Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c’est très important) ?

Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c’est très important) ?

Quitter son travail est souvent difficile, mais effacer des données présentes sur un ordinateur professionnel sur lequel on a travaillé pendant X années l'est encore plus. Il est donc nécessaire de savoir comment le faire sans laisser de données professionnelles ou personnelles derrière soi.

Atlantico : Quelles étapes faut-il suivre avant d'effacer nos données personnelles présentes sur notre futur ancien ordinateur de fonction ?

Denis Jacopini : L'ordinateur professionnel qui vous a été mis à disposition était probablement en état de marche. A moins d'avoir des circonstances ou des consignes particulières, vous devrez donc rendre cet appareil au moins dans l'état initial.

1. En premier lieu, pensez à identifier les données à sauvegarder dont il vous sera nécessaire de conserver copie. Attention aux données professionnelles frappées de confidentialité ou d'une clause de non concurrence, tel que les fichiers clients.

On pourrait bien vous reprocher d'en avoir conservé une copie et de l'utiliser contre votre ancien employeur.

2. Identifiez les données ayant un caractère confidentiel et qui nécessiteront une sauvegarde dans un format protégé par un procédé tel que le cryptage ou le hachage.
3. Identifiez les données devant être conservées pendant un grand nombre d'années tels que des justificatifs d'assurance, de sinistre…
4. Identifiez les données que vous ne devez absolument pas perdre car non reproductibles (contrats, photos de mariage, des enfants, petits-enfants…)
5. Identifiez les données que vous souhaitez rendre accessibles sur plusieurs plateformes (ordinateurs, téléphones, tablettes) que ça soit au bureau à la maison, en déplacement ou en vacances. Ensuite, en fonction des logiciels permettant d'accéder à vos données, identifiez les fonctions de « Sauvegarde », « Enregistrer sous » ou d' »Export ». Vous pourrez alors choisir le support adapté.

Enfin, en fonction des critères de sécurité choisis, vous pourrez sauvegarder sur des supports adaptée soit :

– à la confidentialité (tout support numérique en utilisant un logiciel de cryptage ou de hachage tel de Truecrypt, Veracrypt, ou AxCrypt…) ;
– à l'intégrité (multiplier le nombre de sauvegardes en réalisant plusieurs exemplaires de vos données à n'absolument pas perdre) ;
– à la longévité en utilisant des supports avec une durée de vie adapté à vos attentes. Sachez qu'à ce jour, il est difficile de garantir la lecture d'une information numérique au-delà de plusieurs dizaines d'années (en raison de l'altération des supports avec le temps, mais aussi de l'évolution des versions, des formations et des logiciels). Qui peut vous garantir de pouvoir visualiser vos photos numériques dans cinquante ans ?
– à la disponibilité sur plusieurs plateformes et sur plusieurs lieux, comme le proposent les solutions *cloud* qui sont éclos il y a quelques dizaines d'années seulement ;
– à la quantité (car vous devez rapidement stocker pour ensuite trier et choisir un support adapté) en choisissant par exemple un disque dur USB externe auto-alimenté (si le port USB de votre ordinateur l'autorise), ce support est actuellement celui ayant le meilleur rapport capacité / prix avec une bonne rapidité d'écriture.

Les risques :

Les clés USB sont des outils permettant de conserver une copie facilement accessible et aisément transportable. 100% des clés USB tomberont un jour ou l'autre en panne. Pensez-y pour ne pas leur confier les documents de votre vie.

Idem pour les disques durs. 100% des disques durs tomberont un jour en panne. Cependant, contrairement aux clés USB ou aux cartes mémoire, les disques durs (mécaniques et non SSD) permettront plus facilement de récupérer leur contenu en cas de panne.

Les supports de type lecteurs ZIP, lecteur JAZ, lecteurs magnéto-optiques, lecteurs de bandes etc. sont de plus en plus rares. Conserver des données importantes sur de tels supports peut s'avérer dangereux. En effet, imaginez un instant jour ou vous souhaitez y accéder mais que vous n'avez plus le lecteur pour les consulter et que le lecteur ne se vend même plus. Ne laissez pas la vies de vos données numériques entre les mains du *Bon Coin*…

Voilà, en fonction de tous ces critères et à partir de ces conseils, il ne vous reste plus qu'à sauvegarder vos données importantes avant de les effacer de l'appareil que vous allez rendre.

Comparatif :

Disque dur : Quelques Go à quelques To – Bon marché, rapide mais fragile.
Clé USB : Quelques Go – Rapide, léger mais quasiment impossible de récupérer des données en cas de panne.
Cloud : Quelques Mo à quelques To – Accessible de n'importe où mais aussi par tous ceux qui ont le mot de passe (risqué) – Dépend du fonctionnement et de la rapidité d'Internet – Les services de cloud gratuits peuvent s'arrêter du jour au lendemain et vous perdrez tout.
Disques optiques (CD, DVD,Magnéto Optique) : Bonne tenue dans le temps si conservés dans de bonnes conditions mais utilisables (pérennité des lecteurs de disques) jusqu'à quand ?
Supports spéciaux (ZIP/Jazz/QIC/DAT/DLT/DDS/SDLT) : Supports fragiles, lecteurs trop rares pour garantir une lecture au dela de 5 ans.

Est-il possible d'effacer toutes nos données présentes sur un ordinateur de fonction lorsque l'on quitte son travail et que l'on ne souhaite pas laisser de traces sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé ?

La première étape consiste à identifier les données à supprimer et celles à sauvegarder avant de procéder au nettoyage. Sur la plupart des ordinateurs professionnels, parfois sans le savoir, en plus de nos documents de travail nous stockons :

– Des programmes ajoutés ;
– Nos e-mails ;
– Nos traces de navigation ;
– Nos fichiers téléchargés ;
– Divers identifiants et mots de passe ;
– Les fichiers temporaires

Afin d'éviter l'accès à ces informations par le futur locataire / propriétaire / donataire de votre ordinateur, il sera important de procéder à leur suppression minutieuse.

