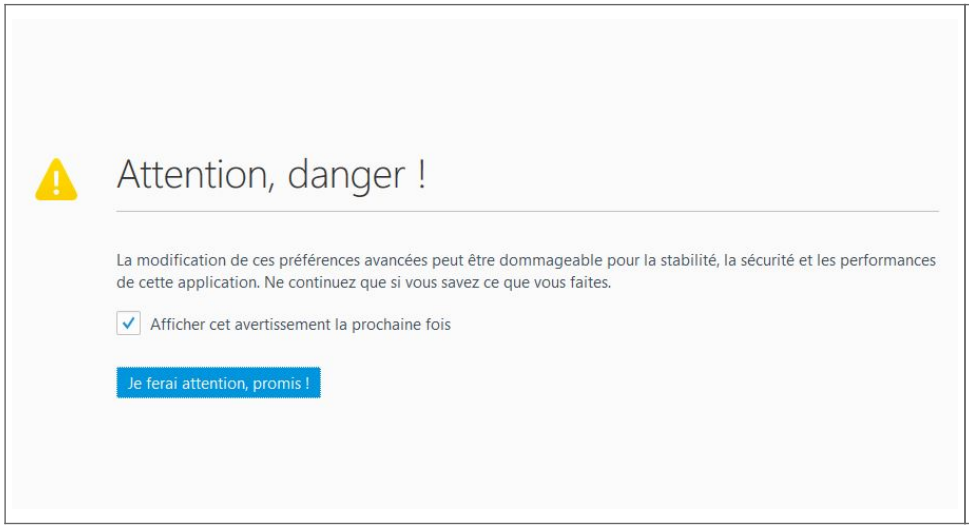
Comment sécuriser Firefox efficacement en quelques clics de souris ?



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

Imprimante 3D : Comment ça marche ? | Denis JACOPINI

	Imprimante 3D : Comment ça marche ?

L'impression 3D n'est pas une technologie qui fonctionne d'une seule et même manière. Il existe en effet des dizaines de procédés permettant d'imprimer des objets en 3D. Si les techniques sont différentes sur la forme, le principe est toujours le même… Il consiste à superposer des couches de matières avec une imprimante 3D selon les cordonnées transmises par un fichier 3D. Le guide suivant révèle le fonctionnement de cette machine étape par étape, ainsi que les logiciels et les matériaux qu'elle utilise.

Fonctionnement de l'imprimante 3D
L'impression 3D fonctionne donc selon plusieurs procédés, les techniques d'impression étant fonction du modèle d'imprimante utilisé. On peut classer ces procédés en trois grands groupes :
– le dépôt de matière
– la solidification par la lumière
– l'agglomération par collage
Le point commun entre ces trois techniques c'est qu'elles fonctionnent toutes selon le « couche par couche ». Seule la façon dont sont appliquées et traitées ses couches est différente ainsi que le matériau utilisé.

Pour la plupart des procédés employés l'utilisateur a besoin :
– d'une imprimante 3D
– de consommable (filament, poudre…)
– d'un fichier 3D (au format STL ou OBJ)
– d'un logiciel de slicing pour trancher le fichier et transmettre les indications à l'imprimante
– d'un ordinateur pour effectuer ces opérations
La manière d'exporter les fichiers vers l'imprimante diffère selon les marques et les modèles : câble USB, Wi-Fi ou carte SD.

1 – L'impression par dépôt de matière

Le FDM ou FFF
La majorité des imprimantes 3D personnelles fonctionnent selon ce principe. FDM est l'acronyme anglais de Fused Deposition Modeling qui signifie « modelage par dépôt de filament en fusion ». Ce procédé qui a été inventé en 1988 par la société Stratasys, est une marque déposée. On parle aussi de FFF (Fused Filament Fabrication) voir même de MPD (Molten Polymer Deposition) qui sont eux des termes libres de droits. Cette technique consiste en fait à déposer couche par couche un filament de matière thermoplastique fondu à 200°C (en moyenne) qui en se surperposant donne forme à l'objet. La tête d'impression se déplace selon les coordonnées X, Y et Z (longueur, largeur et hauteur) transmise par un fichier 3D correspondant au modèle 3D de l'objet à imprimer. Limitée pendant longtemps à des matériaux de type plastique tels que les classiques PLA et l'ABS, l'impression 3D voit arriver de nouveaux filaments composites à base de métal (cuivre, bronze…) et même de bois. Plus rarement certaines machines utilisent des cires ou des polycarbonates. A l'heure actuelle l'industrie agroalimentaire et la médecine sont en train de s'emparer de cette technique pour imprimer des aliments et des cellules en adaptant la tête d'extrusion.

