

Victime d'un prélèvement frauduleux sur votre compte bancaire ? Que faire ? | Quelques conseils... | Denis JACOPINI

| | |
|---|---|
| ✕ | Victime d'un prélèvement frauduleux sur votre compte bancaire ? Que faire ? |
|---|---|

Malgré toutes les actions que nous menons pour vous former au risque en cybercriminalité ou tous les efforts pour vous sensibiliser, vous êtes victime d'une arnaque sur Internet. Alors, que faire ?



Vous avez constaté un débit frauduleux sur votre compte bancaire ?

Les raisons peuvent être multiples. Carte bancaire copiés, votre numéro de carte bancaire généré aléatoirement, numéros de votre carte bancaire interceptés, virus ou logiciel d'espionnage informatique etc.



1) Tout d'abord, faites le plus vite possible opposition sur votre CB

en appelant le service interbancaire des cartes perdues ou volées qui est disponible 7 jours sur 7 au 08 92 705 705 (0,34€/min). Cela permettra d'éviter d'autres prélèvements frauduleux.



2) Contactez votre conseiller bancaire

pour lui expliquer l'arnaque dont vous avez été victime pour récupérer votre argent. La banque devrait vous proposer de vous rembourser sans délai. Si vous rencontrez des difficultés pour vous faire entendre, évoquez l'article de loi suivant :

L'Article L133-18 du code monétaire et financier précise :

« En cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L. 133-24, le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de l'opération non autorisée et, le cas échéant, rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. Le payeur et son prestataire de services de paiement peuvent décider contractuellement d'une indemnité complémentaire »

3) Portez plainte au commissariat ou à la gendarmerie la plus proche.

Le Défenseur des droits a pu constater que les policiers incitent les plaignants à ne déposer qu'une main courante, et non une plainte.

- La main courante est simplement déclarative; elle n'implique pas que la justice soit informée, ni qu'une investigation soit lancée; elle pourra seulement être versée à l'instruction si une procédure judiciaire a lieu.

- La plainte, en revanche, suppose une transmission au procureur de la République qui décide des suites à y donner.

Il est vrai que si les escrocs sont à l'autre bout du monde, il y a peu de chance que la police de notre pays réussisse à mettre un terme à leurs agissements... mais déposez plainte ! Ainsi votre cas sera connu des services de Police et cela pourra vous prémunir contre d'éventuelles complications suite à l'arnaque que vous avez subie. En effet les escrocs pourraient profiter des données qu'ils ont pour multiplier leurs méfaits. En portant plainte, vous montrez à la police que vous êtes bien une victime et que vous en subissez les conséquences.

Enregistrer votre plainte est une obligation des services de Police ou de Gendarmerie en vertu de l'article 15-3 du code de procédure pénale et de la Charte de l'accueil du public et de l'assistance aux victimes.

Ils sont censés enregistrer une plainte dès que la demande est émise, quels que soient le lieu où a été commise l'infraction et le lieu de résidence de la victime, et sans que cette dernière ait besoin d'apporter pour cela un quelconque élément de preuve (certificat médical, devis, etc).

Munissez-vous de tous les renseignements suivants :

- une pièce d'identité ;
- votre relevé bancaire sur lequel figure(nt) le (ou les) paiement(s) contesté(s);
- les coordonnées de votre banque;
- les références de votre carte bancaire;
- tout autre renseignement pouvant aider à l'identification de l'escroc.

Suite à ce dépôt de plainte, une enquête sera ouverte et transmise au procureur de la République.

4) Vous pouvez aussi appeler « Info Escroqueries »

N'oubliez pas le numéro « Info Escroqueries » 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile) à utiliser si à la base, vous avez été la cible d'un e-mail frauduleux ou d'une escroquerie.



5) Rechercher l'origine de l'escroquerie

Une fois les actions précédentes réalisées, afin d'éviter que le problème ne se reproduise, il est indispensable d'identifier l'origine du prélèvement frauduleux.

Par exemple, si votre système informatique s'est fait pirater, l'arnaque se reproduira.

