Quels sont les droits et devoirs des salariés en matière de sécurité informatique | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Quels sont les droits et devoirs des salariés en matière de sécurité informatique				

Il n’est pas rare que des salariés soient surpris en train, au sein de leur entreprise,d’utiliser des outils de type Keylogger – permettant l’enregistrement des touches utilisées sur le clavier – et des logiciels visant à capter et à forcer les mots de passede sessions de systèmes d’exploitation.

Or, dans la majorité des cas, aucune sanction n’est prise par les employeurs, y compris lorsque les auteurs des faits sont animés d’intentions malveillantes et non simplement ludiques.

Dans un raisonnement inspiré du droit du travail, l’employeur – arguant par exemple de ne pas disposer de charte de sécurité informatique spécifiant les comportements à respecter, ainsi que les sanctions applicables – estime qu’à défaut d’avoir porté par écrit à la connaissance de l’employé la réglementation en vigueur au sein de l’entreprise, celui-ci ne peut être légalement sanctionné.

Il est important de rappeler que le seul fait de collecter des données à caractère personnel par un moyen frauduleux est puni de cinq ans d’emprisonnement et de 300 000 euros d’amende (article 226-18 du Code pénal) et ce, quelles que soient les intentions du salarié. De même, le fait de s’introduire frauduleusement dans tout ou partie d’un système de traitement automatisé de données est puni de deux ans de prison et de 30 000 euros d’amende (article 321-1 du même code). La loi est d’application directe et ne nécessite pas d’être citée dans une charte informatique pour en assurer le respect par les salariés. Les employeurs peuvent donc prendre immédiatement les sanctions afférentes à une telle faute.
En outre, la responsabilité de l’employeur peut se voir engagée par ce type d’agissements, sur la base de plusieurs fondements :
• la personne cible/victime des menées de son/ses collègues pourra, en cas de dommage, agir contre l’employeur, responsable de ses salariés. Il reviendra alors à la société de prouver que le mis en cause a agi « hors des fonctions auxquelles il était employé, sans autorisation et à des fins étrangères à ses attributions », ce qui est rarement admis en pratique.
• de par la jurisprudence « Sarenza c/ Jonathan » du 21 février 2013, le juge a précisé que la société devait supporter, à hauteur de 30%, son propre dommage, engendré par les lacunes dans la gestion des identifiants d’accès aux bases de données. Le juge a donc instauré l’obligation, pour l’employeur, de mettre en place des mesures de protection informatique efficaces, afin de prévenir l’installation de tout logiciel espion.
• Enfin, la plupart des logiciels utilisés à ces fins proviennent de téléchargements, susceptibles de contenir des virus. Les réseaux internes des entreprises sont régulièrement infectés par ce biais, ce qui facilite les intrusions informatiques et, partant, l’accès, l’utilisation, l’extraction, voire la destruction de données stratégiques pour l’entreprise.

Préconisations de la DGSI
La DGSI recommande à toute entreprise :
• En priorité, d’établir une charte de sécurité informatique qui permettra de sensibiliser les salariés aux enjeux numériques, tout en les responsabilisant.
• D’organiser régulièrement des conférences de sensibilisation à destination de l’ensemble des collaborateurs, qui insisteront sur leurs droits et obligations à l’ère du tout-numérique et dispenseront des mises à jour sur les évolutions technologiques en cours.
• De mettre en place des mesures de protection efficaces afin de prévenir l’utilisation potentielle de logiciels et matériels espions. L’existence de tels dispositifs de sécurité informatique permettra à l’employeur de dégager sa responsabilité juridique et d’optimiser le bon fonctionnement de son entreprise en augmentant le niveau de protection.

Vous avez besoin de recueillir des preuves, expertiser un système informatique, vérifier des contenus, Denis JACOPINI peut vous conseiller, vous accompagner et réaliser toutes les phases techniques nécessaires à la constitution d’un dossier juridique solide.
Contactez Denis JACOPINI

Réagissez à cet article

Quelques articles sélectionnés par nos Experts :

Quels sont les droits et devoirs des salariés en matière de sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

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

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

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)

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

Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?

Contactez-nous

Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a 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 (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.

« *Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services.* ».