– Ci-dessous une vidéo tutorielle qui vous aidera à mieux comprendre le fonctionnement d'une imprimante 3D FDM et les différentes étapes d'une impression.

TUTORIEL REPLICATOR 3 *par ENSCI*

2 – La solidification par lumière
La stéréolithographie ou SLA
La stéréolitographie est la première technique d'impression 3D à avoir été mise en évidence. Si la paternité de ce procédé est souvent attribuée à l'américain Charles Hull fondateur de 3D Systems, on doit en fait cette invention à trois français (Alain le Méhauté, Olivier de Witte et Jean Claude André) dont leurs brevets bien que déposés 3 semaines plus tôt (16 juillet 1984), n'ont malheureusement pas été renouvelés. Appelée aussi SLA (Stéréolithographie Apparatus) cette technique consiste à solidifier un liquide photosensible par le biais d'un rayon laser ultraviolet. Les imprimantes fonctionnant par SLA ont quatre parties principales: un réservoir qui peut être rempli avec un liquide photopolymère, une plate-forme perforée qui est descendue dans le réservoir, un rayonnement ultraviolet (UV) et d'un ordinateur commandant la plate-forme et le laser.

Tout comme la FDM, l'imprimante va dans un premier analyser le fichier CAO, puis en fonction de la forme de l'objet va lui ajouter des fixations temporaires pour maintenir certaines parties qui pourraient s'affaisser. Puis le laser va commencer par toucher et durcir instantanément la première couche de l'objet à imprimer. Une fois que la couche initiale de l'objet a durci, la plate-forme est abaissée, est ensuite exposée une nouvelle couche de surface de polymère liquide. Le laser trace à nouveau une section transversale de l'objet qui colle instantanément à la pièce durcie du dessous.

Ce processus se répète encore et encore jusqu'à ce que la totalité de l'objet ce soit formé et soit entièrement immergé dans le réservoir. La plateforme va ensuite se relever pour faire apparaitre l'objet fini en trois dimensions. Après qu'il ai été rincé avec un solvant liquide pour le débarrasser de l'excès de résine, l'objet est cuit dans un four à ultraviolet pour durcir la matière plastique supplémentaire.

Les objets fabriqués selon la stéréolithographie ont généralement une bonne qualité de finition et de détail (0,0005 mm) on obtient des surfaces bien lisses et régulières. Qualitativement elle fait partie des meilleurs techniques d'impression 3D actuellement. La durée nécessaire pour créer un objet avec cette technique dépend également de la taille de la machine utilisée. La SLA a aussi l'avantage de pouvoir produire de grosses pièces (de plusieurs mètres). Pour ces objets là il faudra plusieurs jours, quelques heures pour les plus petites.

Parmi ces inconvénients, un coût plus élevé que la FDM et un panel de matériaux et des coloris plus limité du fait des polymères utilisés comme matière première. Les solvants et les liquides polymères dégageant par ailleurs des vapeurs toxiques durant l'impression, votre local devra être équipé d'une hotte aspirante pour l'aération.

La Polyjet
principe de fabrication par polyjetCette Technologie brevetée par la société israélo-américaine Objet Geometries Ltd, fonctionne aussi sur le principe de photopolymérisation. De la même manière, l'objet sera modélisé en 3D avec un logiciel spécialisé (AutoCAD par exemple) puis son fichier envoyé à l'imprimante. Les têtes d'impressions vont alors déposer en goutte à goutte de la matière photosensible sur un support de gel, selon les coordonnées transmises par le fichier. Une fois la matière déposée, celle-ci va être exposée à un rayon ultraviolet qui va alors la durcir instantanément. L'opération sera répétée jusqu'à obtention de l'objet final, il ne restera alors plus qu'à le nettoyer. Avec une précision de l'ordre de 0,005mm il est possible de réaliser des objets avec un haut niveau de détail et des pièces d'assemblage pouvant s'imbriquer comme des engrenages.

Objet Geometries a par la suite affiné cette technique en mettant au point Polyjet Matrix. Avec 96 embouts pour chacune de ses têtes d'impression, il est possible pour l'utilisateur de combiner plusieurs matériaux différents, souples ou plus rigides. En vous permettant de créer votre propre composite, ce procédé vous offre la possibilité d'imprimer des d'objets plus variés et plus complexes.

