Faille de sécurité pour le PARTI SOCIALISTE – Avertissement Public de la CNIL

Faille de sécurité pour le PARTI SOCIALISTE – Avertissement Public de la CNIL

Le 26 mai 2016, la CNIL a été informée de l'existence d'une faille de sécurité entraînant une fuite de données sur le site du Parti Socialiste. Lors d'un contrôle en ligne réalisé dès le lendemain, la CNIL a constaté que les mesures garantissant la sécurité et la confidentialité des données des primo-adhérents du PS étaient insuffisantes.

Les contrôleurs de la CNIL ont en effet pu accéder librement, par la saisie d'une URL, à la plateforme de suivi des primo-adhésions au Parti Socialiste effectuées en ligne. Ils ont notamment pu prendre connaissance des éléments suivants : nom, prénom, adresses électronique et postale, numéros de téléphone fixe et mobile, date de naissance, adresse IP, moyen de paiement et montant de la cotisation de certains adhérents.
Cette faille avait été rendue possible par l'utilisation d'une technique non sécurisée d'authentification à la plateforme. Elle a concerné plusieurs dizaines de milliers de primo-adhérents.
Alerté le même jour par la CNIL de cette faille, le PS a immédiatement pris les mesures nécessaires pour y mettre fin.
Un second contrôle réalisé cette fois dans les locaux du PS le 15 juin 2016, destiné à comprendre les raisons de la faille, a permis de constater que les mesures élémentaires de sécurité n'avaient pas été mises en œuvre initialement. En effet, il n'existait pas de **procédure d'authentification** forte au site ni **de système de traçabilité** permettant notamment d'identifier l'éventuelle exploitation malveillante de la faille.
Le contrôle a aussi permis de constater que le PS conservait sans limitation de durée les données personnelles de la plateforme, ce qui avait accru la portée de la fuite de données. La base active contenait des demandes d'adhésion effectuées depuis 2010 qui auraient dû a minima être stockées en archive.

En conséquence, la Présidente de la CNIL a décidé d'engager une procédure de sanction en désignant un rapporteur. La formation restreinte de la CNIL a prononcé un avertissement public car elle a estimé que le Parti Socialiste avait manqué à ses obligations :
• de veiller à la sécurité des données à caractère personnel des primo-adhérents, en méconnaissance de l'article 34 de la loi Informatique et Libertés ;
• de fixer une durée de conservation des données proportionnelle aux finalités du traitement en méconnaissance de l'article 6-5 de la loi Informatique et Libertés.

Enfin, la formation restreinte a décidé de rendre publique sa décision en raison de la gravité des manquements constatés, du nombre de personnes concernées par la faille et du caractère particulièrement sensible des données en cause qui permettaient notamment d'avoir connaissance de leurs opinions politiques.

Pour en savoir plus

Délibération de la formation restreinte n°2016-315 du 13 octobre 2016 prononçant un avertissement à l'encontre du PARTI SOCIALISTE
[PDF-312.22 Ko]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à 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 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.

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 : Faille de sécurité de données sensibles en ligne : Avertissement public pour le PARTI SOCIALISTE | CNIL

Que faire en cas de harcèlement en ligne ?

Que faire en cas de harcèlement en ligne ?

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.

Un droit à l'oubli pour les mineurs. L'article 40 modifié de la loi informatique et Libertés – au même titre que futur Règlement européen sur la protection des données – consacre un droit à l'oubli spécifique pour les mineurs. Un internaute âgé de moins de 18 ans au moment de la publication ou de la création d'un compte en ligne peut directement demander au site l'effacement des données le concernant et ce, dans les meilleurs délais. En pratique, si le responsable de traitement n'a pas effacé les données ou répondu à la personne dans un délai d'un mois, la personne concernée peut saisir la CNIL. Des exceptions existent, notamment dans le cas où les informations publiées sont nécessaires à liberté d'information, pour des motifs d'intérêt public ou pour respecter une obligation légale.

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.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à 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 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.

