Quelles formalités une pharmacie doit déclarer à la CNIL ? | Denis JACOPINI

Quelles formalités une pharmacie doit déclarer à la CNIL ?

Les fichiers relatifs à la gestion d'une pharmacie doivent être déclarés à la CNIL :Par une déclaration simplifiée de conformité à la norme n°52 si le fichier correspond aux caractéristiques énoncées dans ce texte ;
Par une déclaration normale si le fichier sort du cadre de cette norme.

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;jsessionid=193E337DAA685A15B25C9E90E19E80BF?name=Activit%C3%A9+d%27une+pharmacie+%3A+quelles+formalit%C3%A9s+%C3%A0+la+CNIL+%3F&id=545

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. À 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 raccourcis 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

---

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

---

Sensibilisations et Formations à la Cybercriminalité et au RGPD (Protection des données personnelles) – Redirect

Parce que la Cybercriminalité et la

Protection des données personnelles sont liés, nous couvrons ces sujets concomitamment (Intervention en France et étranger)

Nos formations sont personnalisées en fonction du type de publics présent (Dirigeants, cadres , informaticiens, responsable informatique, RSSI, utilisateurs).

Contactez-nous

PROGRAMME

CYBERCRIMINALITÉ
COMMENT PROTÉGER VOTRE ORGANISME DE LA CYBERCRIMINALITÉ

Présentation

La France a rattrapé sont retard en matière d'équipement à Internet mais à en voir les dizaines de millions de français victimes chaque année, les bonnes pratiques ne semblent toujours pas intégrées dans vos habitudes.

Piratages, arnaques, demandes de rançons sont légions dans ce monde numérique et se protéger au moyen d'un antivirus ne suffit plus depuis bien longtemps.

Avons-nous raison d'avoir peur et comment se protéger ?

Cette formation couvrira les principaux risques et les principales solutions, pour la plupart gratuites, vous permettant de protéger votre informatique et de ne plus faire vous piéger.

Objectifs

Découvrez les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant de naviguer sur Internet en toute sécurité.

Demande d’informations

CYBERCRIMINALITÉ

LES ARNAQUES INTERNET A CONNAÎTRE POUR NE PLUS SE FAIRE AVOIR

Présentation

Que vous vous serviez d’Internet pour acheter, vendre, télécharger ou communiquer, un arnaqueur se cache peut-être derrière votre interlocuteur.

Quels sont les signes qui ne trompent pas ? Comment les détecter pour ne pas vous faire piéger ?

Objectifs

Découvrez les mécanismes astucieux utilisés par les arnaqueurs d’Internet dans plus d’une vingtaine cas d’arnaques différents. Une fois expliqués, vous ne pourrez plus vous faire piéger.

Demande d’informations

PROTECTION DES DONNÉES

RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES) – CE QU’IL FAUT SAVOIR POUR NE PAS LE PAYER CHER

Présentation

Le Règlement Général sur la Protection de Données (RGPD) est entré en application le 25 mai 2018 et toutes les entreprises, administrations et associations ne se sont pas mises en

conformité. Or, quelle que soit leur taille, elles sont toutes concernées et risqueront, en cas de manquement, des sanctions financières jusqu'alors inégalées.

Au delà de ces amendes pouvant attendre plusieurs millions d'euros, de nouvelles obligations de signalement de piratages informatiques risquent désormais aussi d'entacher votre réputation. Quelle valeur lui donnez vous ? Serez-vous prêt à la perdre pour ne pas avoir fais les démarches dans les temps ?

Cette formation non seulement répondra la plupart des questions que vous vous posez, vous offrira des éléments concrets non seulement pour initier la mise en conformité de votre établissement mais surtout pour transformer ce qui peut vous sembler à ce jour être une contrainte en une véritable opportunité.

Objectifs

Cette formation a pour objectif de vous apporter l'essentiel pour comprendre et démarrer votre mise en conformité avec le RGPD dans le but à la fois de répondre à la réglementation et de prévenir en cas de contrôle de la CNIL.

Informations complémentaires

Demande d'informations

PROTECTION DES DONNÉES

RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES) – ANALYSONS CE QUE VOUS AVEZ COMMENCÉ

Présentation

Après avoir suivi notre formation vous permettant de comprendre l'intérêt d'une telle réglementation et de savoir

ce qu'il faut mettre en place pour bien démarrer, vous souhaitez aller plus loin dans la démarche de mise en conformité avec le RGPD.