Le frittage laser
Cette technique crée par un étudiant américain dans une université du Texas en 1980, a été développée plus tard (2003) par la société allemande EOS. Appelée aussi SLS (Selective Laser Sintering), il s'agit également d'un processus d'impression par laser. Cette fois ci un faisceau laser très puissant va fusionner une poudre (1mm d'épaisseur) à des points très précis définis par un fichier STL que communique votre ordinateur à votre imprimante. Les particules de poudre sous l'effet de la chaleur vont alors fondre et finir par se fusionner entres elles. Une nouvelle couche de poudre fine est ensuite étalée et à nouveau durcie par le laser puis reliée à la première. Cette opération est répétée plusieurs fois jusqu'à ce que votre pièce soit finie. Ensuite, votre partie est soulevée de la poudre libre et l'objet est brossé puis sablé ou poncé à la main pour les finitions.

La poudre que l'on utilise le plus souvent pour ce type d'impression est de la polyamide. De couleur blanche ce matériau est en fait un nylon. Il va donner à votre objet une surface poreuse qui pourra d'ailleurs être repeint si vous souhaitez lui donner de la couleur. D'autres composants comme de la poudre de verre, de la céramique ou du plastique sont aussi utilisés. Souvent les fabricants utilisent un mélange de deux sortes de poudres pour obtenir des objets plus aboutis.

Sur le même principe on retrouve aussi le DMLS qui est l'abrégé de Direct Metal Laser Sintering. Ce procédé permet de réaliser des objets en métal en fusionnant cette fois une poudre de fines particules métalliques. Presque tous les métaux peuvent être utilisés, cela va du cobalt au titane en passant par l'acier et des alliages comme l'Inconel.

Même si sa précision d'impression est inférieure au SLA, le frittage laser permet de fabriquer des pièces avec un niveau de détail assez élevé (0.1mm) et à géométrie complexe. De plus la poudre restante qui n'aura pas été passée au laser pourra être réutilisée la fois suivante. Généralement les pièces obtenues avec ce processus demande davantage de finitions (ponçage, peinture, vernis…) que le SLA du fait de son rendu un peu granuleux.

3 – L'agglomération de poudre par collage
Processus de la 3DP.
Initialement développé en 1993 au Massachusetts à l'Institut of Technology (MIT) en 1993, 3DP (Three-Dimensional Printing) constitue la base du processus d'impression 3D de Z Corporation. Le procédé consiste en l'étalement d'une fine couche de poudre de composite sur une plateforme. La tête d'impression va alors déposer sur celle-ci de fines gouttes de glue colorées qui combinées entre elles permetent d'obtenir un large panel de couleur. La plateforme s'abaisse au fur et à mesure que les couches de poudre sont collées jusqu'à obtenir l'objet final. Pour la finition il faut aspirer l'excédent de poudre, brosser et/ou poncer la pièce, puis la chauffer pour finaliser la solidification. La 3DP a l'avantage d'être rapide et de proposer une large gamme de couleurs. Jusqu'à 6 fois moins chère qu'une imprimante SLA son prix est plus attractif malgré une précision et une qualité d'impression parfois inférieure. Parmi les inconvénients, sans traitement post-impression les pièces sont plus fragiles et leur surface est plus rugueuse.

Les matériaux
Un article sur les consommables, les différentes famille de matériaux d'impression 3D, les caractéristiques et les utilisations des matières premières.
http://www.priximprimante3d.com/materiaux/

Les fichiers et les logiciels
Un guide consacré aux fichiers et logiciels 3D, deux éléments importants dans la conception d'un objet.
http://www.priximprimante3d.com/modeliser/

Se former à l'impression 3D
Si vous souhaitez vous initier à l'impression 3D lizez l'article qui suit où diverses formations consacrées à cette technologie sont abordées. Des stages pour mieux comprendre ce procédé aussi bien destinés aux professionnels qu'aux particuliers.
http://www.priximprimante3d.com/accompagnement/

Le frittage laser tombe dans le domaine public
L'un des principaux brevets liés au frittage laser ou SLS a expiré, ce qui devrait entraîner une chute des prix.
http://www.priximprimante3d.com/brevet/

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

Source : http://www.priximprimante3d.com/principe/

Modifiez le mot de passe envoyé par votre banque pour accéder à votre espace sécurisé : Comment protéger ses finances des hackers | Denis JACOPINI

Modifiez le mot de passe envoyé par votre banque pour accéder à votre espace sécurisé : Comment protéger ses finances des hackers – JDN

Quelques jours après la création de votre compte particulier sur le site Internet de votre banque, vous recevrez un mot de passe provisoire par voie postale. Changez-le immédiatement.

