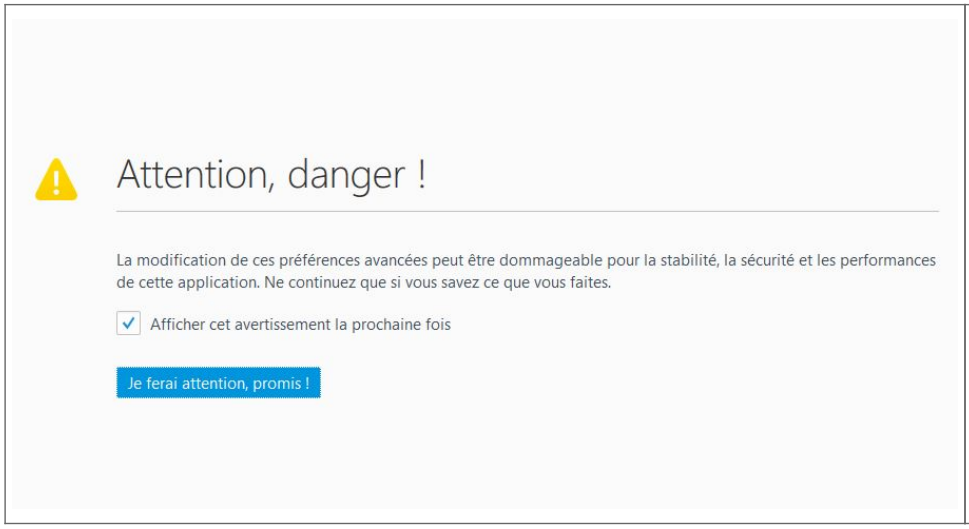
Comment sécuriser Firefox efficacement en quelques clics de souris ?



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/

Qu’est ce qu’un cybercriminel ?

	Qu’est ce qu’un cybercriminel ?

Cette question a été posée à Denis JACOPINI par des étudiants. Ci-dessous une réponse succinte.

Avant de répondre à cette question, il est important de poser la définition de la cybercriminalité.
La définition qui selon moi définit le mieux la cybercriminalité est celle qui considère la cybercriminalité comme une **notion large qui regroupe toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau**. (Wikipedia)
Que ça soit dans le cas d'atteintes aux biens ou d'atteintes aux personnes, il est couramment décomposé 3 types d'infractions :

• **Les infractions spécifiques aux technologies de l'information et de la communication** : parmi ces infractions, on recense les atteintes aux systèmes de traitement automatisé de données, les traitements automatisés de données personnelles (comme la cession des informations personnelles), les infractions aux cartes banquaires , les chiffrements non autorisés ou non déclarés ou encore les interceptions.
• **Les infractions liées aux technologies de l'informations et de la communication** : cette catégorie regroupe la pédopornegraphie, l'incitation au terrorisme et à la haine raciale sur internet, les atteintes aux personnes, les atteintes aux biens.
• **Les infractions facilitées par les technologies de l'information et de la communication**, que sont les escroqueries en ligne, la contrefaçon ou tout autre violation de propriété intellectuelle.

Ainsi, un cybercriminel est une personne qui commet au moins une de ces 3 infractions.