Concernant les programmes ajoutés :

Facile sur Mac en mettant le dossier d'un programme à la corbeille, n'utilisez surtout pas la corbeille pour supprimer des programmes sous Windows. La plupart des programmes apparaissent dans la liste des programmes installés. Pour procéder à leur suppression, nous vous conseillons de procéder :

– soit par le raccourcis de désinstallation que le programme a créé ;
– s'il n'y a pas de raccourci prévu à cet effet, passez par la fonction « Ajout et Suppression de Programmes » ou « Programmes et fonctionnalités » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;
– Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que RevoUninstaller (gratuit).

Concernant les e-mails :

Selon le programme que vous utiliserez, la suppression du/des compte(s) de messagerie dans le programme en question suffit pour supprimer le ou les fichiers contenant les e-mails. Sinon, par précaution, vous pouvez directement les localiser et les supprimer :

– fichiers « .pst » et « .ost » de votre compte et archives pour le logiciel « Outlook » ;
– fichiers dans » » « % »'AppDataLocalMicrosoftWindows Live Mail » pour le logiciel « Windows Live Mail » ;
– les fichiers contenus dans ' » »% »'APPDATA%ThunderbirdProfiles » pour le programme Mozilla Thunderbird
– le dossier contenu dans « …Local SettingsApplication DataIMIdentities » pour le programme Incredimail.

Concernant nos traces de navigation :

En fonction de votre navigateur Internet et de sa version, utilisez, dans les « Options » ou les « Paramètres » la fonction supprimant l'Historique de Navigation » ou les « Données de Navigation ».

Concernant les fichiers téléchargés :

En fonction de votre système d'exploitation l'emplacement de stockage par défaut des fichiers téléchargés change. Pensez toutefois à parcourir les différents endroits de votre disque dur, dans les lecteurs réseau ou les lecteurs externes à la recherche de fichiers et documents téléchargés que vous auriez pu stocker.

Concernant divers identifiants et mots de passe :

Du fait que le mot de passe de votre système d'exploitation stocké quelque part (certes crypté), si vous êtes le seul à le connaître et souhaitez en conserver la confidentialité, pensez à le changer et à en mettre un basic de type « utilisateur ».

Du fait que les mots de passe que vous avez mémorisé au fil de vos consultations de sites Internet sont également stockés dans votre ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passes et les informations qui pré remplissent les champs.

Concernant les fichiers temporaires :

En utilisant la fonction adaptée dans vos navigateurs Internet, pensez à supprimer les fichiers temporaires liés à la navigation Internet (images, cookies, historiques de navigation, autres fichiers).
En utilisant la fonction adaptée dans votre systèmes d'exploitation, supprimez les fichiers temporaires que les programmes et Windows génèrent automatiquement pour leur usage.

Pour finir :

Parce qu'un fichier supprimé n'est pas tout à fait supprimé (il est simplement marqué supprimé mais il est toujours présent) et dans bien des cas toujours récupérable, vous pourrez utiliser une application permettant de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore »…

Ne pas effacer ses données personnelles sur so ordinateur de fonction est-il dommageable ? 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.

Auteur : Denis JACOPINI

Denis Jacopini anime des **conférences et des formations** 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 : Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c’est très important) | Atlantico.fr

---

Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…)| Denis JACOPINI

Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…) | Denis JACOPINI

Une « phrase de passe » est beaucoup plus difficile à pirater qu'un « mot de passe ». Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes et mettraient… plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Atlantico : Selon de nombreuses études menées par des chercheurs de l'Université américaine Carnegie-Mellon, un long mot de passe facile à retenir tel que « *ilfaitbeaudanstoutelafrancesaufdanslebassinparisien* » serait plus difficile à pirater qu'un mot de passe relativement court mais composé de glyphes de toutes sortes, tel que « *p8)J#&=89pE* », très difficiles à mémoriser. Pouvez-vous nous expliquer pourquoi ?

Denis Jacopini : La plupart des mots de passe sont piratés par une technique qu'on appelle « la force brute ». En d'autres termes, les hackers vont utiliser toutes les combinaisons possibles des caractères qui composent le mot de passe.

Donc, logiquement, plus le mot de passe choisi va avoir de caractères (majuscule, minuscule, chiffre, symbole), plus il va être long à trouver. Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes via la technique de « la force brute », et mettraient… plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Un long mot de passe est donc plus difficile à pirater qu'un mot de passe court, à une condition cependant : que **la phrase choisie comme mot de passe ne soit pas une phrase connue de tous**, qui sort dès qu'on en tape les premiers mots dans la barre de recherche de Google. Les pirates du Net ont en effet des bases de données où ils compilent toutes les phrases, expressions ou mots de passe les plus couramment utilisés, et essayent de hacker les données personnelles en les composant tous les uns derrière les autres. Par exemple, mieux vaut avoir un mot de passe court et complexe plutôt qu'une « phrase de passe » comme « *Sur le pont d'Avignon, on y danse on y danse…* ».

Il faut également bien veiller à ce que cette « phrase de passe » ne corresponde pas trop à nos habitudes de vie, car les pirates du Web les étudient aussi pour arriver à leur fin. Par exemple, si vous avez un chien qui s'appelle « Titi » et que vous habitez dans le 93, il y a beaucoup de chance que votre ou vos mots de passe emploient ces termes, avec des associations basiques du type : « *jevaispromenermonchienTITIdansle93* ».

De plus, selon la Federal Trade Commission, changer son mot de passe régulièrement comme il est habituellement recommandé aurait pour effet de faciliter le piratage. Pourquoi ?