Source : http://www.ccirezo-normandie.fr/document/104108-flash-ingerence-economique-n-15-rappel-des-droits-et-devoirs-des-salaries-en-entrepr

---

La cybersécurité pour les débutants – Un lexique informatique

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	La cybersécurité pour les débutants – Un lexique informatique				

Ce texte page 2254 de mon chapitre de Thomas, Denis Diderot dans Tome 1 sur les arts et métiers/Tome 1 et Tome 2 sur les Tome 2 sur les Métiers

ABC

Abc, Abc (genre) (Logiciel textuelle) (nom, Domaine du Développement Numérique Algorithmique), technologie de communication permettant de fonctionnaire de l'information (nom d'Internet) par exemple) à tout abcd sur les fils de nouvel activité (notamment pour les logiciel Développement 2011) (nom 1990), il est possible d'utiliser des abcd(s) pour de fils (applicatif) à nous des numéroteurs.

A.F.A.I.C.

Association Française pour la Promotion d'Internet de Confiance, (ex-pour la capacité des ordre de Nouvelle Français), 1 rue Jacques, 1, 75000 Paris (Paris) de Nouvelle, 1, rue Charles-Lindbergh, 1 Cédex 14 Paris

---

Réagissez à cet article

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

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

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

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

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle… ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Original de l’article mis en page : Lexique – La préfecture de Police

Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Formation RGPD pour TPE / PME / DPO / Délégué à la Protection des Données et formation RGPD pour SSII, ESN, Avocats, Experts comptables et consultants				

Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

2 SOLUTIONS POUR SE METTRE EN CONFORMITÉ AVEC LE RGPD

1.

Vous apprenez à vous mettre en conformité avec le RGPD en suivant une formation (ci-dessous) ;

2.

Vous faites appel à un expert / formateur qui vous accompagne dans votre mise en conformité avec le RGPD de votre établissement (Consultez notre page « Services d'accompagnement à la mise en conformité avec le RGPD »).

Je me présente : Denis JACOPINI. Je suis Expert de justice en informatique **spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel)**, consultant depuis 1996 et formateur depuis 1998. J'ai 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 (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi aisé d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

Pour cela, j'ai créé 3 niveaux de formation.

1. Une formation d'une journée pour les indépendants, TPE et les PME « **Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer** ». Cette formation a pour objectif de vous faire découvrir l'essentiel de ce règlement Européen, de vous apprendre les principes du RGPD permettant à la fois de comprendre l'intérêt de la démarche de mise en conformité RGPD et de réaliser les premières actions ;
2. Une formation de deux jours pour les DPO « **Je veux devenir le Délégué à la Protection des Données de mon établissement** ». Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement ;
3. Une formation sur 4 jours pour les consultants « **J'accompagne mes clients dans leur mise en conformité avec le RGPD** ». Vous êtes une société d'Informatique, un cabinet d'avocat, un cabinet d'expertise comptable et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation est composée de 2 jours de théorie et 2 jours de pratique dont 1 dans l'établissement de votre choix (le votre ou celui d'un client). Suivez LA formation qui vous apportera la plus grande autonomie avec le RGPD de tout notre catalogue.

et des services sur mesure.

1. Vous souhaitez tout faire -> Nous vous apprendrons à mettre votre établissement en conformité. La plupart du temps, le contenu de ces formations est personnalisé et adapté à vos besoins spécifiques ;
2. Vous ne savez pas par où commencer -> Nous ferons l'état des lieux, mettrons en place le registre puis nous vous apprendrons à maintenir la conformité des traitements ;
3. Vous ne souhaitez rien faire -> Nous nous occuperons de tout.

