

Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité | Denis JACOPINI



Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité

La sensibilisation et l'éducation des utilisateurs jouent un grand rôle dans la réduction des risques.

Il importe donc pour les entreprises d'encourager leurs collaborateurs à se comporter de manière cohérente, en respectant des processus et procédures communiqués clairement, dont la conception et la surveillance sont centralisées et qui couvrent la totalité des équipements en usage. Cela n'évitera peut-être pas toute tentative d'attaque mais renforcera certainement la sécurité de l'entreprise.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI et

<http://www.globalsecuritymag.fr/Les-entreprises-revoient-leur,20150826,55304.html>



Nos
ordinateurs
ont-ils la
memoire
courte ?
Video

Que trouveront les archéologues du futur, d'ici quelques siècles ou quelques milliers d'années ? Des pierres taillées du paléolithique, des hiéroglyphes, des rouleaux de parchemins probablement, des livres peut-être.

Quelles images, quels sons, quels écrits de notre société restera-t-il dans 2000 ans ? Auront-ils résisté aux épreuves du temps et aux mutations technologiques comme l'ont fait la première photo, le premier film, le premier enregistrement sonore. Mais que deviendront les milliards d'informations engrangées dans les disques durs qui se démagnétisent, et sur les CD ou DVD, qui redoutent la lumière du soleil ? [lire la suite]

LE NET EXPERT

:

- **MISE EN CONFORMITÉ RGPD / CNIL**
- **AUDIT RGPD ET CARTOGRAPHIE** de vos traitements
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
- **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGPD**
 - **À LA FONCTION DE DPO**
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

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

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



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

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

[Contactez-nous](#)



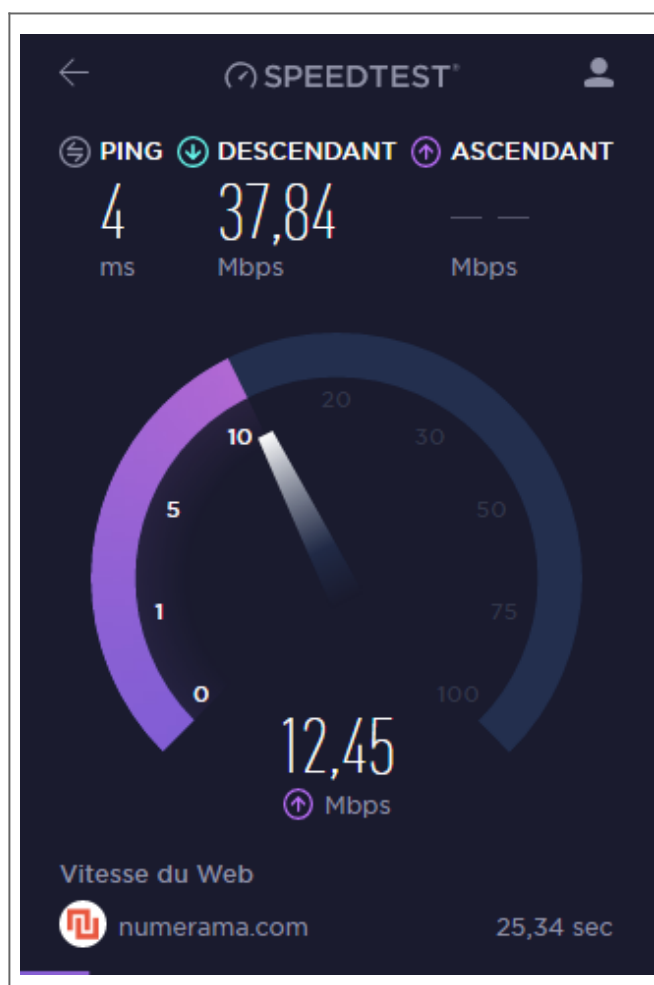
Régissez à cet article

Source : *Nos ordinateurs ont-ils la mémoire courte ?*

Les objets connectés représentent-ils un risque ? | Denis JACOPINI

x	Les #objets connectés représentent-ils un risque ?
---	--

Comment mesurer et tester le débit de votre connexion internet | Denis JACOPINI



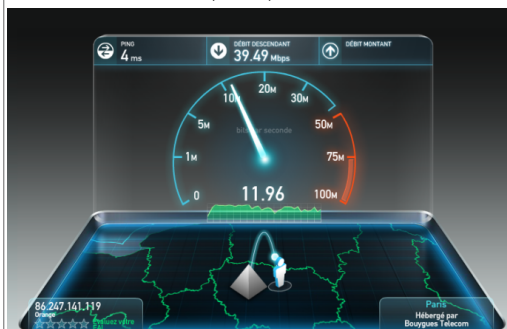
Comment mesurer
et tester le
débit de
votre connexion
internet

Internet c'est bien. Quand c'est rapide, c'est mieux. Nous vous avons listé quelques outils indispensables pour mesurer votre débit, que vous soyez chez Free, SFR, Orange, Numericable ou Bouygues.