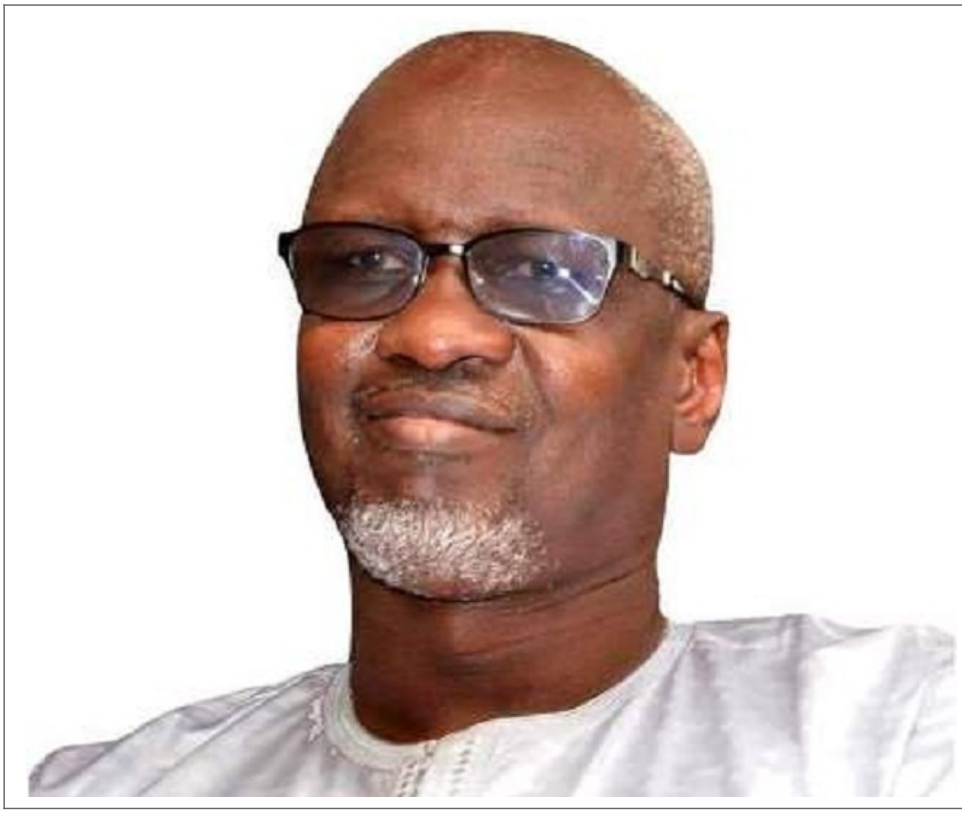
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Réagir en cas de harcèlement en ligne | CNIL

Enquête sur le piratage à La Poste du Sénégal: le DG auditionné par la Gendarmerie



Enquête sur le piratage à La Poste du Sénégal: le DG auditionné par la Gendarmerie

L'enquête sur le piratage de la plate-forme de transfert d'argent de la Poste se poursuit. Après avoir entendu plusieurs responsables de la boite, la section de recherches de Colobane (Dakar) a reçu hier dans ses locaux le directeur général, Ciré Dia. D'après le quotidien sénégalais L'Observateur qui donne l'information dans sa livraison du jour, un important arsenal technique a été mis à contribution pour remonter la filiale.

En s'introduisant dans le système de transfert international du réseau, les cybercriminels avaient emporté près de 400 millions de francs CFA. Un coup dur pour la société qui traverse actuellement des moments difficiles selon L'Enquête qui fait état de problèmes de recouvrement des montants dus par les sociétés de transfert d'argent au groupe, des montants estimés entre 4 et 5 milliards CFA.

Réagissez à cet article

Original de l'article mis en page : Enquête sur le piratage à La Poste du Sénégal: le DG auditionné par la Gendarmerie hier | CIO MAG

Quelles sont les messageries qui protègent le mieux vos données personnelles ?

	Quelles sont les messageries qui protègent le mieux vos données personnelles ?