Pour cela, contactez un expert informatique spécialisé en cybercriminalité.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

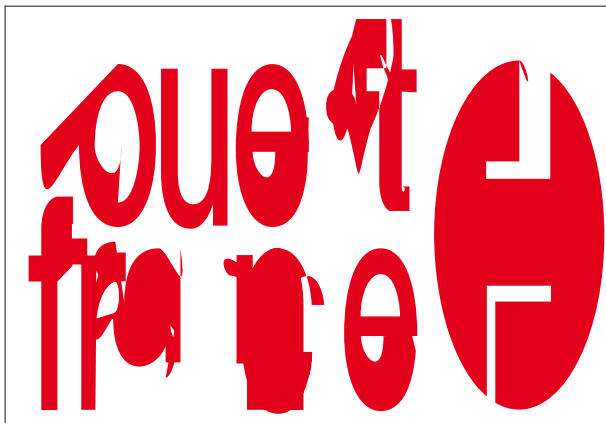
Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI

Comment se connecter de manière sécurisée à un wifi public ? | Denis JACOPINI



Comment se connecter de manière sécurisée à un wifi public ?

En période de vacances ou lors de déplacements professionnels, nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants... En juillet 2015, nous vous avons publié un article « Est-il risqué de se connecter au wifi public ? » pour vous informer des principaux risques à partager ces accès sans fil à internet avec d'autres. Cette fois, nous allons parler des solutions pour surfer sécurisé en utilisant les réseaux Wifi publics. **RAPPEL DU PRINCIPAL RISQUE** Un pirate peut se connecter tout aussi facilement que vous sur un réseau Wifi Public et espionner les données qui y transitent.

Il peut ainsi, en fonction des données qu'il récupère :

- accéder à toutes les informations qui sortent et qui entrent de votre ordinateur (le protocole tcp/ip n'étant pas protégé par défaut) ;
- vous voler, crypter des documents ou exercer un chantage pour que vous puissiez les récupérer ;
- usurper votre identité et réaliser des actes illégaux ou terroristes sous votre identité ;
- accéder à des informations bancaires et vous spolier de l'argent.

LA SOLUTION ?

Utiliser une connexion Wifi qui sera cryptée au moyen d'un logiciel VPN (ce cryptage n'a aucun rapport avec les clés Wifi) .

La connexion Wifi ainsi créée étant cryptée, toutes les informations qui véhiculeront (identifiants, adresses email, mots de passe, numéros de cartes bancaires...) seront illisibles pour tous les pirates qui seront connectés sur le même point d'accès wifi.

Vous pouvez certes partager la connexion 3G ou 4G de votre smartphone, mais l'utilisation d'un logiciel VPN est recommandé.

Un logiciel « VPN » (Virtual Private Network) est un logiciel qui crée un « réseau privé virtuel », une sorte de tunnel crypté pour vos communications internet. Cela ralentit un peu la connexion, mais elle est du coup sécurisée.

**Nous utilisons et conseillons le logiciel VPN HotSpot Shield.
Ce logiciel rendra vos connexions Wifi publiques tranquilles.
Téléchargez et découvrez gratuitement HotSpot Shield
Notre page de présentation de HotSpot Shield**



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

Formation en Cybercriminalité : Arnaques, virus et demandes de rançons, Comment s'en protéger ?

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 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>Formation en Cybercriminalité : Arnaques, virus et demandes de rançons, Comment s'en protéger ?</p> | | | | |

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 DE LA FORMATION EN CYBERCRIMINALITE :

La formation en cybercriminalité a pour but de créer des déclics chez les utilisateurs, mettre à jour les connaissances des informaticiens et faire prendre conscience aux chefs d'entreprises des risques en couvrant les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant d'enrayer le phénomène de la cybercriminalité.

PROGRAMME :

- Etat des lieux de la cybercriminalité en France et dans le monde;
- Les principaux cas de piratages et d'arnaques expliqués ;
- Les bonnes pratiques au quotidien pour limiter les risques ;
- Etude de vos témoignages, analyse de cas et solutions.
- PUBLIC CONCERNÉ : Utilisateurs, chefs d'entreprise, présidents d'associations, élus...

MOYENS PÉDAGOGIQUES :

- Support de cours pour prise de notes
- Résumé remis en fin de cours.
- Vidéo projecteur et sonorisation souhaitée selon la taille de la salle.

