

Rançongiciel et hameçonnage : quelle démarche entreprendre si vous êtes la cible d'une cyberattaque ?



Rançongiciel
et
hameçonnage
: quelle
démarche
entreprendre
si vous êtes
la cible
d'une
cyberattaque
?

Les ordinateurs contiennent des documents privés et données confidentielles (renseignements personnels, identifiants bancaires, codes secrets) qui peuvent être convoités par une tierce personne mal intentionnée. En cas de cyberattaque, il est important de savoir réagir vite pour se protéger d'une utilisation frauduleuse de vos données personnelles. Nous expliquons ici les principales cybermenaces qui planent sur les internautes, les recommandations de sécurité pour s'en prémunir et, surtout, comment agir si vous êtes la victime d'un cybercriminel.

Les recommandations de sécurité pour se protéger des cyber-escrocs

Selon l'ANSII (agence nationale de la sécurité des systèmes d'information), il vous est fortement conseillé de respecter quelques règles simples pour vous protéger contre les cyberattaques. Effectuer des sauvegardes régulières de vos fichiers importants sur des supports de stockage amovibles (CD, clé USB, disque dur externe). Mettre à jour régulièrement les principaux logiciels de vos appareils numériques (ex : Windows, antivirus, lecteur PDF, navigateur, etc.) en privilégiant leur mise à jour automatique. Ne pas avoir une confiance aveugle dans le nom de l'expéditeur de l'email. En cas de doute, n'hésitez pas à contacter directement l'expéditeur par un autre moyen de communication. Se méfier de courriel type « hameçonnage ciblé » qui vous propose un contenu personnalisé pour mieux tromper votre vigilance. Ne pas ouvrir les pièces jointes et ne pas suivre les liens des messages électroniques douteux (fautes d'orthographe, caractères accentués, nom des pièces jointes trop succinct). Ne jamais répondre à une demande d'information confidentielle par courriel.

En cas de cyber-attaque, il faut immédiatement déconnecter du réseau tout appareil susceptible d'être infecté et alerter au plus vite le responsable de sécurité ou le service informatique. Dans le cadre d'un rançongiciel, il est primordial de ne pas payer la rançon, car il n'est nullement garanti que la victime récupère la clé de déchiffrement qui lui permettra de récupérer l'accès à ses données personnelles.

Comment réagir si vous êtes victime d'un rançongiciel ou d'hameçonnage ?

Vous devez vous rendre dans un commissariat de police ou une brigade de gendarmerie pour déposer plainte, ou bien adresser un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

Pour mener correctement l'enquête, il faudra fournir les renseignements suivants.

- Les références du (ou des) transfert(s) d'argent effectué(s).
- Les informations de la (ou des) personne(s) contactée(s) : pseudos utilisés, adresse de messagerie ou adresse postale, numéros de téléphone, fax, copie des courriels...
- Le numéro complet de la carte bancaire ayant servi au paiement, la référence de votre banque et de votre compte, et la copie du relevé de compte bancaire où apparaît le débit frauduleux.
- Tout autre renseignement utile à l'identification du cyber-escroc.

Vous pouvez également utiliser la plateforme de signalement Pharos ou le numéro de téléphone dédié : 0811 02 02 17 pour signaler les faits dont vous avez été victime. La suite de l'enquête sera prise en charge par des services spécialisés...[lire la suite]

NOTRE MÉTIER :

- FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO
- EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES
- AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT
 - MISE EN CONFORMITE RGPD / FORMATION DPO

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, suivez nos formations ;

EXPERTISES TECHNIQUES : Dans le but de prouver un dysfonctionnement, de déposer ou vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettrons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : *Rançongiciel et hameçonnage : quelle démarche entreprendre si vous êtes la cible d'une cyberattaque ?*

Tout ce que vous ne savez pas sur les clés USB | Denis JACOPINI



La majorité des personnes savent très bien que la clé USB est un support de stockage amovible, c'est ce qui leur fait penser qu'une clé USB permet uniquement de stocker des fichiers à partir de tout système disposant de prises USB ou de transférer des données entre ordinateur. Or la clé USB peut être utilisée de plusieurs manières différentes.



Aujourd'hui, je vais vous montrer qu'il existe d'autres fonctions plus intéressantes qu'on peut leur utiliser à l'aide d'une simple clé USB.

