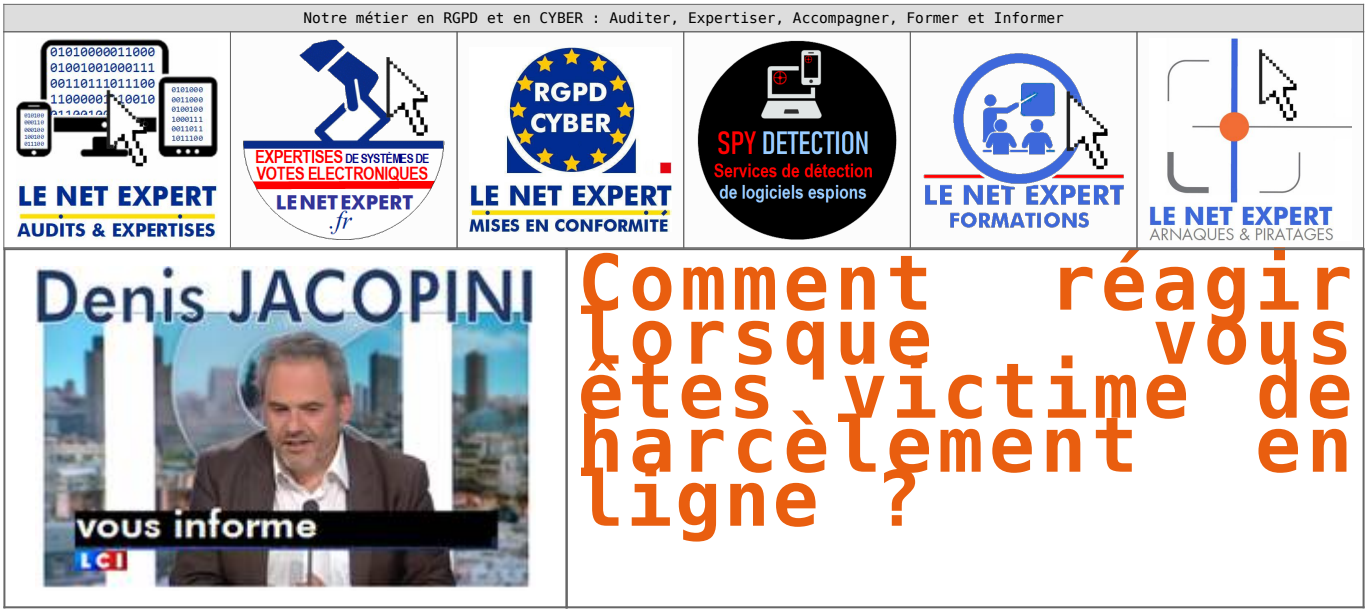
Comment réagir lorsque vous êtes victime de harcèlement en ligne ?

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



Selon un rapport européen, près de 10 % de la population européenne a subi ou subira un harcèlement*. Voici quelques conseils si vous êtes victime de ces violences sur internet et les médias sociaux.

Qui sont les cyber-harceleurs ?

Un(e) internaute peut être harcelé(e) pour son appartenance à une religion, sa couleur de peau, ses opinions politiques, son comportement, ses choix de vie … Le harceleur peut revêtir l'aspect d'un « troll » (inconnu, anonyme) mais également faire partie de l'entourage de la victime (simple connaissance, ex-conjoint, camarade de classe, collègue, voisin, famille …).

A quoi ressemble une situation de cyber-harcèlement ?

• Happy slapping : lynchage en groupe puis publication de la vidéo sur un site
• Propagation de rumeurs par téléphone, sur internet.
• Création d'un groupe, d'une page ou d'un faux profil à l'encontre de la personne.
• Publication de photographies sexuellement explicites ou humiliante
• Messages menaçants, insulte via messagerie privée
• Commande de biens/services pour la victime en utilisant ses données personnelles
• …

Comment réagir ?

Ne surtout pas répondre ni se venger

Vous avez la possibilité de bloquer l'accès de cette personne à vos publications, de la signaler auprès de la communauté ou d'alerter le réseau social sur un comportement qui contrevient à sa charte d'utilisation.

Verrouiller l'ensemble de vos comptes sociaux

Il est très important de limiter au maximum l'audience de vos comptes sociaux. Des options de confidentialité existent pour « ne plus me trouver », « ne pas afficher/partager ma liste d'amis ». Il est également possible de « bannir » les amis indésirables. Sur Facebook, une option vous permet d'être avertis si un autre utilisateur mentionne votre nom sur une photo (tag).

Les paramétrages conseillés sur Facebook :

PARAMÉTRAGE POSSIBLE	CHEMIN D'ACCÈS
Limiter la visibilité de vos photos	Ce type d'option ne fonctionne que photo par photo
Limiter la visibilité de vos informations de profil	Informations générales : page du profil > encart gauche > sélectionner « amis » ou « moi uniquement »
Cacher votre liste d'amis	Page du profil > onglet « amis » > « gérer section » > « modifier la confidentialité » > « liste d'amis » ou « moi uniquement »
Cacher vos mentions « j'aime »	Page du profil > Mentions j'aime (encart gauche) > « modifier la confidentialité » > « moi uniquement »
Être prévenu si quelqu'un vous « tague »	Paramètre > journal et identification > Paramètres d'identification et de journal> « examiner les identifications »
Limiter la visibilité de vos publications	Journal > sélectionner la publication > « moi uniquement » / ou « supprimer »
Examiner votre historique	Page du profil > « afficher l'historique personnel » > supprimer au cas par cas

• Capture écran des propos / propos tenus

Ces preuves servent à justifier votre identité, l'identité de l'agresseur, la nature du cyber-harcèlement, la récurrence des messages, les éventuels complices. Sachez qu'il est possible de faire appel à un huissier pour réaliser ces captures.Fiche pratique : comment réaliser une copie d'écran ?