Plus d'information sur nos services d'accompagnement
à la mise en conformité avec le RGPD ici

Formation pour TPE/PME « Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer » : 1 jour
(Découvrez et comprenez la démarche de mise en conformité)

Découvrez l'essentiel du RGPD, apprenez les principes du RGPD permettant à la fois de comprendre l'intérêt de la démarche de mise en conformité RGPD et de réaliser les premières actions.
Consultez les dates de nos prochaines formations
« Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »

Formation pour DPO « Je veux devenir le Délégué à la Protection des Données de mon établissement » : 2 jours
(Mettez en place une démarche de mise en conformité RGPD)

Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement.
Consultez les dates de nos prochaines formations
« Je veux devenir le Délégué à la Protection des Données de mon établissement »

Formation pour consultants « J'accompagne mes clients dans leur mise en conformité avec le RGPD » : 3 jours + 1 jour dans votre établissement
(C'est le moment ou jamais de vendre des services autour du RGPD)

Enfin, si votre objectif est avant tout de développer l'activité de mise en conformité avec le RGPD afin de vendre cette prestation auprès de vos clients, cette formation est faite sur-mesure pour vous en vous apportant l'ensemble des mesures et des cas qu'il est nécessaire de maîtriser pour que vos clients soient mis sur le chemin de la mise en conformité. Vous êtes une société d'Informatique, un cabinet d'avocat, un cabinet d'expertise comptable, un consultant et souhaitez accompagner vos clients dans leur mise en conformité avec le RGPD, cette formation se passe sur 3 jours en groupe plus une journée supplémentaire en individuel pour superviser la mise en place du RGPD dans votre établissement ou chez un de vos clients (frais liés au déplacement dans cet établissement en sus). Suivez LA formation qui vous apportera la plus grande autonomie dans la mise en conformité de tout notre catalogue.
Consultez les dates de nos prochaines formations
« J'accompagne mes clients dans leur mise en conformité avec le RGPD »

Formation RGPD « Mise en conformité RGPD sur mesure » (pour TPE/PME)
(Pour ceux qui souhaitent une formation ou un accompagnement personnalisé dans la mise en conformité RGPD)

Que ayez bientôt ou déjà désigné « Délégué à la Protection des Données » ou « DPO » dans votre établissement, si vous souhaitez que nous établissions un programme de formation personnalisé dans son contenu ou dans son organisation, nous nous ferons un plaisir d'étudier votre demande et d'élaborer une proposition adaptée à vos besoins.

Accompagnement à la mise en conformité RGPD de mon établissement

Vous souhaitez vous mettre en conformité avec le Règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 (dit RGPD) et vous souhaitez vous faire accompagner. Au fil des années et depuis les mises en conformité avec la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nous avons constaté que les mises en conformité devaient se dérouler (et encore à ce jour avec le RGPD) selon 3 phases principales :

1. « Analyse du contexte » en vue d'établir la liste des traitements et les mesures correctives à adopter ;
2. « Mise en place de la conformité RGPD » avec amélioration des traitements en vue de les rendre acceptables ou conformes. Ceci inclue dans bien des cas l'analyse de risque ;
3. « Suivi de l'évolution des traitements » en fonction de l'évolution du contexte juridique relatif à la protection des Données à Caractère Personnel et des risques Cyber. Ce suivi a pour principal intérêt de maintenir votre conformité avec le RGPD dans le temps.

Pour chacune des phases, nous vous laissons une totale liberté et vous choisissez si vous souhaitez :

- « Apprendre à faire » (nous vous apprenons pour une totale autonomie) ;
- « Faire » ;
- ou « Nous laisser faire ».

Afin de vous communiquer une indication du coût d'un tel accompagnement, nous aurons besoin d'éléments sur votre structure : Durée dépendant de la taille, de l'activité et des ressources de votre établissement.

N'hésitez pas à contacter notre équipe.

Intéressé pour assister à une de nos sessions de formation en France, choisissez la ville qui vous intéresse. Vous souhaitiez que nous nous déplacions au sein de votre établissement pour une formation ou pour un accompagnement individuel, indiquez-le dans les commentaires.

Votre Prénom / NOM (obligatoire)

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (pour faciliter l'organisation)

Vous souhaitez avoir des informations sur :

☐ - la formation « Comprendre le RGPD » : 1 jour
☐ - la formation « Je veux devenir Délégué à la Protection des Données » 2 jours
☐ - la formation « Je mets en conformité mon établissement » 3+1 jours
☐ - la formation « Mise en conformité RGPD sur mesure »
☐ - un accompagnement personnalisé au RGPD

Vous souhaitez réserver une ou plusieurs place(s) à la formation :

Formation pour TPE/PME : **« Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »**

Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour DPO : **« Je veux devenir le Délégué à la Protection des Données de mon établissement »**

Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour consultants : **« J'accompagne mes clients dans leur mise en conformité avec le RGPD »**

Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

☐Autre ville ou sujets souhaités en individuel (indiquez ci-dessous)

Votre message avec vos préférences de date ou vos commentaires

Envoyer

Nos formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre acompte. Si la formation était annulée (nombre de participants insuffisants ou en cas de force majeure), votre acompte sera remboursé en intégralité dans les 5 jours (les chèques seront encaissés à partir du jour de la formation). En cas d'annulation de votre part moins de 48 heures avant la formation, l'acompte pourra ne pas être remboursé car destiné à régler les frais de réservation de salle et d'organisation, eux même non remboursables.

LE FORMATEUR : Denis JACOPINI

Denis JACOPINI est Expert de Justice en informatique spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel). Il est diplômé en Cybercriminalité, e, Droit de l'Expertise Judiciaire et est Certifié en Gestion des Risques des Systèmes d' Information. IL est formateur depuis 1998 et consultant depuis 1996, il a 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 dans la sécurité informatique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD à tout public.

« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

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

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

Contactez-nous

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

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

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

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

Quelques articles sélectionnés par nos Experts :

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

Réagissez à cet article

Source : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes*

Info pratique : Attitude à adopter en cas de réception d’un e-mail étrange voire douteux | Denis JACOPINI

Info pratique : Attitude à adopter en cas de réception d’un e-mail étrange voire douteux
Vous recevez un e-mail étrange voire douteux, vous craignez être victime d’une arnaque ? Apprenez à les identifier et adoptez une attitude visant à contribuer à la destruction de ces réseaux.

Les meilleurs conseils pour choisir vos mots de passe | Denis JACOPINI

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

Réagissez à cet article

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

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

Les meilleurs conseils pour choisir vos mots de passe

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

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

Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

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

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.*
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle… ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

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

Les PME face à la cybercriminalité – Quelques règles de bon sens… | Denis

JACOPINI

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

Les PME face à la cybercriminalité – Quelques règles de bon sens…

Face à l'« industrialisation » de la cybercriminalité, aucune entreprise n'est à l'abri, pas même les plus petites. Il est désormais indispensable de s'y préparer pour éviter des déconvenues qui peuvent se révéler très coûteuses.

De plus en plus variées, les techniques des cybercriminels s'industrialisent.
Un montant impressionnant : 445 milliards de dollars, soit 327 milliards d'euros, c'est le coût annuel de la cybercriminalité et de l'espionnage économique au niveau mondial, selon le Center for Strategic and International Studies (CSIS). Et il n'a sans doute pas fini de croître. « La cybercriminalité ne cesse de se développer et les attaques sont de plus en plus variées et sophistiquées, touchant toutes les entreprises, quelle que soit leur taille », assure Paul-Henri Huckel, consultant au sein du cabinet de conseil en stratégie des systèmes d'information et de la cybersécurité Lexsi.

Virus bancaire permettant d'effectuer des virements frauduleux ; destruction de sites Web d'entreprises d'e-commerce ; vol de données revendues à un concurrent ; « ransomware », autrement dit cryptage de toutes les données d'une entreprise « libérables » après versement d'une rançon… les techniques des cybercriminels s'industrialisent.

Le courrier électronique, maillon faible du système
« La première erreur est de penser que l'on est à l'abri, parce que l'on est petit », prévient Paul-Henri Huckel. Selon un rapport publié en avril 2014 par l'éditeur de logiciels Symantec, 30 % des attaques ciblées visent les PME. « Les dirigeants de petites entreprises ne sont pas suffisamment sensibilisés. Certaines sociétés n'ont même pas mis en place de système de sauvegarde de leurs données. Or, leur perte peut, dans certains cas, entraîner la fermeture de l'entreprise », remarque aussi Frédéric Desclos, responsable de l'Echangeur PME, espace de la chambre de commerce et d'industrie Paris Ile-de-France consacré à la sensibilisation et à la formation aux technologies de l'information des petites et moyennes entreprises.
Face à ce risque croissant de cyberattaque, sécuriser son système d'information est indispensable. Le courrier électronique est le maillon faible du système : selon Symantec, un message électronique sur 392 contiendrait une attaque de « phishing », ces faux courriers officiels destinés à détourner les coordonnées bancaires.

