Fausses applications Pokémon GO. Comment se protéger ? | Denis JACOPINI

	Fausses applications Pokémon GO. Comment se protéger ?

Les chercheurs ESET découvrent des fausses applications sur Google Play qui cible les utilisateurs de Pokémon GO. L'une d'entre elles utilise pour la première fois une application qui verrouille l'écran (Lockscreen) sur Google Play. Les deux autres applications utilisent la fonctionnalité scareware qui oblige l'utilisateur à payer pour des services inutiles.

Toutes les fausses applications découvertes par ESET et détectées grâce à ESET Mobile Security (application lockscreen nommée « Pokémon GO Ultimate » et les applications scareware « Guide & Cheats for Pokémon GO » et « Install Pokemongo ») ne sont plus disponibles sur Google Play. Elles ont été retirées de l'app Store suite à l'alerte donnée par ESET.

Même si ces fausses applications ne sont pas restées longtemps sur le Google Play, elles ont généré quelques milliers de téléchargements. L'application « Pokémon GO Ultimate », a piégé entre 500 et 1.000 victimes, « The Guide & Cheats for Pokémon GO » en a atteint entre 100 et 500, et la plus dangereuse d'entre elles, « Install Pokemongo » a atteint entre 10.000 et 50.000 téléchargements.

« Pokémon GO Ultimate » cultive son extrême ressemblance avec la version officielle du célèbre jeu mais ses fonctionnalités sont très différentes : elle verrouille l'écran automatiquement après le démarrage de l'application. Dans de nombreux cas, réinitialiser le téléphone ne fonctionne pas parce que l'application se superpose à toutes les autres, ainsi qu'aux fenêtres du système. Les utilisateurs doivent redémarrer leurs appareils en retirant la batterie ou en utilisant Android Device Manager. Après la réinitialisation, l'application malveillante fonctionne en arrière-plan, à l'insu de sa victime, en cliquant silencieusement sur des annonces à caractère pornographique. Pour se débarrasser de l'application, l'utilisateur doit aller dans Réglages -> Gestion des Applications -> PI Réseau et la désinstaller manuellement.

« Pokémon GO Ultimate » est la première fausse application sur Google Play qui utilise avec succès une fonction de verrouillage d'écran. Comme la fonctionnalité principale de cette application est le clic sur des annonces pornographiques, il n'y a pas de réels dommages. Mais il suffit de peu pour que la fonction de verrouillage d'écran évolue et ajoute un message de rançon, pour créer le premier ransomware par lockscreen sur Google Play.», explique Lukáš Štefanko, Malware Researcher chez ESET.

Alors que l'application « Pokémon GO Ultimate » porte les signes d'un screenlocker et d'un porncliker, les chercheurs ESET ont également trouvé un autre malware sur Pokémon GO dans Google Play. Les fausses applications nommées « Guide & Cheats for Pokemon GO » et « Install Pokemongo » sur Google Play, appartiennent à la famille des Scarewares. Ils escroquent leurs victimes en leur faisant payer des services inutiles. En leur promettant de leur générer des Pokecoins, Pokeballs ou des œufs chanceux – jusqu'à 999.999 chaque jour – ils trompent les victimes en leur faisant souscrire à de faux services onéreux. (Cette fonctionnalité a récemment été décrite dans un article publié sur WeLiveSecurity).

« Pokémon GO est un jeu si attrayant que malgré les mises en garde des experts en sécurité, les utilisateurs ont tendance à accepter les risques et à télécharger toutes applications qui leur permettraient de capturer encore plus de Pokémons. Ceux qui ne peuvent pas résister à la tentation devraient au moins suivre des règles de sécurité élémentaires. » recommande Lukáš Štefanko.