• Portez plainte auprès de la Gendarmerie/Police si le harcèlement est très grave

Vous avez la possibilité de porter plainte auprès du commissariat de Police, de Gendarmerie ou du procureur du tribunal de grande instance le plus proche de votre domicile.

• En parler auprès d'une personne de confiance

La violence des termes employés par l'escroc et le risque d'exposition de votre vie privée peuvent être vécus comme un traumatisme. Il est conseillé d'en parler avec une personne de confiance.

Si quelqu'un d'autre est harcelé ?

Le fait de « partager » implique votre responsabilité devant la loi. Ne faites jamais suivre de photos, de vidéos ou de messages insultants y compris pour dénoncer l'auteur du harcèlement. Un simple acte de signalement ou un rôle de conseil auprès de la victime est bien plus efficace ! ***Le chiffre :*** *61% des victimes indiquent qu'elles n'ont reçu aucun soutien quel qu'il soit de la part d'organismes ou d'une personne de leur réseau personnel.* *
Source: rapport européen sur le cyber-harcèlement (2013)

Si vous êtes victime et avez moins de 18 ans …

Composez le 3020. Il est ouvert du lundi au vendredi de 9h à 18h (sauf les jours fériés). Le numéro vert est géré par la plateforme nonauharcelement.education.gouv.fr qui propose de nombreuses ressources pour les victimes, témoins, parents et professionnels (écoles, collèges, lycées). **Si le harcèlement a lieu sur internet,**vous pouvez également composer le 0800 200 000 ou vous rendre sur netecoute.fr. La plateforme propose une assistance gratuite, anonyme, confidentiel par courriel, téléphone, chat en ligne, Skype. Une fonction « être rappelé par un conseiller » est également disponible. La réponse en ligne est ouverte du lundi au vendredi de 9h à 19h. **Un dépôt de plainte est envisagé ?** Renseignez vous surle dépôt de plainte d'un mineur. Celui-ci doit se faire en présence d'un ou de plusieurs parents ou d'un représentant légal. N'hésitez pas à contacter les télé-conseillers du fil santé jeune au 0800 235 236.

Quelles sanctions encourues par l'auteur de ces violences en ligne ?

L'auteur de tels actes est susceptible de voir sa responsabilité engagée sur le fondement du Droit civil, du Droit de la presse ou du Code pénal.
Quelques exemples de sanctions :
• Une injure ou une diffamation publique peut être punie d'une amende de 12.000€ (art. 32 de la Loi du 29 juillet 1881).
• Pour le droit à l'image, la peine maximum encourue est d'un an de prison et de 45.000 € d'amende (art. 226-1, 226-2 du Code pénal).
• L'usurpation d'identité peut être punie d'un an d'emprisonnement et de 15.000€ d'amende (art. 226-4-1 du Code pénal).

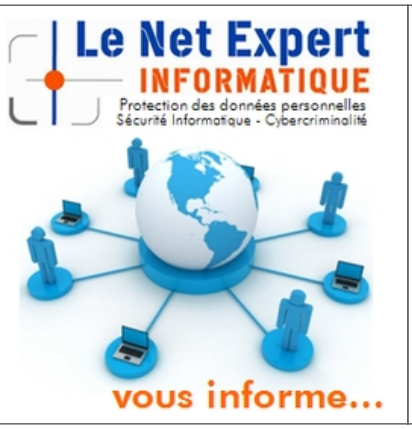
Quels sont les recours auprès de la CNIL ?

La qualification et la sanction de telles infractions relève de la seule compétence des juridictions judiciaires. En parallèle de telles démarches, **vous pouvez demander la suppression de ces informations à chaque site ou réseau social d'origine, en faisant valoir votre droit d'opposition**, pour des motifs légitimes, sur le fondement de l'article 38 de la loi du 6 janvier 1978 modifiée dite « Informatique et Liberté ». Le responsable du site dispose d'un délai légal de deux mois pour répondre à votre demande. La majorité des sites propose un bouton « signaler un abus ou un contenu gênant ». Si aucun lien n'est proposé, contactez directement par courriel ou par courrier le responsable du site en suivant la procédure expliquée sur notre site. Par ailleurs, **si ces informations apparaissent dans les résultats de recherche à la saisie de vos prénom et nom, vous avez la possibilité d'effectuer une demande de déréférencement auprès de Google en remplissant le formulaire**. En cas d'absence de réponse ou de refus, vous pourrez revenir vers la CNIL en joignant une copie de votre demande effectuée auprès du moteur de recherche incluant le numéro de requête Google. Pour plus d'informations, consulter la fiche.
Source : CNIL
[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :
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 : Réagir en cas de harcèlement en ligne | CNIL

Les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données | Denis JACOPINI



Les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données

Varonis a mené une enquête en mars auprès des informaticiens professionnels participant au CeBIT, le plus grand salon IT d'Allemagne, afin de recueillir leur opinion sur la nouvelle réglementation régissant la protection des données qui doit entrer en vigueur cette année ou l'année prochaine. Le constat est sans appel : les entreprises ne sont pas prêtes pour la nouvelle législation européenne sur la protection des données. Les professionnels interrogés par Varonis ne pensent pas que leurs entreprises soient en mesure de respecter les délais imposés par l'UE pour la notification des violations de données.