1. Transformer votre clé USB en une barrette mémoire RAM

Une clé USB peut être utilisée pour améliorer les performances de votre ordinateur et augmenter la vitesse de son fonctionnement. L'astuce consiste à utiliser une clé USB pour augmenter la mémoire de votre ordinateur et booster ses performances à l'aide de logiciel eBoostr. Pour en savoir plus, je vous invite à lire cet article: l'utilisation de clé USB en tant que barrette.

2. Sécuriser votre PC avec une clé USB

On peut aussi utiliser une clé USB pour sécuriser son PC. L'utilitaire Rohos Logon Key fera en sorte que votre ordinateur s'ouvrira automatiquement au moment où vous insérerez la clé USB et se verrouillera lorsque vous la retirerez. Vous pourrez donc quitter votre ordinateur en toute sérénité. Pour en savoir plus, je vous invite à lire l'article suivant: la sécurité de votre pc avec une clé USB

3. Création d'une clé USB rootkit

Une autre fonction qu'on peut l'utiliser avec une clé USB, c'est la récupération des mots de passe d'un ordinateur. La clé USB s'exécute automatiquement et récupère la plupart des mots de passe stockés sur votre ordinateur. Il est vraiment très utile surtout quand on perd les mots de passe. Pour en savoir les étapes pour créer une clé USB rootkit, je vous invite à lire cet article: création d'une clé USB rootkit.

4. Injecter une backdoor dans une machine Windows avec une clé USB

On peut aussi utiliser une clé USB pour accéder à votre PC à distance depuis n'importe quelle machine. Pour créer votre USB backdoor suivez les étapes de notre article: injection d'une backdoor dans une machine Windows avec une clé USB.

5. Emporter dans une clé USB vos logiciels préférés sans avoir besoin de les installer

Enfin, une autre fonction qui pourrait vous intéresser: c'est d'utiliser des logiciels stockés sur votre clé USB sans avoir besoin de les installer. Pour cela, il faut installer le programme gratuit **PortableApps**.

Il devient alors très facile d'ajouter vos logiciels préférés au lanceur d'applications portable « PortableApps ». Un outil principalement destiné aux développeurs qui enrichit et complète la suite logicielle référence en la matière. Le logiciel Open Source PortableApps propose déjà un panel très large d'applications portables : Firefox, LibreOffice, Google Chrome, Skype ou encore Dropbox. Ce lanceur vous permet d'utiliser les logiciels stockés sur la clé USB depuis un autre PC sans avoir à les installer.

Comme nous l'avons vu précédemment, une clé USB peut servir à autre chose qu'à stocker des données. Elle possède d'autres avantages. Si vous avez d'autres fonctions d'une clé USB, n'hésitez pas de les partager avec nous dans un commentaire. □

Article original de Ahmed



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

10 bonnes pratiques pour des soldes sur Internet en sécurité

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

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
	<p>10 bonnes pratiques pour des soldes sur Internet en sécurité</p>				

Pour réaliser vos achats en ligne en toute sécurité, ESET vous donne des conseils pour éviter de se faire pirater sa carte bancaire.

– **Faites attention aux sites Internet que vous ne connaissez pas.** Au moindre doute, n'effectuez pas vos achats, car il peut s'agir d'un faux site Internet qui tente de récupérer les informations de votre carte bancaire.

– **Préparez-vous aux attaques par phishing.** Elles se diffusent massivement par e-mail lors des soldes, car c'est à cette période que les internautes passent le plus de temps sur les sites Internet de vente en ligne. ESET a réalisé une courte vidéo pour vous expliquer comment éviter le phishing par e-mail.

– **Utilisez des méthodes de paiement sécurisé.** Vérifiez que l'URL mentionne HTTPS. Effectuez toujours vos paiements sur des sites Internet chiffrés.

– **Attention aux annonces sur Facebook.** Les plateformes des réseaux sociaux abondent de fausses annonces et sites Internet proposant des offres intéressantes. Évitez également de partager les détails de votre carte bancaire par message : vous ne pouvez pas vérifier l'identité des personnes qui ont accès au compte et qui recevront ces informations.

– **Effectuez toujours vos achats sur des appareils sécurisés et évitez de vous connecter à un Wi-Fi public.** Ce genre d'arnaque, appelé Man-in-the-Middle (MiTM) est très répandu. En 10 minutes, le pirate peut voler toutes les informations vous concernant.