CONDITIONS D'ORGANISATION

- Formations individuelles ou en groupe
- Formations dispensées dans vos locaux ou organisées en salle de formation partout en France en fonction du nombre de stagiaires.

Téléchargez la fiche de présentation / Contactez-nous

QUI EST LE FORMATEUR ?

Denis JACOPINI est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire et a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

Il anime dans toute la France et à l'étranger des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles.

A ce titre, il intervient régulièrement sur différents médias et sur La Chaîne d'Info LCI pour vulgariser les sujets d'actualité en rapport avec ces thèmes.

Spécialisé en protection des données personnelles, il accompagne les établissements dans leur mise en conformité CNIL en les accompagnant dans la mise en place d'un Correspondant Informatique et Libertés (CIL).

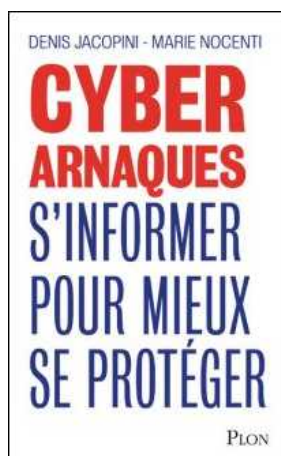
Enfin, il intervient en Master II dans un centre d'Enseignement et de Recherche en Informatique, en Master Lutte contre la Criminalité Financière et Organisée, au Centre National de la Fonction Publique Territoriale et anime le blog LeNetExpert.fr sur lequel il partage et publie de très nombreuses informations sur ses thèmes de prédilection.

Denis JACOPINI peut facilement être contacté sur :

<http://www.leNetExpert.fr/contact>

[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)

**Vie privée en danger :
pourquoi nous sommes tous**

concernés | Denis JACOPINI

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



LE NET EXPERT
AUDITS & EXPERTISES



EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES
LE NET EXPERT
fr



LE NET EXPERT
MISES EN CONFORMITE



LE NET EXPERT
FORMATIONS



LE NET EXPERT
ARNAQUES & PIRATAGES



vous informe...

Vie privée en danger : pourquoi nous sommes tous concernés

Est-il possible de rentrer chez nous, d'écouter nos conversations et de s'immiscer dans notre intimité sans y être invité ? Nous avons découvert qu'il suffit pour cela d'une simple connexion Internet. Ordinateur, téléphone portable, réseaux sociaux et même cartes bancaires : désormais nous sommes en permanence connectés les uns aux autres. Mais nos informations personnelles sont-elles réellement bien protégées ? Pas si sûr...

Chaque semaine, de nouveaux scandales éclatent comme, par exemple, le vol, il y a quelques jours, de milliers de photos intimes de stars américaines. Et cela nous concerne tous : « phishing », vol d'identité, harcèlement numérique, vols de compte bancaire : chaque seconde, 17 personnes sont victimes de cyber-escroqueries à travers le monde. Car Internet a créé une nouvelle génération d'escrocs 2.0. Leur butin s'élèverait l'année dernière à 400 milliards de dollars. Un chiffre en constante augmentation. Nous avons découvert les failles des nouvelles cartes bancaires NFC, sans contact. Désormais, les pickpockets n'ont plus besoin de mettre la main dans votre sac pour voler votre argent.

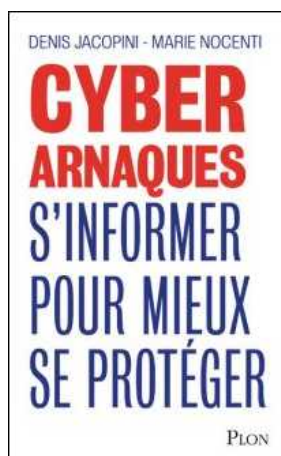
Nous allons vous raconter l'histoire de différentes victimes françaises. Celle de Laetitia, en proie au cyber-harcèlement, qui a failli mettre fin à ses jours. Stéphane, lui, pensait avoir rencontré l'amour sur la toile ; il était en fait entre les mains de brouteurs de Côte d'Ivoire. Nous avons remonté leurs traces à Abidjan.