On entend souvent dire qu'aujourd'hui on ne peut plus vivre sans Internet. Cette affirmation est fausse. Dire qu'on ne peut plus vivre sans **bonne** connexion Internet serait plus juste. Et justement, pour connaître la qualité de votre bande passante, il existe quelques outils extrêmement simple d'utilisation. Petit tour d'horizon des indispensables pour ceux qui ne les connaîtraient pas.

SPEEDTEST

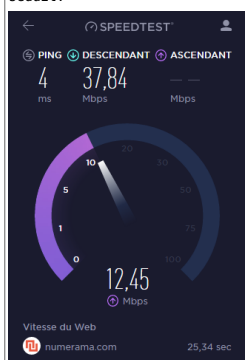
C'est le plus connu des outils présentés ici. Speedtest est complet et calcule votre débit montant et descendant ainsi que le temps de latence. Vous avez ainsi en main absolument toutes les informations en main pour connaître la vitesse de votre connexion. On regrette seulement le temps assez long que peut prendre un test (environ 47 secondes) et l'interface qui manque de sobriété.



Cela devrait bientôt changer grâce à la version HTML5 – encore en version beta – plus simple et efficace. Attention, celle-ci ne fonctionne pas lorsque le bloqueur de publicité est activé. Speedtest se décline également en application mobile pour profiter des mêmes fonctionnalités sur son smartphone.

EXTENSION OOKLA

Cet outil est extrêmement pratique. Ookla, l'entreprise qui a créé Speedtest, a sorti une extension Chrome rapide et ergonomique. À l'instar du site Internet, elle calcule le download, l'upload et le ping. Le test est réalisé en un peu moins de 30 secondes mais c'est surtout par son extrême simplicité d'utilisation que l'extension séduit.



En effet, pas besoin de taper l'adresse d'un site ou de lancer une recherche Google. Un simple clic en haut à droite de votre navigateur suffit à y accéder. Ainsi, si vous remarquez certaines lenteurs de connexion, pas besoin d'attendre une éternité avant d'accéder à la page qui pourra vous confirmer que votre débit est pourri. Vous pouvez d'ailleurs fermer la fenêtre de l'extension, celle-ci continuera à faire le test de débit discrètement.

Malheureusement pour tous ceux qui n'utilisent pas le navigateur web de Google, l'add-on Ookla est disponible uniquement sur Chrome.

FAST.COM

En moins de dix secondes, Fast.com calcule votre vitesse de téléchargement (débit descendant uniquement). Si vous n'en avez rien à faire du temps de latence ou que vous n'avez rien à uploader, il s'agit du site idéal.



37 Mbps

Ce site est en accord avec la vision de Netflix, son créateur, qui s'adresse plus aux internautes qui consomment plutôt qu'à ceux qui produisent. Ainsi, si vous ne surfez sur le web que pour consulter et télécharger des fichiers, Fast.com représente la meilleure solution. Le service en HTML 5 fonctionne aussi bien sur PC que sur mobiles, smart TV ou tablettes.

Article original de Omar Belkaab



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

Attention, l'employeur peut lire les SMS des téléphones professionnels | Denis JACOPINI

23

x	Attention, l'employeur peut lire les SMS des téléphones professionnels
---	---

Une décision de la Cour de cassation permet désormais à une entreprise de lire les messages reçus et envoyés sur un téléphone professionnel. Comme elle pouvait déjà le faire avec les e-mails. 

Gare aux sanctions si vous refusez l'accès à vos SMS à votre employeur.

Appelée à statuer sur le litige opposant deux sociétés de courtage, la Cour de cassation a pris une décision qui va concerner des centaines de milliers de salariés : elle a validé le principe selon lequel les SMS envoyés ou reçus par un téléphone mis à la disposition par une entreprise sont « présumés avoir un caractère professionnel ». Par conséquent, les employeurs sont autorisés à lire ces messages, même hors de la présence des salariés.