Il ressort de cette enquête que 80 % des personnes interrogées pensent qu'une banque sera très probablement la première entreprise à être frappée par l'amende maximale de 100 millions d'euros pour non-respect de la réglementation européenne sur la protection des données. À la question concernant le pays le plus probable de cette banque, les répondants indiquent l'Allemagne (30 %), les États-Unis (28 %) et 22 % mentionnent un autre pays européen. 48 % seulement des personnes interrogées pensent que leur entreprise pourrait signaler une violation dans le délai obligatoire de 72 heures.
Seuls 31 % disposent d'un plan leur permettant de se conformer à la nouvelle législation et seulement un tiers des personnes enquêtées a mis en place les processus et la technologie nécessaires pour empêcher leur entreprise de se voir infliger une amende importante dans le cadre de cette loi. 71 % des répondants sont incapables de dire ce que les entreprises doivent faire pour se conformer à la nouvelle réglementation.
Seuls 22 % des répondants savaient que l'amende maximale prévue par la nouvelle législation est de 100 millions d'euros, 41 % pensaient qu'elle ne serait que de 10 millions d'euros et 32 % l'estimaient à 1 million d'euros, avec un nombre réduit de personnes interrogées croyant qu'elle pouvait s'élever à un milliard d'euros. Un tiers a déclaré que la réglementation européenne sur la protection des données entrera en vigueur en 2015, 28 % ont indiqué que tel serait le cas en 2016, 7 % estiment que la loi ne verra jamais le jour et 32 % des personnes interrogées ont dit ne pas savoir quand la loi entrerait en vigueur.
« Nous pouvons attendre une refonte majeure de la loi européenne sur la protection des données au cours des prochains 12 à 24 mois », déclare David Gibson, vice-président du marketing de Varonis. « Les amendes devraient s'élever à 2 % du revenu annuel avec un plafond de 100 millions d'euros ou de dollars pour la non-protection des données personnelles des citoyens européens. Il pourrait également y avoir un nombre important de plaintes individuelles en plus des amendes et les sommes mises en jeu pourraient donc représenter des coûts substantiels, même pour les grandes entreprises. La nouvelle loi marquera aussi le passage d'un environnement autoréglementé à un régime d'application obligatoire qui aura une incidence sur toute entreprise stockant des informations d'identification personnelle concernant les citoyens européens (y compris sur les sociétés américaines menant des activités dans l'UE). Les entreprises doivent être préparées à protéger les données de leurs clients et prouver qu'elles le font avec le soin approprié, rendre compte de toute violation et supprimer les données à la demande des citoyens de l'UE. »
« Compte tenu de la vaste portée de la nouvelle réglementation et de l'importance accrue des amendes, cette enquête révèle des inquiétudes très importantes quant aux efforts que les entreprises sont prêtes à fournir pour se conformer aux conditions de la réglementation et gérer les scénarios de violation de données », indique Mark Deem, partenaire de Cooley LLP au Royaume-Uni. « En fait, l'échelle des amendes potentielles sera plus proche de celles infligées pour corruption ou violation antitrust, ou dans le secteur des services financiers. La conformité en matière de protection des données sera tout aussi importante que la conformité aux réglementations de la FCA. Même si la législation n'entre pas en vigueur avant 2017, un travail considérable doit être accompli par ceux qui souhaitent offrir des biens et des services aux habitants de l'UE et s'assurer qu'ils se trouvent dans la meilleure situation possible pour respecter la loi. »
Varonis propose 7 conseils pour garantir la conformité des données non structurées et permettre aux entreprises de se préparer à la réglementation européenne sur la protection des données :

1. Minimiser la collecte des données : la proposition de loi de l'UE comporte de fortes exigences en ce qui concerne la limitation des données recueillies auprès des consommateurs.

2. Favoriser le signalement des violations de données : la notification des atteintes à la protection des données constitue une nouvelle exigence que les entreprises européennes devront respecter.

3. Conserver les données avec attention : les règles de minimisation de la nouvelle loi concernent non seulement l'étendue des données collectées, mais aussi leur durée de rétention. En d'autres termes, une entreprise ne doit pas stocker les données plus longtemps que nécessaire aux fins prévues.

4. Nouvelle définition des identifiants personnels : l'UE a étendu la définition des identifiants personnels et ce changement s'avère important parce que les lois de l'UE portent sur la protection de ces identifiants.

5. Employez un langage clair : il faudra à une entreprise le consentement préalable et explicite des consommateurs lors de la collecte des données.

6. Bouton d'effacement : le « droit d'effacement » signifie qu'en cas de retrait du consentement accordé par les consommateurs, les sociétés devront supprimer les données concernées.

7. Le Cloud computing n'échappe pas à cette nouvelle loi de l'UE, car celle-ci suit les données.

Méthodologie de l'enquête
Les 145 personnes interrogées constituent un échantillon représentatif des participants du plus grand salon informatique d'Allemagne qui a compté 221 000 visiteurs en mars 2015. Parmi les répondants, 16 % sont issus de banques allemandes, 3 % de banques américaines, 3 % de banques européennes, 45 % d'entreprises allemandes hors du secteur financier, 26 % d'entreprises européennes hors du secteur financier et 7 % d'entreprises américaines.

Loi Renseignement : la boîte à outils pour apprendre à protéger votre vie privée, en chiffrant vos données et

communications | Denis JACOPINI

	Loi Renseignement : la boîte à outils pour apprendre à protéger votre vie privée, en chiffrant vos données et communications

Maintenant que la Loi Renseignement est votée, et en attendant la suite du processus législatif, apprenons à résister à la surveillance de masse avec quelques outils cryptographiques plus ou moins simples, mais efficaces et légaux.

