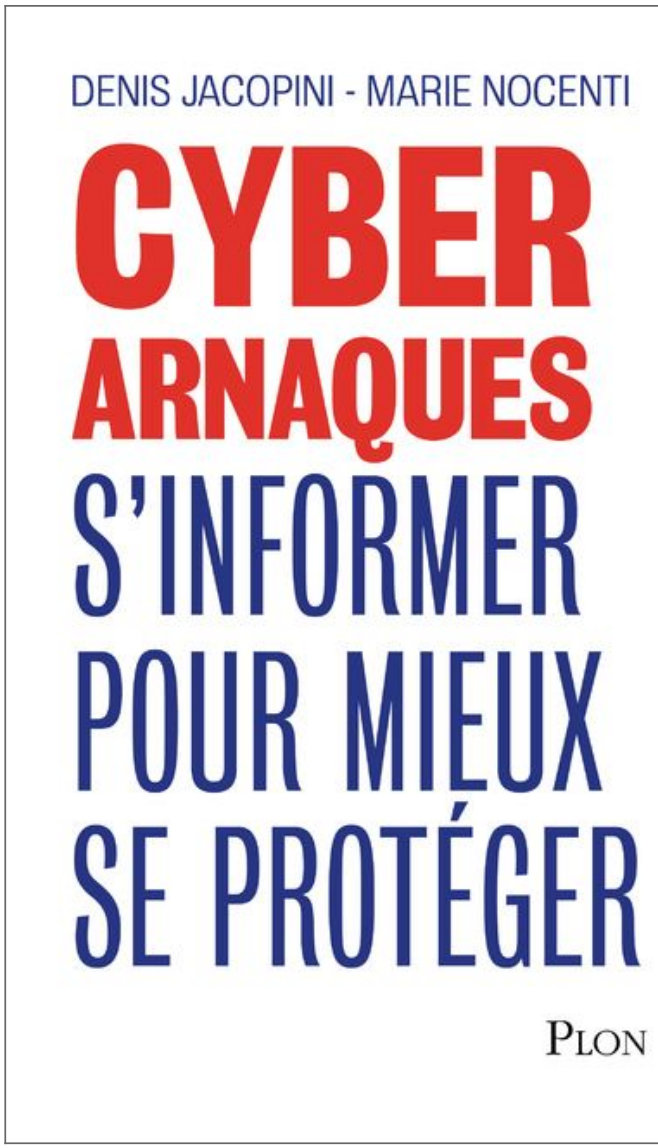
Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

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

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

Source : http://www.lesechos.fr/thema/02167451759-conseils-pour-assurer-la-securite-numerique-des-nomades-1121036.php
Par Julie Le Bolzer

Comment se protéger sur Internet ? Denis JACOPINI vous répond sur Sud Radio à l'occasion de la présentation de son livre « CYBERARNAQUES : S'informer pour mieux se protéger »

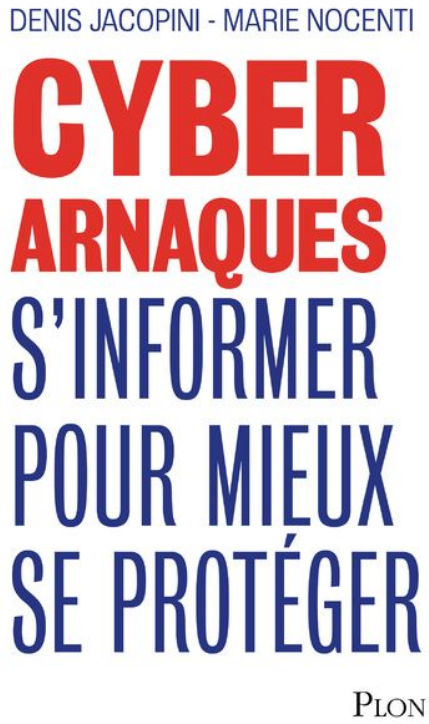


Comment se protéger sur Internet ? Denis JACOPINI vous répond sur Sud Radio à l'occasion de la présentation de son livre « CYBERARNAQUES : S'informer pour mieux se protéger »

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

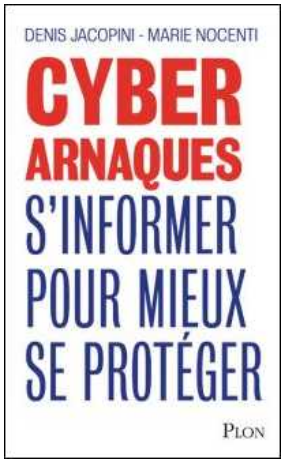
Commandez CYBERARNAQUES



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*

Le site Internet d’une entreprise peut-il être contrôlé à distance par la Cnil ? | Denis JACOPINI

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

La réponse de Benjamin Vialle, agent au service des contrôles, Commission nationale de l’informatique et des libertés.

Oui. Depuis la loi du 17 mars 2014 relative à la consommation, la Commission nationale de l’informatique et des libertés (Cnil) a la possibilité de procéder à des contrôles en ligne, sur internet.
Ils permettent de constater à distance, depuis un ordinateur connecté à internet, des manquements à la loi informatique et libertés. Ces constatations sont relevées dans un procès-verbal adressé aux organismes concernés et leur seront opposables.

