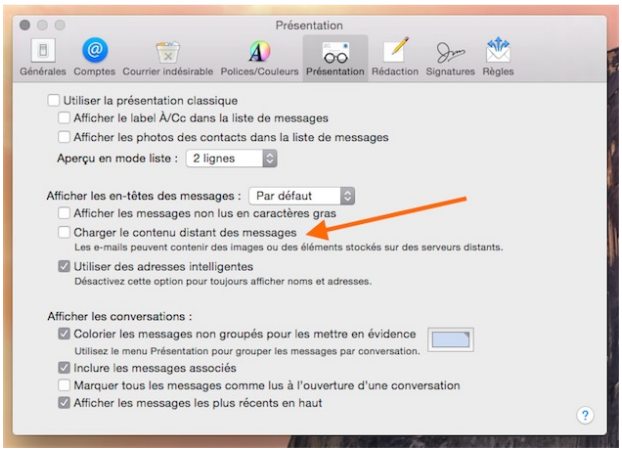
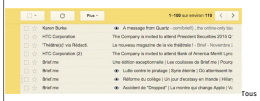
Comment se protéger des emails trop curieux | Denis JACOPINI



Comment se protéger des emails trop curieux

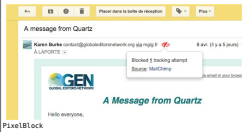
Sans même que vous visitiez un site web, les publicitaires peuvent récolter des informations vous concernant. L'une des techniques utilisées, très répandue et pas illégale, est le pixel tracking.

Une image transparente de 1 x 1 pixel liée à une URL est insérée dans un email. Quand l'email est ouvert, cette minuscule image est chargée et communique avec les serveurs du publicitaire qui a alors accès à des données personnelles, comme l'adresse IP, l'emplacement géographique (via l'IP), l'heure de la consultation et le terminal utilisé.
Les éditeurs ne font pas toujours preuve de tant de discrétion pour récolter des informations à partir des emails (une simple image, comme un logo d'entreprise, suffit), mais le résultat est le même ; des données sont récoltées sans le consentement de l'utilisateur.



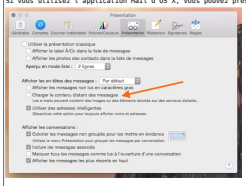
Tous les éditeurs n'utilisent pas le pixel tracking ou une autre technique de traçage à des fins publicitaires. Brief.me, un mini-journal disponible uniquement par email, l'exploite par exemple pour avoir des statistiques de consultation.

L'extension Chrome UglyEmail met en lumière les emails exploitant des techniques de traçage d'entreprises spécialisées (Streak, Yesware, Mandrill, MailChimp, Postmark, TinyLetter, Sidekick, MixMax et Bananatag). Quand UglyEmail repère dans la boîte de réception de Gmail un email trop curieux, il le signale avec une petite icône d'œil.
L'extension n'enregistre et ne transmet aucune donnée provenant de Gmail, assure son auteur à Wired. Des versions pour Firefox et Safari sont en développement.
PixelBlock, une autre extension Chrome réservée elle aussi à Gmail, va plus loin puisqu'elle bloque carrément le tracking. En cliquant sur l'œil rouge à côté du nom de l'expéditeur, on découvre la source du service de traçage.



PixelBlock

Si vous utilisez l'application Mail d'OS X, vous pouvez préserver votre confidentialité en désactivant le chargement des contenus distants des emails (l'option se trouve dans l'onglet Présentation des préférences). Cela fonctionne avec tous les fournisseurs de courrier électronique (Gmail, iCloud, Outlook, Yahoo…).



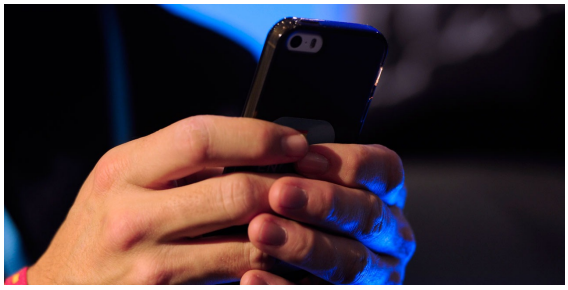
Puisque le lien avec le serveur distant est coupé, les informations personnelles ne sont pas divulguées. Cela a aussi pour effet de « casser » la mise en page des emails qui utilisent des images distantes, mais Mail permet très simplement de charger le contenu distant au cas par cas (un bouton est présent en haut du courrier quand le cas se présente).

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 protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.macg.co/logiciels/2015/04/confidentialite-comment-se-proteger-des-emails-trop-curieux-88326
Par Stéphane Moussie

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*

Télécharger tout votre historique Google est maintenant possible | Denis JACOPINI

	Télécharger tout votre h2istorique Google est maintenant possible

En attendant une fonction d'importation qui pourrait devenir standard pour tous les moteurs de recherche, Google propose aux internautes de télécharger une copie de tout leur historique de recherches effectuées depuis qu'ils utilisent un compte Google.