Des administrateurs informatiques, qui auraient accès aux combinaisons secrètes générées par l'établissement financier, pourraient tout à fait les collecter pour s'en servir à des fins malveillantes, prévient Mauro Israël, du cabinet Fidens, spécialisé dans le pilotage des cyber-risques.

C'est une règle d'hygiène : tout mot de passe fourni par un tiers doit être modifié. Le but est bien évidemment de réduire les intermédiaires pour être le seul détenteur de ses codes… [Lire la suite]

Réagissez à cet article

Source : *Modifiez le mot de passe envoyé par votre banque pour accéder à votre espace sécurisé : Comment protéger ses finances des hackers – JDN*

L'ANSSI donne 12 bons conseils pour la sécurité | Denis JACOPINI

	12 bons conseils pour la sécurité de votre entreprise

L'ANSSI renouvelle ses recommandations aux entreprises en matière de sécurité. Elle publie un nouveau document dans lequel elle livre douze conseils pour mieux sécuriser ses installations.

Depuis 2013, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) publie une liste de mesures non-contraignantes à l'attention des professionnels. Ce document donne des indications et conseils clairs pour sécuriser au mieux leurs installations informatiques.
Les recommandations servent également à faire comprendre à l'ensemble des collaborateurs l'importance d'adopter certains comportements. L'objectif de la mesure est que chacun comprenne les risques en termes de sécurité au sein de l'entreprise, mais également en situation de mobilité.
Les recommandations, au nombre de douze, regroupent des instructions classiques dans le domaine de la sécurité. L'ANSSI conseille ainsi de :

1. Choisir avec soin son mot de passe.
2. Mettre à jour régulièrement vos logiciels.
3. Bien connaître ses utilisateurs et ses prestataires.
4. Effectuer des sauvegardes régulières.
5. Sécuriser l'accès Wi-Fi de votre entreprise.
6. Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur.
7. Protéger ses données lors de ses déplacements.
8. Être prudent lors de l'utilisation de sa messagerie.
9. Télécharger ses programmes sur les sites officiels des éditeurs.
10. Être vigilant lors d'un paiement sur Internet.
11. Séparer les usages personnels des usages professionnels.
12. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique.

Au-delà de ces conseils, l'ANSSI recommande de nommer un référent pour la sécurité informatique au sein de la société. Pour ce faire, il est possible de rédiger une charte dans laquelle des références au chiffrement de certaines informations sensibles figureront tout comme des recommandations quant à l'installation d'un antivirus ou d'un pare-feu.

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

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-760239-bonnes-pratiques-securite-anssi.html
http://www.ssi.gouv.fr/uploads/2015/03/guide_cgpme_bonnes_pratiques.pdf
Par Olivier Robillart

Arnaques par courriel (scam, phishing) : la CNIL peut-elle agir ? | Denis JACOPINI

Arnaques par courriel (scam, phishing) : la CNIL peut-elle agir ?

Non, la CNIL n’est pas compétente dans ce domaine.

Ces procédés ne sont pas liés à la protection des données personnelles : ce sont des tentatives d’escroquerie ou d’extorsion de fonds.
Si vous en êtes victime, signalez-les sur le service PHAROS du ministère de l’Intérieur et au service phishing-initiative mis en place par plusieurs acteurs de l’internet.
Vous pouvez également joindre par téléphone le service Info Escroquerie de la police nationale au 0811 02 02 17 (coût d’un appel local).

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d’abord commencer par un Audit de l’ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l’hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d’informations complémentaires ?

Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=5318D41E172CDCBFD4A28353ED692C06?id=194&back=true

---

RGPD : Impact sur l’Email Marketing

RGPD : Impact sur l’Email Marketing

En mai 2018 entrera en vigueur le fameux RGPD : le Règlement Européen sur la Protection des Données. Il vise avant tout à renforcer la protection des données personnelles des internautes. De nombreux articles en ont déjà parlé et beaucoup imaginent que cette réglementation touchera de plein fouets les acteurs de l'email marketing français et leurs utilisateurs.