Changer fréquemment de mot de passe est en soi une très bonne recommandation, mais elle a un effet pervers : plus les internautes changent leurs mots de passe, plus ils doivent en inventer de nouveaux, ce qui finit par embrouiller leur mémoire. **Dès lors, plus les internautes changent fréquemment de mots de passe, plus ils les simplifient, par peur de les oublier, ce qui, comme expliqué plus haut, facilite grandement le piratage informatique.**

Plus généralement, quels seraient vos conseils pour se prémunir le plus efficacement du piratage informatique ?

Je conseille d'avoir une « phrase de passe » plutôt qu'un « mot de passe », qui ne soit pas connue de tous, et dont on peut aisément en changer la fin, pour ne pas avoir la même « phrase de passe » qui vérouille nos différents comptes.

Enfin et surtout, je conseille de ne pas se focaliser uniquement sur la conception du mot de passe ou de la « phrase de passe », parce que c'est très loin d'être suffisant pour se prémunir du piratage informatique. Ouvrir par erreur un mail contenant un malware peut donner accès à toutes vos données personnelles, sans avoir à pirater aucun mot de passe. Il faut donc rester vigilant sur les mails que l'on ouvre, réfléchir à qui on communique notre mot de passe professionnel si on travail sur un ordinateur partagé, bien vérrouiller son ordinateur, etc…

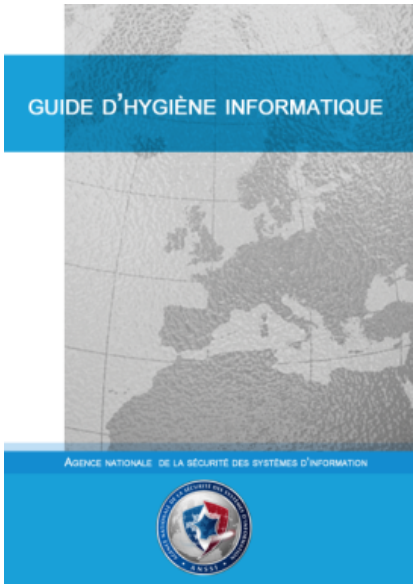
Article original de Denis JACOPINI et Atlantico

Réagissez à cet article

Original de l’article mis en page : Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que…) | Atlantico.fr

---

Les guides des bonnes pratiques de l’Anssi en matière de sécurité informatique | Denis JACOPINI



Les guides des bonnes pratiques de l’Anssi en matière de sécurité informatique

Vous voulez éviter que le parc informatique soit utilisé pour affaiblir votre organisation ? L'un des guides publiés par l'ANSSI vous aidera à vous protéger.

Initialement destinés aux professionnels de la sécurité informatique, les guides et recommandations de l'ANSSI constituent des bases méthodologiques utiles à tous. Vous trouverez sans peine votre chemin en utilisant les mots-clés, qu'un glossaire vous permet d'affiner, ou le menu thématique.

LISTE DES GUIDES DISPONIBLES

- Guide pour une formation sur la cybersécurité des systèmes industriels
- Profils de protection pour les systèmes industriels
- Sécuriser l'administration des systèmes d'information
- Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du rgs
- Recommandations pour le déploiement sécurisé du navigateur mozilla firefox sous windows
- Cryptographie – les règles du rgs
- Recommandations de sécurité concernant l'analyse des flux https
- Partir en mission avec son téléphone sa tablette ou son ordinateur portable
- Recommandations de sécurité relatives à active directory
- Recommandations pour le déploiement sécurisé du navigateur microsoft internet explorer
- l'homologation de sécurité en neuf étapes simples,
- bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,
- recommandations pour le déploiement sécurisé du navigateur google chrome sous windows,
- usage sécurisé d'(open)ssh,
- la cybersécurité des systèmes industriels,
- sécuriser une architecture de téléphonie sur ip,
- mettre en œuvre une politique de restrictions logicielles sous windows,
- prérequis à la mise en œuvre d'un système de journalisation,
- vulnérabilités 0-day, prévention et bonnes pratiques,
- le guide des bonnes pratiques de configuration de bgp,
- sécuriser son ordiphone,
- sécuriser un site web,
- sécuriser un environnement d'exécution java sous windows,
- définition d'une politique de pare-feu,
- sécuriser les accès wi-fi,
- sécuriser vos dispositifs de vidéoprotection,
- guide d'hygiène informatique,
- la sécurité des technologies sans contact pour le contrôle des accès physiques,
- recommandations de sécurité relatives à ipsec,
- la télé-assistance sécurisée,
- sécurité des systèmes de virtualisation,
- sécurité des mots de passe,
- définition d'une architecture de passerelle d'interconnexion sécurisée,
- ebios – expression des besoins et identification des objectifs de sécurité,
- la défense en profondeur appliquée aux systèmes d'information,
- externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques,
- archivage électronique… comment le sécuriser ?
- pssi – guide d'élaboration de politiques de sécurité des systèmes d'information,
- tdbssi – guide d'élaboration de tableaux de bord de sécurité des systèmes d'information,
- guide relatif à la maturité ssi,
- gissip – guide d'intégration de la sécurité des systèmes d'information dans les projets

---

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

Source : http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/

Votre responsabilité engagée en cas de piratage de vos données | Denis JACOPINI

Votre responsabilité engagée en cas de piratage de vos données

Si vous vous faites pirater votre ordinateur ou votre téléphone, votre responsabilité pourrait bien être engagée vis-avis des données que ce support numérique renferme.

Imaginez que vous disposiez de différents appareils numériques informatiques renfermant une multitude de données, dont des données d'amis, de prospects, de clients, de fournisseurs (tout ce qu'il y a de plus normal), et tout à coup, à cause d'un Malware (Méchangiciel selon D. JACOPINI), un pirate informatique en prend possession de ces données, les utilise ou pire, les diffuse sur la toile. Que risquez-vous ?