Les mots de passe doivent être modifiés au moins tous les six mois
« Il est indispensable de sensibiliser les salariés à cet aspect, ainsi qu'au caractère critique des mots de passe qui doivent être modifiés régulièrement, au moins tous les six mois », remarque Frédéric Desclos. Ce qui n'empêche pas, par ailleurs, de sécuriser au maximum son système d'information par le biais d'antivirus, d'anti-spam et de firewalls efficaces. « Un plan de sauvegarde des données est également indispensable », complète Paul-Henri Huckel. Une procédure qui n'est pas forcément coûteuse. Il suffit par exemple au dirigeant de l'entreprise de quitter chaque soir son bureau avec sa sauvegarde sous le bras…

Réagissez à cet article

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

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

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se**

protéger des pirates informatiques.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

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

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.*
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Source : Jean-Marc Engelhard
http://www.leparisien.fr/economie/les-pme-face-a-la-cybercriminalite-15-09-2014-4136531.php

Comment protéger son site internet des pirates

informatiques ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Comment protéger son site internet des pirates informatiques ?				

Il n’y a rien de plus stressant que de se faire hacker ou pirater un compte. Cependant, les criminels virtuels ne s’attaquent pas seulement à votre identité, ils prennent votre argent ou même la source de vos revenus. Ici, cette source ce sont les commerces en ligne et les sites web de vente. Que faire pour y remédier ?

La première précaution quand il s’agit de se protéger contre le piratage ? Mettre un plug-in de sécurité sur votre CMS. La deuxième précaution consiste à changer les droits de vos fichiers. Néanmoins, cette option n’est pas sans difficulté, car certains hébergeurs refusent ce genre de modification. Une autre astuce serait de sauvegarder régulièrement vos données pour pouvoir l’effacer en cas de piratages afin de ne laisser aucune trace de ce dernier. Dans le cas contraire, il est fort possible que vous perdiez votre crédibilité auprès de vos internautes et clients.
Pour conclure, le piratage est un sujet et un fléau courant actuellement, qu’il est toutefois possible de contrôler. Par contre, les pirates ne s’arrêtent jamais. Ils peuvent revenir pour hacker votre site ou votre serveur : une mise à jour constante de votre système de protection est donc de mise…[lire la suite]

Conseil de Denis JACOPINI :
Nous remarquons de nombreux piratages causés par une relation physique ou logique avec votre Système Informatique d’entreprise. Une autre recommandation consiste en plus de les héberger sur des machines différentes, à utiliser des identifiants et des mots de passe évidemment complexes mais aussi différents non seulement pour chacun de services du site Internet mais surtout des autres éléments de votre Système Informatique.

Réagissez à cet article

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

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

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

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

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Source : *Piratage informatique : comment protéger son site internet ?*

Les grands principes de la cryptologie et du chiffrement

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Les grands principes de la cryptologie et du chiffrement				

Historiquement, la cryptologie correspond à la science du secret, c'est-à-dire au chiffrement. Aujourd'hui, elle s'est élargie au fait de prouver qui est l'auteur d'un message et s'il a été modifié ou non, grâce aux signatures numériques et aux fonctions de hachage. À l'occasion du mois européen de la cybersécurité, la CNIL vous explique ce que c'est et à quoi ça sert.

Étymologiquement, la cryptologie est la science (λόγος) du secret (κρυπτός) . Elle réunit la cryptographie (« écriture secrète ») et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie).
La cryptologie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions : assurer l'**authenticité** d'un message (qui a envoyé ce message ?) ou encore assurer son **intégrité** (est-ce qu'il a été modifié ?).
Pour assurer ces usages, la cryptologie regroupe quatre principales fonctions : le hachage avec ou sans clé, la signature numérique et le chiffrement.
Pour expliquer la cryptologie, nous utiliserons dans nos exemples les personnages traditionnels en cryptographie : Alice et Bob.
Pour découvrir les grandes phases de l'histoire de la cryptologie, rendez-vous sur le webdocumentaire réalisé par l'ANSSI.

Pourquoi la cryptologie existe-t-elle ?

1.