« Cet arrêt est dans la droite ligne de décisions prises depuis quelques années, nous explique Olivier Iteanu, avocat à la cour d'appel de Paris. Peu à peu la jurisprudence en vient à plus protéger l'entreprise que le salarié. »

L'avocat rappelle ainsi qu'en 2012, un employeur avait été autorisé à consulter le contenu de la clé USB d'un salarié car celui-ci l'avait branchée sur le système informatique de l'entreprise. Un an plus tard, la Cour de cassation confirmait que les employeurs pouvaient consulter les e-mails de la boîte professionnelle de leurs salariés, même hors de leur présence, s'ils n'étaient pas identifiés comme personnels.

Concrètement, grâce à la décision prise en ce mois de février 2015, un employeur ayant « un motif légitime » peut vérifier les SMS en prenant le téléphone de son salarié ou « placer, en passant par des outils de Mobile Device Management (gestion de terminaux mobiles), des logiciels qui vont monitorer ce qui se passe sur le smartphone, pour en extraire les SMS qui pourront être analysés », nous précise Jean Pujol, manager au sein de l'entité conseil en stratégie SI du cabinet Kurt Salmon. « Les SMS peuvent aussi être stockés sur des serveurs centraux, comme cela était le cas dans l'affaire jugée par la Cour de cassation. »

Refuser le contrôle entraînera une sanction

Pour Me Martine Ricouart-Maillet, vice-présidente de l'Association française des correspondants à la protection des données personnelles et associée au sein du cabinet BRM Avocats, « afin d'éviter tout litige, le salarié doit être informé de l'usage qu'il peut faire des outils mis à sa disposition dans la charte informatique de l'entreprise. Cette charte doit aussi l'avertir des moyens de surveillance dont dispose son employeur. »

« Et s'il refuse de se soumettre à ce contrôle, ajoute Me Iteanu, le salarié pourra être sanctionné. » La sanction « suprême » étant le licenciement. Pour lui, cette décision risque d'induire des comportements abusifs de la part de certains employeurs. « Les juges devront très probablement se saisir de cas pour rétablir l'équilibre entre les parties », estime-t-il.

La seule solution pour protéger certains SMS est de les identifier comme personnels. Même si cela n'interdit pas à l'employeur de les lire, cela l'empêche de les utiliser contre un employé. Autre méthode, plus radicale : disposer de deux appareils, un professionnel et un personnel.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source :

<http://www.01net.com/editorial/646337/attention-votre-employeur-va-pouvoir-lire-les-sms-de-votre-telephone-pro/>
Par Cécile Bolesse

Piratage de ses comptes sociaux : prévenir, repérer

et réagir | Denis JACOPINI

x	Piratage de ses comptes sociaux : prévenir, repérer et réagir !
---	--

Sur les réseaux sociaux, la plus grande vigilance est requise si l'on veut protéger ses données personnelles.

Les réseaux sociaux se multipliant de façon considérable, il convient de se montrer attentif à la protection des données personnelles, car ces dernières peuvent d'autant plus facilement être piratées.

A ce titre, la Commission nationale de l'informatique et des libertés (CNIL) publie une fiche pratique, agrémentée de liens directs vers les principaux réseaux sociaux, afin de mettre en oeuvre le contrôle des données personnelles.

Parmi les conseils donnés par la Commission, citons :

- le choix de mots de passe complexes, mais aussi différents les uns des autres, et avec un sens n'ayant aucun rapport avec une donnée personnelle relative à la vie privée du titulaire du compte (comme une date de naissance, etc...) ;
- l'absence totale de communication du mot de passe à une tierce personne ;
- l'activation d'un dispositif d'alerte en cas d'intrusion (dans ce cas, la personne titulaire du compte et qui se connecte depuis un poste informatique inconnu doit confirmer l'accès en entrant un code, reçu préalablement par sms ou par mail) ;
- la déconnexion à distance des terminaux encore liés au compte ;
- la désactivation des applications tierces encore connectées au compte ;
- le réglage précis des paramètres de confidentialité.

En outre, la CNIL donne des astuces pour repérer le piratage d'un compte. Des signes doivent en effet alerter l'utilisateur, par exemple un mot de passe invalide, ou des comportements inhabituels ayant lieu sur le compte, sans consentement préalable (comme suivre, se désabonner, ou encore bloquer...).