Nous sommes le soir du mardi 5 mai, et c'est un jour funeste pour la démocratie. La France s'était autoproclamée « pays des Lumières » parce qu'il y a 250 ans notre pays éclairait l'Europe et le monde grâce aux travaux philosophiques et politiques de Montesquieu, qui prônait la séparation des pouvoirs, et de Voltaire et Rousseau.
À dater d'aujourd'hui, jour du vote en première lecture du projet de loi sur le renseignement, à cause d'une classe politicienne d'une grande médiocrité, s'enclenche un processus au terme duquel le peuple français va probablement devoir subir une loi dangereuse, qui pourrait s'avérer extrêmement liberticide si elle tombait entre de mauvaises mains, par exemple celles de l'extrême droite.
Même si la loi doit encore passer devant le Sénat puis peut-être revenir en seconde lecture à l'Assemblée Nationale, même si une saisine du Conseil Constitutionnel va être déposée par une soixantaine de courageux députés en complément de celle déjà annoncée par François Hollande, mieux vaut se préparer au pire, en imaginant que cette loi sera un jour promulguée. En faisant un peu de mauvais esprit, j'ai imaginé un nom pour le dispositif qui sera chargé de collecter nos données personnelles afin de détecter les comportements suspects : « Surveillance Totalement Automatisée via des Systèmes Informatiques » et bizarrement l'acronyme est STASI !
Dès lors, à titre préventif et sans préjuger de l'avenir, il me semble important d'apprendre à protéger sa vie privée. Ceci passe par le chiffrement de ses communications, qu'il s'agisse d'échanges sur Internet ou via SMS, et cela peut se faire au moyen de différents outils à la fois efficaces et légaux.
Bien évidemment, les « vrais méchants » que sont les terroristes, djihadistes, gangsters et autres trafiquants connaissent et utilisent déjà ces outils : vous vous doutez bien qu'ils n'ont pas attendu ce billet de blog pour les découvrir….

Une boîte à outils pour protéger votre vie privée

Anonymat sur Internet

Pour protéger votre identité sur Internet et notamment sur le web, vous pouvez combiner l'utilisation d'un réseau privé virtuel, ou VPN, et de TOR, un système d'anonymisation qui nécessite l'installation d'un logiciel spécifique, TOR Browser. Je ne vous donne pas de référence particulière en matière de VPN, car l'offre est pléthorique.

MAJ : un lecteur m'a indiqué l'existence de La brique Internet, un simple boîtier VPN couplé à un serveur. Pour que la Brique fonctionne, il faut lui configurer un accès VPN, qui lui permettra de créer un tunnel jusqu'à un autre ordinateur sur Internet. Une extension fournira bientôt aussi en plus un accès clé-en-main via TOR en utilisant la clé wifi du boîtier pour diffuser deux réseaux wifi : l'un pour un accès transparent via VPN et l'autre pour un accès transparent via Tor.

Chiffrement des données

Pour chiffrer le contenu de vos données, stockées sur les disques durs de vos ordinateurs ou dans les mémoires permanentes de vos smartphones, vous pouvez mettre en œuvre des outils tels que LUKS pour les systèmes Linux ou TrueCrypt pour les OS les plus répandus : même si TrueCrypt a connu une histoire compliquée, son efficacité ne semble pas remise en cause par le dernier audit de code effectué par des experts.

Je vous signale aussi que l'ANSSI – Agence nationale de la sécurité des systèmes d'information – signale d'autres outils alternatifs comme Cryhod, Zed !, ZoneCentral, Security Box et StormShield. Même si l'ANSSI est un service gouvernemental il n'y a pas de raison de ne pas leur faire confiance sur ce point

Chiffrement des e-mails et authentification des correspondants

GPG, acronyme de GNU Privacy Guard, est l'implémentation GNU du standard OpenPGP. Cet outil permet de transmettre des messages signés et/ou chiffrés ce qui vous garantit à la fois l'authenticité et la confidentialité de vos échanges. Des modules complémentaires en facilitent l'utilisation sous Linux, Windows, MacOS X et Android.

MAJ : un lecteur m'a signalé PEPS, une solution de sécurisation française et Open Source, issue d'un projet mené par la DGA – Direction générale de l'armement – à partir duquel a été créée la société MLState.

Messagerie instantanée sécurisée

OTR, Off The Record, est un plugin à greffer à un client de messagerie instantanée. Le logiciel de messagerie instantanée Jitsi, qui repose sur le protocole SIP de la voix sur IP, intègre l'outil de chiffrement ZRTP.

Protection des communications mobiles

A défaut de protéger les métadonnées de vos communications mobiles, qu'il s'agisse de voix ou de SMS, vous pouvez au moins chiffrer les données en elles-mêmes, à savoir le contenu de vos échanges :

RedPhon est une application de chiffrement des communications vocales sous Android capable de communiquer avec Signal qui est une application du même fournisseur destinée aux iPhone sous iOS.

TextSecure est une application dédiée pour l'échange sécurisé de SMS, disponible pour Android et compatible avec la dernière version de l'application Signal. Plus d'information à ce sujet sur le blog de Stéphane Bortzmeyer.

MAJ : un lecteur m'a indiqué l'application APG pour Android qui permet d'utiliser ses clés GPG pour chiffrer ses SMS.

Allez vous former dans les « cafés Vie Privée »

Si vous n'êtes pas geek et ne vous sentez pas capable de maîtriser ces outils sans un minimum d'accompagnement, alors le concept des « cafés Vie Privée » est pour vous : il s'agit tout simplement de se réunir pour apprendre, de la bouche ceux qui savent le faire, comment mettre en œuvre les outils dont je vous ai parlé plus haut afin de protéger sa vie privée de toute intrusion, gouvernementale ou non.