Pour assurer l'intégrité du message : le hachage

La cryptologie permet justement de détecter si le message, ou l'information, a été involontairement modifié. Ainsi, une « **fonction de hachage** » permettra d'associer à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous. Cette empreinte est souvent matérialisée par une longue suite de chiffres et de lettres précédées du nom de l'algorithme utilisé, par exemple « SHA2» ou « SHA256 ».
Il ne faut pas confondre le chiffrement, qui permet d'assurer la confidentialité, c'est-à-dire que seules les personnes visées peuvent y avoir accès (voir « **Pour assurer la confidentialité du message** »), et le hachage qui permet de garantir que le message est intègre, c'est-à-dire qu'il n'a pas été modifié.
Le hachage, pour quoi faire ?
Pour sauvegarder vos photos sur votre espace d'hébergement (de type « cloud » par exemple) et vérifier que votre téléchargement s'est bien déroulé ?
Pour sychroniser vos dossiers et détecter ceux qu'il faut sauvegarder à nouveau et ceux qui n'ont pas été modifiés ?

Il existe aussi des « **fonctions de hachage à clé** » qui permettent de rendre le calcul de l'empreinte différent en fonction de la clé utilisée. Avec celles-ci, pour calculer une empreinte, on utilise une clé secrète. Pour deux clés différentes l'empreinte obtenue sur un même message sera différente. Donc pour qu'Alice et Bob calculent la même empreinte, ils doivent tous les deux utiliser la même clé.
C'est parmi ces fonctions de hachage à clé que l'on trouve celles utilisées pour stocker les mots de passe de façon sécurisée.
Le hachage à clé, pour quoi faire ?
Votre service préféré reconnait votre mot de passe quand vous vous connectez ?
Vous voulez pouvoir détecter si quelqu'un modifie des documents sans vous le dire ?

2.

Pour assurer l'authenticité du message : la signature

Au même titre que pour un document administratif ou un contrat sur support papier, le mécanisme de la « **signature** » – numérique – permet de vérifier qu'un message a bien été envoyé par le détenteur d'une « clé publique ». Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

La signature numérique, pour quoi faire ?
Vous voulez garantir être l'émetteur d'un courriel ?
Vous voulez vous assurer qu'une information provient d'une source sûre ?
Pour pouvoir signer, Alice doit se munir d'une paire de clés :
• l'une, dite « publique », qui peut être accessible à tous et en particulier à Bob qui est le destinataire des messages qu'envoie Alice ;
• l'autre, dite « privée », qui ne doit être connue que d'Alice.
En pratique, Alice génère sa signature avec sa clé privée qui n'est connue que d'elle. N'importe quelle personne ayant accès à la clé publique d'Alice, dont Bob, peut vérifier la signature sans échanger de secret.

3.

Pour assurer la confidentialité du message : le chiffrement

Le chiffrement d'un message permet justement de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connaissent le contenu. C'est une sorte d'enveloppe scellée numérique. Une fois chiffré, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.
Le chiffrement, pour quoi faire ?
Vous voulez vous assurer que seul le destinataire ait accès au message ?
Vous souhaitez envoyer ces informations sous enveloppe numérique et non lisible par tous comme sur une carte postale ?
Il existe deux grandes familles de chiffrement : le chiffrement symétrique et le chiffrement asymétrique.
Le **chiffrement symétrique** permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée alors la « clé secrète ». Le chiffrement symétrique est particulièrement rapide mais nécessite que l'émetteur et le destinataire se mettent d'accord sur une clé secrète commune ou se la transmettent par un autre canal. Celui-ci doit être choisi avec précautions, sans quoi la clé pourrait être récupérée par les mauvaises personnes, ce qui n'assurerait plus la confidentialité du message.
Le **chiffrement asymétrique** suppose que le (futur) destinataire est muni d'une paire de clés (clé privée, clé publique) et qu'il a fait en sorte que les émetteurs potentiels aient accès à sa clé publique. Dans ce cas, l'émetteur utilise la clé publique du destinataire pour chiffrer le message tandis que le destinataire utilise sa clé privée pour le déchiffrer.
Parmi ses avantages, la clé publique peut être connue de tous et publiée. Mais attention : il est nécessaire que les émetteurs aient confiance en l'origine de la clé publique, qu'ils soient sûrs qu'il s'agit bien de celle du destinataire.
Autre point fort : plus besoin de partager une même clé secrète ! Le chiffrement asymétrique permet de s'en dispenser. Mais il est malheureusement plus lent.
Pour cette dernière raison, il existe une technique combinant chiffrements « symétrique » et « asymétrique », mieux connue sous le nom de « **chiffrement hybride** ».
Cette fois, une clé secrète est déterminée par une des deux parties souhaitant communiquer et celle-ci est envoyée chiffrée par un chiffrement asymétrique. Une fois connue des deux parties, celles-ci communiquent en chiffrant symétriquement leurs échanges. Cette technique est notamment appliquée lorsque **vous visitez un site dont l'adresse débute par « https ».**