Après un retour éclair sur les règles de base, nous ferons un point sur la démarche de mise en conformité que vous avez initiée ces derniers mois dans votre établissement. Nous détaillerons ensuite les démarches à réaliser en cas de détection de données sensibles et d'analyse d'impact. Enfin, nous approfondirons des démarches périphériques essentielles pour répondre à vos obligations.

Objectifs

Après avoir déjà découvert l'essentiel pour comprendre et démarrer votre mise en conformité avec le RGPD, cette formation aura pour objectif de vous perfectionner afin de devenir référent protection des données ou DPO (Data Protection Officer = Délégué à la Protection des Données).

Demande d'informations

CYBERSÉCURITÉ
DÉTECTER ET GÉRER LES CYBER-ATTAQUES

Présentation

Que vous ayez déjà été victime d'une cyber-attaque ou que vous souhaitiez l'anticiper, certaines procédures doivent absolument être respectées pour conserver un maximum de preuves et pouvoir les utiliser.

Objectifs

Que votre objectif soit de découvrir le mode opératoire pour savoir quelles sont les failles de votre système ou si vous avez été victime d'un acte ciblé avec l'intention de vous

nuire, découvrez les procédures à suivre.

Demande d’informations

CYBERSÉCURITÉ
APPRENEZ À RÉALISER DES AUDITS SÉCURITÉ SUR VOTRE SYSTÈME INFORMATIQUE

Présentation

Votre système informatique a très probablement de nombreuses vulnérabilités présentées aux pirates informatiques comme de nombreux moyens de nuire à votre système informatique.

Avant de procéder à un test d’intrusion, apprenez à réaliser l’indispensable audit sécurité de votre système informatique afin d’appliquer les mesures de sécurité de base présentes dans les référentiels internationalement utilisés.

Objectifs

Vous apprendrez au cours de cette formation la manière dont doit être mené un audit sécurité sur un système informatique, quelques référentiels probablement adaptés à votre organisme et nous étudierons ensemble le niveau de sécurité informatique de votre établissement.

Demande d’informations

CYBERSÉCURITÉ
APPRENEZ À RÉALISER DES TESTS D’INTRUSION

SUR VOTRE SYSTÈME INFORMATIQUE

Présentation

Cette formation vous apporte l'essentiel de ce dont vous avez besoin pour adopter l'approche du Hacker pour mieux s'en protéger en élaborant vos tests de vulnérabilité, mettre en place une approche offensive de la sécurité informatique permettant d'aboutir à une meilleure sécurité et réaliser des audits de sécurité (test d'intrusion) au sein de votre infrastructure.

La présentation des techniques d'attaques et des vulnérabilités potentielles sera effectuée sous un angle « pratique ».

Objectifs

Cette formation vous apportera la compréhension technique et pratique des différentes formes d'attaques existantes, en mettant l'accent sur les vulnérabilités les plus critiques pour mieux vous protéger d'attaques potentielles.

Demande d'informations

QUI EST LE FORMATEUR ?

Denis JACOPINI est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale, Investigation numérique pénale, et en Droit de l'Expertise Judiciaire et a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

Il anime dans toute le France et à l'étranger des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données

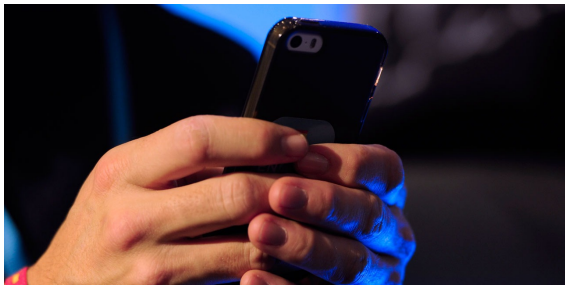
personnelles.
A ce titre, il intervient régulièrement sur différents médias et sur La Chaine d'Info LCI pour vulgariser les sujets d'actualité en rapport avec ces thèmes.

Spécialisé en protection des données personnelles, il accompagne les établissements dans leur mise en conformité CNIL en les accompagnant dans la mise en place d'un Correspondant Informatique et Libertés (CIL).

Enfin, il intervient en Master II dans un centre d'Enseignement et de Recherche en Informatique, en Master Lutte contre la Criminalité Financière et Organisée, au Centre National de la Fonction Publique Territoriale et anime le blog LeNetExpert.fr sur lequel il partage et publie de très nombreuses informations sur ses thèmes de prédilection.