Google donnait depuis longtemps la possibilité aux internautes de consulter leur historique de recherches, à condition d'utiliser le moteur de recherche en étant identifié sur le service. Désormais, il est également possible de télécharger un archive qui contient l'ensemble des recherches effectuées depuis la création de votre compte. Il suffit de vous rendre sur la page de l'historique, et de cliquer sur l'icône des options tout en haut à droite :

Lors de la demande de téléchargement de l'historique, une pop-up s'ouvre qui prévient qu'un lien permettant de télécharger le fichier stocké sur l'espace personnel Google Drive de l'archive sera envoyé à l'adresse Gmail. Etant donnée la sensibilité des informations que peuvent contenir vos recherches (sans doute beaucoup plus nombreuses que vous ne l'imaginez), Google conseille tout de même de ne pas télécharger le fichier depuis un ordinateur public, et d'utiliser la validation en deux étapes de l'identification.
Alors que vous ne voyez sans doute pas l'intérêt de télécharger votre historique, l'intérêt est d'assurer la portabilité des données personnelles, au cas où vous souhaiteriez changer de moteur de recherche sans perdre toute la personnalisation des résultats et des suggestions créée à partir des milliers de requêtes effectuées précédemment. Il sera ainsi peut-être un jour possible d'importer son historique de recherches dans Yahoo, Bing, Qwant ou DuckDuckGo, et réciproquement, d'importer ses recherches vers Google. Ce n'est sans doute pas très utile vu d'Europe où Google écrase le marché des moteurs de recherche, mais ça peut avoir un intérêt aux Etats-Unis où Google représente autour de 65 % du marché.
Le fichier reçu est une archive .ZIP qui contient l'ensemble des recherches réunies dans un fichier par trimestre, au format JSON. Qui sait ce que les développeurs auront l'idée d'en faire ?

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

Source : http://www.numerama.com/magazine/32852-telecharger-tout-votre-historique-google-est-maintenant-possible.html

---

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…

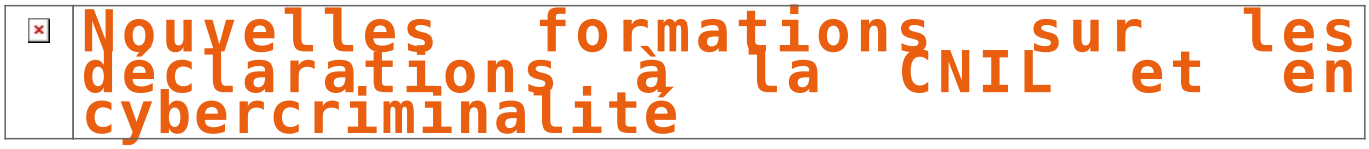
Article original de Denis JACOPINI et Atlantico

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

---

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



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

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 : Supprimer vos données personnelles avant de donner ou recycler un ordi – FrancoisCharron.com

---

Huit lois en dix ans pour encadrer le Web français | Denis JACOPINI

Huit lois en dix ans pour encadrer le Web français

Géolocalisation des véhicules de l’entreprise : la CNIL modifie la donne ! | Denis JACOPINI

Géolocalisation des véhicules de l’entreprise : la CNIL modifie la donne !

La CNIL avait adopté en 2006 une norme simplifiée permettant à tout employeur de recourir à un dispositif de géolocalisation tout en respectant les libertés individuelles des salariés. La CNIL vient à présent d'apporter des modifications significatives à cette norme, notamment en matière de contrôle du temps de travail.

Géolocalisation d'un salarié : les règles à suivre

La géolocalisation est un procédé qui équipe les véhicules d'entreprise d'un dispositif GPS permettant leur localisation géographique immédiate. Dans le BTP, il peut être utilisé, par exemple, pour contrôler et vérifier les déplacements du personnel de chantier.

Il est possible d'y recourir à condition de ne pas aboutir à un contrôle permanent du salarié.

La mise en œuvre du dispositif de géolocalisation doit être proportionnelle au but recherché et justifiée par l'activité de l'entreprise. Le CE doit être informé et consulté (ou à défaut les DP), préalablement à tout projet de mise en place d'un dispositif de géolocalisation au sein des véhicules de l'entreprise. Ensuite, vous devrez en informer l'ensemble du personnel (lettre remise en mains propres, note de service, etc.).

Pour cela, les Editions Tissot mettent à votre disposition un modèle d'attestation d'information de mise en place d'un système de géolocalisation extrait de la documentation « Formulaire Social BTP commenté ».

Il faut également déclarer le dispositif à la CNIL.