Apple, Google, Snapchat, Blackberry, ou encore le Chinois Tencent, tous ces géants du web proposent à leurs utilisateurs des messageries instantanées. Aujourd'hui, ce sont plusieurs milliards de personnes qui les utilisent quotidiennement. Au sein de ceux-là, des minorités opprimées, des militants pour les droits de l'Homme, des dissidents politiques, des lanceurs d'alertes… Mais comment ces messageries protègent-elles nos données ?

Amnesty International a rendu un rapport accablant sur la question, dans lequel elle effectue un classement des messageries privées.

Classement des messageries privées

Quelle messagerie privée est la plus sécurisée selon le classement d'Amnesty International ?

Entreprises ▼	Messageries	Siège	Nombre d'utilisateurs	Classement Amnesty (sur 100)
Apple	iMessage, Facetime	USA	Inconnu, mais 1 milliard d'iPhone vendus	67
Blackberry	Blackberry Messenger	Canada	100 millions	20
Facebook	Facebook Messenger, WhatsApp	USA	1 milliard chacune	73
Google	Allo, Duo, Hangouts	USA	Inconnu, mais plus de deux milliards d'utilisateurs Google	53
Kakao Inc	Kakao Talk	Corée du Sud	49 millions	40
Line	Line	Japon	218 millions	47
Microsoft	Skype	USA	300 millions	40
Snapchat	Snapchat	USA	200 millions	26
Telegram	Telegram Messenger	Allemagne	100 millions	67
Tencent	QQ, We Chat	Chine	697 millions, 853 millions	0
Viber media	Viber	Luxembourg	250 millions	47

Source: Amnesty Internationale Récupérez les données Créé avec Datawrapper

Classement Amnesty International

Les onze grandes entreprises évaluées affichent toutes des engagements écrits en termes de protection de la vie privée. Et pourtant, aucune n'est irréprochable, toutes ne respectent pas les normes internationales en vigueur et peu proposent un niveau élémentaire de protection. Facebook, Apple ou Google sont en haut du classement, quand Microsoft, Snapchat, ou Tencent font figure de mauvais élèves. L'ONG a mis au point un barème.

Les critères du classement

Amnesty International attribue une note de 0 à 100 aux entreprises, selon leur résultat sur cinq critères provenant des normes internationales en la matière. Trois sont primordiaux pour assurer la sécurité des données personnelles.

Les entreprises sont jugées sur leur capacité à **reconnaître les menaces contre la vie privée et la liberté d'expression**. En clair, que mettent-elles en place pour protéger les droits de leurs utilisateurs ?

Elles doivent ensuite **appliquer par défaut le chiffrement de bout en bout**. Une question au cœur des préoccupations d'Amnesty International. L'ONG estime que seul le chiffrement de bout en bout est apte à protéger la vie privée. Ici, seul l'émetteur et le receveur détiennent la clef de chiffrement. Les acteurs intermédiaires du processus (fournisseur d'accès, entreprise de messagerie) n'ont donc pas accès au contenu de la conversation.

Les messageries doivent enfin **rendre publiques les informations sur les demandes de données d'utilisateurs par des gouvernements et refuser de contourner les clefs de chiffrements.**

Facebook, Apple, Telegram et Google en tête

La messagerie de Facebook est la mieux classée, avec un score de 73 points. Le bébé de Mark Zuckerberg totalise environ un milliard de fidèles quotidiens. C'est lui qui offre le plus de garanties à ses utilisateurs. Mais ses deux messageries ne sont pas équivalentes. Si WhatsApp propose un chiffrement de bout en bout par défaut (l'utilisateur n'a pas à choisir, c'est automatique), cette option récente de Facebook Messenger doit être activée.

Apple cumule 67 points. La marque à la pomme offre un chiffrement de bout en bout sur ses deux messageries (iMessenger et Facetime). Mais Amnesty International relève qu'elle « *devrait adopter un protocole de chiffrement plus ouvert qui permette une vérification indépendante complète* ».