Les principales motivations sont :
• Gagner de l'argent (ou ne pas en dépenser ce qui revient au même) en réalisant par exemple des actes de piratages d'oeuvres intellectuelles telles que des musiques ou des films. D'autres peuvent aussi prendre le risque de chercher à en tirer des bénéfices soit en les revendant ces oeuvres, en les mettant à disposition sur des sites internet mitraillant de publicités rémunérées leurs visiteurs ou permettant le téléchargement contre un appel vers un numéro surtaxe. D'autres vont réaliser des vols d'informations (Magasins TARGET en 2013), des blocages de systèmes informatiques (TV5 Monde en 2015) ou des cryptages de fichiers en demandant à l'issue de l'opération une rançon en échange de tranquillité (Laboratoires Labio en 2015, Disney en 2017) ou de rétablir le système dans son état initial, une technique semblable à celles utilisées par la mafia (Pirates informatiques : des techniques très proches de la mafia – Gilles Fontaine) ;
• Terroriser la population en répandant des messages idéologiques (+ de 25000 sites Internet piratés diffusant un message pro islamiste à la suite des attentats de Charlie Hebdo) ou bien en coupant les ressources en électricité d'une population (Ukraine en 2015 et 2016) ;
• S'attaquer à un état dans un but politique (Attaque informatique de la centrale nucléaire de Bouchehr en Iran destinée à détruire des centrifugeuses d'enrichissement d'uranium en 2010) ou militaire (Attaque de la Georgie par la Russie en 2007) ou d'espionnage (Bercy en 2011) ;
• Dans un but de montrer ses capacités ou se lancer un défi (comme David Dennis en 1974). Débrouille-vous pour faire venir aux oreilles de hackers qu'un système informatique est inattaquable, vous verrez alors fleurir des volontaires masqués qui passeront leurs journées et leurs nuits à tenter de trouver la faille dans le but de prouver leur supériorité ;

Ainsi, selon moi, un cybercriminel est un individu qui commet avec ou sans intention une ou plusieurs infractions répréhensibles concernées par le champ couvert par la cybercriminalité, sans autorisation expresse du tiers concerné, quel que soit l'intention et l'objectif poursuivis.

Source : *Cybercrime — Wikipédia*

Comment est née la cybercriminalité ?

Comment est née la cybercriminalité ?

Cette question a été posée à Denis JACOPINI par des étudiants. Ci-dessous une réponse succinte.

Avant de répondre à cette question, il est important de poser la définition de la cybercriminalité.
La définition qui selon moi définit le mieux la cybercriminalité est celle qui considère la cybercriminalité comme une **notion large qui regroupe toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau**. (Wikipedia)
Que ça soit dans le cas d'atteintes aux biens ou d'atteintes aux personnes, il est couramment décomposé 3 types d'infractions :

• **Les infractions spécifiques aux technologies de l'information et de la communication** : parmi ces infractions, on recense les atteintes aux systèmes de traitement automatisé de données, les traitements automatisés de données personnelles (comme la cession des informations personnelles), les infractions aux cartes banquaires , les chiffrements non autorisés ou non déclarés ou encore les interceptions.
• **Les infractions liées aux technologies de l'informations et de la communication** : cette catégorie regroupe la pédopornegraphie, l'incitation au terrorisme et à la haine raciale sur internet, les atteintes aux personnes, les atteintes aux biens.
• **Les infractions facilitées par les technologies de l'information et de la communication**, que sont les escroqueries en ligne, la contrefaçon ou tout autre violation de propriété intellectuelle.

En France la cybercriminalité est prise juridiquement en compte depuis la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, mais j'aurai tendance à penser que la cybercriminalité est née bien avant, bien avant l'informatique puisque dans la définition retenue, la notion d'informatique n'y est pas, il est fait mention de la notion de réseau (informatique mais aussi téléphonique…).

Ainsi, le premier cas d'infraction pénale que nous avons retrouvé est le détournement d'usage réalisé par John Draper, connu également sous le nom Captain Crunch, en 1969. Il parvint, à l'aide d'un sifflet qui possède la même tonalité que le réseau téléphonique américain, à passer des appels longues distance gratuitement lorsqu'il sifflait dans le combiné. Captain Crunch a été condamné pour ces actes à deux mois de prison en 1976. Les actes cybercriminels ont ensuite dans les années 80 évolué dans le monde informatique.
On pourrait ainsi conclure que même si la cybercriminalité doit son expansion à l'usage de plus en plus répandu de l'informatique, la cybercriminalité est née dans les années 60 au travers de piratages de lignes téléphoniques à partir d'un simple objectif propre aux êtres vivants : détourner l'environnement à son propre avantage.