Nous nous sommes également rendus en Roumanie dans une ville hors du commun que le FBI a surnommée Hacker-ville. Là-bas, une grande partie de la population vivrait des cyber-escroqueries. Certains escrocs ont accepté de nous rencontrer ; d'autres après avoir été arrêtés par les forces de l'ordre ont décidé de mettre leur génie informatique au service de la société.

Enfin, vous découvrirez que pour protéger leurs ados des dangers du web, des parents ont trouvé une solution radicale. Christophe est un papa espion : il contrôle les moindres faits et gestes de ses trois enfants. Grâce à une panoplie de logiciels et d'applications, il a accès à l'intégralité du contenu de leur téléphone et ordinateur. Internet est sans aucun doute la principale révolution de ces trente dernières années mais c'est peut-être aussi la fin de la vie privée.

[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

Source : http://www.m6.fr/emission-zone_interdite/28-09-2014-vie_privee_en_danger_pourquoi_nous_sommes_tous_concernes/

Mot de passe Wifi : trois quarts des foyers français à la merci d'une attaque | Denis JACOPINI

| 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 détection de logiciels espions</p> |  <p>LE NET EXPERT FORMATIONS</p> |  <p>LE NET EXPERT ARNAQUES & PIRATAGES</p> |
|  | <p>#Mot de passe Wifi : trois quarts des foyers français à la merci d'une attaque</p> | | | | |

Trois ménages français sur quatre ne protègent pas correctement leur borne wifi, rendant leurs ordinateurs, téléphones et tablettes accessibles aux pirates informatiques.

Près de trois ménages français sur quatre ne protègent pas correctement leur borne wifi domestique, rendant leurs ordinateurs, téléphones et autres équipements connectés aisément accessibles aux pirates informatiques, selon une étude publiée jeudi par l'éditeur de logiciels antivirus Avast Software.

D'après cette enquête, menée en novembre auprès de plus de 16 000 internautes français équipés d'un réseau wifi domestique, « la vaste majorité des routeurs (...) ne sont pas sécurisés ».

Mot de passe inexistant... ou évident

Les Français sont ainsi 10% à déclarer ne pas utiliser de mot de passe pour protéger leur réseau wifi et 24% à utiliser comme mot de passe « leur adresse, leur nom, leur numéro de téléphone, le nom de leur rue ou d'autres mots faciles à deviner ».

En outre, plus de la moitié des routeurs sont « mal sécurisés par défaut », avec des combinaisons de codes d'accès « beaucoup trop évidentes, telles que 'admin/admin' ou 'admin/motdepasse' », selon Avast.

Selon l'éditeur d'antivirus, 5% des bornes wifi françaises sont même « accessibles de l'extérieur » du domicile. Une proportion identique de sondés admet d'ailleurs avoir utilisé le réseau d'un de leurs voisins à son insu.

Un Français sur cinq a déjà été piraté

Le manque de sécurité des routeurs en fait « des points d'entrée très faciles d'accès pour les hackers, qui sont dès lors capables de pirater des millions de réseaux domestiques en France », a affirmé Vince Steckler, directeur général d'Avast, lors d'un point de presse.

Un Français sur cinq rapporte avoir déjà subi un piratage informatique, et 34% redoutent un vol d'informations personnelles ou de données bancaires et financières. Cependant, 42% sont persuadés que leur réseau domestique est suffisamment sûr.

Rappelons qu'un mot de passe, pour être le plus efficace possible, doit comporter des caractères alpha-numériques (lettres minuscules, majuscules, chiffres) et, si possible, des caractères spéciaux.

Et que les mots de passe les plus utilisés l'an dernier – et donc les plus faciles à « craquer » – étaient les suivants :

123456

password

12345678

qwerty

abc123

123456789

111111

1234567

iloveyou

123123

Admin

1234567890

Un conseil : évitez-les !