La CNIL a en effet adopté en 2006, une recommandation portant sur la géolocalisation des véhicules utilisés par les salariés. L'objectif étant d'encadrer la mise en œuvre d'un tel dispositif tout en respectant la loi relative à l'informatique et aux libertés mais également au Code du travail. De cette recommandation est née une norme simplifiée dite « Norme 51 ».

Ainsi, dès lors que vous souhaitez équiper vos véhicules d'un système de géolocalisation, vous devez au préalable effectuer une déclaration de conformité à la norme 51 auprès de la CNIL afin d'attester que vous respectez scrupuleusement ce que prescrit la CNIL.

Or cette norme 51 vient d'être modifiée par la CNIL.

Géolocalisation : les principales modifications apportées par la CNIL

La nouvelle norme du 4 juin 2015, consolidée le 29 juin 2015, vous défend de collecter des données de géolocalisation durant le trajet domicile/travail mais également pendant le temps de pause de vos salariés. En effet, la précédente norme précisait seulement que le salarié avait la possibilité de désactiver le dispositif en dehors de son temps de travail ou bien durant son temps de pause.

En revanche, cette nouvelle norme rend possible la désactivation par le salarié du dispositif et ce à tout moment de la journée. En effet, l'article 6 de ladite norme précise que : « les employés doivent avoir la possibilité de désactiver la fonction de géolocalisation des véhicules, en particulier à l'issue de leur temps de travail ou pendant leur temps de pause ».

Toutefois, ce droit dont bénéficie le salarié s'accompagne d'une contrepartie vous permettant de recueillir toutes explications de sa part en cas de désactivations trop fréquentes.

Par ailleurs, s'agissant du recueil des données traitées, il est possible de collecter la date ainsi que l'heure d'une activation ou d'une désactivation du dispositif par le salarié et ce durant le temps de travail. En conséquence, une procédure disciplinaire pourrait être engagée à l'encontre d'un salarié qui désactive fréquemment le dispositif de géolocalisation sans raison valable.

Enfin, la norme vous rappelle que le dispositif de géolocalisation n'a pas pour objectif de contrôler la vitesse de vos salariés. En effet, vous ne pourrez relever des infractions aux dispositions relatives au Code de la route puisque celles-ci ont trait à des données à caractère personnel que seuls les agents de services compétents peuvent sanctionner.

Source : http://www.batiactu.com/edito/geolocalisation-vehicules-entreprise-cnil-modifie-donne-42230.php

Quelques conseils pour vendre sur internet | Denis JACOPINI

	Quelques conseils pour vendre sur internet…

La vente en ligne est souvent perçue par les TPE comme un moyen simple et rapide de faire croître de manière importante leur chiffre d'affaires. Cependant, force est de constater que la réalité est plus contrastée. En effet, selon une étude CCM Benchmark, 36% des sites marchands ne gagnent pas d'argent. (http://stratup.net/l-e-commerce-la-fin-d-un-eldorado/)

La vente en ligne peut être un canal de vente complémentaire aux canaux de ventes traditionnels. Avant de créer son propre site de vente en ligne, une TPE devra donc se poser certaines questions :

• Est-ce que mon produit se prête à un achat sur internet ?
• Est-ce que j'ai du temps à consacrer à la création et surtout à l'animation / gestion de mon site ?
• Comment vais-je faire connaître mon site et attirer des visiteurs ?

Pour aider les dirigeants à mettre en place de tels projets, des spécialistes du monde des TPE existent. Ils peuvent faciliter la mise en œuvre d'une boutique en ligne notamment en déchargeant les dirigeants des aspects techniques (référencement naturel, lien avec plateformes de paiement) et des opérations de web marketing. Ce dernier aspect est particulièrement critique pour la réussite du projet et nécessite des efforts importants. En effet, il ne suffit pas de créer une boutique en ligne pour commencer à vendre. Il faut aller chercher le client et le convaincre que ce produit est celui qui lui faut.

Différentes opérations marketing peuvent être envisagées :

• Campagne d'e-mailings à destination de la base de clients connue de la TPE (ou plus large)
• Améliorer sa position sur les moteurs de recherche pour être placé dans les premières positions
• Diffusion de bannières redirigeant vers le site de la TPE sur un réseau de sites internet affiliés
• Référencement du catalogue de la TPE au sein de sites de comparateurs tels que Kelkoo ou Shopping

L'ensemble du plan marketing doit être soigneusement étudié entre la TPE et le partenaire en fonction de la cible client et des objectifs à atteindre. Aux exemples précédents peuvent ainsi s'ajouter d'autres moyens ONLINE (animation de communautés) ou OFFLINE (pubs papiers, relations presse), tout en veillant à ce qu'ils soient adaptés à la taille de la TPE.

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

Source : http://www.fiducial.fr/Espace-Conseils/Vendre-sur-internet2
Par Julien Nirom, responsable marketing – FIDUCIAL