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

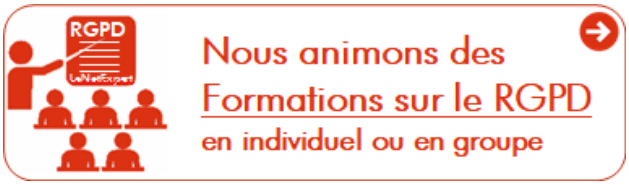
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

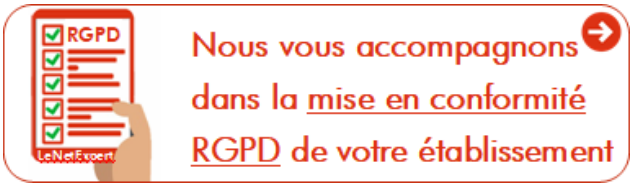
Contactez-nous

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 : http://www.courrierdesmaires.fr/51195/le-site-de-la-mairie-peut-il-etre-controle-a-distance-par-la-cnil

Voici 320 millions de mots de passe … à éviter pour votre cybersécurité !

Le spécialiste en sécurité informatique Troy Hunt a mis à disposition un nouvel outil recensant 320 millions de mots de passe corrompus. Une base de données impressionnante qui devrait limiter de futurs impairs.

Boites mail corrompues, comptes piratés… chaque jour les cas se multiplient : virus et hackers sont bien présents, et ce, partout sur la toile. Personne n'est à l'abri et sans le savoir, vous utilisez peut-être vous-même un mot de passe corrompu. L'expert en sécurité informatique Troy Hunt en a détecté 320 millions !
Sur son site *Have I been pwned ?*, il était déjà possible de savoir si un compte avait été compromis. En indiquant son adresse mail ou son nom d'utilisateur, sans révéler le mot de passe associé, vous pouvez savoir si votre compte a été piraté et fait l'objet d'une fuite de données.
Depuis ce jeudi, le site propose désormais l'outil inverse : une collection de 320 millions de mots de passe consultables, déjà compromis, sans les identifiants associés. Car avec la multiplication des fuites de données, mieux vaut être armé. La CNIL conseille ainsi d'utiliser au moins 12 caractères et 4 types différents (minuscules, majuscules, chiffres et caractères spéciaux). Il faut également en changer régulièrement…[lire la suite]

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

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :
Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez

plainte mais d’après quel article de loi ?
Attaques informatiques : comment les repérer ?

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

Source : *Cyber-sécurité : voici 320 millions de mots de passe … à éviter ! – LCI*

Les 5 règles essentielles pour se protéger de la Cybercriminalité que les PME doivent absolument respecter | Denis JACOPINI

La protection des données numériques est rarement une priorité pour les dirigeants de PME alors même que les petites structures sont de plus en plus affectées par les problèmes de sécurité informatique et de cybercriminalité. Comment protéger votre entreprise ?

Des PME de plus en plus touchées par la cybercriminalité

Les PME n'ont pas toujours conscience d'être devenues les cibles de prédilection des pirates informatiques, et pourtant celles-ci concentrent désormais **près de 80 % des attaques** en France ! Un chiffre en constante augmentation qui démontre un changement de stratégie de la part des *«hackers»* et *«crackers»* qui ciblent les petites structures du fait de leur sécurité souvent défaillante.

Cette montée de la cybercriminalité concerne surtout le **vol de données numériques** (les fichiers clients, les coordonnées bancaires ou les contrats) qui sont ensuite revendues au plus offrant sur le marché noir. On note également des cas d'**espionnages économiques**, d'**escroqueries financières** ou de **sabotages des sites de commerce en ligne**.

Cibler une PME peut aussi être un moyen de s'attaquer à un plus gros poisson, dans le cadre d'une attaque de long terme. Puisqu'en infiltrant le réseau de cette petite structure, il devient plus facile de pénétrer par la suite dans celui d'un grand groupe dont elle est le sous-traitant.

Une problématique sérieuse d'autant que les entreprises victimes de cyberattaques font face à de sévères répercussions en termes de **pertes économiques** et d'**impact sur l'image de marque**. Ce risque peut néanmoins être réduit en appliquant quelques bonnes pratiques.

Les règles essentielles pour bien protéger votre entreprise

1.

Sensibiliser les employés de l'entreprise

Il est recommandé d'organiser une campagne de sensibilisation pour informer les employés sur le danger bien réel de la cybercriminalité en insistant sur la nécessité de :

• choisir des mots de passe d'au moins 12 ou 14 caractères mélangeant chiffres et lettres,
• effectuer des sauvegardes fréquentes sur des supports externes ou une plateforme cloud,
• adopter un usage prudent des messageries électroniques et des systèmes de paiement.

2.

Sécuriser l'ensemble des accès Internet

L'entreprise doit protéger tous les accès Internet (y compris les accès Wi-Fi) qui sont les principaux points d'entrée des pirates. De plus en plus de sociétés choisissent d'ailleurs d'installer un réseau privé virtuel (VPN) comprenant un seul et unique point d'échange sécurisé avec Internet.