Denis JACOPINI peut facilement être contacté sur :
http://www.leNetExpert.fr/contact

Les données personnelles des portables d’occasion toujours accessibles | Denis JACOPINI

	Les données personnelles des portables d’occasion toujours accessibles

De nombreux smartphones reconditionnés contiennent toujours des informations sensibles sur leurs anciens propriétaires.

Avant de revendre votre portable, veillez à bien effacer toutes vos données personnelles. En effet, de nombreux smartphones reconditionnés – c'est-à-dire d'occasion et revendus dans les boutiques – contiennent toujours des informations de leurs anciens propriétaires, selon une étude réalisée par l'entreprise Avast, spécialisée dans les antivirus, et révélée en exclusivité par Europe 1.
Emails, photos, SMS, factures personnelles ou même clichés à caractère sexuel : ces téléphones renferment souvent des données extrêmement sensibles.

Un contrat de travail, des mails et des SMS retrouvés

Le problème concerne une part croissante du marché des téléphones portables. 10% des Français ont en effet acheté un mobile de seconde main en 2015. Avast a ainsi mené une expérimentation sur vingt anciens modèles de smartphone, achetés à New York, Paris, Barcelone et Berlin. Les résultats sont édifiants : sur cet échantillon test, de nombreuses données personnelles ont été retrouvées.
Avast a ainsi pu accéder à 2.000 photos, dont des clichés d'enfants, d'autres à caractère sexuel, mais aussi un contrat de travail ou encore 300 mails et SMS. Pire : deux propriétaires de téléphone avaient oublié de déconnecter leurs comptes Gmail, prenant le risque que les nouveaux acheteurs lisent ou envoient des mails en leur nom.

« Important de faire une démarche complète »

Bien que 40% des portables vendus dans les boutiques d'occasion soient reconditionnés, les anciens propriétaires réinitialisent souvent mal, voire pas du tout, leurs terminaux. Les revendeurs spécialisés le constatent ainsi tous les jours. « Ça arrive à un client sur deux : quand il nous propose son téléphone, il ne l'a pas effacé au préalable », explique Frédéric Bertinet, de Cash Express.
« Les téléphones ont été mal réinitialisés, donc on pense qu'on a fait le travail parce qu'on a enlevé les mots de passe et les réglages, mais le contenu lui n'a pas été effacé. Il est important de faire une démarche complète, un peu procédurière », conclut Frédéric Bertinet.

Des applications sécurisées pour effacer les données

Mais pour éviter tout risque, une simple réinitialisation ne suffit pas. « Lorsqu'un fichier est effacé, c'est seulement la référence de ce fichier qui disparaît. Pour que ces fichiers disparaissent complètement, il faut les remplacer par d'autres données quelconques, c'est-à-dire des 0 et des 1. Sinon, c'est théoriquement récupérable », détaille Arnaud Matthieu, représentant d'Avast pour la France.
Pour vider à jamais votre téléphone portable, des applications sécurisées sont disponibles gratuitement sur Internet. Mais attention : si vous n'écrasez pas correctement vos données personnelles, les risques sont immenses. Les anciens propriétaires de smartphones s'exposent à du chantage, à des photos personnelles publiées sur internet ou encore à de l'usurpation d'identité.

Réagissez à cet article

Source : *Les données personnelles des portables d’occasion toujours accessibles*

Nouvelles formations sur les déclarations à la CNIL et en cybercriminalité | Denis JACOPINI

	Nouvelles formations sur les déclarations à la CNIL et en cybercriminalité

Pour information, Denis JACOPINI propose depuis quelques mois deux nouveaux sujets de formation à destination des chefs d’entreprise, de leurs salariés mais aussi des administrations et de leurs agents :

– La cybercriminalité, un vrai risque pour les chefs d’entreprises– Mettre son entreprise en conformité avec la CNIL, secrets et mode d’emploi
– Cybercriminalité, sécurité informatique et CNIL, bonnes pratiques et cadre juridique
– La cybercriminalité, un vrai risque pour administrations

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

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

Règlement européen sur la protection des données : Evolution du cadre juridique

	Règlement européen sur la protection des données : Evolution du cadre juridique

Le nouveau règlement européen sur la protection des données personnelles est paru au journal officiel de l'Union européenne le 4 mai 2016 et entré en application le 25 mai 2018. L'adoption de ce texte permet à l'Europe de s'adapter aux nouvelles réalités du numérique.

