

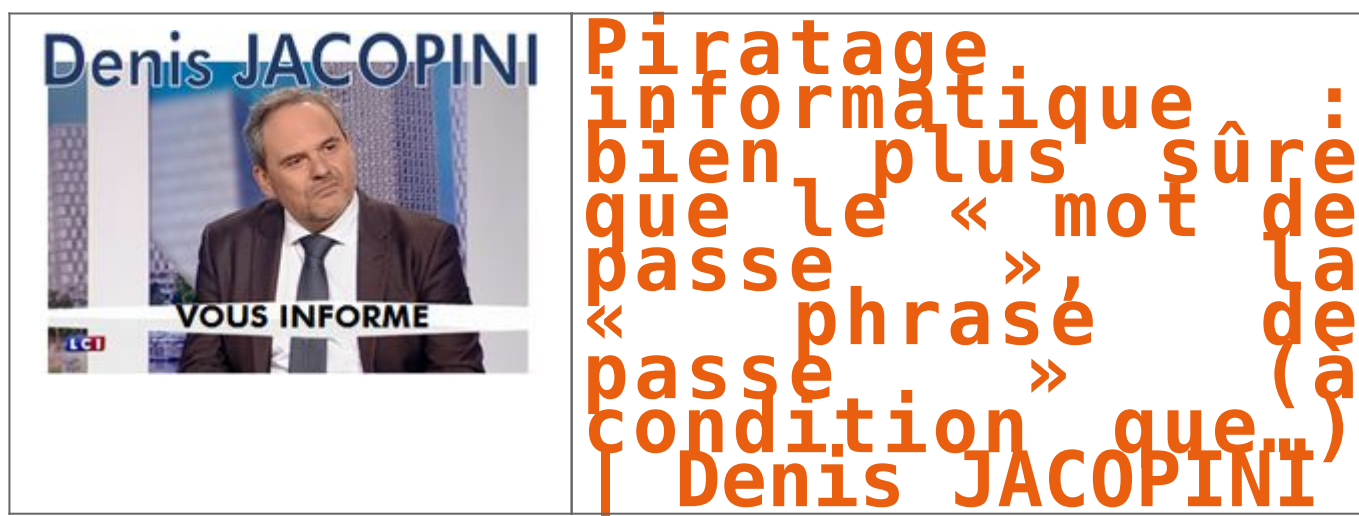
Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) ?



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) ?

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



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 essaient 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 verrouille 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 travaille sur un ordinateur partagé, bien verrouiller son ordinateur, etc...

Article original de Denis JACOPINI et Atlantico

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.

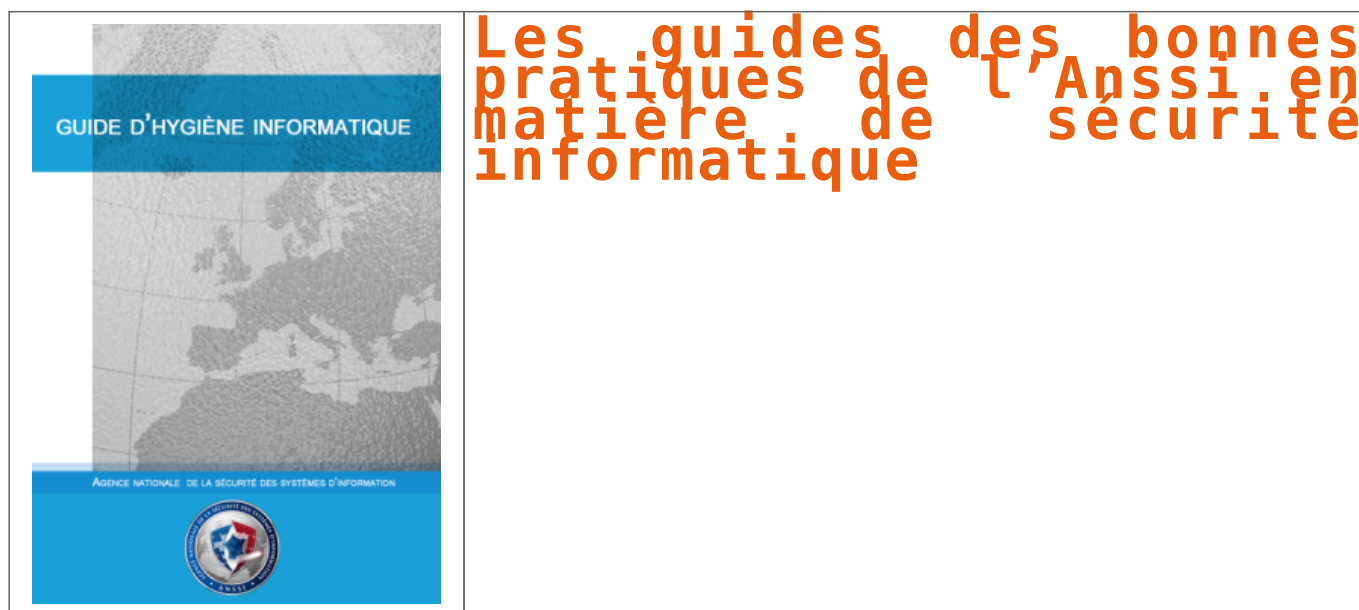


[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : 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



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

Expert Informatique 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 protection juridique du chef d'entreprise.

Contactez-nous

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-à-vis des données que ce support numérique renferme.

Imaginez que vous disposez de différents appareils numériques 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 (maliciel 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 de piratage (intrusion causée par une faille, un virus, un cryptovirus, 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 Cochabonairails 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 Cochabonairails n'était pas en règle avec la CNIL la dénonça auprès de cette dernière.