3.

Uniformiser les logiciels et les maintenir à jour

Pour faire face aux nouvelles techniques d'attaques, il faut régulièrement mettre à jour les logiciels installés sur votre parc, dont les dernières versions doivent toujours être téléchargées sur les sites officiels des éditeurs. Une démarche qui peut être simplifiée en uniformisant le parc informatique avec un système d'exploitation et un logiciel de protection unique pour l'ensemble des appareils.

4.

Redoubler de vigilance avec les appareils mobiles

Il convient de faire preuve d'une vigilance particulière avec tous les appareils mobiles (smartphones et tablettes tactiles) qui sont généralement beaucoup moins sécurisés que les ordinateurs fixes, car chaque machine constitue une porte d'entrée potentielle pour les attaques informatiques.

5.

Adopter une politique de sécurité informatique

L'entreprise doit enfin mettre en place une politique de sécurité informatique précisant clairement les responsabilités de chacun et les procédures prévues en cas d'attaque, afin que les équipes ne soient pas prises au dépourvu et puissent reprendre l'activité le plus rapidement possible… [Lire la suite]

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

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

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

Les meilleurs conseils pour choisir vos mots de passe

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

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

Attaques informatiques : comment les repérer ?

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

Source : *Cybercriminalité & PME : 5 règles pour se protéger | Microsoft pour les PME*

Mise en conformité RGPD : ce que les PME doivent faire

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 ?

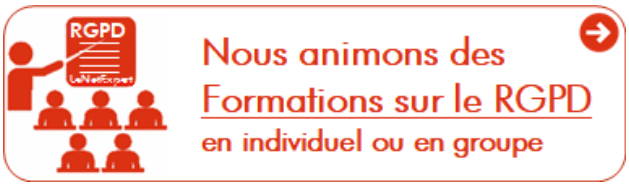
Contactez-nous

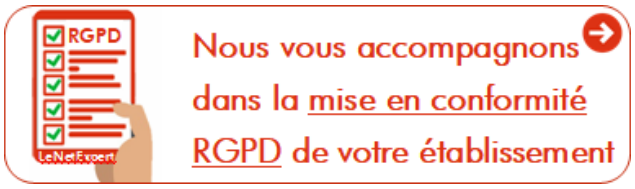
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

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

Pouvez-vous refuser la carte sans contact délivrée par

votre banque ? | Denis JACOPINI

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

Pouvez-vous refuser la carte sans contact délivrée par votre banque ?

La Cnil rappelle que les banques doivent informer leurs clients que leur carte bancaire dispose de la fonction paiement sans contact, une option que ces derniers sont libres de refuser.

En France, plus de 33 millions de cartes de paiement ont des fonctionnalités sans contact, ce qui représente plus de 50 % des cartes en circulation, rappelle la Cnil (Commission nationale de l'informatique des libertés). Grâce à ce système, il est possible d'utiliser sa carte bancaire sans avoir à taper son code secret lorsque les achats sont inférieurs à 20 euros. Depuis la recommandation de la Cnil de juillet 2013, les porteurs de ce type de carte doivent être clairement informés de la fonctionnalité sans contact et doivent pouvoir la refuser.

Comment exercer son droit d'opposition ?

Dans un premier temps, le client doit se tourner vers sa banque pour lui demander la désactivation ou la réédition gratuite d'une nouvelle carte dépourvue de la fonctionnalité paiement sans contact.

Les banques sont libres de choisir les moyens à engager pour respecter ce droit d'opposition. Certaines proposent de distribuer une nouvelle carte identique aux anciens modèles, d'autres incitent à une désactivation via le site internet de la banque.

Si la banque ne respecte pas son devoir d'information ou si elle refuse de désactiver le paiement sans contact, le client peut alors s'adresser au service des plaintes de la Cnil, sur le site internet de la Commision, en appelant le 01 53 73 22 22 (du lundi au vendredi de 10h à 12h et de 14h à 16h) ou en écrivant un courrier à la Cnil – Service des plaintes – 8, rue Vivienne – CS 30223- 75083 Paris cedex 02

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 ?

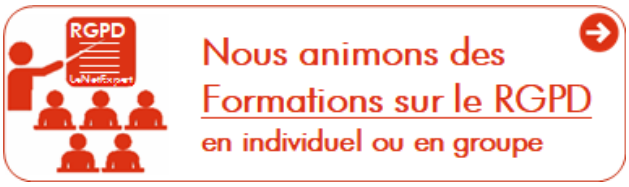
Contactez-nous

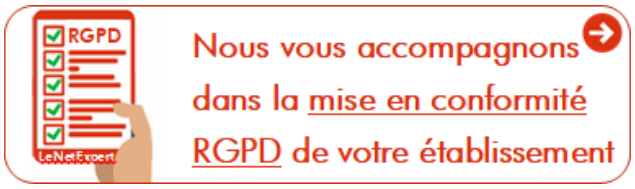
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

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"]