– **Utilisez des mots de passe forts ou un gestionnaire de mots de passe.** Plusieurs études ont montré que les utilisateurs ayant plus de 20 comptes en ligne et étant actifs sur Internet sont plus susceptibles de réutiliser les mêmes mots de passe pour plusieurs accès. Selon le rapport de recherche et de stratégie Javelin, cette méthode augmente de 37% le risque de voir ses comptes compromis. Aussi, les experts ESET recommandent d'utiliser des mots de passe forts mélangeant des minuscules et des majuscules à des symboles et chiffres. Les gestionnaires de mots de passe peuvent être utilisés pour ne pas avoir à les apprendre par cœur. Retrouvez les erreurs les plus courantes lors de l'utilisation d'un mot de passe en cliquant [ici](#).

– **Soyez prudent avec votre smartphone.** Le nombre de cybermenaces sur cette plateforme a considérablement augmenté. Pour commencer, faites vos achats uniquement via des applications certifiées et supprimez les applications dont vous ne vous servez pas. Pensez à désactiver le Wi-Fi lorsque vous faites votre shopping dans un lieu public, privilégiez les données cellulaires, ceci permettra d'empêcher les cybercriminels de vous diriger vers un faux Wi-Fi afin de voler vos informations bancaires.

– **Utilisez une e-carte bleue.** Non seulement elle est déconnectée de vos comptes bancaires et est également assurée contre les fraudes.

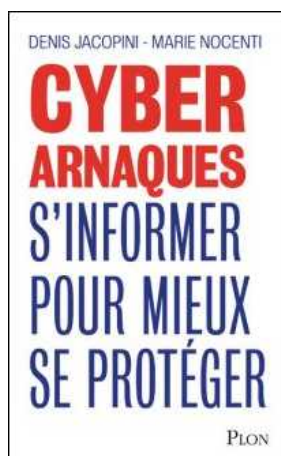
– **Respectez les règles de sécurité de base.** Cela peut paraître évident, mais avant de faire vos achats, assurez-vous d'être correctement protégé : installez une solution de sécurité efficace et mise à jour. Optez pour une solution qui offre une navigation sécurisée pour les transactions bancaires. Enfin, ajoutez des mots de passe à votre écran de verrouillage ou un code PIN à votre smartphone.

– **Évitez de réaliser vos achats sur différents appareils (1 à 2 maximum).** Plus vous entrerez les informations de votre carte de crédit sur des appareils différents (PC, tablette, smartphone...), plus vous multipliez le risque d'être victime d'une fraude.

[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 Millions de victimes de la Cybercriminalité 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](https://www.fnac.fr)

Article original de ESET

Victime d'un piratage

informatique, quelles sont les bonnes pratiques ?

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

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
---	---	---	--	--	--

Denis JACOPINI
vous informe

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

Les cas de piratages informatiques ne se comptent plus depuis bien longtemps. Cependant, si vous vous êtes retrouvés victimes, il est urgent de mettre en pratique des règles de base.

Les 3 axes vers lesquels votre structure devra progresser seront :

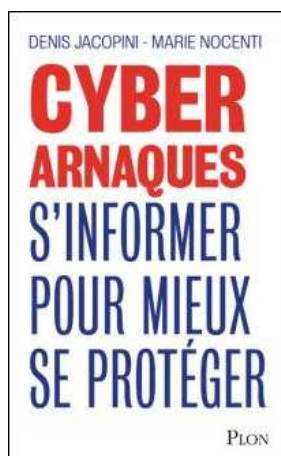
- Technique, par une amélioration des mesures de sécurité en place ;
- Juridique, par une présentation, auprès des principaux acteurs de votre structure pour une meilleure acceptation, des principales mesures de mise en conformité avec les règles françaises et européennes relatives à la protection des données personnelles ;
- Humain, par une meilleure prise de conscience des dangers numériques, pour une évolution des comportements vers une utilisation plus responsable des outils numériques.

Face à vos besoins d'accompagnement, nos formateurs ont élaboré un parcours destinés aux équipes de direction de votre structure, à l'équipe informatique et aux utilisateurs susceptibles d'être piégés.

En vous accompagnant sur ces 3 axes et auprès de ces 3 profils, vous pourrez alors comprendre comment les pirates informatiques vous ont piégé, découvrir s'ils pourront encore vous piéger et surtout, le plus important, quelles changements mettre en place pour limiter les risques à l'avenir.

[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 Millions de victimes de la Cybercriminalité 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.

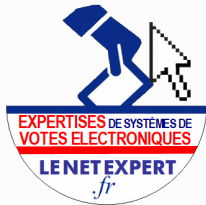
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur [Fnac.fr](https://www.fnac.fr)

**Formation en cybercriminalité
: Virus, arnaques et**

piratages informatiques, Solutions pour nos entreprises

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



Denis JACOPINI



vous informe

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

Présentation

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

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

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

Objectif

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

Durée

1 journée

ou conférence de 2 heures.