Sarbacane Software propose une infographie* résumant les réels changements qui seront apportés par le RGPD, et son implication pratique dans le domaine de l'emailing.

[lire la suite]

LE NET EXPERT

• ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)

- **ANALYSE DE VOTRE ACTIVITÉ**
- **CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES**
- **IDENTIFICATION DES RISQUES**
- **ANALYSE DE RISQUE (PIA / DPIA)**
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

• FORMATIONS / SENSIBILISATION :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• RECHERCHE DE PREUVES (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• EXPERTISES & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Sarbacane : Tout comprendre sur le RGPD, le règlement européen qui va impacter toutes les entreprises en 2018 – Global Security Mag Online*

et Sarbacane.com

Vote électronique – Mode d'emploi | Denis JACOPINI

Le vote électronique, souvent via internet, connaît un développement important depuis plusieurs années, notamment pour les élections professionnelles au sein des entreprises. La mise en place des traitements de données personnelles nécessaires au vote doit veiller à garantir la protection de la vie privée des électeurs, notamment quand il s'agit d'élections syndicales ou politiques.

Les mesures de sécurité sont donc essentielles pour un succès des opérations de vote mais mettent en œuvre des mesures compliquées, comme par exemple l'utilisation de procédés cryptographiques pour le scellement et le chiffrement. Pour éclairer les responsables de traitement, les fournisseurs de solution de vote et les experts sur les sécurités que la CNIL estime indispensables, une recommandation a été adoptée en 2003 et mise à jour en 2010.
Pour être valide, un système de vote électronique doit strictement respecter les obligations légales applicables aux systèmes de vote électronique, énoncées notamment dans le décret n° 2007-602 et l'arrêté correspondant du 25 avril 2007 relatifs aux conditions et aux modalités de vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise, et dans le décret n° 2011-595 du 26 mai 2011 relatif aux conditions et modalités de mise en œuvre du vote électronique par internet pour l'élection des représentants du personnel au sein des instances de représentation du personnel de la fonction publique de l'Etat.

Le système de vote électronique doit également respecter la délibération n°2010-371 du 21 octobre 2010 de la CNIL portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique qui précise notamment :
• Tout système de vote électronique doit faire l'objet d'une expertise indépendante.
• L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).
• Le rapport d'expertise doit être remis au responsable de traitement. Les prestataires de solutions de vote électronique doivent, par ailleurs, transmettre à la CNIL les rapports d'expertise correspondants à la première version et aux évolutions substantielles de la solution de vote mise en place.

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

A Lire aussi :
Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :
• Expert en Informatique **assermenté et indépendant** ;
• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.
Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.
Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.
Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Source : http://www.cnil.fr/les-themes/vie-citoyenne/vote-electronique/
http://www.cnil.fr/documentation/deliberations/deliberation/delib/249/

L'adresse IP est-elle une

donnée à caractère personnel ? | Denis JACOPINI

L’adresse IP est-elle une donnée à caractère personnel ?

La nature juridique de l'adresse IP ne cesse de susciter les interrogations. Si la réponse à cette question semble a priori tranchée par la loi 6 janvier 1978 modifiée en 2004 en prévoyant une définition large de la donnée personnelle permettant d'inclure aisément des données numériques à partir du moment où elles permettent d'identifier même indirectement la personne physique, ainsi que par la CNIL qui s'est prononcée en faveur à cette assimilation, la jurisprudence quant à elle, ne cesse de changer de position, tantôt elle prône pour cette qualification, tantôt elle la rejette catégoriquement.

I/ L'adresse IP au regard de la loi du 6 janvier 1978.

L'article 2 alinéa 2 de la loi du 6 janvier 1978, dite loi informatique et libertés telle que modifiée par la loi du 6 aout 2004, définit la donnée personnelle comme étant « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »

Par cette vague définition, le législateur, conscient de l'évolution rapide et constante des nouvelles technologies, a sciemment élargi la définition de la donnée personnelle afin d'y inclure toute nouvelle donnée qui est susceptible d'identifier directement ou indirectement une personne physique, dans le but de la protéger.

Ainsi, dans cet éventail d'informations, peuvent se glisser aussi bien des informations personnelles « classiques » telles que le nom, prénom, adresse postale, photo, numéro de téléphone, empreintes digitales etc, que des informations du monde numérique. Tel est le cas de l'adresse IP (Internet Protocol) d'un ordinateur.