Réagissez à cet article

Source : *Cybercrime — Wikipédia*

Comment se préparer aux incidents de sécurité ?

Comment se préparer aux incidents de sécurité ?

Les entreprises doivent être prêtes à agir face à des incidents de sécurité et à des attaques. Et cela passe notamment par sept points précis (par Peter Sullivan).

Un plan de préparation à la cybersécurité présente et détaille les objectifs fondamentaux que l'organisation doit atteindre pour se considérer comme prête à faire face à des incidents de sécurité informatique. La liste de contrôles qui va suivre n'est pas exhaustive, mais elle souligne des objectifs qui constituent un minimum requis pour donner un niveau raisonnable de sensibilisation à la cybersécurité et se concentrer sur la protection des actifs informationnels essentiels.
Ici, la préparation à la cybersécurité est définie comme l'état permettant de détecter et de réagir efficacement aux brèches et aux intrusions informatiques, aux attaques de logiciels malveillants, aux attaques par hameçonnage, au vol de données et aux atteintes à la propriété intellectuelle – tant à l'extérieur qu'à l'intérieur du réseau.
Un élément essentiel de cette définition est de « pouvoir détecter ». La détection est un domaine où une amélioration significative peut être atteinte en abaissant le délai de détection, couramment observé entre 9 et 18 mois. Une capacité de détection plus rapide permet de limiter les dommages causés par une intrusion et de réduire le coût de récupération de cette intrusion. Être capable de comprendre les activités régulières du réseau et de détecter ce qui diverge de la norme est un élément important de la préparation à la cybersécurité. Voici une sept objectifs que les entreprises devraient considérer.

Les objectifs à atteindre

1. Plan de cybersécurité
2. Gestion du risque
3. Gestion de l'identité
• **Contrôle d'accès**
• **Authentification**
• **Autorisation**
• **Responsabilité**
4. Surveillance de réseau
5. Architecture de sécurité
6. Contrôle des actifs, des configurations et des changements
7. Cartographie de la gestion des incidents
…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation 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 : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Se préparer aux incidents de sécurité*

Un baccalauréat en cybersécurité à Polytechnique Montréal

Un baccalauréat en cybersécurité à Polytechnique Montréal

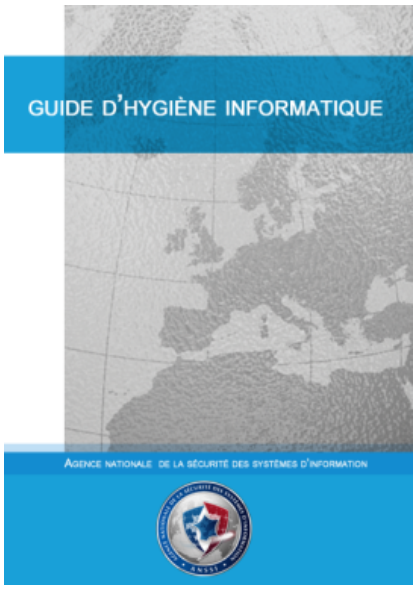
La Commission des études a approuvé la création d'un nouveau baccalauréat en cybersécurité qui sera offert à Polytechnique Montréal à l'automne 2017.