Conseils des experts en sécurité ESET pour les afficionados de Pokémon GO :

– téléchargez uniquement ce qui vient d'une source connue
– lisez les avis en prêtant attention aux commentaires négatifs (gardez en tête que les commentaires positifs ont pu être créés par le développeur)
– lisez les termes et conditions de l'application, concentrez-vous sur la partie qui concerne les permissions requises
– utilisez une solution de sécurité mobile de qualité pour vérifier toutes vos applications

Conseils de Denis JACOPINI

Pour anticiper et vous protéger pour moins de 10€ (10€ est prix de la licence initiale. Une forte réduction sera appliquée au moment du renouvellement au bout d'un an)

Article original de ESET

Réagissez à cet article

Formation RGPD : L’essentiel sur le règlement Européen pour la Protection des Données Personnelles

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	**Formation RGPD : l’essentiel sur le règlement Européen pour la Protection des Données Personnelles**				

Contenu de nos formations :

Le Règlement Général sur la Protection de Données (RGPD) entre en application le 25 mai 2018 et les entreprises ne s'y sont pas préparées. Or, elles sont toutes concernées, de l'indépendant aux plus grosses entreprises, et risqueront, en cas de manquement, des sanctions pouvant aller jusqu'à 4% de leur chiffre d'affaires.

Au delà des amendes pouvant attendre plusieurs millions d'euros, c'est aussi la réputation des entreprises qui est en jeu. Quelle valeur lui donnez vous ?

Serez-vous prêt à la perdre pour ne pas avoir fais les démarches dans les temps ?

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

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)

Réagissez à cet article

Formation en Cybercriminalité : Arnaques, virus et demandes de rançons, Comment s’en protéger ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Formation en Cybercriminalité : Arnaques, virus et demandes de rançons, Comment s’en protéger ?				

Le contexte de l'Internet et l'ampleur du phénomène de la cybercriminalité, nous poussent à modifier nos comportements au quotidien.
Avons-nous raison d'avoir peur ? De quoi doit-on avoir peur ? Comment se protéger ?
Les réponses évidentes sont techniques, mais il n'en est pas moins vrai que des règles de bonnes pratiques et des attitudes responsables seront les clés permettant d'enrayer le phénomène.

OBJECTIF DE LA FORMATION EN CYBERCRIMINALITE :

La formation en cybercriminalité a pour but de créer des déclics chez les utilisateurs, mettre à jour les connaissances des informaticiens et faire prendre conscience aux chefs d'entreprises des risques en couvrant les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant d'enrayer le phénomène de la cybercriminalité.

PROGRAMME :

• Etat des lieux de la cybercriminalité en France et dans le monde;
• Les principaux cas de piratages et d'arnaques expliqués ;
• Les bonnes pratiques au quotidien pour limiter les risques ;
• Etude de vos témoignages, analyse de cas et solutions.
• PUBLIC CONCERNÉ : Utilisateurs, chefs d'entreprise, présidents d'associations, élus….

MOYENS PÉDAGOGIQUES :

• **Support de cours pour prise de notes**
• **Résumé remis en fin de cours.**
• **Vidéo projecteur et sonorisation souhaitée selon la taille de la salle.**

CONDITIONS D'ORGANISATION

• Formations individuelles ou en groupe
• Formations dispensées dans vos locaux ou organisées en salle de formation partout en France en fonction du nombre de stagiaires.

Téléchargez la fiche de présentation / Contactez-nous

QUI EST LE FORMATEUR ?

Denis JACOPINI est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire et a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.
Il anime dans toute le France et à l'étranger des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles.
A ce titre, il intervient régulièrement sur différents médias et sur La Chaine d'Info LCI pour vulgariser les sujets d'actualité en rapport avec ces thèmes.
Spécialisé en protection des données personnelles, il accompagne les établissements dans leur mise en conformité CNIL en les accompagnant dans la mise en place d'un Correspondant Informatique et Libertés (CIL).
Enfin, il intervient en Master II dans un centre d'Enseignement et de Recherche en Informatique, en Master Lutte contre la Criminalité Financière et Organisée, au Centre National de la Fonction Publique Territoriale et anime le blog LeNetExpert.fr sur lequel il partage et publie de très nombreuses informations sur ses thèmes de prédilection.
Denis JACOPINI peut facilement être contacté sur :
http://www.leNetExpert.fr/contact