Toutefois, le fait de ne pas dresser une nomenclature des informations qui constituent les données à caractère personnel, présente la souplesse d'inclure de nouvelles données, mais l'absence d'une telle précision laisse planer le doute en cas de conflit, d'où le nombre d'affaires porté devant les tribunaux et dont la qualification est laissée à l'appréciation des juges.

Interrogée sur cette question, la CNIL (Commission Nationale Informatique et Libertés), à travers ses interventions (recommandation ou déclaration), a répondu favorablement à la reconnaissance de l'adresse IP comme une donnée à caractère personnel en se basant sur la définition large de l'article 2 de la loi du 6 janvier 1978 précité.

II/ L'adresse IP selon les recommandations de la CNIL.

Dans un article du 2 aout 2007, la CNIL [1] [2] comme le G29 [3] ont soutenu que l'adresse IP, à l'instar d'une plaque d'immatriculation d'un véhicule ou d'un numéro de téléphone, entre dans le champ d'application large de la définition de l'article 2 de la loi du 6 janvier 1978 modifiée étant donné qu'elle permet l'identification directe ou indirecte de la personne physique [4]. La CNIL a rappelé à ce titre, que l'ensemble des autorités de protection des données des Etats membres ont précisé dans un avis du 20 juin 2007 relatif au concept de données à caractère personnel que l'adresse IP lié à l'ordinateur d'un internaute constitue une donnée à caractère personnel. S'inquiétant ainsi des décisions judiciaires qui refusent de considérer cette donnée comme personnelle. L'évolution récente de la jurisprudence va dans ce sens.

III/ l'adresse IP et l'évolution jurisprudentielle.

La position de la CNIL n'est pas toujours partagée par la jurisprudence française. Si dans certains arrêts elle a à juste titre prôné pour cette assimilation en affirmant que « L'adresse IP, est, au sens strict, un identifiant d'une machine lorsque celle-ci se connecte sur l'Internet et non d'une personne. Mais au même titre qu'un numéro de téléphone n'est, au sens strict, que celui d'une ligne déterminée mais pour laquelle un abonnement a été souscrit par une personne déterminée ; un numéro IP associé à un fournisseur d'accès correspond nécessairement à la connexion d'un ordinateur pour lequel une personne déterminée a souscrit un abonnement auprès de ce fournisseur d'accès. L'adresse W de la connexion associée au fournisseur d'accès constitue un ensemble de moyens permettant de connaitre le nom de l'utilisateur » [5]. Dans cet arrêt, les juges du fond se sont basés sur la définition légale de la donnée personnelle de l'article 2 de la loi du 6 janvier 1978 précité comme étant une information qui peut identifier indirectement une personne physique par référence à un numéro d'identification.

Dans d'autres arrêts, les juges du fond français [6]ont refusé toute assimilation de l'adresse IP à une donnée personnelle [7] en ce qu'elle ne permet pas d'identifier l'auteur de la connexion [8]. Dans ce contexte, par un arrêt du 5 septembre 2007, la chambre criminelle de la Cour de cassation a considéré que l'adresse IP est une donnée parmi d'autres d'un faisceau d'indices, et donc, insuffisante à elle seule pour être qualifiée de donnée personnelle [9]

La problématique de l'adresse IP ne semble pas être résolue étant donné que cette question a été soulevée récemment devant la Cour d'appel de Rennes du 28 avril 2015, qui s'est prononcée en défaveur de cette qualification en considérant que « (….) le simple relevé d'une adresse IP aux fins de localiser un fournisseur d'accès ne constitue pas un traitement automatisé de données à caractère personnel au sens des articles 2, 9 et 25 de la loi « informatique et libertés » du 6 janvier 1978. L'adresse IP est constituée d'une série de chiffres, n'est pas une donnée, même indirectement nominative alors qu'elle ne se rapporte qu'à un ordinateur et non à l'utilisateur (….) ».

Analyse.

La problématique de cette question se résume ainsi : si l'adresse IP est considérée comme donnée personnelle cela implique qu'il s'agit d'un traitement de donnée personnelle régi par la loi du 6 janvier 1978, et de ce fait, bénéficie de l'arsenal de dispositions protectrices prévu pour protéger la personne physique d'une part, et risque de tomber sous le coup des sanctions prévues en cas de non respect des dispositions légales prévues à cet effet d'autre part.