Tout simplement, il s'agit de passer un après-midi à échanger et à pratiquer la cryptographie. Pour cela sont proposés des ateliers d'une durée minimum de 1 heure, axés autour de la sécurité informatique et de la protection de la vie privée.

Et comme le disent avec humour les organisateurs, « les ateliers sont accessibles à tout type de public, geek et non-geek, chatons, poneys, loutres ou licornes. ». Bref, le « café Vie Privée » est à la protection de la vie privée ce que la réunion Tupperware était à la cuisine

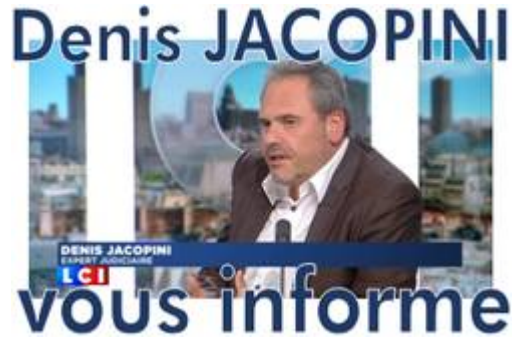
Voilà, vous avez je l'espère suffisamment d'éléments pratiques pour commencer à protéger votre vie privée… en espérant vraiment que le Conseil Constitutionnel abrogera les points les plus contestables de cette loi et nous évitera d'avoir à déployer un tel arsenal sécuritaire.

PS : l'image « 1984 was not a manual » a été créée par Arnaud Velten aka @Bizcom.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/loi-renseignement-la-bo-te-a-outils-pour-apprendre-a-proteger-votre-vie-privee-en-chiffrant-vos-donnees-et-communications-39818894.htm
Par Pierre Col

Un outil gratuit pour analyser et nettoyer votre ordinateur



Un outil gratuit pour analyser et nettoyer votre ordinateur

Avec plus de 40.000 visiteurs uniques par an, ESET Online Scanner apparaît comme l'un des outils gratuits les plus plébiscités par les internautes soucieux de leur sécurité. Fort de ce constat, ESET améliore son scanner basé sur le moteur d'analyse ThreatSense® permettant d'analyser et nettoyer son ordinateur sans contrainte d'installation logicielle.

Conçue pour être conviviale, cette dernière version devient complètement indépendante des navigateurs Internet. De plus, l'installation est désormais possible sans les droits d'administrateur, ce qui rend l'analyse et le nettoyage des ordinateurs contenant des logiciels malveillants encore plus simples.
ESET Online Scanner améliore l'élimination des logiciels malveillants, par l'ajout de ces nouvelles fonctions :
• **Analyse des emplacements de démarrage automatique** et du secteur d'amorçage pour les menaces cachées – choix de cette option dans setup / cibles d'analyse avancées
• **Nettoyage du registre système** – Supprime les traces des logiciels malveillants du registre système
• **Nettoyage après analyse lors du redémarrage** – Si nécessaire, ESET Online Scanner est capable de repérer les malwares les plus persistants afin de les nettoyer après redémarrage
Pour plus d'informations sur l'outil gratuit ESET Online Scanner, contactez-nous ou rendez-vous sur http://www.eset.com/fr/home/products/online-scanner/

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées 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.

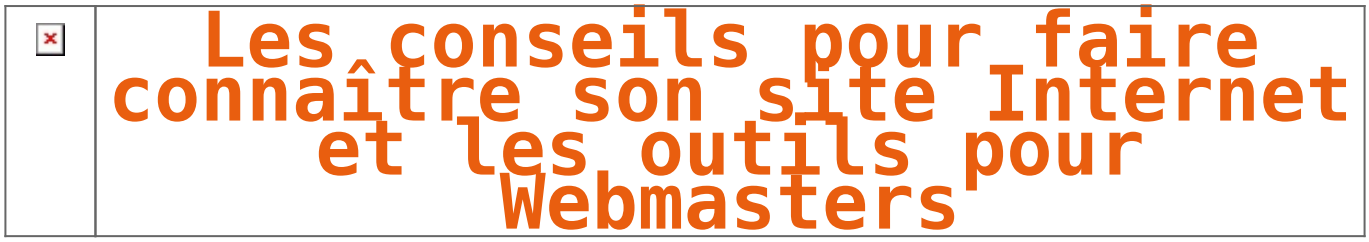
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Boîte de réception (10) – denis.jacopini@gmail.com – Gmail

Les conseils pour faire connaître son site Internet et les outils pour Webmasters | Denis JACOPINI



AUDIT DE CONTENU DE SITES INTERNET

Google Webmaster Tools
Google Webmaster Tools est un outil pertinent et facile d'utilisation pour les éditeurs qui cherchent à optimiser le référencement naturel de leurs pages web. De l'exploration des pages par les robots, à l'analyse des mots-clés, en passant par la qualité/quantité des liens retours et le positionnement des pages : il analyse de nombreux paramètres SEO décisifs pour améliorer la visibilité d'un site web sur Google.

Screaming Frog
Disponible pour Mac et PC,Screaming Frog audite un site, ses liens, images, CSS et scripts pour en ressortir des indicateurs utiles à l'indexation et au SEO. Au-delà des erreurs HTTP rencontrées lors du crawl, l'outil va également faire remonter les balises Title, H1 ou H2 manquantes, dupliquées ou trop longues. L'ancre des liens rencontrés est précisée, tout comme leur éventuel attribut *nofollow*.