Telegram est deuxième ex aequo, avec 67 points aussi. Ce nom vous dit quelque chose ? C'est normal, cette messagerie a beaucoup defrayé la chronique car elle est l'application de messagerie instantanée la plus prisée des milieux djihadistes. Elle perd des points car son système de chiffrement n'est pas automatique et doit être activé.

Vient ensuite Google avec un score de 53. Le moteur de recherche est critiqué par Amnesty International car ses trois messageries instantanées ne proposent pas toutes des systèmes de chiffrement.

Les quatre entreprises qui caracolent en tête se sont toutes publiquement prononcées contre les moyens de contournement des clés de chiffrement par les États. Et toutes, à l'exception de Telegram, préviennent leurs utilisateurs des demandes faites par les gouvernements.

Skype, Snapchat et Tencent, les mauvais élèves

Snapchat, c'est cette messagerie qui permet de s'envoyer une photo ou un texte sur un temps très court. Skype, propriété de Microsoft, c'est celle qui vous permet de faire des appels vidéo. Les deux applications sont mauvaises élèves aux quatrième et troisième plus mauvaises places.

Aucun chiffrement de bout à bout n'est proposé par les deux géants, qui présentent tous deux un système « *très vulnérable* », selon Amnesty. Les deux sont utilisées par des millions de jeunes quotidiennement, un public très menacé et très exposé à la cybercriminalité.

BlackBerry occupe l'avant-dernière place. La messagerie privée canadienne n'offre pas un système de chiffrement de bout en bout, elle le vend. Ainsi, si on ne paie pas, on n'est pas protégé sur BlackBerry. Qui plus est, d'après le site américain Vice, BlackBerry aurait donné sa clef de chiffrement à la police canadienne qui a alors pu intercepter des messages.

À la dernière place, on retrouve Tencent, le mastodonte chinois. L'entreprise accuse un score de 0 point. Aucun des critères n'est rempli et les données personnelles de plus d'un un milliard et demi de personnes ne sont absolument pas protégées, conséquence de la censure que subit l'Internet chinois. En 2013, un développeur de Tencent confiait au journal *Le Monde* , « *Les autorités ont le privilège d'accéder aux historiques, donc elles savent tout sur vous dès lors que vous utilisez nos services*. » Le ton est donné…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à 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 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.

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 : Quelles sont les messageries qui protègent le mieux vos données personnelles ? – La Voix du Nord