Le responsable de traitement, apparemment 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, boîtes e-mail.

Autre cas concret

Monsieur Roudbouou-Maitout 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, réfère vous au cas ci-dessus. Si par contre le téléphone portable est personnel, vis à vis de la loi Informatique et Libertés, les particuliers ne sont 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 04 62042 04).

Nous pouvons vous assister des actions de sensibilisation en 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.lesnetexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles>

Denis JACOPINI



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

- Expertises techniques (virus, spyware, phishing, malware, attaques DDoS, etc.) et analyses forensiques (logiciels, données, etc.)
- Expertise de sécurité de vos dispositifs ;
- Formations et conférences en cybersécurité ;
- Rédaction de PIA (Compendium Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL en entreprise.

Le Net Expert
INFORMATIQUE
COURSIL.COM

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**

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITE</p>	 <p>LE NET EXPERT SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
	<p>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 !</p>				

2022 Les entreprises sont soumises à des obligations de transparence de traitement de données personnelles à la CNIL. Ne pas se soumettre à ces obligations, rend pleinement responsable le chef d'entreprise et possible d'une amende jusqu'à 300 000 euros. Une loi et des obligations seulement tout le temps applicables. Depuis le 25 mai 2018, les sanctions sont portées à 20 millions d'euros ou 4% du chiffre d'affaires.

Qui est le DPO ?
 Personne chargée d'assurer en tant que consultant, lorsque vous communiquez, achetez, communiquez, avez accès à vos informations personnelles ou confidentielles que vous confiez au traitement de données personnelles ou confidentielles que vous communiquez en toute confiance à des tiers et le retour de données par la suite et à la suite de tout le monde ? L'empêcher que vous vous soumettiez à la loi que tous les tiers peuvent avoir accès à vos informations personnelles ou confidentielles pour certains.

La CNIL est-elle un organisme public ?
 C'est une mission de service public. Elle a pour mission de garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles. Plus généralement, elle veille à ce que les données personnelles soient traitées de manière transparente et responsable. Elle a pour mission de garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles. Plus généralement, elle veille à ce que les données personnelles soient traitées de manière transparente et responsable.

Les entreprises ont-elles des obligations de transparence ?
 Oui, elles ont des obligations de transparence. Elles doivent informer les personnes concernées de la collecte et de l'usage de leurs données personnelles. Elles doivent également garantir la sécurité de ces données et leur confidentialité. Elles doivent également garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles. Plus généralement, elles doivent garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles.

Comment les entreprises peuvent-elles se conformer à ces obligations ?
 Elles peuvent se conformer à ces obligations en mettant en place des mesures de protection des données. Elles peuvent également consulter un expert en matière de protection des données. Elles doivent également garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles. Plus généralement, elles doivent garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles.

Quelles sont les sanctions en cas de non-conformité ?
 Les sanctions peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires. Elles peuvent également aller jusqu'à 300 000 euros. Elles doivent également garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles. Plus généralement, elles doivent garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles.

Comment les entreprises peuvent-elles éviter ces sanctions ?
 Elles peuvent éviter ces sanctions en mettant en place des mesures de protection des données. Elles peuvent également consulter un expert en matière de protection des données. Elles doivent également garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles. Plus généralement, elles doivent garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles.

Quelles sont les obligations de transparence de traitement de données personnelles à la CNIL ?
 Les entreprises doivent informer les personnes concernées de la collecte et de l'usage de leurs données personnelles. Elles doivent également garantir la sécurité de ces données et leur confidentialité. Elles doivent également garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles. Plus généralement, elles doivent garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles.

Comment les entreprises peuvent-elles se conformer à ces obligations ?
 Elles peuvent se conformer à ces obligations en mettant en place des mesures de protection des données. Elles peuvent également consulter un expert en matière de protection des données. Elles doivent également garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles. Plus généralement, elles doivent garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles.

Quelles sont les sanctions en cas de non-conformité ?
 Les sanctions peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires. Elles peuvent également aller jusqu'à 300 000 euros. Elles doivent également garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles. Plus généralement, elles doivent garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles.

Comment les entreprises peuvent-elles éviter ces sanctions ?
 Elles peuvent éviter ces sanctions en mettant en place des mesures de protection des données. Elles peuvent également consulter un expert en matière de protection des données. Elles doivent également garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles. Plus généralement, elles doivent garantir la transparence et l'efficacité de la collecte et l'usage des données personnelles.

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.



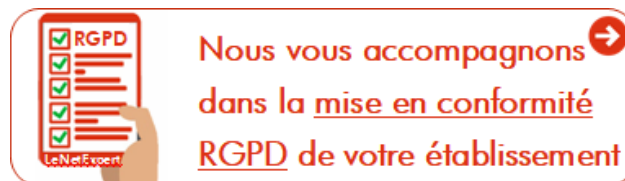
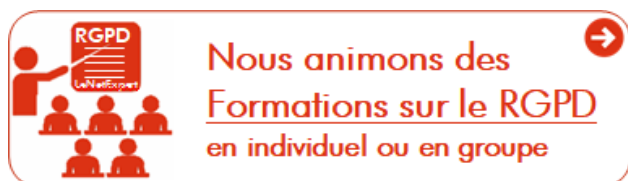
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

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)

[block id="24761" title="Pied de page HAUT"]

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 entraîné 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.



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, soit 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%20emission-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 côté 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 tâche 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)**