Cela implique le recours à la CNIL en amont de tout traitement pour autorisation, et en cas de conflit, c'est le tribunal de grande instance qui sera matériellement compétent.

Encore faut il que cela concerne une personne physique dans la mesure où la loi du 6 janvier 1978 ne protège que cette catégorie de personnes.

Le seul moyen de mettre fin à cette incertitude c'est l'adoption d'une disposition légale claire et précise sur la notion de donnée personnelle. Cela pourra bientôt se concrétiser après l'adoption de la proposition de Règlement européen relatif à la protection des données à caractère personnel et sa transposition ultérieure dans le droit positif français.

Auteure : Zahra Reqba

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

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"]

Victime d’une arnaque sur Internet ? Faites-nous part de votre témoignage

	Victime d’une arnaque sur Internet ? Faites-nous part de votre témoignage

Vous êtes victime d'une arnaque ou d'un piratage sur Internet ? Votre témoignage nous permettra peut-être de vous aider.

Devant une explosion de cas d'arnaques et de piratages par Internet et des pouvoirs publics débordés par ce phénomène, nous avons souhaité apporter notre pierre à l'édifice.
Vous souhaitez nous faire part de votre témoignage, contactez-nous.

Vous devez nous communiquer les informations suivantes (tout message incomplet et correctement rédigé ne sera pas traité) :

• une présentation de vous (qui vous êtes, ce que vous faites dans la vie et quel type d'utilisateur informatique vous êtes) ;
• un déroulé chronologique et précis des faits (qui vous a contacté, comment et quand et les différents échanges qui se sont succédé, sans oublier l'ensemble des détails même s'ils vous semblent inutiles, date heure, prénom nom du ou des interlocuteurs, numéro, adresse e-mail, éventuellement numéros de téléphone ;
• Ce que vous attendez comme aide (je souhaite que vous m'aidiez en faisant la chose suivante : ….)
• Vos nom, prénom et coordonnées (ces informations resteront strictement confidentielles).

Contactez moi
Conservez précieusement toutes traces d'échanges avec l'auteur des actes malveillants. Ils me seront peut-être utiles.

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

Comment les salariés peuvent lutter contre la cybercriminalité | Denis JACOPINI

	Comment les salariés peuvent lutter contre la cybercriminalité

Les entreprises -quels que soient leur taille économique et leur secteur d'activité- subissent des cyberattaques ciblées qui visent leurs actifs stratégiques. Ce qui entraîne des pertes de plusieurs millions de dollars. Au-delà des offres technologiques de sécurité et des discours méthodologiques qui fleurissent sur le marché, une véritable politique organisationnelle formée et informée face aux dangers doit être développée dans l'entreprise. Quel rôle pour les RH?

Le cybercrime est un phénomène complexe intégrant en son sein un spectre très large de méthodes, de cibles et de motivations. On assiste de moins en moins aux actions de l'hacker isolé uniquement motivé par la mise en lumière de ses exploits ou à celles de l'hacktiviste politique développant des attaques à des fins de sabotage. Le cybercrime est aujourd'hui de plus en plus organisé. Appâté par des gains financiers directs, il met en œuvre ses exactions via des mécaniques sophistiquées comme le spear fishing, l'ingénierie sociale ou encore les menaces furtives APT (Advanced Persistent Threats) au travers d'attaques ciblées, de grande envergure et de plus en plus dévastatrices. Et comme l'a dévoilé la retentissante affaire Edward Snowden aux Etats-Unis, les cyber armées misent en branle par les gouvernements à des fins de renseignement ou d'espionnage industriel sont également très actives.

Un contexte technologique propice aux failles mais pas uniquement …

Si les attaques cybercriminelles réussissent aujourd'hui, c'est que les évolutions technologiques majeures comme le Cloud, le BYOD (Bring Your Own Devive) ou encore les objets connectés… – en augmentant de manière exponentielle les données disponibles au niveau mondial – ont ouvert et donc fragilisé le réseau de l'entreprise. Ce contexte de démultiplication des périphériques, des utilisateurs et des usages génère des failles et des vulnérabilités, largement exploitées par les cyber assaillants. Mais même si leur impact est bel et bien réel, les transformations technologiques ne sont pas les seules au banc des accusés. En 2015, selon un rapport de sécurité Check Point, 81% des entreprises ont subi des fuites de données causées par des négligences humaines. L'humain, ce « maillon faible » est un élément clé de toute stratégie cyber défense même s'il n'est toujours pas appréhendé sérieusement par les entreprises. Et c'est là que les RH ont leur carte à jouer.