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

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

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

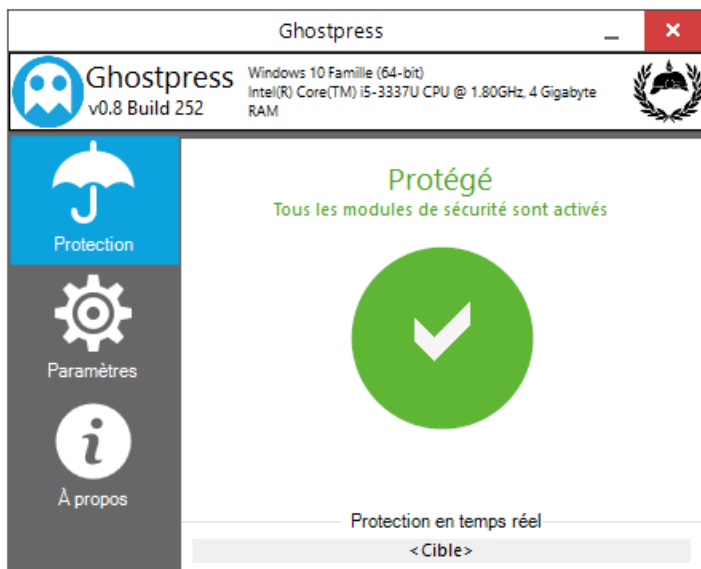
[block id="24760" title="Pied de page BAS"]

Source :
<http://www.ouest-france.fr/informatique-wifi-trois-quarts-des-foyers-francais-la-merci-dune-cyberattaque-3026280>

Astuce : Un logiciel anti-espions gratuit pour Windows | Denis JACOPINI

| | | | | | |
|---|---|---|--|---|---|
| Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer | | | | | |
|  |  |  |  |  |  |
|  <p>vous informe</p> | | <h2>Astuce : Un logiciel anti-espions gratuit pour Windows</h2> | | | |

Ghostpress un logiciel anti-keylogger portable gratuit qui est en mesure de protéger votre ordinateur contre les logiciels espions.



Dans cet article, je vous présente **Ghostpress**, un logiciel anti-keylogger portable totalement gratuit qui est en mesure de protéger votre ordinateur des logiciels espions.

Mais qu'est-ce qu'un keylogger ?

En informatique, un keylogger (enregistreur de frappe) est un logiciel espion qui espionne l'utilisateur d'un ordinateur. Le but d'un tel outil est de s'introduire entre la frappe au clavier et l'apparition du caractère à l'écran. Cela permet à un pirate informatique de récupérer toutes les informations que vous avez tapé avec votre clavier comme un login et un mot de passe, une adresse, des informations bancaires etc. [Source]

Ghostpress

Ghostpress est un outil très simple d'utilisation et peu gourmand en ressource système. Il vous suffit simplement de le télécharger, puis de le lancer pour que tous les modules de sécurité soient activés. Ainsi, chaque actions que vous exécuterez sur l'ordinateur seront cachés des regards indiscrets.

Vous pouvez également désactiver temporairement le programme en cliquant sur le gros bouton vert et exécuter le programme automatiquement au démarrage de Windows en cochant une petite case dans les paramètres de l'outil.

[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"]

Article original de @justgeekOriginal
<http://www.justgeek.fr/ghostpress-logiciel-anti-keylogger-windows-47093>

10 conseils pour protéger sa vie privée sur Internet | Denis JACOPINI

| | | | | | |
|---|---|---|--|---|---|
| Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer | | | | | |
|  |  |  |  |  |  |
|  | <h2>10 conseils pour protéger sa vie privée sur Internet</h2> | | | | |

Les données numériques que nous produisons sur Internet sont utilisées à notre insu à des fins publicitaires. Nos conseils pour protéger vos données personnelles.

Le big data ou mégadonnées (J.O. n° 0193, 22 août 2014) désigne le volume exponentiel des données numériques et leur exploitation.

Tous producteurs de données

Les principaux acteurs du big data sont tout d'abord les États qui ont créé de multiples bases de données statistiques, mais aussi leurs services de renseignements (et tous leurs fichiers). Viennent ensuite les acteurs du Web, les opérateurs des télécoms ou les grands de la distribution. Mais aussi chaque habitant de la planète qui produit tous les jours une quantité importante de données : courriels, photos, vidéos, posts sur les blogs, achats en ligne.

La prolifération des données a des aspects positifs :

- personnalisation respectueuse des données du client ;
- prévision des phénomènes météo graves ;
- arrivée des services de police rapidement sur les lieux d'un crime ;
- détection des mouvements de fonds dans le but de démanteler des réseaux de blanchiment d'argent.