Les demandes pour un programme de formation en ligne en cybercriminalité, incluant des stages en entreprise, se sont faites pressantes au cours des dernières années et Polytechnique Montréal a décidé de créer un baccalauréat par cumul avec appellation en cybersécurité. La Commission des études de l'Université de Montréal a donné son approbation à ce projet à sa réunion du 21 mars.
Le nouveau programme permettra de combiner deux certificats liés à la thématique (cyberenquête, cyberfraude ou cybersécurité) avec un autre programme de 30 crédits de l'UdeM ou de HEC Montréal en vue de l'obtention d'un diplôme de baccalauréat. L'école de génie, rappellent les responsables, offre une formation en cybersécurité au premier cycle depuis 2007. Le projet vise à répondre «le plus adéquatement possible aux nouveaux besoins du marché du travail, qui est confronté à une pénurie de main-d'œuvre amplifiée par un taux de cybercriminalité en hausse exponentielle. De plus, la multiplication des supports mobiles ainsi que l'émergence de l'infonuagique posent de nouveaux défis».
Considérant qu'une proportion importante des étudiants de ces programmes ne possèdent pas de diplôme universitaire de premier cycle, et considérant le manque de main-d'œuvre dans ces domaines, «il apparaît essentiel que le diplôme de baccalauréat qui pourrait être décerné par cumul de certificats présente une dénomination spécifique [du] domaine d'études et de pratique, dans une perspective de valeur ajoutée, tant pour la formation que pour l'employabilité et la reconnaissance des entreprises qui emploient ces diplômés», fait valoir Polytechnique Montréal.
Le nouveau programme devrait voir le jour l'automne prochain.
(MATHIEU-ROBERT SAUVÉ)

Réagissez à cet article

Source : *Un baccalauréat en cybersécurité à Polytechnique Montréal | UdeMNouvelles*

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



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

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

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

LISTE DES GUIDES DISPONIBLES

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

---

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

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

La webcam, Est-ce une une vraie menace pour les utilisateurs d’ordinateurs

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

La webcam, est-ce une vraie menace pour les utilisateurs d’ordinateurs

Après Mark Zuckerberg et sa webcam masquée par du scotch, voilà que c'est le directeur du FBI, James Comey, qui admet avoir adopté le même réflexe.

Une webcam cachée pour s'éviter bien des ennuis

A l'heure où les hackers multiplient les attaques contre les machines des entreprises et des particuliers, beaucoup se sont moqués de Mark Zuckerberg et de son bout de scotch sur la webcam et sur la prise jack, certains allant même jusqu'à le traiter de « parano ».
Pourtant, il semblerait qu'il s'agisse d'un réflexe à prendre et ce pour tout le monde. En effet, un pirate talentueux peut assez simplement prendre le contrôle d'une webcam à distance et pousser ainsi l'utilisateur à télécharger un malware sur sa machine.
Aussi, lors d'une interview, James Comey, le directeur du FBI, a défendu l'idée de masquer la webcam. Il a même précisé que ce devait être un réflexe de base en matière de sécurité. En prenant le contrôle de votre caméra, un pirate peut effectivement visionner vos saisies sur clavier et récupérer ainsi identifiants, mots de passe et coordonnées bancaires pour ne citer qu'eux…[lire la suite]

Conseils de Denis JACOPINI :

Les personnes averties croient utiliser la méthode miracle pour protéger leur vie privée en masquant leur Webcam.
Certes, je recommande toutefois de masquer votre Webcam car, même si, en l'absence de logiciel de sécurité adapté, le pirate peut la mettre en fonction sans que vous vous rendez compte de rien. Le pirate peut en effet voir votre tête en train de taper au clavier ou de jouer (ce qui en soit n'aura rien d'intéressant) mais selon l'orientation, voir le reste de la pièce lorsque vous vous éloignez de l'ordinateur.

Mais avez-vous pensé à protéger votre microphone ?

A l'instar des baby phones piratés, mettre en route à distance le microphone de votre ordinateur est tout aussi facile que de mettre en route votre Webcam et même mieux d'ailleurs, car à ma connaissance, il n'existe pas de logiciel de sécurité qui empêche l'accès au microphone. Certes tout le monde n'est pas Mark Zuckerberg, mais tout professionnel devrait en plus de couper son téléphone pendant les réunions, penser aussi à boucher le microphone de son appareil ou mieux, enficher une fiche Jack vide.
[block id="24761" title="Pied de page HAUT"]

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220

Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.
Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.
Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?
Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.
Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !
Commandez sur Fnac.fr

---

https://www.youtube.com/watch?v=lDw3kI7ra2s
06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.
Commandez sur Fnac.fr