Réagissez à cet article

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/usg12zkRD9I?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

---

10 bonnes pratiques pour des soldes sur Internet en sécurité

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	10 bonnes pratiques pour des soldes sur Internet en sécurité				

Pour réaliser vos achats en ligne en toute sécurité, ESET vous donne des conseils pour éviter de se faire pirater sa carte bancaire.

– **Faites attention aux sites Internet que vous ne connaissez pas.** Au moindre doute, n'effectuez pas vos achats, car il peut s'agir d'un faux site Internet qui tente de récupérer les informations de votre carte bancaire.

– **Préparez-vous aux attaques par phishing.** Elles se diffusent massivement par e-mail lors des soldes, car c'est à cette période que les internautes passent le plus de temps sur les sites Internet de vente en ligne. ESET a réalisé une courte vidéo pour vous expliquer comment éviter le phishing par e-mail.

– **Utilisez des méthodes de paiement sécurisé.** Vérifiez que l'URL mentionne HTTPS. Effectuez toujours vos paiements sur des sites Internet chiffrés.

– **Attention aux annonces sur Facebook.** Les plateformes des réseaux sociaux abondent de fausses annonces et sites Internet proposant des offres intéressantes. Évitez également de partager les détails de votre carte bancaire par message : vous ne pouvez pas vérifier l'identité des personnes qui ont accès au compte et qui recevront ces informations.

– **Effectuez toujours vos achats sur des appareils sécurisés et évitez de vous connecter à un Wi-Fi public.** Ce genre d'arnaque, appelé Man-in-the-Middle (MiTM) est très répandu. En 10 minutes, le pirate peut voler toutes les informations vous concernant.

– **Utilisez des mots de passe forts ou un gestionnaire de mots de passe.** Plusieurs études ont montré que les utilisateurs ayant plus de 20 comptes en ligne et étant actifs sur Internet sont plus susceptibles de réutiliser les mêmes mots de passe pour plusieurs accès. Selon le rapport de recherche et de stratégie Javelin, cette méthode augmente de 37% le risque de voir ses comptes compromis. Aussi, les experts ESET recommandent d'utiliser des mots de passe forts mélangeant des minuscules et des majuscules à des symboles et chiffres. Les gestionnaires de mots de passe peuvent être utilisés pour ne pas avoir à les apprendre par cœur. Retrouvez les erreurs les plus courantes lors de l'utilisation d'un mot de passe en cliquant ici.

– **Soyez prudent avec votre smartphone.** Le nombre de cybermenaces sur cette plateforme a considérablement augmenté. Pour commencer, faites vos achats uniquement via des applications certifiées et supprimez les applications dont vous ne vous servez pas. Pensez à désactiver le Wi-Fi lorsque vous faites votre shopping dans un lieu public, privilégiez les données cellulaires, ceci permettra d'empêcher les cybercriminels de vous diriger vers un faux Wi-Fi afin de voler vos informations bancaires.

– **Utilisez une e-carte bleue.** Non seulement elle est déconnectée de vos comptes bancaires et est également assurée contre les fraudes.

– **Respectez les règles de sécurité de base.** Cela peut paraître évident, mais avant de faire vos achats, assurez-vous d'être correctement protégé : installez une solution de sécurité efficace et mise à jour. Optez pour une solution qui offre une navigation sécurisée pour les transactions bancaires. Enfin, ajoutez des mots de passe à votre écran de verrouillage ou un code PIN à votre smartphone.

– **Évitez de réaliser vos achats sur différents appareils** (1 à 2 maximum). Plus vous entrerez les informations de votre carte de crédit sur des appareils différents (PC, tablette, smartphone…), plus vous multipliez le risque d'être victime d'une fraude.