Collecte de données et marketing ciblé

Mais, ces collectes d'informations peuvent aussi devenir très intrusives ou être détournées de leur finalité. Par exemple, Facebook possède aujourd'hui la base de données de visages la plus importante au monde et a mis au point le logiciel de reconnaissance faciale le plus abouti.

Cet usage généralisé des technologies a fait émerger de nouveaux acteurs qui ont compris tout l'intérêt de collecter des flux d'informations : les entreprises de la distribution qui cherchent toujours à proposer davantage d'offres commerciales, adaptées à vos besoins, à vos désirs.

Cerner l'individu, tel est le but du marketing ciblé ! Grâce à lui, vous serez aidé dans vos achats, vos déplacements, dans la gestion de votre argent, dans le soin que vous prenez de votre santé.

Vos données personnelles aussi sont collectées par les applis mobiles.

3 applications sur 4 collectent les données personnelles contenues dans le téléphone : principalement la localisation, l'identifiant du téléphone et les données d'accès aux comptes personnels (sans que cela soit toujours justifié par la finalité de l'application).

C'est le résultat d'une enquête menée en mai 2014 par les autorités européennes de protection des données.

Le droit à l'oubli pour effacer ses données sur le Web

Ces collectes de données ont conduit les individus à réclamer – légitimement – la possibilité de garder une forme de contrôle sur leurs usages futurs.

Et comme rien ne se perd sur la Toile, les citoyens sont de plus en plus nombreux à demander la création d'un droit à l'oubli, c'est-à-dire le moyen d'effacer ses données personnelles sur le Net. Ils sont soutenus par plusieurs institutions judiciaires.

Ainsi, pour la première fois, la Cour de justice de l'Union européenne a contraint, en mai 2014, Google à mettre en ligne un formulaire permettant à chacun de procéder à la suppression de ses données nominatives.

Pourtant, selon une étude réalisée par Reputation VIP en juin 2014, Google n'aurait satisfait que 36 % des demandes de suppression de données.

10 conseils pour protéger vos données personnelles

1. Maîtriser son smartphone

Les applications installées sur le téléphone sont une mine d'or pour le marketing. Elles accumulent des informations sur nos comportements ou nos déplacements tout au long de la journée.

Pour éviter d'être suivi à la trace, désactiver la géolocalisation par GPS dans les paramètres de réglage (attention, cela interdit l'accès à certains services).

2. N'autoriser le partage de données (contacts, photos, vidéos) que lorsque c'est vraiment utile

refuser dans les autres cas.

3. Bloquer les cookies

Sur son site, la Commission nationale de l'Informatique et des Libertés (Cnil) délivre plusieurs astuces pour échapper aux cookies, ces petits fichiers installés à l'insu de l'internaute lorsqu'on navigue sur le Web, et propose Cookieviz, un logiciel d'identification des cookies en temps réel.

Ces fichiers détectent et enregistrent les achats, les sites consultés, dans le but de proposer de la publicité ciblée.

On peut les refuser à l'entrée des sites, les bloquer (en configurant les paramètres du navigateur Firefox, Internet Explorer...), activer la navigation privée et effacer l'historique.

4. Utiliser un serveur proxy et un pseudo

Un serveur proxy agit comme un intermédiaire entre le navigateur et Internet, cachant ainsi l'identité de l'utilisateur. Il en existe des dizaines que l'on peut télécharger gratuitement sur Internet puis installer sur son ordinateur : AnonymoX, Privoxy, Squid.

Le but est de rendre son nom et/ou son prénom invisible sur Internet, les réseaux sociaux et dans les courriels.

Avec un pseudo, on peut s'abonner à des newsletters, réaliser des achats en ligne ou accéder à des services sans délivrer d'informations personnelles.

5. Sécuriser son mot de passe

Choisir un mot de passe compliqué, c'est protéger ses données, un peu comme une porte blindée protégerait sa maison.

Il est préférable qu'il soit composé de chiffres et de lettres en minuscule et en majuscule. Il faut aussi soigner celui de sa boîte mail.

6. Utiliser le réseau Tor

Ce logiciel, téléchargeable sur Internet, permet de naviguer anonymement et son système de serveurs-relais empêche le suivi des données de l'utilisateur.