Un cadre juridique unifié pour l'ensemble de l'UE

Le texte adopté est un règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres. Le même texte s'appliquera donc dans toute l'Union. Le règlement est applicable à partir du 25 mai 2018. Dès lors, les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du règlement.

Un champ d'application étendu

• **Le critère du ciblage**

Le règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anglais monitor).

En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet.

• **La responsabilité des sous-traitants**

Par ailleurs, alors que le droit de la protection des données actuel concerne essentiellement les « responsables de traitements », c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le projet de règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.

Un guichet unique : le « one stop shop »

Les entreprises seront en contact avec un « guichet unique », à savoir l'autorité de protection des données de l'État membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ». Cet établissement sera soit le lieu de leur siège central dans l'Union, soit l'établissement au sein duquel seront prises les décisions relatives aux finalités et aux modalités du traitement. Les entreprises bénéficieront ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettront en œuvre des traitements transnationaux.

Une coopération renforcée entre autorités pour les traitements transnationaux

Toutefois, dès lors qu'un traitement sera transnational – donc qu'il concernera les citoyens de plusieurs États membres –, les autorités de protection des données des différents États concernées seront juridiquement compétentes pour s'assurer de la conformité des traitements de données mis en œuvre.

Afin d'assurer une réponse unique pour l'ensemble du territoire de l'Union, l'autorité « chef de file » coopérera avec les autres autorités de protection des données concernées dans le cadre d'opérations conjointes. Les décisions seront adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanctions.

Les autorités de protection nationales sont réunies au sein d'un Comité européen de la protection des données (CEPD), qui veille à l'application uniforme du droit sur la protection des données. Il a vocation à remplacer l'actuel G29.

En pratique, l'autorité « chef de file » propose les mesures ou décisions (constatant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposent alors d'un délai de quatre semaines pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas suivie, la question est portée devant le CEPD qui rend alors un avis. Cet avis est contraignant et doit donc être suivi par l'autorité « chef de file ».

Que le CEPD soit ou non saisi, l'autorité « chef de file » portera la décision ainsi partagée par ses homologues. Il y aura donc une décision conjointe, susceptible de recours devant le juge des décisions de l'autorité « chef de file ».

• **Par exemple**, dans le cas d'une entreprise dont l'établissement principal est en France, la CNIL sera le guichet unique de cette entreprise et lui notifiera les décisions adoptées dans le cadre de ce mécanisme de cohérence. Ses décisions seront ensuite, si elles sont défavorables, susceptibles de recours devant le Conseil d'État. Ce mécanisme permet ainsi aux autorités de protection des données de se prononcer rapidement sur la conformité d'un traitement ou sur un manquement au règlement et garantit une sécurité juridique élevée aux entreprises en leur assurant une réponse unique sur l'ensemble du territoire de l'Union.

source : CNIL

Réagissez à cet article

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

Etapes à suivre si vous comptez rendre votre ordinateur professionnel à votre employeur

	Etapes à suivre si vous comptez rendre votre ordinateur professionnel à votre employeur

---

Quelles étapes faut-il suivre avant d'effacer nos données personnelles présentes sur notre futur ancien ordinateur de fonction (sauvegarder des fichiers importants et personnelles (contacts importants, copier des fichiers et tout ce qui nous concerne (photo, pdf, CV etc…) sur un disque dur ou un système de Cloud etc…) ?

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 hashage.
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 hashage 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 informations 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.

Denis JACOPINI anime des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux CyberRisques.
Il est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire et ai été pendant a une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.
http://www.leNetExpert.fr/contact
https://twitter.com/lenetexpert
https://www.linkedin.com/in/lenetexpert

Réagissez à cet article

Original de l'article mis en page : Supprimer vos données personnelles avant de donner ou recycler un ordi – FrancoisCharron.com

RGPD : Faire face aux exigences

	RGPD : Faire face aux exigences

À compter du 25 mai 2018, le nouveau règlement européen relatif à la protection des données personnelles connu sous l'acronyme RGPD s'appliquera à toutes les entreprises publiques ou privées.

