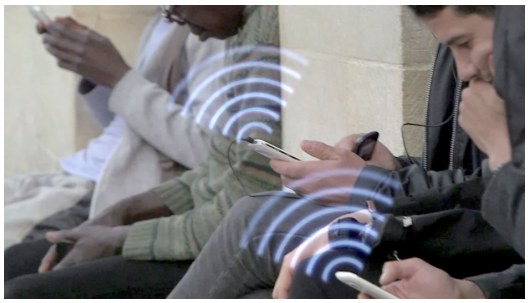
Comment se comporte notre cerveau surchargé par le numérique

	Comment se comporte notre cerveau surchargé par le numérique

Samedi 3 septembre, ARTE a diffusé un excellent reportage sur la manière dont notre cerveau se comporte face à nos vies de plus en plus hyper connectées : « HYPERCONNECTÉS : LE CERVEAU EN SURCHARGE ».

Grâce aux smartphones, ordinateurs et autres tablettes, nous sommes reliés au monde en continu. Mais ce déluge d'informations menace notre bien-être. Alliant témoignages de cadres victimes de burn out et explications de chercheurs en neurosciences, en informatique ou en sciences de l'information et de la communication, ce documentaire captivant passe en revue les dangers de cette surcharge sur le cerveau. Il explore aussi des solutions pour s'en prémunir, des méthodes de filtrage de l'information aux innovations censées adapter la technologie à nos besoins et à nos limites.

Chaque jour, cent cinquante milliards d'e-mails sont échangés dans le monde. Les SMS, les fils d'actualité et les réseaux sociaux font également partie intégrante de notre quotidien connecté, tant au bureau qu'à l'extérieur. Nous disposons ainsi de tout un attirail technologique qui permet de rester en contact avec nos amis, nos collègues, et qui sollicite sans cesse notre attention. Comment notre cerveau réagit-il face à cette avalanche permanente de données ? Existe-t-il une limite au-delà de laquelle nous ne parvenons plus à traiter les informations ? Perte de concentration, stress, épuisement mental, voire dépression… : si les outils connectés augmentent la productivité au travail, des études montrent aussi que le trop-plein numérique qui envahit nos existences tend à diminuer les capacités cognitives.

Un documentaire de Laurence Serfaty (France, 52′), diffusé sur ARTE le samedi 3 septembre à 22h20

A voir et à revoir sur Arte +7 pendant encore quelques jours !

si vous ne voyez pas la vidéo, le lien

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 : Hyperconnectés : le

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

---

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

---

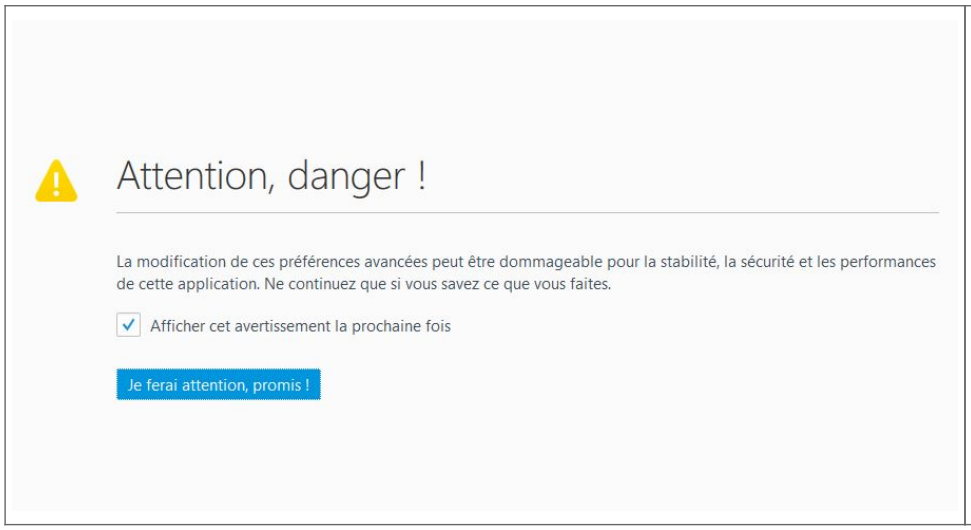
Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

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

---

Comment sécuriser Firefox efficacement en quelques clics de souris ?



Comment sécuriser Firefox efficacement en quelques clics de souris ?

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

C'est sur le blog des Télécoms que j'ai vu pointer l'information concernant le réglage de plusieurs paramètres de Firefox afin de rendre le navigateur de la fondation Mozilla encore plus sécurisé. L'idée de ce paramétrage, empêcher par exemple Google de vous suivre à la trace ou de bloquer la géolocalisation qui pourrait être particulièrement big brotherienne.
Commençons par du simple. Il suffit de taper dans la barre de navigation de votre Firefox la commande about:config. Une alerte s'affiche, pas d'inquiétude, mais lisez là quand même. recherchez ensuite la ligne security.tls.version. Les valeurs affichées doivent osciller entre 1 et 3. Ensuite, recherchez la ligne geo.enabled pour annuler la géolocalisation. Passez le « true » en « False ». Pour que les sites que vous visitiez ne connaisse pas la dernière page que vous avez pu visiter, cherchez la ligne network.http.sendRefererHeader et mettre la valeur 1. Elle est naturellement placée à 2. Passez à False la ligne browser.safebrowsing.malware.enabled.
Ici, il ne s'agit pas d'autoriser les malwares dans Firefox, mais d'empêcher Google de vous tracer en bloquant les requêtes vers les serveurs de Google. Pour que Google cesse de vous profiler, cherchez la ligne browser.safebrowsing.provider.google.lists et effacez la valeur proposée.
Pour finir, vos données peuvent être encore accessibles en « offlire », en mode hors connexion. Cherchez les lignes offline-apps.allow_by_default et offline-apps.quota.warn. La première valeur est à passer en Fasle, la seconde valeur en 0.
Il ne vous reste plus qu'à tester votre navigateur via le site de la CNIL ou celui de l'Electronic Frontier Foundation.
Article original de Damien Bancal

Réagissez à cet article

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

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*