---

https://youtu.be/usgl2zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA
12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet
Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).
Commandez sur Fnac.fr

Original de l'article mis en page : La webcam, une vraie menace pour les utilisateurs d'ordinateurs

---

Nos ordinateurs ont-ils la mémoire courte ? Vidéo

Nos ordinateurs ont-ils la mémoire courte ? Vidéo

Que trouveront les archéologues du futur, d'ici quelques siècles ou quelques milliers d'années ? Des pierres taillées du paléolithique, des hiéroglyphes, des rouleaux de parchemins probablement, des livres peut-être.

Quelles images, quels sons, quels écrits de notre société restera-t-il dans 2000 ans ? Auront-ils résisté aux épreuves du temps et aux mutations technologiques comme l'ont fait la première photo, le premier film, le premier enregistrement sonore.Mais que deviendront les milliards d'informations engrangées dans les disques durs qui se démagnétisent, et sur les CD ou DVD, qui redoutent la lumière du soleil ?[lire la suite]

LE NET EXPERT

:

• MISE EN CONFORMITÉ RGPD / CNIL

- **AUDIT RGPD ET CARTOGRAPHIE** de vos traitements
- **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 ;

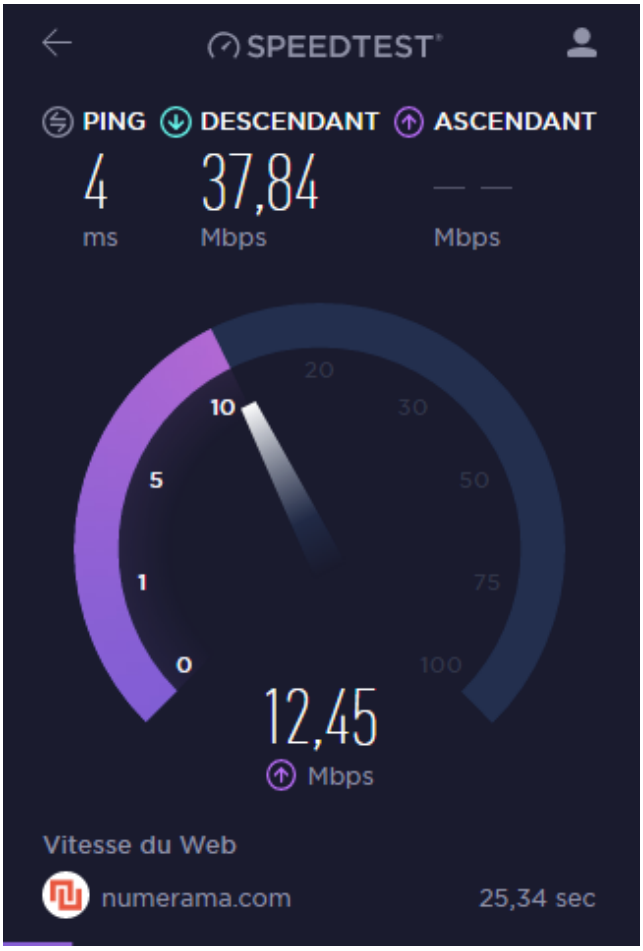
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Nos ordinateurs ont-ils la mémoire courte ?*

Comment mesurer et tester le débit de votre connexion internet | Denis JACOPINI



Comment mesurer et tester le débit de votre connexion internet

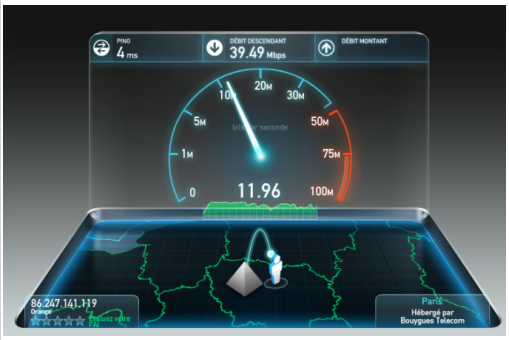
---

Internet c'est bien. Quand c'est rapide, c'est mieux. Nous vous avons listé quelques outils indispensables pour mesurer votre débit, que vous soyez chez Free, SFR, Orange, Numericable ou Bouygues.