Ces dernières devront entrer dans une démarche proactive de mise en conformité du nouveau règlement. L'enjeu est de taille, car tout manquement à ces nouvelles obligations pourrait être lourdement sanctionné par l'autorité de contrôle, la CNPD, qui sera habilitée dès l'entrée en vigueur du règlement à infliger des amendes allant jusqu'à 20 millions d'euros et 4 % du chiffre d'affaires mondial.
Le champ d'application du RGPD est particulièrement large : toutes les entités, européennes ou non, sont concernées à partir du moment où elles collectent et effectuent des traitements de données à caractère personnel d'un citoyen européen. Le RGPD vient renforcer les droits de la personne, et par conséquent augmenter les devoirs et les responsabilités de toute la chaîne d'acteurs, du responsable de traitement aux partenaires commerciaux, y compris les sous-traitants fournisseurs de services. Tous les flux de données sont concernés par cette nouvelle réglementation.
Ces nouvelles contraintes s'appuient notamment sur le principe d'accountability qui impose à chaque entreprise une obligation de rendre compte, notamment en se dotant d'une politique globale de protection des données conforme à la réglementation, et en étant à même de prouver à tout moment que des mesures concrètes et des procédures adéquates ont été mises en place. Dans ce nouveau contexte, il est préconisé que les responsables de traitement aient recours à des prestataires externes leur permettant d'assurer une mise en conformité effective…[lire la suite]

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD ?** ?
Besoin d'une **formation pour apprendre à vous**
mettre en conformité avec le RGPD ?
Contactez-nous

A Lire aussi :
Mise en conformité RGPD : Mode d'emploi
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
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
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
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)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

---

Réagissez à cet article

Source : *«Faire face aux exigences posées par le RGPD» | Paperjam News*

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

	Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

1. CHOISISSEZ AVEC SOIN VOS MOTS DE PASSE

Entrer un mot de passe permettant de s'authentifier pour accéder à son ordinateur, sa tablette ou son téléphone portable est un geste quotidien de sécurité.
Choisir un mot de passe difficile à déceler par une tierce personne ou par du piratage informatique est ainsi un rempart efficace pour protéger ses données personnelles contre les intrusions frauduleuses.

Comment bien choisir son mot de passe ?

Définissez des mots de passe composés d'au moins 12 caractères

• mélangeant majuscules, minuscules, chiffres et caractères spéciaux
• n'ayant aucun lien avec vous comme votre nom, date ou lieu de naissance
• ne formant pas de mots figurant dans le dictionnaire

Comment faire en pratique ?

Pour cela 2 méthodes simples :
• la méthode phonétique : « J'ai acheté 5 CD pour cent euros cet après-midi » : ght5CD%E7am
• la méthode des premières lettres : « Un tiens vaut mieux que deux tu l'auras » : 1tvmQ2tl'A

Quelques recommandations supplémentaires

• n'utilisez pas le même mot de passe pour tout, notamment pour accéder à votre banque en ligne et votre messagerie personnelle ou professionnelle
• méfiez-vous des logiciels qui vous proposent de stocker vos mots de passe

2. ENTRETENEZ RÉGULIÈREMENT VOS APPAREILS NUMÉRIQUES

En mettant à jour régulièrement les logiciels de vos appareils numériques

Dans chaque système d'exploitation (Android, MacOS, Linux, Windows,…), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs des mises à jour de sécurité.
Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations longtemps encore après leur découverte ou même leur correction. Il donc **nécessaire de procéder aux mises à jour régulières des logiciels.**

Comment faire ?

• configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible
• ou téléchargez les correctifs de sécurité disponibles en utilisant pour cela exclusivement les sites Internet officiels des éditeurs
• en effectuant couramment des sauvegardes

3. Effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple) permet de disposer de ses données après un dysfonctionnement ou une panne d'ordinateur

Comment faire ?

• utilisez des supports externes tels qu'un disque dur externe, un CD ou un DVD enregistrable pour enregistrer et sauvegarder vos données.

4. PRENEZ SOIN DE VOS INFORMATIONS PERSONNELLES ET DE VOTRE IDENTITÉ NUMÉRIQUE

Les données que vous laissez sur Internet vous échappent instantanément.
Des personnes malveillantes récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité ou de conduire des activités d'espionnage industriel.
Une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet.

Voici quelques recommandations générales :

• soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir : ne transmettez que les informations strictement nécessaires et pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos données, par exemple avec des partenaires commerciaux
• ne donnez accès qu'à un minimum d'informations personnelles sur les réseaux sociaux
• utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle…) et une adresse destinée aux autres services en ligne (forums, jeux concours…)

5. PROTÉGEZ VOS DONNÉES LORS DE VOS DÉPLACEMENTS

L'emploi d'ordinateurs portables, d'ordiphones (*smartphones*) ou de tablettes facilite le quotidien lors des déplacements professionnels. Pourtant, voyager avec ces appareils nomades peut mettre en péril des informations sensibles sur l'entreprise ou vous travaillez.