En tant que particulier victime, pas grand chose, sauf s'il est prouvé que votre négligence est volontaire et l'intention de nuire retenue.
Par contre, en tant que professionnel, en plus d'être victime du piratage (intrusion causée par une faille, un virus, un crypto virus, un bot, un spyware), et d'avoir à assumer les conséquences techniques d'un tel acte illicite pourtant pénalement sanctionné notamment au travers de la loi godfrain du 5 janvier 1988 (première loi française réprimant les actes de criminalité informatique et de piratage), vous risquez bien de vous prendre une seconde claque vis à vis de la loi Informatique et Libertés du 6 janvier 1978.

En effet, Les entreprises, les sociétés, tous ceux exerçant une activité professionnelle réglementée ou non, les associations, les institutions, administrations et les collectivités, sont tenues de respecter la loi Informatique et Libertés du 6 janvier 1978 et notamment la sécurité des données selon les termes de son Article n°34 :

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

De plus, les sanctions jusqu'alors limitées à 5 ans d'emprisonnement et 300 000 euros d'amendes vont à partir du 25 mai 2018, par la mise en application du RGPD (Règlement Général sur la Protection des Données) être portées à 20 millions d'euros et 4% du chiffre d'affaire mondial.

Partons d'un cas concret.
La société Cochamboptnalds voit son système informatique piraté. Des investigations sont menées et le pirate informatique arrêté.
Vis à vis de la loi Godfrain du 5 janvier 1988, le voyou risque jusqu'à 2 ans de prison et 20 000 euros d'amende. Or ce dernier, après avoir découvert que la société Cochamboptnalds n'était pas en règle avec la CNIL la dénonce auprès de cette dernière.
Le responsable de traitement, généralement le chef d'entreprise risquera, lui, 5 ans de prison et 300 000 euros d'amende, une peine bien supérieure à son voleur.
Est-ce bien normal ?
Non, mais pourtant c'est comme ça et ça peut être le cas de toutes les entreprises, administrations et administrations françaises en cas de piratage de leurs ordinateurs, téléphones, boites e-mail…

Autre cas concret
Monsieur Roudoudou-Maxitout voit son téléphone portable mal protégé et exposé aux virus et aux pirates. Un jour il apprend par un ami que les contacts de son téléphone se sont fait pirater. Il se déplace à la Police ou à la Gendarmerie, dépose une plainte mais le voleur n'est jamais retrouvé. Qui est responsable de cette fuite d'informations ?
La première chose à savoir, c'est si ce téléphone est professionnel ou personnel. S'il est professionnel, référez vous au cas contrés précédent. Si par contre le téléphone portable est personnel, vis à vis de la loi Informatique et Libertés, les particuliers ne sont pour l'instant pas concernés par l'obligation de sécurisation des données.
Ainsi, si la faute volontaire du propriétaire de l'appareil n'est pas retenue, le seul responsable de cette fuite de données sera et restera l'auteur du piratage.

Denis JACOPINI est Expert Informatique et aussi ***formateur en Protection des données personnelles*** *(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).*
Nous pouvons vous animer des ***actions de sensibilisation ou de formation*** *à la Protection des Données Personnelles, au risque informatique, à l'hygiène informatique et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.*
Plus d'informations sur : ***https://www.lenetexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles***
Denis JACOPINI

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 Protection des Données Personnelles

Contactez-nous

Réagissez à cet article
Original de l'article mis en page : ***Informatique et Libertés : suis-je concerné ? | CNIL***

Se mettre en conformité avec la CNIL – Oui mais comment ? | Denis JACOPINI

Se mettre en conformité avec la CNIL – Oui mais comment ?
Encore plus fort que la peur du gendarme, la peur d'avoir mauvaise réputation est la principale crainte des entreprises concernées par des actes illicites (C'est ce qui ressort d'une étude de PWC).

Des années pour la construire, une fraction de seconde pour la salir; Et si votre manque de respect des données personnelles de vos clients vous rattrapait..

Protection des données personnelles : Les entreprises ne respectent pas la Loi et jouent avec les données de leur clients. Ca pourrait bien leur coûter cher ! | Denis JACOPINI

Protection des données personnelles : Les entreprises ne respectent pas la Loi et jouent avec les données de leur clients. Ca pourrait bien leur coûter cher !

Depuis 1978, les entreprises sont soumises à des obligations en terme de déclaration de traitements de données personnelles à la CNIL. Ne pas se soumettre à ces obligations, rend pénalement responsable le chef d'entreprise et passible d'une amende jusqu'à 300 000 euros. Une loi et des obligations quasiment tout le temps oubliées. Depuis le 25 mai 2018, les sanctions sont portées à 20 millions d'euros ou 4% du chiffre d'affaire.

A quoi sert la CNIL ?

Positionnez-vous d'abord en tant que consommateur. Lorsque vous commandez, achetez, communiquez, savez-vous où vont les informations personnelles ou confidentielles que vous confiez aveuglément ?Seriez-vous d'accord si toutes les données (coordonnées postales, e-mail, bancaires, santé, politique, religion, habitudes de consommation etc.) que vous communiquez en toute confiance à des tiers se retrouvent dispersées dans la nature et à la vue de tout le monde ? J'imagine que non ! Vous vous attendez plutôt à ce que tous les tiers prennent soin de conserver précieusement vos informations qui sont pour chacun d'entre nous précieuses et confidentielles pour certaines.

A la place de ça, que font les entreprises ?