En cas de piratage, il convient donc :

- en premier lieu, de signaler le compte piraté auprès du réseau social ;
- cette première étape franchie, il convient alors de demander une réinitialisation du mot de passe. Si la réponse apportées par les modérateurs du réseau n'est pas satisfaisante, la CNIL peut être saisie.

Consultez la fiche pratique de la CNIL

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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

<http://www.net-iris.fr/veille-juridique/actualite/34642/comment-prevenir-le-piratage-de-son-compte-en-ligne.php>

© 2015 Net-iris

10 conseils pour garder vos appareils protégés pendant les vacances | Denis JACOPINI



10 conseils pour
garder vos
appareils protégés
pendant les
vacances

Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, voici un mini-guide conçu par les experts ESET pour voyager et surfer en toute tranquillité.

Brosse à dents ? ok.
Serviette de bain ? ok.
Ordinateur, téléphone, tablette ? ok.

Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, méfiez-vous des menaces lorsque vous utilisez un Wi-Fi public pour vous connecter à votre banque en ligne, boutique en ligne ou tout simplement pour vérifier vos e-mails. Pas de panique ! Stephen Cobb et d'autres professionnels ESET ont créé un guide pour vous permettre de voyager en toute sécurité et garder ainsi toutes vos données personnelles et vos appareils protégés.

Conseils



1. Avant de prendre la route, assurez-vous d'exécuter sur vos appareils une mise à jour complète du système d'exploitation ainsi que des logiciels, et de posséder une solution de sécurité de confiance.
2. Sauvegardez vos données et placez-les dans un endroit sûr. Pensez à déplacer les données sensibles du disque dur de votre ordinateur portable sur un disque dur externe chiffré le temps de vos vacances.
3. Ne laissez jamais vos appareils sans surveillance dans les lieux publics. Activez la fonction antivol de vos appareils pour tracer les appareils volés ou perdus, et au besoin d'effacer les contenus à distance.
4. Mettez un mot de passe fort et activez la fonction « délai d'inactivité » sur tous vos appareils, que ce soit votre ordinateur portable, votre tablette ou votre téléphone. Retrouvez tous nos conseils pour un mot de passe efficace en cliquant ici.
5. Dans la mesure du possible, utilisez uniquement des accès internet de confiance. Demandez à votre hôtel ou l'endroit où vous logez le nom de leur Wi-Fi et utilisez exactement le même nom : faites attention aux arnaques qui essaient de ressembler aux Wi-Fi publics en ajoutant le mot « gratuit » au nom de la connexion Wi-Fi.
6. Si l'Internet de votre hôtel vous demande de mettre à jour un logiciel afin de pouvoir vous connecter, déconnectez-vous immédiatement et informez-en la réception.
7. Ne vous connectez pas à des connexions Wi-Fi qui ne sont pas chiffrées avec WPA2. Toutes les normes inférieures à celle-ci ne sont tout simplement pas assez sûres et peuvent être facilement piratées.
8. Si vous devez utiliser le Wi-Fi public pour vous connecter à votre réseau d'entreprise, utilisez toujours votre VPN (réseau virtuel privé).
9. Si ce n'est pas urgent, évitez les banques et boutiques en ligne quand vous utilisez le Wi-Fi public. Sinon, nous vous conseillons d'utiliser le partage de connexion de votre téléphone et de surfer en utilisant internet sur votre téléphone portable.
10. Si vous n'utilisez pas encore d'antivirus de confiance et suspectez votre ordinateur portable d'être infecté, vous pouvez utiliser gratuitement le scanner ESET Online qui ne nécessite aucune installation et peut être utilisé pour détecter et retirer des logiciels malveillants

Article original de ESET

[Cliquez ici](#)



Denis JACOPINI est Expert Informatique, spécialisé en cybersécurité et en protection des données personnelles.

- Expertises techniques (virus, spyware, phishing, fraude, arnaques Internet...) et judiciaires (investigation numérique, disparition d'emails, contenus, déblocage de données...);
- Expertises de systèmes de vote électronique;
- Formations et conférences en cybersécurité;
- Formation de C.I.L. (Correspondant Informatique et Clientèle);
- Accompagnement à la mise en conformité CNIL de votre établissement.


