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 maiuscules
- 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 passepour 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.

 $Plus \ d'informations \ sur: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles \ formation in the protection of t$



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 : Comment choisir ses mots de passe ? / Cybercrime / Dossiers / Actualités — Police nationale — Ministère de l'Intérieur

Lutte contre le blanchiment d'argent : quelles formalités à la CNIL ? | Denis JACOPINI



Lutte contre le blanchiment d'argent : quelles formalités à la CNIL ? Les fichiers relatifs à la lutte contre le blanchiment d'argent et le financement du terrorisme mis en oeuvre par les organismes financiers doivent être déclarés à la CNIL :

- Par une déclaration simplifiée de conformité à l'autorisation unique 003 si le fichier correspond aux caractéristiques énoncées dans ce texte ;
- Par une demande d'autorisation si le fichier sort du cadre de cette norme.

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. 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

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 : http://www.aide.cnil.fr/selfcnil/site/template.do?id=537&back=true

Vidéosurveillance en entreprise : règles et limites | Denis JACOPINI

#Vidéosurveillance en entreprise : règles et limites

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.

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

 $\verb|http://www.comptanoo.com/assurance-prevention/actualite-tpe-pme/23794/videosurveillance-entreprise-regles-et-limites | the compact of the$

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 foir 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 »). ct de la protection des données personnelles, à la fois 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. 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'étrangerpour 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).

découvrir et comprendre les **arnaques** et les **piratages informatiques** pour Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, 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

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



- Expertises de systèmes de vote électronique ;
- Formation de C.I.L. (Correspondants Information et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

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

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.



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.tfl.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

Lutte contre les cyberattaques : bien choisir son mot de passe | Denis JACOPINI



Lutte contre les cyberattaques : bien choisir son mot de passe

Chaque année, les cyberattaques coûtent plus de 400 milliards de dollars à l'économie mondiale.

Pour renforcer la sécurité sur internet, il est important de bien choisir ses mots de passe : huit caractères avec au moins une majuscule et un mélange de chiffres et de lettres. Le mot de passe doit être le plus compliqué possible et différent pour chaque compte afin d'être le plus sécurisé. Il reste tout de même de plus en plus facile à déceler pour les hackers et difficile à mémoriser pour les utilisateurs. Résultat : on opte pour la facilité. En 2014, le mot de passe le plus utilisé sur internet était la suite de chiffres : 1 2 3 4 5 6.

Un enjeu de taille

Le mot de passe serait à l'origine de 31% des cyberattaques avec un coût de 445 milliards de dollars chaque année pour l'économie mondiale. L'enjeu économique est de taille. Un consortium d'entreprises et d'États planche sur de nouvelles techniques d'authentification : scan de l'iris, empreinte digitale, reconnaissance vocale ou faciale... Des éléments propres au véritable utilisateur et donc plus sécurisés.

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.francetvinfo.fr/monde/lutte-contre-les-cyberattaques-bien-choisir-son-mot-de-passe_968535.html

Pourquoi, malgré le danger

connu, cliquons nous sur des e-mails d'expéditeurs inconnus ?



Pourquoi, malgré le danger connu, cliquons nous sur des e-mails d'expéditeurs inconnus ?

Links are negative. In PRI Columnity of Engine Annexes, part of the Market Statement on Statement and Statement of the Columnity of Engine Annexes, part of the Market Statement of the Statement of the Statement of the Columnity of Engine Annexes of the Statement of the Statemen

Original de l'article mis en page : One in two users click on links from unknown senders > FAU.EU

10 techniques de
cybercriminels pour vous
pirater votre carte bancaire
| Denis JACOPINI



10 techniques de cybercriminels pour vous pirater votre carte bancaire

the course close I
Man agent of plant of the second of the seco
La a sa
See Chart and and a short district the contract of a price of the contract of price of the contract of the con
The official for the processing profession of the market transport of the contract of the cont
To regard 1. The contract of t
19 to the fill of the control of the
The State of the Control of the Cont
TO AND
The official for the production of the significant
Are quality and an additional and a second a
The state of the s
to appear to a recognition of the contract of
Section 1. The sectio
The state of the s
th stage that may be a start of the start of
The contract of the policy of
No Mandage And the State of St
See A Control
Manages Of Virginians the security of the sec
See Degree of the Control of the Con
Moral or in the Propagation Mandriage in State of the Sta
See The Control of th
Topic cond for the final tension as process and the set of cond and discriment to constitute the constitute of the constitute the constitute of the constitu
Force on This desiration per centre is her than it has the control in the control
principle part on the part of the control of the co
No. 1 And 1 And 2
See Distinger. We will be a seen of the seed of the s
Million or organized by our control that in shifted the second of controls.
MINIST AND
Management of the Control of the Con
Name of the state
New 1,000