Bing pour Webmasters

Certes, « Bing Webmaster » est plus intéressant pour des sites positionnés dans des pays où Bing a une part de marché significative, mais même en France, il a plusieurs intérêts. Puisqu'il peut par exemple auditer un site, ou retrouver des liens pointant vers n'importe quelle page.

MajesticSEO
MajesticSEO analyse des liens entrants de n'importe quel site web. Ses indicateurs maison, le score de citation (« Citation Flow ») et le score de crédibilité (« Trust Flow »), sont souvent cités par les SEO pour évaluer la qualité d'un site web et de ses liens sortants. Bâti sur des centaines de milliards d'URL crawlées, le service est régulièrement actualisé, et propose souvent de nouvelles fonctionnalités.

Open Site Explorer
Open Site Explorer ou OSE est un outil est bien connu pour ses analyses de backlinks et de l'autorité de leur origine.
OSE peut être utilisé gratuitement, mais en version bridée. L'analyse complète, et certains indicateurs, comme ceux concernant les partages sociaux d'une page, sont cependant réservés à la version payante.

Moz
Certains outils de cette suite sont gratuits, comme la météo des pages de résultats de Google.com ou l'analyse des comptes Twitter. Mais les plus utiles (analyse de mot clé, crawl et audit de site, suivi de position…) nécessitent un abonnement, facturé à partir de 99 dollars par mois.

AUDIT DE TEST DE SITE INTERNET

WebPageTest – Mesure de vitesse d'ouverture des pages

FAIRE CONNAITRE SON SITE INTERNET SUR LES RESEAUX SOCIAUX

15/04/2014 26 idées pour obtenir plus d’abonnés Google+

Cet article vous à plu ? Laissez-nous un commentaire
(notre source d’encouragements et de progrès)

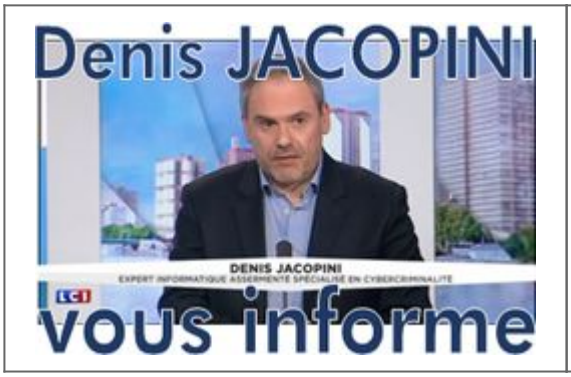
Références :

28/02/2014
http://www.journaldunet.com/solutions/seo-referencement/seo-les-meilleurs-outils/google-webmaster-tools.shtml

27/02/2014
http://ecommerce-live.net/event/nouvelle-strategie-de-referencement-en-2014-quand-le-virtuel-rencontre-le-reel-3/

**Cet article vous à plu ? Laissez-nous un commentaire
(notre source d’encouragements et de progrès)**

Comment bien choisir ses mots de passe ?



Comment bien choisir ses mots de passe ?

Les mots de passe sont une protection incontournable pour sécuriser l'ordinateur et ses données ainsi que tous les accès aux services sur Internet. Mais encore faut-il en choisir un bon.Un bon mot de passe doit être difficile à deviner par une personne tierce et facile à retenir pour l'utilisateur.

Qu'est ce qu'un bon mot de passe ?

Un bon de passe est constitué d'au moins **12 caractères** dont :

• des lettres majuscules
• des lettres minuscules
• des chiffres
• des caractères spéciaux

Un mot de passe est d'autant plus faible qu'il est court. L'utilisation d'un alphabet réduit ou de mot issu du dictionnaire le rend très vulnérable.
Les mots du dictionnaire ne doivent pas être utilisés.
Aussi à proscrire, les mots en relation avec soi, qui seront facilement devinables : nom du chien, dates de naissances…
Réseaux sociaux, adresses mail, accès au banque en ligne, au Trésor public, factures en ligne.
Les accès sécurisés se sont multipliés sur internet.
Au risque de voir tous ses comptes faire l'objet d'utilisation frauduleuse, il est impératif de **ne pas utiliser le même mot de passe**pour des accès différents.
Alors, choisir un mot de passe pour chaque utilisation peut vite devenir un vrai casse-tête.

Comment choisir et retenir un bon mot de passe ?

Pour créer un bon mot de passe, il existe plusieurs méthodes :

La méthode phonétique

Cette méthode consiste à utiliser les sons de chaque syllabe pour créer une phrase facilement mémorisable.
Exemple : « j'ai acheté huit cd pour cent euros ce après-midi» donnera : ght8CD%E7am

La méthode des premières lettres

Utiliser les premières lettres d'une phrase en variant majuscules, minuscules et caractères spéciaux.
Exemple : « un tiens vaut mieux que deux tu l'auras » donnera : 1TvmQ2tl'@

Diversifier facilement les mots de passe

Opter pour une politique personnelle avec, par exemple, un préfixe pour chaque type d'activité. Comme BANQUE-MonMotDePassz pour la banque, IMP-MonMotDePasse pour les impôts. Quelque chose de très facile à mémoriser qui complexifie votre mot de passe et, surtout, vous permet de le diversifier.

Diminuer les imprudences

Pour finir, il est utile de rappeler de **ne pas stocker ses mots de passe à proximité de son ordinateur** si il est accessible par d'autres personnes. L'écriture sur le post-it déposé sous le clavier est à proscrire par exemple, de même que le stockage dans un fichier de la machine.
En règle général, les logiciels proposent de **retenir les mots de passe**, c'est très **tentant mais imprudent**. Si votre ordinateur fait l'objet d'un piratage ou d'une panne, les mots de passe seront accessibles par le pirate ou perdus.