Le Net Expert
INFORMATIQUE
Kiosque et accompagnement en
Protection des Données Personnelles

[Contacter nous](#)

Réagissez à cet article

Original de l'article mis en page : ESET – Actualités

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits | Denis JACOPINI



Wi-Fi
Attention
au
piratage
sur les
vrais et
faux
réseaux
gratuits

Ce sont les vacances mais nombre de touristes ne se séparent pas de leurs smartphones, tablettes ou ordinateurs portables. Et pour se connecter à l'internet, quoi de mieux qu'attraper un wi-fi gratuit. Une pratique qui peut se révéler très dangereuse. Des proies faciles pour les « sniffeurs » de données. Explications de Laurent Heslault, expert sécurité chez Symantec.

Vous êtes sur votre lieu de vacances et vous avez envie de vous connecter à l'internet. Pour consulter votre messagerie ou vos réseaux sociaux, envoyer des photos à vos proches, surfer sur le net ou consulter votre compte en banque ou faire une réservation.

Solution la plus simple : se connecter à un réseau Wi-Fi gratuit. Dans votre hôtel, camping, à la terrasse d'un café ou d'un restaurant... Les accès gratuits pullulent et se généralisent.

Expert en sécurité à Symantec, Laurent Heslault tire le signal d'alarme. « Rien de plus simple que de pirater les données qui transitent sur un réseau Wi-Fi gratuit » assure-t-il. « Par exemple, je m'installe à la terrasse d'un café et je crée un vrai faux point d'accès gratuit en empruntant le nom du café. Des gens vont s'y connecter et je n'ai plus qu'à récupérer toutes les données qui m'intéressent. Des mots de passe, des identifiants... »

Des sniffeurs de données

Il exagère ? Non. « L'expérience a été faite à la terrasse d'un café. Nous avons installé un logiciel qui permet de sniffer tous les appareils qui se branchaient sur le Wi-Fi. Ensuite, des complices, qui se faisaient passer pour des magiciens, allaient voir les gens en disant que par magie, ils avaient réussi à changer le code de leur téléphone ou leur image sur Facebook. Ils étaient étonnés ! » Rien de magique mais des logiciels de piratage qui se trouvent facilement sur le net.

Les données sur le Wi-Fi ne sont pas chiffrées

« Les données qui transitent sur le Wi-Fi ne sont pas chiffrées. Sauf quand vous vous connectés à un site sécurisé avec le protocole HTTPS. Donc ce sont des données faciles à intercepter. » Danger sur les vrais faux points d'accès Wi-Fi mais aussi sur les vrais qui ne sont, dans la grande majorité des cas, pas chiffrés non plus. « Par contre pas de problème pour une connexion 3G ou 4G qui sont chiffrées. Mais pour économiser leur forfait, les gens préfèrent se connecter au Wi-Fi ».

Conseils

Alors quels conseils ? « Ne jamais, sur un Wi-Fi public, entrer un mot de passe. D'autant que la plupart des internautes utilisent le même mot de passe pour tous leurs sites. » En clair, limiter les dégâts en ne consultant que des sites qui ne demandent aucune identification.

Autre solution : protéger son smartphone ou sa tablette en y installent un logiciel qui va chiffrer toutes les données qui vont en sortir. Plusieurs types de logiciels existent dont le Wi-Fi Privacy de Norton qui est gratuit pendant 7 jours et peut s'installer sur des périphériques fonctionnant sous Ios et Android.

Article original de Samuel NOHRA.

Nous prodiguons une multitude d'autres conseils durant les formations que nous animons à destination des élus, chef d'entreprises, agents publics et salariés. [Consultez la liste de nos formations]



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

Original de l'article mis en page : Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

Mise en conformité RGPD : Accompagnement personnalisé par des Experts

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>
---	--	---	---	--	--



RGPD
LeNetExpert

**Mise en conformité RGPD :
Accompagnement personnalisé
par des Experts**

Vous souhaitez assister en présentiel pour le RDSP (peut-être un peu par obligation) et vous souhaitez nous faire part d'un projet. Nous vous remercions pour votre confiance.

Informé(e) sur des missions RDSP depuis 2012, après avoir identifié différents types d'attentes, nous avons adapté nos offres pour qu'elles correspondent au mieux à vos besoins.

1. Nos interventions d'accompagnement :

1.1. **Notre intervention d'accompagnement :** Nous venons vous accompagner pour appréhender l'essentiel de la réglementation Européenne relative à la Protection des Données à Caractère Personnel et le nécessaire pour comprendre et observer une mise en conformité, que soit la formation ad-hoc, vous êtes actives mais pouvez toujours compter sur notre soutien soit sous forme de formation personnalisée, soit sous forme d'accompagnement personnalisé ;

1.2. **L'issue de cette formation :** nous vous apportons une orientation précieuse la mise en place d'une démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général) sur la Protection des Données). Nos interventions, nous sommes référencés auprès de la CNIL.