Ce système est utilisé par plus de deux millions d'internautes, que ce soient des dissidents dans les pays où Internet est contrôlé, ou des journalistes ou des militaires, pour des raisons professionnelles.

7. Être prudent sur les réseaux sociaux

La première précaution consiste à paramétrer ses comptes pour qu'ils soient privés, les paramètres par défaut rendant les comptes publics.

Puis à publier ses photos avec discernement, à bien choisir les amis avec lesquels on va les partager, à sélectionner les groupes que l'on rejoint.

8. Faire du tri

Trier ses followers (« suiveurs » ou « abonnés » sur les réseaux sociaux) avec des logiciels gratuits : Tweet Block sur Twitter ; Privacy Fix sur Facebook, LinkedIn et Google.

9. Veillez à son e-réputation

Vérifier régulièrement ce qui est publié sur soi-même en tapant son nom et son prénom dans les moteurs de recherche, essentiellement Google en France.

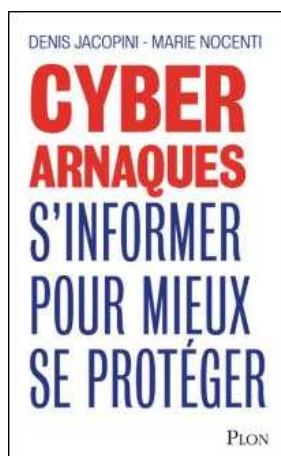
Adresser un courriel aux sites, blogs, moteurs de recherche pour faire supprimer les contenus qui portent atteinte à la vie privée.

10. Porter plainte

Si, après plusieurs demandes, vos données personnelles ne sont pas supprimées, il est possible d'adresser une plainte en ligne directement sur le site de la Cnil (sur cnil.fr).

[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)

Auteur : Laurence Fritsch

Source

<http://www.dossierfamilial.com/10-conseils-pour-proteger-sa-vie-privee-sur-internet-21122.html>

5 conseils pour combattre le piratage informatique



Pour beaucoup d'entre nous, acheter en ligne est devenu une habitude sans laquelle nous pouvons pas vivre. Les achats online simplifient notre quotidien car ils nous permettent de acheter des voyages, des vêtements, des cadeaux et aussi de faire nos courses alimentaires sans bouger ! Internet à changé notre système de vie et, aujourd'hui, presque tout peut s'acheter sur Internet.

Oui, il est beaucoup plus simple et confortable mais, au moment de payer, les doutes aflorent : **comment garantir la sécurité d'une transaction pour pouvoir faire nos achats avoir la mouche à l'oreille ?** Voici 5 conseils donnés pour le cabinet de sécurité ESET pour se prémunir contre les risques de piratage en ligne.

Vérifiez l'URL du site internet

Lorsque vous effectuez un paiement en ligne, l'URL doit impérativement commencer par « https:// ». Cela signifie que le site Internet est sécurisé. De plus, **votre navigateur vous indiquera, au moyen d'un symbole en forme de cadenas, que la sécurité entre votre ordinateur et le site est bien établie.** Doc, si vous n'êtes pas complètement sûrs du site dont vous êtes en train de mettre vos coordonnées, il vaut mieux faire demi-tour.

Faites vos achats que sur votre ordinateur personnel

À priori évident, **il ne faut pas profiter d'un réseau WiFi ouvert pour faire des achats et, non plus, sur un ordinateur que ne soit pas le vôtre.** Il est important de rappeler que quand vous fêtes ce type d'activité, vous apprêtez à transmettre des données sensibles, telles que votre numéro de carte bleue ou votre adresse personnelle.

Il est dès lors déconseillé d'utiliser un ordinateur public, ou même l'ordinateur d'un ami car vous ne connaissez pas si l'appareil est bien protégé. Il suffirait alors qu'un logiciel malveillant soit installé sur la machine pour que vos données privées soient récupérées par des cybercriminels.

Privilégiez les réseaux privés

On vient de le dire: les réseaux publics doivent, par essence, être faciles d'accès : c'est pourquoi ils sont le plus souvent dépourvus de toute protection. **Si vous pouvez y accéder, un cybercriminel peut le faire aussi.** On comprend donc facilement pourquoi il vaut mieux ne pas utiliser ce type de réseau pour effectuer un achat en ligne. **Un hacker pourrait facilement accéder à votre ordinateur et à ce que vous y faites,** et donc dérober sans difficulté votre numéro de carte bleue et autres données sensibles.