---

Cloud Microsoft – Les Etats-Unis bien décidés à accéder à des données en Europe

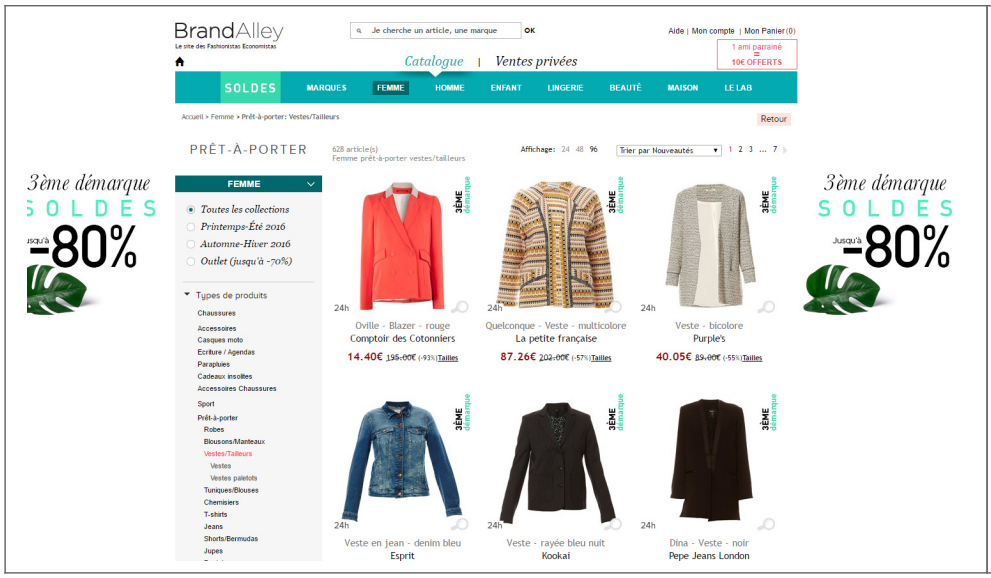
Cloud Microsoft – Les Etats-Unis bi

Législation : Le gouvernement US estime être en droit d'exiger de Microsoft qu'il livre les données d'un utilisateur étranger stockées sur un serveur en Irlande. Un tribunal avait dit non, mais le Département de la Justice revient à la charge.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur notre page formations.

Réagissez à cet article

La Cnil s'énerve contre Brandvalley mais la sanction est faible



La Cnil s'énerve contre Brandvalley mais la sanction est faible

La Cnil a dressé un constat sévère de l'irrespect de la loi Informatique et Libertés par le site de ventes privées BrandValley, spécialisé dans les grandes marques. Mais le site qui génère environ 300 millions d'euros de chiffre d'affaires n'a été condamné qu'à 30 000 euros d'amende.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.

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

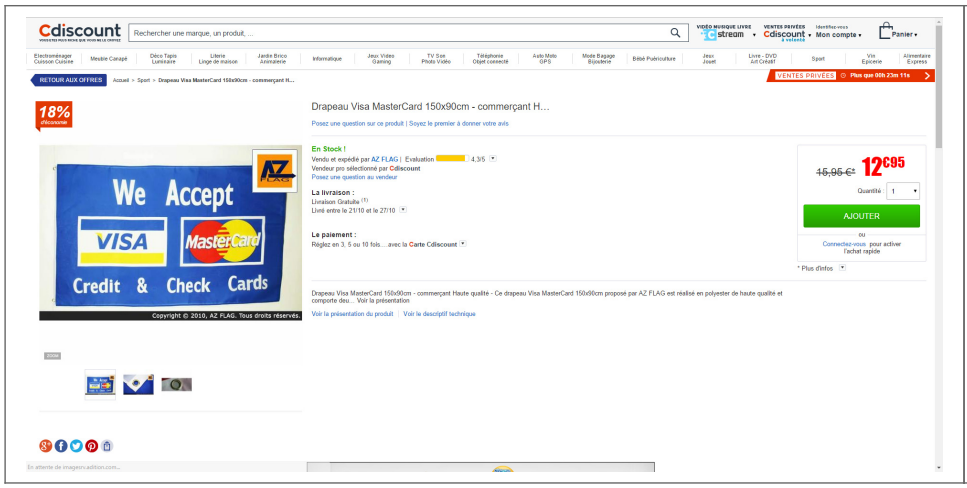
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation 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

Pourquoi CDiscount avait conservé plus de 4 000 numéros de CB avec cryptogramme



Pourquoi CDiscount avait conservé plus de 4 000 numéros de CB avec cryptogramme

La Cnil a mis en demeure CDiscount après la découverte d'une dizaine de manquements à la loi Informatique et Libertés, dont la conservation en clair de numéros de cartes bancaires sur une base de données. La faute d'un sous-traitant, a tenté de se défendre le site e-commerce.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur notre page formations.