Précautions à prendre avant de partir en mission

• utilisez le matériel dédié à la mission prêté par votre entreprise (ordinateur, clefs USB, téléphone)
• sauvegardez aussi vos données sur un support amovible pour les retrouver en cas de perte
• si vous comptez profiter des trajets pour travailler, emportez un filtre de protection écran pour votre ordinateur
• apposez un signe distinctif (comme une pastille de couleur) sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport

Pendant la mission

• gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel)
• si vous êtes contraint de vous séparer de votre téléphone, retirez la carte SIM et la batterie
• en cas d'inspection ou de saisie de votre matériel par des autorités étrangères, informez votre organisation
• n'utilisez pas les équipements que l'on vous offre si vous ne pouvez pas les faire vérifier par un service de sécurité de confiance
• évitez de connecter vos équipements à des postes qui ne sont pas de confiance. Par exemple, si vous avez besoin d'échanger des documents lors d'une présentation

6. SÉCURISEZ VOTRE WI-FI

Si l'utilisation du Wi-Fi est une pratique attractive, elle permet, lorsque le point d'accès n'est pas sécurisé, à des personnes malintentionnées d'intercepter vos données et d'utiliser votre connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes.
C'est pour cette raison que l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre de l'entreprise.
Le Wi-Fi, solution pratique et peu coûteuse, peut cependant être le seul moyen possible d'accéder à Internet, il convient dans ce cas de sécuriser l'accès en configurant votre box. Pour ce faire, n'hésitez pas à contacter l'assistance technique de votre fournisseur d'accès.

Quelques recommandations générales :

• modifiez le nom d'utilisateur et le mot de passe par défaut (généralement « admin » et « 0000 ») de votre page de configuration accessible via votre navigateur Internet
• vérifiez que votre box dispose du protocole de chiffrement WPA2 et activez-le. Sinon, utilisez la version précédente WPA-AES (ne jamais utiliser le chiffrement WEP cassable en quelques minutes)
• modifiez la clé de connexion par défaut avec une clé (mot de passe) de plus de 20 caractères de types différents (cf. Choisissez des mots de passe robustes)
• ne divulguez votre clé de connexion qu'à des tiers de confiance et changez-la régulièrement
• activez et configurez les fonctions pare-feu / routeur.
• désactivez le Wi-Fi de votre borne d'accès lorsqu'il n'est pas utilisé

7. SÉPAREZ VOS USAGES PERSONNELS DES USAGES PROFESSIONNELS

Monsieur Paul, directeur commercial, rapporte souvent du travail chez lui le soir. Sans qu'il s'en aperçoive son ordinateur personnel a été attaqué. Grâce aux informations qu'il contenait, l'attaquant a pu pénétrer le réseau interne de l'entreprise de Monsieur Paul. Des informations sensibles ont été volées puis revendues à la concurrence.
Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone,…) personnels et professionnels.
Dans ce contexte, il est recommandé de séparer vos usages personnels de vos usages professionnels :
• ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles
• ne stockez pas de données professionnelles sur vos équipements communicants personnels
En savoir plus sur le AVEC ou BYOD :
Le AVEC (Apportez Votre Equipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, ordiphone, tablette) dans un contexte professionnel. Si cette solution est de plus en plus utilisée aujourd'hui, elle est cependant très problématique pour la sécurité des données personnelles et professionnelles (vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur).
De la même façon, il faut éviter de connecter des supports amovibles personnels (clés USB, disques durs externes) aux ordinateurs de l'entreprise.