Le rôle déterminant des RH: transformer l'humain en un atout pour la sécurité de l'entreprise

Redoublant d'ingéniosité pour arriver à leurs fins, les cyber assaillants mettent en œuvre des attaques d'ingénierie sociale et d'hameçonnage qui exploitent les faiblesses humaines (vanité, reconnaissance, ignorance, gentillesse…) avec pour finalité le vol de données sensibles, le gain direct ou encore l'espionnage industriel. Ces attaques sont très difficiles à détecter par les entreprises car elles ne sont pas identifiées par leurs barrages technologiques et peuvent même passer inaperçues aux yeux de leurs victimes! Pour déjouer les manœuvres des cybercriminels, une culture « sécurité » portée par les RH doit être mise en œuvre pour sensibiliser et responsabiliser les employés de l'entreprise, à chaque couche fonctionnelle et dans le cadre d'une véritable démarche collaborative. Comment?

1/ En assumant la responsabilité des risques de sécurité posés par les collaborateurs de l'entreprise. La grande majorité des employés ne se sent pas vraiment concernée par les problématiques de sécurité de leur entreprise. Elle les considère comme seule responsabilité du département informatique et cette attitude rend les entreprises bien trop vulnérables. Une politique de sécurité interne ne sera efficace que si elle est comprise et intégrée par les collaborateurs via un véritable état d'esprit associé à une somme de comportements quotidiens. Les RH doivent mener des politiques de sensibilisation actives, sur la durée, portant sur les dangers, les techniques employées par les cyber délinquants et l'impact comportemental des employés sur la sécurité de l'entreprise.

2/ En identifiant le personnel vulnérable. Un des risques majeurs en matière de sécurité est l'accès des employés aux données sensibles de l'entreprise. Dans le cas du piratage de Sony Pictures, les experts ont évoqué l'implication d'un ou de plusieurs ex-employés du Groupe dont l'accès toujours actif au réseau a permis le vol d'informations critiques. En outre, les cybercriminels ont besoin du support de collaborateurs ou de partenaires de l'entreprise qui vont les aider volontairement ou non à arriver à leur fins. Ils utilisent ainsi les réseaux sociaux pour identifier leur cible/victime potentielle, celle qui aura une prédisposition à briser les systèmes de sécurité de l'entreprise, sera démotivée ou en désaccord avec sa hiérarchie. Au cœur de ces informations, les RH doivent ainsi redoubler de vigilance vis-à-vis de ressources à risques ou plus exposées comme les nouveaux arrivants, les employés sur le départ, des fonctions spécifiques (accueil/helpdesk, secrétariats, …) ou stratégiques tels que les directeurs financiers …

3/ En sensibilisant la Direction Générale. La mise en place d'une culture de la sécurité au sein de l'entreprise doit bénéficier du support du top management. Or les Directions Générales ne sont pas encore forcément sensibles à la mise en place de ces programmes de formations, orientant leurs investissements sécuritaires plutôt vers des dispositifs technologiques. Messieurs les Directeurs, comme l'a si justement souligné Derek Bok, Président de la prestigieuse université d'Harvard « Si vous pensez que l'éducation est chère, alors tentez l'ignorance » ! Il est aujourd'hui impératif pour les entreprises de mettre en place une vraie stratégie de sécurité basée sur une mobilisation interne transverse associant les métiers, le comité de direction, les RH et le RSSI.

Le cybercrime est bien réel, organisé, déterminé et atteint son but même pour les plus grandes organisations internationales aux murailles technologiques dites « infranchissables ». C'est aux entreprises maintenant de penser et de développer une organisation de sécurité en miroir, dotée d'un niveau de maturité technique et organisationnel tout aussi élevé que celui de leurs cybers assaillants. La sensibilisation de l'humain, clé de voûte d'une bonne stratégie de cyberdéfense ne doit pas être négligée et les RH devront vite s'emparer du sujet avant que l'ennemi ne soit dans la place !

Source : http://www.challenges.fr/tribunes/20150624.CHA7247/comment-les-salaries-peuvent-lutter-contre-la-cybercriminalite.html
par Emmanuel Stanislas, fondateur du cabinet de recrutement Clémentine.