Réagissez à cet article

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

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

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

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

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Source : https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

Le livre du jour : CYBERARNAQUES – a l’écoute des livres, Radio Massabielle (97.8 Mhz et 101.8 Mhz)

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Le livre du jour : CYBERARNAQUES – a l’écoute des livres, Radio Massabielle (97.8 Mhz et 101.8 Mhz)				

Comme les langues d’ Esope, Internet peu être la meilleure et la pire des choses. En effet s’il permet de relier les femmes et les hommes à travers le monde, de travailler, de s’informer, etc.. il es également le point de toutes sortes d’escrocs. Aussi, en répondant à une annonce ou au message que vous pensez être envoyé par un ami, vous risquez de voir votre compte en banque vidé ou d’être victime d’un chantage.
Les CYBERARNAQUES sont légion et il convient de s’informer pour mieux protéger votre famille et vos biens.
Combien d’entre-nous n’on pas vérifié…[lire la suite]

Réagissez à cet article

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

Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.
Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.
Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?
Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.
Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !
Commandez sur Fnac.fr

---

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

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

Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

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

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : *Le livre du jour : CYBERARNAQUES – a l'écoute des livres*

Objets connectés : les inquiétantes failles de sécurité dont vous n'avez pas conscience | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Objets connectés : les inquiétantes failles de sécurité dont vous n'avez pas conscience				

Les objets connectés doivent-ils vraiment recueillir autant de données personnelles pour fonctionner correctement ? Télévision, pèse-personne, thermostat et autres hubs domotiques… les objets connectés tentent d'envahir nos maisons et de s'infiltrer au coeur même de leur réseau numérique.

Pourtant, malgré leur objectif de nous simpliflier la vie, leur développement semble encore assez poussif ; en raison sans doute de leur manque criant de sécurité. C'est ce que révèle une étude menée par la division Sécurité de Hewlett Packard : rien de moins que 250 vulnérabilités ont été relevées par les experts d'HP Fortify au sein des 10 objets connectés les plus populaires.
Ces failles de sécurité seraient, selon Mike Amistead, le manager général d'HP Fortify, le symptome de la ruée des entreprises sur le créneau des objets connectés. Il estime en effet que les start-ups se lançant sur ce marché tenteraient de commercialiser leur produit le plus rapidement possible avant la concurrence… au mépris de la garantie d'un niveau de sécurité suffisant des réseaux et des données personnelles.
Vos données personnelles en clair sur la toile Parmi les failles de sécurité relevées, HP a constaté que :
• 90 % des objets connectés étudiés solliciteraient une information personnelle sensible (ex : adresse email ou postale, nom, date de naissance, etc) ; une information ensuite véhiculée en clair sur la toile ;
• 70 % des objets connectés ne crypteraient pas les données échangées avec le réseau ;
• 80 % des objets connectés ne nécessiteraient pas de mot de passe complexe pour identifier les demandes de connexion tierces ;
• 60 % des objets connectés seraient vulnérables aux attaques dites de « cross-site scripting » (type de faille de sécurité permettant d'injecter du contenu dans une page, et provoquant ainsi des actions sur les navigateurs web visitant la page).

Réagissez à cet article

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

Quel est notre métier ?
Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS
- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

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

« *Mon métier consiste à mettre à votre disposition*

l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Source :

http://www.archimag.com/vie-numerique/2014/07/30/objets-connectes-internet-failles-securit