8. SOYEZ AUSSI PRUDENT AVEC VOTRE ORDIPHONE (SMARTPHONE) OU VOTRE TABLETTE QU'AVEC VOTRE ORDINATEUR

Alexandre possède un ordiphone. Lors de l'installation d'une application, il n'a pas désactivé l'accès de l'application à ses données personnelles. Désormais, les éditeurs peuvent accéder à tous les SMS présents sur son téléphone.
Bien que proposant des services innovants, les ordiphones (smartphones) sont aujourd'hui très peu sécurisés. Il est donc indispensable d'appliquer certaines règles élémentaires d'hygiène informatique :
• n'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques…). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement : il faut éviter de les installer
• en plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et configurez votre téléphone pour qu'il se verrouille automatiquement
• effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les retrouver en cas de panne de votre ordinateur ou ordiphone

9. SOYEZ PRUDENT LORSQUE VOUS OUVREZ VOS MESSAGES ÉLECTRONIQUES

Suite à la réception d'un courriel semblant provenir d'un de ses amis, Madame Michel a cliqué sur un lien présent dans le message. Ce lien était piégé. Sans que Madame Michel le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants diffusant des images pédopornographiques.
Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées,…).

Lorsque vous recevez des courriels, prenez les précautions suivantes :
• l'identité d'un expéditeur n'est en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message
• n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts
• si un lien ou plusieurs figurent dans un courriel, vérifiez l'adresse du site en passant votre souris sur chaque lien avant de cliquer. L'adresse complète du site s'affichera alors dans la barre d'état en bas de la page ouverte. Si vous avez un doute sur l'adresse affichée, abstenez-vous de cliquer
• ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire)
• n'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc.

10. SOYEZ VIGILANT LORS D'UN PAIEMENT SUR INTERNET

Lorsque vous réalisez des achats en ligne, vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants, directement sur votre ordinateur.
Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :
• contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs)
• assurez-vous que la mention « https:// » apparait au début de l'adresse du site Internet
• vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple
Si possible, lors d'un achat en ligne, privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS.
De manière générale, ne transmettez jamais le code confidentiel de votre carte bancaire.

11. TÉLÉCHARGEZ LES PROGRAMMES, LOGICIELS SUR LES SITES OFFICIELS DES ÉDITEURS

Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui le plus souvent contiennent des virus ou des chevaux de Troie. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données personnelles, lancer des attaques, etc.

• C'est la raison pour laquelle il est vivement recommandé de télécharger vos programmes sur les sites officiels des éditeurs
• Enfin, désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir, afin de vérifier qu'ils ne sont pas infectés par un quelconque virus ou spyware.

Réagissez à cet article

Original de l’article mis en page : Conseils aux usagers | Gouvernement.fr

---

Comment sécuriser Firefox efficacement en quelques clics de souris ?

Comment sécuriser Firefox efficacement en quelques clics de souris ?

Vous utilisez Firefox est vous souhaitez que cet excellent navigateur soit encore plus sécurisé lors de vos surfs sur Internet ? Voici quelques astuces qui supprimerons la géolocalisation, le profilage de Google ou encore que vos données offline disparaissent du regard d'espions locaux.

C'est sur le blog des Télécoms que j'ai vu pointer l'information concernant le réglage de plusieurs paramètres de Firefox afin de rendre le navigateur de la fondation Mozilla encore plus sécurisé. L'idée de ce paramétrage, empêcher par exemple Google de vous suivre à la trace ou de bloquer la géolocalisation qui pourrait être particulièrement big brotherienne.

Commençons par du simple. Il suffit de taper dans la barre de navigation de votre Firefox la commande about:config. Une alerte s'affiche, pas d'inquiétude, mais lisez là quand même. recherchez ensuite la ligne security.tls.version. Les valeurs affichées doivent osciller entre 1 et 3. Ensuite, recherchez la ligne geo.enabled pour annuler la géolocalisation. Passez le « true » en « False ». Pour que les sites que vous visitiez ne connaisse pas la dernière page que vous avez pu visiter, cherchez la ligne network.http.sendRefererHeader et mettre la valeur 1. Elle est naturellement placée à 2. Passez à False la ligne browser.safebrowsing.malware.enabled.

Ici, il ne s'agit pas d'autoriser les malwares dans Firefox, mais d'empêcher Google de vous tracer en bloquant les requêtes vers les serveurs de Google. Pour que Google cesse de vous profiler, cherchez la ligne browser.safebrowsing.provider.google.lists et effacez la valeur proposée.

Pour finir, vos données peuvent être encore accessibles en « offlire », en mode hors connexion. Cherchez les lignes offline-apps.allow_by_default et offline-apps.quota.warn. La première valeur est à passer en Fasle, la seconde valeur en 0.

Il ne vous reste plus qu'à tester votre navigateur via le site de la CNIL ou celui de l'Electronic Frontier Foundation.

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : Sécuriser Firefox efficacement en quelques clics de souris – Data Security BreachData Security Breach