Sources:

http://www.agefi.fr/banque-assurance/actualites/hebdo/20160210/oberthur-technologies-lance-carte-a-cvv-dynamique-155903

http://www.challenges.fr/economie/20130912.CHA4249/la-verite-sur-les-fraudes-a-la-carte-bancaire.html

https://www.jegardecapourmoi.com

http://www.challenges.fr/economie/20130912.CHA4249/la-verite-sur-les-fraudes-a-la-carte-bancaire.html

http://www.bienpublic.com/actualite/2013/10/10/dijon

http://www.lanouvelletribune.info/societe/vie-societale/techno logie/25616-greendispenser-un-nouveau-virus-voleur-de-billets-de-banque

https://securelist.com/analysis/quarterly-spam-reports/69932/s pam-and-phishing-in-the-first-quarter-of-2015

Les obligations des Associations vis à vis de la CNIL | Denis JACOPINI



Les obligations des Associations vis à vis de la CNILDans le cadre de leur activité, les associations sont amenées à constituer des fichiers de leurs adhérents, de leurs donateurs ou de donateurs potentiels. Quelles sont les règles à respecter ?

Dans le cadre de leur activité, les associations sont amenées à constituer des fichiers de leurs adhérents, de leurs donateurs ou de donateurs potentiels. Quelles sont les règles à respecter ?

Nous allons tenter d'y répondre au travers de réponses par Oui ou par Non à des questions correspondant à des cas concrets : Une association peut-elle céder, louer ou vendre le fichier de ses adhérents à des fins commerciales ?

OUI. La loi « informatique et libertés » n'interdit pas cette pratique. Il y a toutefois des précautions à prendre : Il faut d'abord informer les adhérents de cette possible revente de leurs coordonnées à des fins commerciales et leur permettre de s'y opposer. Cette opposition peut se faire par exemple au moyen d'une case à cocher figurant sur le bulletin d'adhésion.

Une association peut-elle diffuser sur son site web l'annuaire de ses adhérents ?

OUI. Dans ce cas, comme pour la réponse précédente, les adhérents doivent en être informés au préalable. Ils ont tout à fait le droit de s'opposer à une telle diffusion compte-tenu des risques particuliers de capture des informations diffusées sur le web.

La CNIL propose des mentions type à faire figurer sur les bulletins d'adhésion pour bien informer les adhérents de leurs droits.

Mention d'information à inscrire sur le bulletin d'adhésion

Les informations recueillies sont nécessaires pour votre adhésion. Elles font l'objet d'un traitement informatique et sont destinées au secrétariat de l'association. En application des articles 39 et suivants de la loi du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent.

Il arrive que des mairies demandent aux associations de leur transmettre le fichier de ses adhérents en vue d'obtenir des subventions ? Est-ce légal ?

NON. Un maire ne peut pas demander, même au titre de la subvention qu'il accorde à une association, la liste nominative des adhérents. Une telle pratique est contraire au principe constitutionnel de la liberté d'association.

En revanche, les mairies peuvent demander, au titre du contrôle des subventions qu'elles versent aux associations, la copie certifiée du budget et des comptes de l'exercice écoulé, ainsi que la communication de tous les documents faisant apparaître les résultats de l'activité de l'association.

Un membre d'association peut-il exiger la communication de la liste de tous les autres adhérents ?

OUI, si les statuts de l'association prévoient cette possibilité. Une association est en effet libre de préciser dans ses statuts que l'adhésion implique d'accepter que ses coordonnées puissent être communiquées à tout adhérent qui en fait la demande, à la condition que cette communication ait un lien direct avec l'activité de l'association.

Dans ce cas, un membre ne peut s'opposer à cette diffusion.

Lors du renouvellement du bureau d'une association, un candidat peut-il obtenir la liste des adhérents ?

OUI. Si les statuts de l'association le prévoient, tout candidat peut demander que la liste des adhérents lui soit transmise, à partir du moment où il s'engage à ne pas l'utiliser à d'autres fins que l'élection et à la détruire à la fin des opérations électorales.

Les membres du bureau d'une association, dont les statuts ont été déposés en préfecture, peuvent ils s'opposer à la

diffusion de leurs identités et coordonnées ?

NON. La loi du 1er juillet 1901 relative au contrat d'association prévoit qu'une association ne peut obtenir la capacité juridique qu'en rendant publics, par une insertion au Journal officiel, son titre, son objet, l'adresse de son siège et les noms, professions, domiciles et nationalités de ceux qui sont chargés de son administration. Cette diffusion peut aussi se faire sur en ligne via la version Internet du journal Officiel.

Néanmoins, des mesures techniques empêchent d'accéder directement à la page de l'association concernée lorsqu'on interroge les différents moteurs de recherche sur la base de l'identité des membres de son bureau.

Les fichiers de membres et donateurs d'une association doivent-ils être déclarés à la CNIL ?

NON, ces fichiers sont dispensés de déclaration à la CNIL.

Attention, être dispensé de déclaration n'exonère pas pour autant des obligations que la loi informatique et libertés impose aux responsables de fichiers. Cela signifie qu'il faut informer les personnes qu'un fichier est constitué et qu'elles ont un droit d'accès aux informations qui les concernent. Enfin bien sûr, le responsable du fichier doit prendre toutes les mesures utiles afin d'assurer la sécurité des informations personnelles collectées.

Source : Denis JACOPINI et www.cnil.fr

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