Ils utilisent vos coordonnées pour envoyer de la publicité et surcharger votre boite e-mail, votre téléphone, votre boite aux lettres. Plus grave, certains vont vendre ou louer vos coordonnées à des tiers pour monnayer vos informations personnelles. Plus grave encore, d'autre encore vont stocker vos précieux éléments sur des systèmes informatiques non sécurités… Et c'est aussi comme ça qu'on se retrouve rapidement noyé par les spams ou les virus, victime d'usurpation d'identité ou pire… C'est pour canaliser cela que la CNIL (Commission Nationale de l'Informatique et des Libertés) existe. Sa mission officielle est de *« veiller à ce que le développement des nouvelles technologies ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »*.

Qui est concerné ?

Tout professionnel, organisme, association qui gère un fichier client, contact, mail, salariés, élèves, patients… que ce fichier soit informatisé ou géré sur papier. Les seuls qui n'ont pas à faire de telles déclarations sont les particuliers et les association, mais seulement pour les traitements qui concernent les données de leurs membres.

Les réactions les plus courantes lors de mes conférences

Lorsque j'anime des ateliers, des tables rondes ou des conférences sur le sujet des risques juridiques du chef d'entreprise face aux nouveaux usages de l'informatique ou des obligations des entreprises vis à vis de la CNIL, et que le volet des obligations par rapport à la #loi Informatique et Libertés est abordé, il m'est systématiquement posé la question suivante :

« Mais, comment se fait-il qu'on ne soit pas informé de ces obligations ? »

Et ma réponse au chef d'entreprises est systématiquement toujours la même :
« Par pure négligence de votre part . Que votre entreprise ait 0 ou 100 000 salariés, les obligations sont les mêmes et existent depuis 1978 au travers de la Loi Informatique et Libertés. Lorsque vous avez créé votre entreprise, vous vous êtes engagés à respecter la réglementation pendant toute la vie de votre entreprise. Et cette loi, je vous l'accorde, longtemps restée dans l'ombre, fait partie des règles qui doivent être obligatoirement respectées. Comme vous avez vu tout à l'heure, si vous vous positionnez en tant que consommateur, il vous semble évident que vos données personnelles soient protégées. Comme cette précaution absolue n'est pas une priorité naturelle pour les entreprises, un gendarme a été créé pour informer, surveiller, contrôler et sanctionner les entreprises fautives. Vous faites certainement partie des patrons qui essaient de gérer leur entreprise du mieux possible et avec vos problèmes et vos priorités vous y arriver je pense très bien. Vous vous souciez probablement d'abord de la réglementation à respecter en matière sociale, fiscale et en rapport de votre activité professionnelle. Je sais qu'il est matériellement impossible de tout savoir, et de connaitre toutes les lois. C'est ce que moi j'appelle faire des impasses. Sauf que là, c'est des impasses qui peuvent vous coûter jusqu'à 300 000 euros. »

Pourquoi parle-t-on de la CNIL si souvent aujourd'hui ?

Parce qu'elle tire la sonnette d'alarme devant les changements de nos habitudes et l'évolution de la technologie Fait très important qui s'est passé depuis le début des années 80 : L'informatique s'est répandue dans quasiment tous les domaines sans réellement tenir compte de la sécurité des données. Peu savent que depuis les années 90, Internet qui s'impose à nous utilise un protocole de communication qui à la base ne sont pas sécurisées . Ensuite, nous sommes entrés dans l'ère des objets connectés avec un risque permanent de se faire « pomper » nos données. On ne va plus seulement parler de coordonnées postales téléphoniques ou bancaires, mais aussi de données de santé, d'habitudes alimentaires, de sommeil, de sortie, de loisirs… Que vos joujoux hi-tech connectés, votre smartphone ou votre ordinateur soient perdus ou piratés, les données qu'ils stockent sont librement accessibles… De plus, il ne se passe pas un jour sans qu'un opérateur, une société Web, une entreprise se fasse pirater son système informatique et par la même occasion les données de ses clients. Il y a deux types de cibles : celles qui ont beaucoup de trésorerie à se faire voler, et les millions de malchanceux qui dont le manque de sécurité a été automatiquement détecté qui vont être la proie de cybercriminels. Pour vous donner une idée, 144 milliards d'emails sont échangés chaque jour et 68,8% d'entre eux sont des spams et nombreux cachent des réseaux cybercriminels. 400 Millions de personnes sont concernées par des cyberattaques chaque année. Vous comprenez maintenant pourquoi il devient urgent de canaliser tous ces usages et déjà les premier débordements avant que ça continue à s'aggraver.

Est-ce risqué de ne pas respecter la Loi Informatique t Libertés

Même si en référence la loi du 29 mars 2011 relative au défenseur des droits, la CNIL peut rendre publiques les sanctions pécuniaires qu'elle prononce, il n'y a jusqu'à maintenant eut que très peu de sanctions prononcées. En 2013, 414 contrôles ont abouti à 14 sanctions.
On eut en avoir liste sur http://www.cnil.fr/linstitution/missions/sanctionner/les-sanctions-prononcees-par-la-cnil/
Cependant, le niveau de risque devrait exploser en 2015 ou du moins, dès la mise en application du règlement européen relatif aux traitements de données à caractère personnel. Selon les infractions, le montant des sanctions peut aujourd'hui s'élever jusqu'à 300 000 euros. Cenpendant, compte tenu de leur chiffre d'affaire démesuré, certaines entreprises peuvent continuer à sourire avec de telles amendes (par exemple google et ses 60 milliards de chiffre d'affaire, ou Facebook, Appel, Orange…) .
Devant ces situations, la Commission Européenne décidé de frapper un grand coup avec un règlement européen et au travers de deux principales actions répressives :
1) Augmenter plafond des amendes jusqu'à 5% du chiffre d'affaire (ça pourrait donner 3 milliards de dollars d'amende maximale par infractions pour google)
2) Rendre Obligatoire pour toute entreprise, de déclarer sous 24h à la CNIL le moindre incident de sécurité (virus, perte données, perte ou vol de matériel, piratage…), laquelle pourra vous obliger d'informer tous vos clients que la sécurité de leurs données personnelles a été compromise. Cette obligation existe déjà depuis juin 2013 mais seulement pour les OIV (Opérateurs d'importance Vitale).
Souvenez-vous l'affaire du piratage d'Orange en janvier et avril 2014 et les articles de presse peux valorisants pour la marque et inquiétant pour ses clients. Le règlement européen prévoir d'obliger toutes les entreprises d'informer l'ensemble des propriétaires dont la sécurité a été compromise suite à un piratage, une perte ou à un vol de données personnelles ou de matériel contenant des données personnelles. Ainsi, on ne parle plus d'un risque financier, mais d'un risque de mauvaise réputation des entreprises face à leurs clients et concurrents…