Que faire en cas de piratage ?

Il est recommandé de préserver les traces liées à l'activité du compte.
Ces éléments seront nécessaires en cas de dépôt de plainte au commissariat de Police ou à la Gendarmerie.
Exemple
Compte email piraté
Vos contacts ont reçu des messages suspects envoyés de votre adresse.
Contactez-les pour qu'ils conservent ces messages.
Ils contiennent des informations précieuses pour l'enquêteur qui traitera votre dépôt de plainte.
Récupérez l'accès à votre compte afin de changer le mot de passe et re-sécurisez l'accès à votre compte.

Changer de mots de passe régulièrement

Cette dernière règle est contraignante mais assurera un niveau supérieur de sécurité pour vos activités sur Internet.
Un **bon mot de passe doit être renouvelé plusieurs fois par an** et toujours en utilisant les méthodes décrites ci-dessus.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées 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.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Comment choisir ses mots de passe ? / Cybercrime / Dossiers / Actualités – Police nationale – Ministère de l’Intérieur

---

Vidéosurveillance en entreprise : règles et limites | Denis JACOPINI

Un système de vidéosurveillance en entreprise se doit d'observer certaines limites pour rester dans un cadre de protection des biens et personnes.

Le cadre législatif de la vidéosurveillance
C'est la loi dite « informatique et libertés » du 6 janvier 1978, modifiée par la loi du 6 août 2004, qui fixe le cadre de mise en place d'une vidéosurveillance sur un lieu à usage professionnel.
Ainsi dans des lieux non accessibles au public (bureaux, entrepôts, réserves, locaux d'administration) l'installation d'une vidéosurveillance doit faire l'objet d'une déclaration à la CNIL (Commission Nationale Informatique et Libertés).
C'est également une obligation pour les guichets de réception de clients et les commerces, lorsque le système enregistre les images dans un fichier et permettant de conserver d'identité des personnes filmées.
Si toutefois les fichiers ne sont pas conservés à des fins d'identification, un assouplissement de la loi permet de solliciter une simple autorisation préfectorale (pour les lieux accueillant du public).

Information des salariés et du public
Une information préalable est requise auprès des représentants des salariés avant tout installation d'un dispositif de vidéosurveillance, en mettant l'accent sur les objectifs de sécurité et en spécifiant que les enregistrements ne sont pas conservés plus d'un mois.
De la même manière, l'entreprise doit mettre en place une signalisation informant les visiteurs de la présence d'un système de vidéosurveillance.
Cet affichage doit se faire dès l'entrée dans l'établissement, en précisant les raisons ainsi que les coordonnées de l'autorité ou de la personne chargée de l'exploitation du système et en rappelant les modalités d'exercice du droit d'accès des personnes filmées aux enregistrements qui les concernent (loi du 6 août 2004).

Le principe de proportionnalité
On pourrait dire aussi principe de bon sens. L'employeur doit en premier lieu démontrer l'intérêt légitime à la mise en place d'un système de surveillance. Il peut s'agir de la nécessité de protéger des personnes ou des biens, ou de se prémunir contre des risques tels que le vol.
Partant de là, le dispositif installé doit être proportionnel au regard des intérêts à protéger.
Il y a une différence notoire entre installer une caméra dans un entrepôt à des fins de sécurité et le fait d'en installer une permettant d'observer en permanence des postes de travail.
Bien évidemment des caméras installées dans des lieux de repos des salariés ou dans des toilettes constituent une surveillance excessive. La CNIL a récemment mis à l'amende des entreprises pour des situations de surveillance jugées excessives et non proportionnées par rapport aux risques à prévenir.
La CNIL a fait valoir que des caméras peuvent être installées au niveau des entrées et sorties des bâtiments, des issues de secours et des voies de circulation, ou encore filmer les zones où de la marchandise ou des biens de valeur sont entreposés. Pas question en revanche de filmer en permanence un employé sur son poste de travail, sauf si celui-ci manipule par exemple de l'argent, en vertu du principe de proportionnalité.
En synthèse, bien que frappée du sceau du bon sens, la mise en place d'un système de vidéosurveillance doit s'accompagner de certaines précautions. Eventuellement prenez avis auprès de votre conseiller en assurances, qui saura vous orienter vers un prestataire de vidéosurveillance homologué et bien au fait des contraintes législatives.

Source :
http://www.comptanoo.com/assurance-prevention/actualite-tpe-pme/23794/videosurveillance-entreprise-regles-et-limites

Règlement européen sur la protection des données : Transparence et responsabilisation

	Règlement européen sur la protection des données : Transparence et responsabilisation

Alors que la directive de 1995 reposait en grande partie sur la notion de « formalités préalables » (déclaration, autorisations), le règlement européen repose sur une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur.

Une clé de lecture : la protection des données dès la conception et par défaut (*privacy by design*)

Les responsables de traitements devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut. Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).

Un allègement des formalités administratives et une responsabilisation des acteurs

Afin d'assurer une protection optimale des données personnelles qu'ils traitent de manière continue, les responsables de traitements et les sous-traitants devront mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment (*accountability*).

La conséquence de cette responsabilisation des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes. Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

De nouveaux outils de conformité :

- la tenue d'un registre des traitements mis en œuvre
- la notification de failles de sécurité (aux autorités et personnes concernées)
- la certification de traitements
- l'adhésion à des codes de conduites
- le DPO (délégué à la protection des données)
- les études d'impact sur la vie privée (EIVP)

Les « études d'impact sur la vie privée » (EIVP ou PIA)

Pour tous les traitements à risque, le responsable de traitement devra conduire une étude d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques), et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.