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

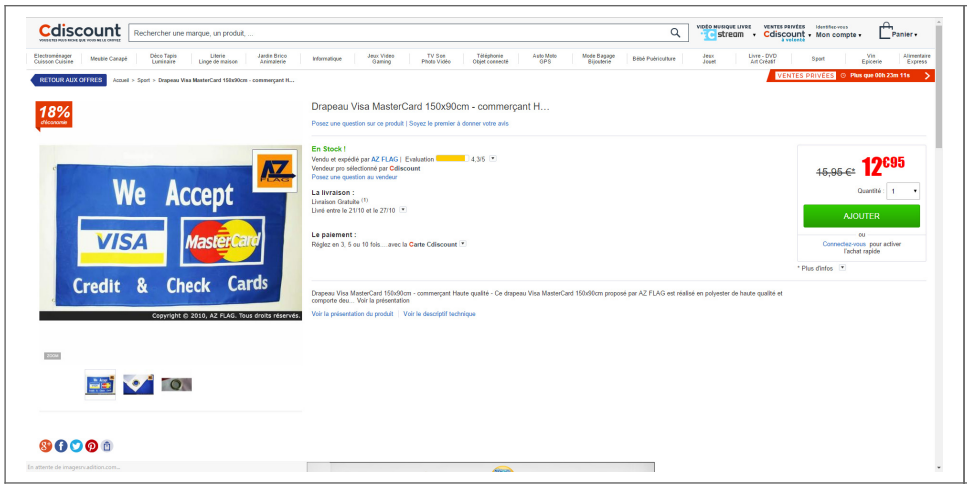
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation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

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

Contactez-nous

Réagissez à cet article

Pourquoi CDiscount avait conservé plus de 4 000 numéros de CB avec cryptogramme



Pourquoi CDiscount avait conservé plus de 4 000 numéros de CB avec cryptogramme

La Cnil a mis en demeure CDiscount après la découverte d'une dizaine de manquements à la loi Informatique et Libertés, dont la conservation en clair de numéros de cartes bancaires sur une base de données. La faute d'un sous-traitant, a tenté de se défendre le site e-commerce.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur notre page formations.

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

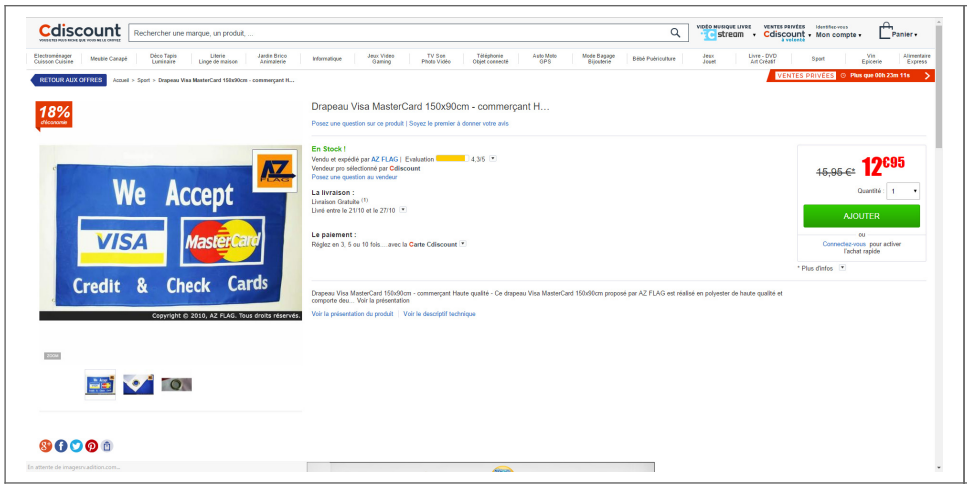
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation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

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

Contactez-nous

Réagissez à cet article

Pourquoi CDiscount avait conservé plus de 4 000 numéros de CB avec cryptogramme



Pourquoi CDiscount avait conservé plus de 4 000 numéros de CB avec cryptogramme

La Cnil a mis en demeure CDiscount après la découverte d'une dizaine de manquements à la loi Informatique et Libertés, dont la conservation en clair de numéros de cartes bancaires sur une base de données. La faute d'un sous-traitant, a tenté de se défendre le site e-commerce.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur notre page 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.

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

Contactez-nous

Réagissez à cet article

Google condamné à 375 Millions d'euros…

Google condamné à 375 Millions d'euros…

44 participants ont condamné Google – par sondage – à environ 375 millions d'euros pour une infraction à la protection des données personnelles – et au titre du nouveau règlement européen ! La condamnation était entièrement virtuelle et objet d'un test.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des

données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur notre page 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.

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

Contactez-nous

Réagissez à cet article