Concrètement, que faut-il faire pour de mettre en conformité avec la CNIL ?

L'aritcle premier de la Loi définit que l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.
L'article 2 précise que la loi s'applique aux traitements de données à caractère personnel contenues ou appelées à figurer dans des fichiers.
Enfin l'article 22 indique que les traitements de données à caractère personnel font l'objet d'une déclaration auprès de la CNIL
En d'autres termes, pour se mettre en conformité, il faut déclarer à la CNIL l'ensemble des traitements de données qui concernent des informations permettant d'identifier des personnes.
Je tiens à préciser qu'on ne déclare pas ou on ne donne pas à la CNIL ses données, on ne déclare que des traitements de données à caractères personnel.
Lien vers le Loi Informatique et Libertés http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/

Mon conseil en 4 étapes pour se mettre en conformité avec la CNIL

1) Identifier l'ensemble des traitements de données permettant d'identifier des personnes.
2) Procéder à l'analyse détaillée de ses traitements et corriger les actions qui ne sont pas conformes à la Loi Informatique et Libertés en terme de sécurité des fichiers, de confidentialité des données, de durée de conservation des documents, d'information des personnes, de demande d'autorisation et de finalité des traitements.
3) Déclarer le traitement à la CNIL ou désigner un Correspondant Informatique et Libetés qui sera chargé de tenir à jour un registre des traitements sans avoir à les déclaréer séparément.
4) Faire un à deux points par an pour reporter dans le registre les changements sur les traitements existants et les y ajouter les nouveaux.
En cas d'impossibilité d'adapter votre traitement de données personnelles par rapport à la loi Informatique et Libertés, une demande d'avis ou d'autorisation doit être formulée à la CNIL.
Bien évidemment, la réponse de la CNIL doit être attendue avant d'utiliser le traitement concerné.
Une fois ces étapes de « mise sur rails » accomplie, la personne qui aura en charge la fonction de correspondant dans votre entreprise aura obligation de tenir un registre des traitements mis en œuvre au sein de l'organisme (consultable par la CNIL ou tout demandeur sur simple demande) et de veiller au respect des dispositions de la loi « informatique et libertés » au sein de l'organisme.

Est-on obligé de faire une déclaration pour chaque traitement ?

Oui et Non
Non si vous nommez un #correspondant Informatique et Libertés (#CIL). Qu'il soit interne à l'entreprise ou externe (si vous souhaitez déléguer la responsabilité à quelqu'un d'externe à l'entreprise, comme je le fais pour de nombreuses entreprises). Le Cil n'aura alors qu'à tenir à jour un registre répertoriant l'ensemble des traitements de données à caractères personnel et leurs caractéristiques détaillées. Ce registre devra pouvoir être consultable par la CNIL mais auss par quiconque vous en fera la demande.
Oui si vous décidez de ne pas déclarer un Correspondant Informatique et Libertés.

Qui peut être ou devenir CIL ?

La loi prévoit que le correspondant Informatique et Libertés est une personne bénéficiant des qualifications requises pour exercer ses missions.
Aucun agrément n'est prévu et aucune exigence de diplôme n'est fixée.
Néanmoins, le CIL doit disposer de compétences variées et adaptées à la taille comme à l'activité du responsable des traitements.
Ces compétences doivent porter tant sur l'informatique et les nouvelles technologies que sur la réglementation et législation relative à la protection des données à caractère personnel.
…
L'absence de conflit d'intérêts avec d'autres fonctions ou activités exercées parallèlement est également de nature à apporter les garanties de l'indépendance du CIL. C'est pourquoi la fonction de correspondant est incompatible avec celle de responsable de traitements. Sont concernés le représentant légal de l'organisme (ex. : le maire / le PDG) et les autres personnes participant à la prise de décisions en matière de mise en oeuvre des traitements (ex. : les conseillers municipaux / les personnes disposant d'une délégation de pouvoirs).

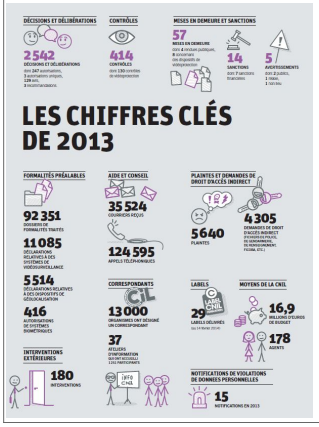
Des difficultés pour vous mettre en conformité ?

Pour vous mettre en conformité avec la CNIL, il vaut mieux être sensibilisé à la loi Informatique et Libertés et aux règles et obligations qui en découlent (obligation d'information, droit d'accès, traitement des réclamations…).
Pour que votre mise en règle se fasse dans de bonnes conditions, nous pouvons nous charger de former et de suivre une personne de votre entreprise qui jouera le rôle de CIL (Correspondant Informatique et Libertés) ou bien, si vous le préférez, pour encore plus de tranquillité, Denis JACOPINI, expert Informatique spécialisé en protection des données personnelles, peut se charger d'être votre CIL externe en se chargeant de prendre en charge l'ensemble des formalités.