Réagissez à cet article

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/usg12zkRD9I?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

Article original de ESET

Victime d’un piratage

informatique, quelles sont les bonnes pratiques ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Victime d'un piratage informatique, quelles sont les bonnes pratiques ?				

Les cas de piratages informatiques ne se comptent plus depuis bien longtemps. Cependant, si vous vous êtes retrouvés victimes, il est urgent de mettre en pratique des règles de base.

Les 3 axes vers lesquels votre structure devra progresser seront :

• Technique, par une amélioration des mesures de sécurité en place ;

• Juridique, par une présentation, auprès des principaux acteurs de votre structure pour une meilleure acceptation, des principales mesures de mise en conformité avec les règles françaises et européennes relatives à la protection des données personnelles ;

• Humain, par une meilleure prise de conscience des dangers numériques, pour une évolution des comportements vers une utilisation plus responsable des outils numériques.

Face à vos besoins d'accompagnement, nos formateurs ont élaboré un parcours destinés aux équipes de direction de votre structure, à l'équipe informatique et aux utilisateurs susceptibles d'être piégés.

En vous accompagnant sur ces 3 axes et auprès de ces 3 profils, vous pourrez alors comprendre comment les pirates informatiques vous ont piégé, découvrir s'ils pourront encore vous piéger et surtout, le plus important, quelles changements mettre en place pour limiter les risques à l'avenir.

Réagissez à cet article

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/usg12zkRD9I?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).

Objets connectés : les inquiétantes failles de sécurité dont vous n'avez pas conscience | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	**Objets connectés : les inquiétantes failles de sécurité dont vous n'avez pas conscience**				

Les objets connectés doivent-ils vraiment recueillir autant de données personnelles pour fonctionner correctement ? Télévision, pèse-personne, thermostat et autres hubs domotiques… les objets connectés tentent d'envahir nos maisons et de s'infiltrer au coeur même de leur réseau numérique.

Pourtant, malgré leur objectif de nous simpliflier la vie, leur développement semble encore assez poussif ; en raison sans doute de leur manque criant de sécurité. C'est ce que révèle une étude menée par la division Sécurité de Hewlett Packard : rien de moins que 250 vulnérabilités ont été relevées par les experts d'HP Fortify au sein des 10 objets connectés les plus populaires.
Ces failles de sécurité seraient, selon Mike Amistead, le manager général d'HP Fortify, le symptome de la ruée des entreprises sur le créneau des objets connectés. Il estime en effet que les start-ups se lançant sur ce marché tenteraient de commercialiser leur produit le plus rapidement possible avant la concurrence… au mépris de la garantie d'un niveau de sécurité suffisant des réseaux et des données personnelles.
Vos données personnelles en clair sur la toile Parmi les failles de sécurité relevées, HP a constaté que :
• 90 % des objets connectés étudiés solliciteraient une information personnelle sensible (ex : adresse email ou postale, nom, date de naissance, etc) ; une information ensuite véhiculée en clair sur la toile ;
• 70 % des objets connectés ne crypteraient pas les données échangées avec le réseau ;
• 80 % des objets connectés ne nécessiteraient pas de mot de passe complexe pour identifier les demandes de connexion tierces ;
• 60 % des objets connectés seraient vulnérables aux attaques dites de « cross-site scripting » (type de faille de sécurité permettant d'injecter du contenu dans une page, et provoquant ainsi des actions sur les navigateurs web visitant la page).

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique 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).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.*

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Source : http://www.archimag.com/vie-numerique/2014/07/30/objets-connectes-internet-failles-securit

---

Existe-t-il quelques mesures simples pour éviter que de mon ordinateur et mes boites mail se fassent pirater ? | Denis JACOPINI

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

Existe-t-il quelques mesures simples pour éviter que de mon ordinateur et mes boites mail se fassent pirater ?