Si l'organisme ne parvient pas à réduire ce risque élevé par des mesures appropriées, il devra consulter l'autorité de protection des données avant de mettre en œuvre ce traitement. Les « CNIL » pourront s'opposer au traitement à la lumière de ses caractéristiques et conséquences.

Une obligation de sécurité et de notification des violations de données personnelles pour tous les responsables de traitements

Les données personnelles doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées.

Lorsqu'il constate une violation de données à caractère personnel, le responsable de traitement doit notifier à l'autorité de protection des données la violation dans les 72 heures.

L'information des personnes concernées est requise si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne.

Le Délégué à la Protection des données (*Data Protection Officer*)

Les responsables de traitement et les sous-traitants devront obligatoirement désigner un délégué :

- s'ils appartiennent au secteur public,
- si leurs activités principales les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
- si leurs activités principales les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations.

En dehors de ces cas, la désignation d'un délégué à la protection des données sera bien sûr possible.

Les responsables de traitement peuvent opter pour un délégué à la protection des données mutualisé ou externe.

Le délégué devient le véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Il est ainsi chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
- de contrôler le respect du règlement européen et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA) et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

source : CNIL

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger**pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées 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.

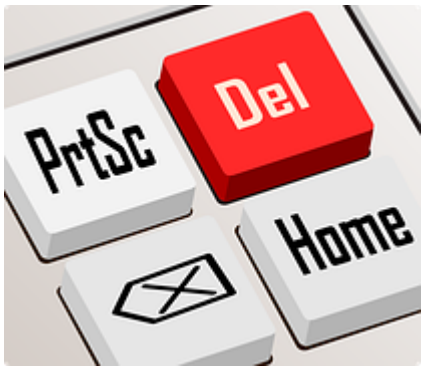
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Règlement européen sur la protection des données : ce qui change pour les professionnels | CNIL

Pourquoi supprimer vos données personnelles si vous rendez votre ordinateur professionnel à votre employeur ?



Pourquoi supprimer vos données personnelles si vous rendez votre ordinateur professionnel à votre employeur ?

Ne pas effacer ses données personnelles sur son ordinateur de fonction est-il dommageable (risque d'accès à nos données personnelles, vol d'identité ou accès frauduleux etc…)? Si oui, pourquoi ?

Imaginez, votre ordinateur, protégé ou non, tombe entre les mains d'une personne malveillante. Il pourra :
• Accéder à vos documents et découvrir les informations qui peuvent soit être professionnelles et être utilisées contre vous, soit personnelles permettant à un voyou de les utiliser contre vous soit en vous demandant de l'argent contre son silence ou pour avoir la paix ;
• Accéder aux identifiants et mots de passe des comptes internet que vous utilisez (même pour des sites Internet commençant par https) et ainsi accéder à nos comptes facebook, twitter, dropbox… ;
• Avec vos identifiants ou en accédant à votre système de messagerie, le pirate pourra facilement déposer des commentaires ou envoyer des e-mails en utilisant votre identité. Même si l'article 226-4 du code pénal complété par la loi LOPPSI du 14 mars 2011 d'un article 226-4-1, l'usurpation d'identité numérique est un délit puni de deux ans d'emprisonnement et de 20 000 euros d'amende, il sera fastidieux d'une part pour vous, de prouver que vous n'êtes pas le véritable auteur des faits reprochés, et difficile pour les enquêteurs de retrouver le véritable auteur des faits.

Ne pas effacer ses données personnelles sur l'ordinateur que l'on rend, donne, vend, c'est laisser l'opportunité à un inconnu de fouiller dans vos papier, violer votre intimité et cambrioler votre vie.
Pire ! vous connaissez bien le donataire de votre matériel et vous savez qu'il n'y a aucun risque qu'il ait des intentions répréhensibles. Mais êtes vous certain qu'il sera aussi prudent que vous avec son matériel ?
Êtes-vous prêt à prendre des risques s'il perdait ce matériel ?
Dormiriez-vous tranquille si vous imaginiez que votre ancien ordinateur est actuellement sous l'emprise d'un pirate informatique prêt à tout pour tricher, voler et violer en utilisant votre identité ?

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**.
Nos actions peuvent être personnalisées et organisées 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.

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : 5 applications pour effacer des données de façon sécurisée – ZDNet

Denis JACOPINi en direct sur LCI : « Les fraudeurs ont toujours une longueur d’avance – MYTF1News | Denis JACOPINI

Denis JACOPINi en direct sur LCI : « Les fraudeurs ont toujours une longueur d’avance – MYTF1News

Denis Jacopini, expert informatique assermenté spécialisé en cybercriminalité, explique que quoi que l’on fasse, les fraudeurs auront une longueur d’avance. Néanmoins, il y a des failles dans le système, et en particulier au niveau du cryptogramme visuel.

En direct sur LCI avec Serge Maître Maître, président de l’AFUB (Association Française des Usagers des Banques) et Nicolas CHATILLON, Directeur du développement-fonctions transverses du groupe BPCE et Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité débattent sur les techniques des cybercriminels pour vous pirater votre CB.


http://lci.tf1.fr/france/societe/cartes-bancaires-les-fraudeurs-ont-toujours-une-longueur-d-avance-8722056.html

Réagissez à cet article

Source : *Cartes bancaires : « Les fraudeurs ont toujours une longueur d’avance » – Société – MYTF1News*