Public concerné

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

Moyens pédagogiques

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

Animateur

Denis JACOPINI

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

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

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

Différentes interventions pour :

- Le **Conseil de l'Europe** ;
- Un **Centre d'Enseignement et de Recherche en Informatique** ;
- Le **Centre d'Etudes des Techniques Financières** et d'Ingénierie d'Aix en Provence ;
- Des **écoles d'avocats** ;
- Des **Compagnies d'Experts Judiciaires** ;
- De nombreux clubs ou associations de chefs d'entreprises dans la **France entière et à l'étranger** ;
- Le **Centre National de la Fonction Publique Territoriale (CNFPT)** pour des élus, des S.G. et des agents publics.

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

Plus d'informations sur

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

[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"]

La cybersécurité pour les débutants – Un lexique informatique

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

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES <i>.fr</i></p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
 <p>Denis JACOPINI EXPERT INFORMATIQUE EQUIPEMENT SPECIALISE EN CYBERCRIMINALITE vous informe</p>	<p>La cybersécurité pour les débutants – Un lexique informatique</p>				

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

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

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

Les meilleurs conseils pour choisir vos mots de passe

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

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

Attaques informatiques : comment les repérer ?

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

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

Comment protéger son site internet des pirates informatiques ?





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.

[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 : *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					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES</p>	 <p>LE NET EXPERT MISES EN CONFORMITÉ</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
 <p>Denis JACOPINI vous informe</p>		<p>Les grands principes de la cryptologie et du chiffrement</p>			

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 synchroniser 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 reconnaît 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** ».

[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

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

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



Denis JACOPINI



vous informe

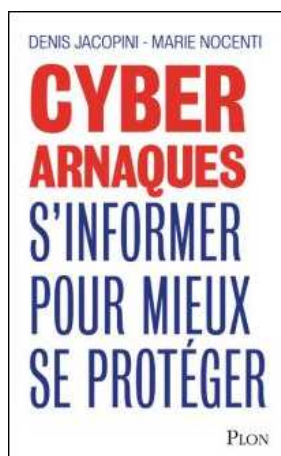
Le livre du jour
: CYBERARNAQUES
- à l'écoute des
livres, Radio
Massabielle
(97.8 Mhz et
101.8 Mhz)

Comme les langues d'Esopé, 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]

[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 Millions de victimes de la Cybercriminalité 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](https://www.fnac.fr)

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

Comment empêcher Android de

sauvegarder automatiquement nos données personnelles ?

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



Comment empêcher de
Android de
sauvegarder
automatiquement
nos données
personnelles ?

Nos smartphones et tablettes Android sauvegardent certaines de nos données personnelles sur les serveurs de Google sans forcément nous demander notre avis. Un système qui peut s'avérer aussi pratique pour certains qu'il peut être déroutant pour d'autres. Encore faut-il savoir quelles sont les données sauvegardées par Google et celles qui ne le sont pas. Nous allons donc aujourd'hui nous pencher sur la question.



N'avez-vous jamais remarqué que lorsque vous entrez vos identifiants Google dans un nouvel appareil Android, ce dernier retrouvait automatiquement certaines de vos informations personnelles, notamment vos contacts. Pourtant, vous n'avez jamais rien fait pour, et pour cause puisque cette option est activée par défaut. Ce qui signifie que vous pouvez également la désactiver. La plupart des utilisateurs la conservent néanmoins activée pour des raisons de praticité.

Il faut dire que cette sauvegarde automatique peut s'avérer utile lorsque vous changez de smartphone, lorsque vous disposez de plusieurs appareils Android ou si par malheur, vous vous faisiez voler votre téléphone. Mais certains ne veulent pas que leur vie privée se retrouve sur le cloud de Google. Ce tutoriel est pour eux mais avant de passer à la pratique, un peu de théorie.