Évitez d'enregistrer vos données en ligne

Avec le développement d'intérêt et les services de pub sur la toile. De plus en plus de sites Internet vous proposent d'enregistrer vos coordonnées, numéro de carte bleue compris, afin que vous n'ayez pas à les saisir à nouveau à chaque achat.

C'est vrai que, si vous êtes des fous des achats en ligne, celle-ci est une fonctionnalité très pratique – surtout sur les sites sur lesquels vous achetez souvent, mais attention : **si vous permettez au site Web de se rappeler de vos coordonnées, l'accès à votre compte doit absolument être protégé par un mot de passe fort** pour éviter que ces données soient facilement récupérables par les cybercriminels. Voici quelques conseils pour créer un mot de passe efficace.

Utilisez un navigateur sécurisé

Même si le site sur lequel vous vous apprêtez à payer vous paraît fiable et que vous utilisez un réseau sécurisé, il se peut que des pirates informatiques parviennent à contourner les sécurités pour voler votre numéro de carte bleue. **L'idéal est donc d'utiliser un navigateur sécurisé,** comme celui inclut dans la solution **ESET Internet Security.** Grâce à cet outil, **vos données sont cryptées directement entre le clavier et le navigateur,** ce qui empêche toute possibilité de récupération de vos données bancaires.

Notre métier : Nous réalisons des audits sécurité, nous vous apprenons comment vous protéger des pirates informatiques et vous aidons à vous mettre en conformité avec le règlement Européen sur la protection des données personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



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

Toujours sous Windows XP ? Vous êtes une menace pour la société



Windows XP ne bénéficie plus de correctif de sécurité depuis 2014 et représente par conséquent un risque. Les utilisateurs ont donc une responsabilité. Et si vous êtes un professionnel de l'IT avec des capacités de décision en entreprise, vous devriez être licencié pour maintenir l'usage d'XP. La réaction à mon dernier article – « Pourquoi Windows doit mourir pour la troisième fois » – était considérable. Des centaines de milliers de personnes ont lu cet article, et nous avons eu des discussions très spirituelles, en effet.

Un tas d'entre vous l'a déclaré sans ambages : vous ne souhaitez pas mettre à niveau Windows XP. Vous êtes fâchés que Microsoft vous ait fait passer de XP à 7 et de 7 à 10. Vous êtes en colère de devoir en permanence mettre à jour le logiciel.

Une poignée d'entre vous a même suggéré de s'en prendre physiquement aux développeurs qui codent le logiciel vers lequel vous refusez de migrer...[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 : *Toujours sous Windows XP ? Vous êtes une menace pour la société – ZDNet*

Formation pour DPO externe mutualisé et Délégués à la protection des données externalisé



Depuis 2012, nous accompagnons des établissements dans leur mise en conformité avec la réglementation sur les Données à Caractère Personnel.



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.

Formation pour DPO externe ou Délégué à la protection des données externalisé : « J'accompagne mes clients dans leur mise en conformité avec le RGPD » : 3 jours + 1 jour d'accompagnement personnalisé (C'est le moment ou jamais de vendre des services « RGPD »)

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 prochaines dates d'animation autour de chez vous ?



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 et 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. »

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.

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 ?

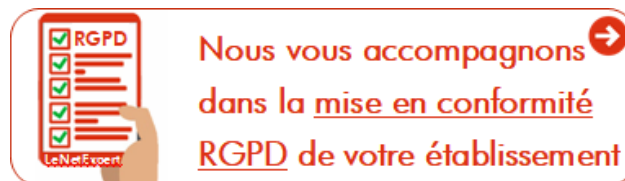
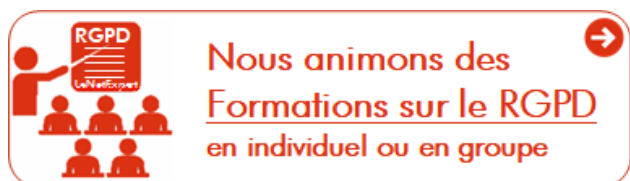
Contactez-nous

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