2. **Nous souhaitons être accompagné pour la mise en place de la mise en conformité ?**

Nous intervenons pour vous l'aider à mettre en œuvre les plans d'actions, au terme de cette étape vous pourrez, si vous le souhaitez, valider la mise en conformité de votre établissement ou nous laisser procéder aux améliorations que vous aurez validées ;

3. **Nous souhaitons valider la mise en conformité de votre établissement ?** La mise en place de corrections dans le cadre de votre démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général) sur la Protection des Données) ;

4. **Notre intervention complémentaire :** nous venons vous accompagner dans votre démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général) sur la Protection des Données) et les différentes réglementations relatives à la protection des Données à Caractère Personnel.

Après de vous assurer une présentation personnalisée adaptée à la fois aux besoins de votre structure, conforme à votre stratégie et à vos priorités, nous discuterons que vous répondiez à nos questions.

Nous vous garantissons une confidentialité extrême sur les informations communiquées. Les personnes habilitées à les consulter sont soumises au secret professionnel.

1. Nom et Prénom / Nom (obligatoire)

2. Adresse e-mail

3. Votre adresse de messagerie (obligatoire)

4. Numéro de téléphone (ce sera peut-être utilisé pour la démo)

5. Pouvez-vous nous décrire brièvement votre activité ? (obligatoire)

Remarque : Vous pouvez nous écrire directement un message dans la case « **FORMATIONS COMPLÉMENTAIRES QUE VOUS VOUS DÉSIREZ UTILISER** ». Mentionnez, si vous souhaitez que nous vous établissions un chiffrage précis, nous aurons besoin dans un premier temps des informations ci-dessus.

1. Nos missions d'accompagnement :

1.1. **Notre intervention d'accompagnement :** Nous venons vous accompagner pour appréhender l'essentiel de la réglementation Européenne relative à la Protection des Données à Caractère Personnel et le nécessaire pour comprendre et observer une mise en conformité, que soit la formation ad-hoc, vous êtes actives mais pouvez toujours compter sur notre soutien soit sous forme de formation personnalisée, soit sous forme d'accompagnement personnalisé ;

1.2. **L'issue de cette formation :** nous vous apportons une orientation précieuse la mise en place d'une démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général) sur la Protection des Données). Nos interventions, nous sommes référencés auprès de la CNIL.

2. **Nous souhaitons être accompagné pour la mise en place de la mise en conformité ?**

Nous intervenons pour vous l'aider à mettre en œuvre les plans d'actions, au terme de cette étape vous pourrez, si vous le souhaitez, valider la mise en conformité de votre établissement ou nous laisser procéder aux améliorations que vous aurez validées ;

3. **Nous souhaitons valider la mise en conformité de votre établissement ?** La mise en place de corrections dans le cadre de votre démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général) sur la Protection des Données) ;

4. **Notre intervention complémentaire :** nous venons vous accompagner dans votre démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général) sur la Protection des Données) et les différentes réglementations relatives à la protection des Données à Caractère Personnel.

Après de vous assurer une présentation personnalisée adaptée à la fois aux besoins de votre structure, conforme à votre stratégie et à vos priorités, nous discuterons que vous répondiez à nos questions.

Nous vous garantissons une confidentialité extrême sur les informations communiquées. Les personnes habilitées à les consulter sont soumises au secret professionnel.

Le nom, prénom et e-mail à régler à : info@sestager.fr

Denis JACQZ est notre Expert qui vous accompagnera dans votre mise en conformité avec le RGPD



Je me présente : Denis JACQZ. Je suis expert en informatique avancée et spécialisé en RGPD, Protection des Données à Caractère Personnel et en cybersécurité. Consultant depuis 1996 et Formateur depuis 2006, j'ai une expérience depuis 2012 dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. Je formation d'abord technique, Correspondant OMI (CC) ; Correspondant Informatique et Libertés puis de mon métier à la Protection des Données (RGPD) ; en tant que praticien de la mise en conformité de l'établissement ; de mon expérience dans l'accompagnement de la mise en conformité avec le RGPD.

Mon objectif est de mettre à disposition toute mon expérience pour mettre en conformité votre établissement avec le RGPD. =