Les données automatiquement sauvegardées par Google

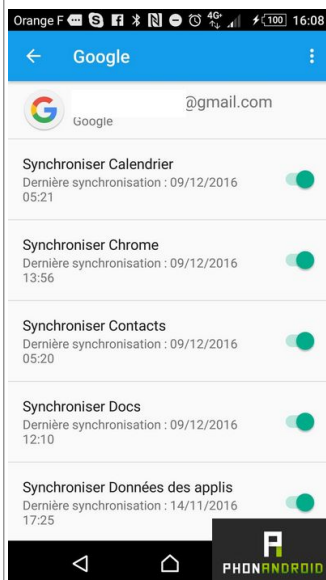
Au sein de son OS, Google a intégré un outil du nom d'Android Backup Service qui sauvegarde certaines données liées aux services que vous utilisez. Ces données sont les suivantes :

- **Contacts** qui sont sauvegardés au sein de Google Contacts. Vous pouvez ainsi les retrouver sur tous vos appareils et même sur votre PC en vous connectant simplement à votre compte.
- **Emails** qui sont sauvegardés au sein de Gmail
- **Documents**, ce qui vous permet d'ailleurs d'éditer vos documents sauvegardés dans le cloud à partir de n'importe lequel de vos appareils
- **Calendriers**
- **Chrome** : vos favoris et votre historique de navigation sont synchronisés avec votre compte. Idem pour vos mots de passe si vous avez activé la fonction Smart Lock
- **Hangouts** : vos conversations sont sauvegardées
- **Google Play Store** : les applications que vous avez téléchargées sont automatiquement sauvegardées. Vous pouvez ensuite les retrouver dans l'onglet « Mes applications » de la boutique. C'est très pratique lorsque vous changez de smartphone car vous n'avez pas besoin de les rechercher une par une, en outre, les applications achetées sont également sauvegardées
- Vos **photos** et vidéos, à condition d'utiliser l'application Google Photos et d'avoir activé la sauvegarde automatique de vos médias
- Certaines **données d'applications**

Comment empêcher Google de sauvegarder vos données

Vous n'êtes pas ravis à l'idée que Google en sache autant sur vous et vous souhaiteriez que certaines de vos données ne soient pas sauvegardées ? Et bien rassurez-vous, c'est possible et en quelques clics. Il vous suffit pour cela de :

- Vous rendre dans le menu **Paramètres > Personnel > Comptes de votre smartphone**
- Sélectionner votre compte Google
- Décocher toutes les données que vous ne voulez pas que Google sauvegarde



Et pour aller plus loin, n'hésitez pas à jeter un œil à notre tutoriel comment préserver sa vie privée sur Android.

Les données non sauvegardées par Google

Les données listées ci-dessous ne sont pas sauvegardées par Google. Pour éviter de les perdre en changeant de smartphone, il faudra donc utiliser une application tierce mais nous y viendrons après.

- Les **SMS**, il est néanmoins possible de sauvegarder ses SMS sur Android en utilisant une application
- **Google Authenticator** : pour des raisons de sécurité, les données d'authentification Google en deux étapes ne sont pas sauvegardées
- **Réglages** : les paramètres personnalisés de votre smartphone ne sont pas sauvegardés
- **Bluetooth** : Android ne synchronise pas les périphériques Bluetooth appairés vers votre smartphone

Comment sauvegarder toutes ses données personnelles

Bien que Google ne le permette pas par défaut, il est tout à fait possible de sauvegarder toutes les données de votre smartphone Android à l'aide de notre précédent tutoriel. Certaines de vos données iront directement sur votre support externe, d'autres seront sauvegardées en ligne afin de pouvoir ensuite être réintégrées à votre nouveau smartphone si votre but est de sauvegarder vos données pour les retrouver sur un nouvel appareil.

N'oubliez pas non plus de jeter un œil à notre sélection d'applications pour sauvegarder ses données personnelles. Certaines nécessiteront que votre téléphone soit rooté, d'autres non, et elles vous permettront de sauvegarder toutes vos applications et pas seulement les données.

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 ?

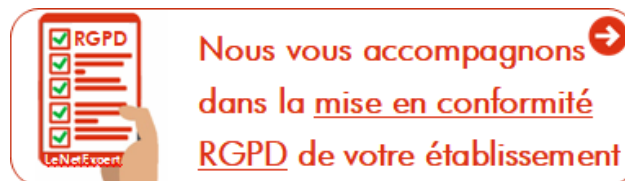
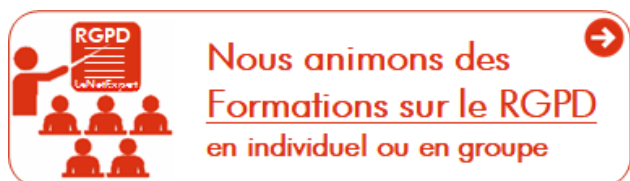
Contactez-nous

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)

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

Source :
<http://www.phonandroid.com/comment-empecher-android-sauvegarde-r-automatiquement-donnees-personnelles.html>