Il est très difficile de savoir si un ordinateur est piraté / piratable ou pas. Qu'il soit PC ou Mac, il possède ses failles qui peuvent sans limite être exploitées.
Il n'y a plus beaucoup de protections qui résistes aux plus grands hackers.
La divulgation de documents dévoilant les techniques qu'utilise la NSA pour nous espionner (c.f. http://www.lenetexpert.fr/les-10-outils-les-plus-incroyables-utilises-par-la-nsa-pour-nous-espionner-le-net-expert-informatique) et les dessous de société d'espionnage informatique Hacking Team récemment piratée (c.f. http://www.lenetexpert.fr/les-dessous-de-la-societe-despionnage-hacking-team-le-net-expert-informatique) nous ont récemment démontré qu'il n'y a aucune limite au piratage.

Mais alors, comment se protéger ?
Comme pour votre maison ou votre appartement, il n'existe aucun moyen d'empêcher les voleurs de rentrer. Les moyens qu'ils utiliseront seront généralement à la hauteur de l'intérêt qu'ils y trouveront.
Cependant, les conseils que je peux donner, sont comme pour les moyens de protection de vos habitions. Au plus on met des barrières de sécurité, au plus on retarde l'intrusion et au plus on décourage l'auteur. Il sera en effet plus difficile de rentrer chez vous si vous avez la dernière serrure de protection avec les volets anti-effraction dernier cri, avec une alarme ultra perfectionnée etc. plutôt qu'un simple cadenas pour vous protéger.

Pour sécuriser un système informatique
1) J'analyse généralement ce qui, dans nos habitudes quotidiennes correspond à une attitude numérique dangereuse ou irresponsable. Pour cette phase, il est difficile de vous dire quoi faire exactement, puisque c'est généralement notre expérience, nos connaissances passées et notre intuition qui servent à produire une bonne analyse.

2) La phase suivante va consister à détecter la présence d'espions dans votre ordinateur. Compte tenu que la plupart des outils d'espionnage sont capables de détecter qu'on est en train de les détecter, vaut mieux déjà, faire des sauvegardes, puis couper d'internet votre appareil (du coup, il sera nécessaire de télécharger les logiciels de détection à partir d'un autre ordinateur, et les copier sur l'ordinateur à analyser à partir d'une clé USB par exemple).
Cette phase de détection est très difficile. En effet, les logiciels espions, programmés pour espionner ce que vous tapez au clavier, ce que voit votre webcam ou entend votre micro, sont aussi programmés pour ne pas être détectés.
Le dernier outil connu pour réaliser une détection de logiciels espions est le logiciel **Detekt**. Ce logiciel a pour but de détecter des logiciels espions (spywares) sur un système d'exploitation Windows.
Les spywares actuellement détectés sont :
• DarkComet RAT ;
• XtremeRAT ;
• BlackShades RAT ;
• njRAT ;
• FinFisher FinSpy ;
• HackingTeam RCS ;
• ShadowTech RAT ;
• Gh0st RAT.
Attention, car les développeurs de ce logiciels précisent cependant :
« Certains logiciels espions seront probablement mis à jour en réponse à la publication de Detekt afin d'éviter la détection. En outre, il peut y avoir des versions existantes de logiciels espions […] qui ne sont pas détectés par cet outil ».
Vous trouverez plus d'informations et le lien de téléchargement sur http://linuxfr.org/news/detekt-un-logiciel-de-detection-de-logiciels-espions
Sur Mac, il n'existe pas un tel outil. Vous pouvez cependant utiliser le logiciel MacScan pou des antispaywares du commerce.
Cependant, que ça soit sur PC ou sur Mac, ce n'est qu'une analyse approfondie (et souvent manuelle) des fichiers systèmes, des processus en mémoire et qui se lancent au démarrage qui permettra de détecter les applications malveillantes installées sur votre ordinateur.