Plus de détails sur la CNIL

La CNIL est une AAI (Autorité Administrative Indépendante). C'est une structure gérée par l 'état qui ne dépent d'aucun ministère et qui peut dresser des procès verbaux et sanctionner sans même à avoir à passer par un juge. La CNIL dépend directement du premier ministre qui peut en dernier recours, directement prendre des mesures pour mettre fin aux manquements.

Quelques chiffres



Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84 — Liberté • Égalité • Fraternité — RÉPUBLIQUE FRANÇAISE

Datadock — Organisme validé et référencé

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

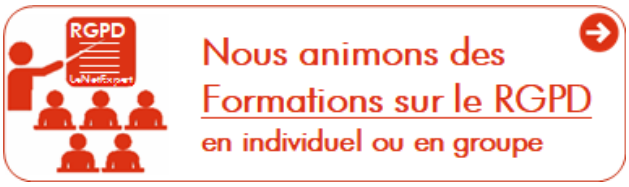
Contactez-nous

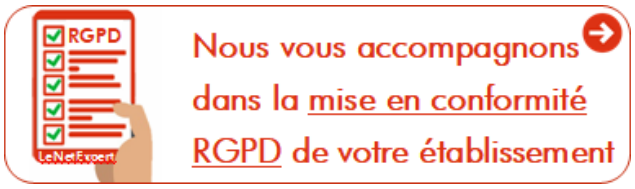
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles

en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Auteur : Denis JACOPINI

Les Conseils du Net Expert – Bien choisir ses mots de passe pour protéger ses données sur Internet

Les Conseils du Net Expert
Bien choisir ses mots de passe pour protéger ses données sur Internet

Bien choisir ses mots de passe pour protéger ses données sur Internet

Entre les affaires de piratage de données personnelles de serveurs informatiques et les attaques dévoilant au grand jour les mots de passe les plus utilisés (c.f. liste des mots de passe récupérée lors du piratage de certains serveurs de la multinationale Adobe en Octobre 2013), il devient urgent de reconsidérer la manière dont nous choisissons nos mots de passe.

La liste des mots de passe les plus utilisés sur Internet

Octobre 2013, Adobe confirmait avoir subi une cyberattaque d'envergure, ayant entrainé le vol du code source de ses applications Photoshop, Adobe Acrobat, ColdFusion, et la compromission de 38 millions de comptes utilisateurs.

Jeremi Gosney, un chercheur en sécurité, a réussi à casser les mots de passe des comptes utilisateurs volés à d'Adobe. IL révèle une liste aberrante des 100 mots de passe les plus utilisés.

Selon la liste, près de 1,9 million de comptes ont utilisé « 123456 » comme mots de passe, plus de 440 000 ont opté pour « 123456789 ». Le top 5 est complété par les mots de passe « password », « adobe123 » et « 12345678 ».

Il devient donc urgent que les utilisateurs, responsable de leur mot de passe, modifient leur manière de le choisir.

	Mot de passe	Nombre d'utilisateurs
1	123456	1911938
2	123456789	446162
3	password	345834
4	adobe123	211659
5	12345678	201580
6	qwerty	130832
7	1234567	124253
8	111111	113884
9	photoshop	83411
10	123123	82694
11	1234567890	76910
12	000000	76186
13	abc123	70791
14	1234	61453
15	adobe1	56744
16	macromedia	54651
17	azerty	48850
18	iloveyou	47142
19	aaaaaa	44281
20	654321	43670

Cinq paramètres pour bien choisir ses mots de passe

Vous pouvez remarquer dans le tableau ci-dessus la manière la plus répandue de choisir un mot de passe. Il devient à mon avis urgent d'abandonner cette habitude d'utiliser une succession de chiffres ou de lettres ou bien un prénom, une date de naissance ou un mot connu le tout le plus facile à retenir). Il est de toute évidence primordial que les mots de

passe doivent aujourd’hui non seulement être :

– faciles à retenir

– le plus long possible

– le plus complexe possible

– changé souvent

– différent pour chaque service

Ceci dit, si vous avez aussi la main sur le système chargé de gérer les accès, je recommande non seulement une action de blocage temporaire ou permanent d’un compte lorsqu’un nombre de tentatives maximum (généralement 10) est dépassé, ou bien bloquer les tentatives pendant un certain nombre de minutes au delà d’un certain nombre d’échecs successifs.

Pour ceux qui le désirent, je peux soit sous forme d’audit, sois sous forme de formation vous apprendre les bases des usages recommandés de l’informatique comprenant tout un chapitre sur les choix des mots de passe.

Vous trouverez ci-dessous, des informations essentielles pour comprendre et revoir votre politique de choix des mots de passe car il faut bien retenir quelque chose :

Au plus le mot de passe sera long (nombre de symboles) et complexe (mixité des types de symboles), au plus il sera difficile et long pour le retrouver !

Le tableau ci-dessous donne le nombre **maximum** d’essais nécessaires pour trouver des mots de passe de longueurs variables.