On entend souvent dire qu'aujourd'hui on ne peut plus vivre sans Internet. Cette affirmation est fausse. Dire qu'on ne peut plus vivre sans **bonne** connexion Internet serait plus juste. Et justement, pour connaître la qualité de votre bande passante, il existe quelques outils extrêmement simple d'utilisation. Petit tour d'horizon des indispensables pour ceux qui ne les connaîtraient pas.

SPEEDTEST

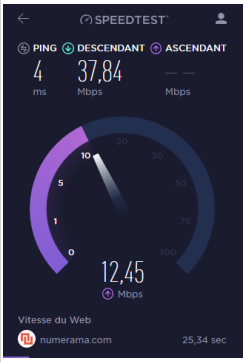
C'est le plus connu des outils présentés ici. Speedtest est complet et calcule votre débit montant et descendant ainsi que le temps de latence. Vous avez ainsi en main absolument toutes les informations en main pour connaître la vitesse de votre connexion. On regrette seulement le temps assez long que peut prendre un test (environ 47 secondes) et l'interface qui manque de sobriété.



Cela devrait bientôt changer grâce à la version HTML5 – encore en version beta – plus simple et efficace. Attention, celle-ci ne fonctionne pas lorsque le bloqueur de publicité est activé. Speedtest se décline également en application mobile pour profiter des mêmes fonctionnalités sur son smartphone.

EXTENSION OOKLA

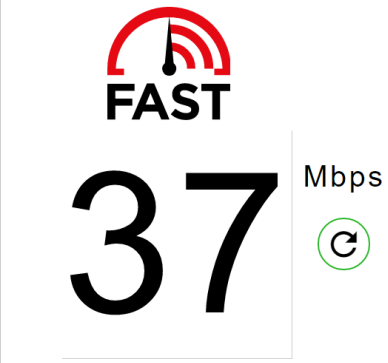
Cet outil est extrêmement pratique. Ookla, l'entreprise qui a créé Speedtest, a sorti une extension Chrome rapide et ergonomique. À l'instar du site Internet, elle calcule le download, l'upload et le ping. Le test est réalisé en un peu moins de 30 secondes mais c'est surtout par son extrême simplicité d'utilisation que l'extension séduit.



En effet, pas besoin de taper l'adresse d'un site ou de lancer une recherche Google. Un simple clic en haut à droite de votre navigateur suffit à y accéder. Ainsi, si vous remarquez certaines lenteurs de connexion, pas besoin d'attendre une éternité avant d'accéder à la page qui pourra vous confirmer que votre débit est pourri. Vous pouvez d'ailleurs fermer la fenêtre de l'extension, celle-ci continuera à faire le test de débit discrètement.
Malheureusement pour tous ceux qui n'utilisent pas le navigateur web de Google, l'add-on Ookla est disponible uniquement sur Chrome.

FAST.COM

En moins de dix secondes, Fast.com calcule votre vitesse de téléchargement (débit descendant uniquement). Si vous n'en avez rien à faire du temps de latence ou que vous n'avez rien à uploader, il s'agit du site idéal.



Ce site est en accord avec la vision de Netflix, son créateur, qui s'adresse plus aux internautes qui consomment plutôt qu'à ceux qui produisent. Ainsi, si vous ne surfez sur le web que pour consulter et télécharger des fichiers, Fast.com représente la meilleure solution. Le service en HTML 5 fonctionne aussi bien sur PC que sur mobiles, smart TV ou tablettes.
Article original de Omar Belkaab

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 : Guide : comment mesurer et tester le débit de sa connexion internet – Tech – Numerama