Type	1 caractère	3 caractères	6 caractères	9 caractères
lettres minuscules	26	17 576	308 915 776	$5{,}4 \times 10^{12}$
lettres minuscules et chiffres	36	46 656	2 176 782 336	$1{,}0 \times 10^{14}$
minuscules, majuscules et chiffres	62	238 328	$5{,}6 \times 10^{10}$	$1{,}3 \times 10^{16}$

Ci-dessous, une estimation de temps pour retrouver votre mot de passe avec de puissants ordinateurs :

123456 (le plus utilisé dans le monde) : instantané

654321 : instantané

toto : instantané

toto84 : 0.544195584 seconds

toto84# : 3 minutes

toto84#26 :6 jours

toto84#26% : 344 jours

toto84#26% : 344 jours

totototo84#26% : 6 millions d’années

Des outils pour nous aider

Que ça soit des outils de génération automatique de mots de passe (qui pourra être considéré comme quasi-incassable mais sera impossible à retenir et donc obligatoire à stocker quelque part pour être capable de le retrouver) ou des coffre fort à mots de passe, certains éditeurs mettent en oeuvre leur imagination débordante pour nous aider à résoudre ce casse tête des très nombreux mots de passe que nous devons retenir

pour chacun des sites internet sur lesquels nous disposons d'un compte personnel.

Il ne faut pas l'oublier, disposer d'un seul mot de passe pour plusieurs sites Internet peut vite devenir dangereux. En effet, si un système informatique (orange, sfr, ebay, sony…) se fait pirater, il est fort probable que si vous aviez un compte sur ce site Internet, votre mot de passe soit volé. Une fois volé et décodé, votre mot de passe rentre dans la longue liste des mots de passe connus et automatiquement tentés par les robots des pirates sur d'autres sites Internet. Si votre mot de passe est utilisé sur d'autres sites Internet dont ceux qui se feront pirater, les malfrats auront donc plus facilement accès à votre compte.

Enfin, il ne faut pas trop aller vers l'opposé (ne plus aller sur Internet, ou fuir la technologie). Utiliser des mots de passe trop compliqués peuvent vite vous rendre la vie bien compliquée. Si vous finissez pas les oublier ou par les noter sur un post-it sur votre écran ne répondra peut-être pas aux besoins d'utilisation que nous oblige de vivre l'ère numérique que nous traversons.

Outils à ne pas manquer :

Dashlane : Gestionnaire de mots de passe et portefeuille numérique pour ordinateur et smartphone mis au point par une jeune entreprise française, qui a pour but de simplifier la manière dont nous jonglons avec nos nombreux éléments d'identité numérique. Au lieu d'avoir à taper à chaque fois nos noms-prénoms-adresses ou lorsque l'on fait un achat sur Internet ou que l'on s'inscrit à un service, il suffit de renseigner une seule fois au départ le logiciel et ensuite à chaque fois qu'on en a besoin Dashlane remplit automatiquement les champs demandés. Il peut également stocker vos numéros de cartes bancaires toujours pour éviter d'avoir à

les taper à chaque fois si vous êtes un cyberacheteur compulsif. Il garde un historique des achats que vous effectuez en ligne. Le système conserve en mémoire tous les mots de passe ce qui permet de se connecter plus vite à ses services habituels.
https://www.dashlane.com/fr
http://www.franceinfo.fr/emission/Unknown%20token%20emisaison-type-url/noeud-diffusion-temporaire-pour-le-nid-source-721447-05-05-2014-11-47

KeePass : Ce logiciel facilite la gestion des mots de passes en les enregistrant dans une base de données.
http://keepass.info

Password Keeper : Le logiciel Password Keeper Expert est à la fois une base de stockage et un puissant gestionnaire de mots de passe.
http://www.password-keeper.net

1Password : Gestionnaire de mot de passe qui vous offre un moyen simple et facile de gérer votre mot de passe.
https://agilebits.com/

Du coté des développeurs

Les administrateurs de sites Internet, de serveurs Web ou de serveurs informatiques en tout genre doivent aussi être sensibilisés et à mon avis responsabilisés par les conséquences que peuvent engendrer l'utilisation de systèmes de sécurité. La future mise en place d'un CDO (Chief DataOfficer), prévue par la commission européenne chargée de faire respecter en Europe les règles fondamentales de protection des données personnelles, a pour but, au sein d'une structure qui collectera des données personnelles, de rendre responsable jusqu'au niveau pénal, une personne chargée de

veiller que cette protection respecte toute une série de paramètres, dont tout un volet consacré à la sécurité d'accès aux données.

Ainsi, les développeur en interne, les administrateurs des systèmes informatiques et les éditeurs de logiciels devront renforcer leurs méthodes de contrôle d'accès jusqu'à, sans aller jusqu'à imposer les mots de passe aux utilisateurs, les obliger tout au moins d'utiliser des mots de passe plus difficiles à retrouver par la simple utilisation de dictionnaires ou par tables de hashages.

Sans revenir sur l'utilisation indispensable aujourd'hui du hashage des mots de passe au moins en sha256, (sha1 et MD5 étant à ce jour facilement cassable), une des méthodes qui à mon sens peut rendre encore plus difficile la tache de conversion vers des tables de hashage est l'utilisation de grains de sel. Il s'agit d'un mot, qui de manière transparente pour l'utilisateur, sera systématiquement ajouté au mot de passe initial, avant hashage.

Le résultat sera que dans les bases de données, un mot de passe de taille déraisonnable sera stocké, et probablement impossible à retrouver par les technologies de dizaines de prochaines années (hashage en sha256 d'un mot de passe par exemple de 500 caractères si le grain de sel fait par exemple 490 caractères et le mot de passe 10 caractères minimum.

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

Références :

23/01/2014
http://www.programme-tv.net/news/buzz/47672-quels-sont-mots-de-passe-plus-utilises-internet

05/11/2013
http://www.developpez.com/actu/63730/Piratage-d-Adobe-la-liste-aberrante-des-mots-de-passe-des-utilisateurs-plus-de-1-9-million-de-comptes-utilisent-123456-comme-mot-de-passe

http://assiste.com.free.fr/p/abc/a/attaque_des_mots_de_passe.html

http://www.openwall.com/john/

https://howsecureismypassword.net/

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