Et si on dispose d'un Mac plutôt que d'un PC ?
Il y a quelques années, avoir un Mac « garantissait » d'être un peu à l'abris des virus et des pirates informatiques. En effet, pouquoi un pirate informatique perdrait du temps à développer un logiciel malveillant et prendrait des risques pour seulement 5% de la population numérique mondiale. Désormais, avec l'explosion d'Apple, de ses téléphones, tablettes et aussi ordinateur, les systèmes IOS se sont répandu sur la planète numérique. De plus, c'est très souvent les plus fortunés qui disposent de ces types d'appareils… une aubaine pour les pirates qui trouvent tout de suite un intérêt à développer des dangereuxwares.

3) La troisième et dernière phase de ces recommandations est la protection. Une fois votre système considéré comme sain (il est complètement inutile de protéger un système qui est infecté car ça ne soignera pas l'équipement et les conséquences pourraient être pires), il est temps d'adopter l'attitude d'un vrai utilisateur responsable et paranoïaque.
• Mettez à jour votre système d'exploitation (Windows, MasOs, IOS, Androis, Linux…) avec la version la plus récente. En effet, l'enchaînement des mises à jour des systèmes d'exploitation est peu souvent fait pour améliorer le fonctionnement ou ajouter des fonctions à votre appareil. Le ballet incessant des « updates » sert prioritairement à corriger les « boulettes » qu'ont fait volontairement ou involontairement les informaticiens « développeurs » détectées par d'autres informaticiens plus « contrôleurs ».
• Mettez à jour vos logiciels avec leurs versions les plus récentes (et particulièrement pour vos navigateurs Internet et les logiciels Adobe). En effet, la plupart des intrusions informatiques se font pas des sites Internet malveillants qui font exécuter sur votre ordinateur un code informatique malveillant chargé d'ouvrir un canal entre le pirate et vous. Ces codes informatiques malveillants utilisent les failles de vos logiciels pour s'exécuter. Lorsque l'utilisation d'une faille inconnue (sauf par les pirates) d'un logiciel est détectée par les « Gardiens de la paix numérique », un correctif (ou patch) est généralement développée par l'éditeur dans les jours qui suivent leur découverte. Ceci ne vous garantira pas une protection absolue de votre ordinateur, mais renforcera son blindage.Les pirates utilisent parfois d'anciens serveurs ou d'anciens postes de travail connecté sur le réseau, qui ont de vieux systèmes d'exploitation qui ne se mettent plus à jour et qui ont des failles ultra-connues pour pénétrer votre réseau et des postes pourtant ultra-sécurisés. Pensez donc à les déconnecter du réseau ou à copier le contenu ou les virtualiser sur des systèmes plus récents et tenus à jour.
• Mettez à jour les firmwares des matériels et objets connectés. Pour les mêmes raisons qu'il est important de mettre à jour vos logiciels avec leurs versions les plus récentes, il est aussi important de mettre à jour les logiciels de vos matériels et objets connectés (routeurs, modems, webcams etc.).
• Adoptez une politique sécurisée dans l'utilisation des mots de passe. Vos mots de passe doivent êtres longs, complexes et doivent changer souvent. Conseil primordial dans l'utilisation des mots de passe au bureau : Il doit être aussi précieux et aussi secret que le code de votre carte bancaire. Personne ne doit le connaître, sinon… quelqu'un pourra facilement se faire passer pour vous et vous faire porter le chapeau pour ses actes malveillants.
• Méfiez-vous des sites Internet proposant des vidéos gratuites, du streaming gratuit ou autres services inespérément gratuit. Les sites sont souvent piégés et ont destinés soit à collecter des données personnelles, soit contaminer votre ordinateur par des petits codes malveillants.
• Méfiez-vous également des e-mails douteux de demande d'aide (même d'un ami) ou autre participation humanitaire utilisant le paiement par Manda Cash, Western Union ou monnaie virtuelle telle le Bitcoin. Ce sont des moyen de paiement qui sont généralement utilisés par les pirates pour se faire payer et disparaître dans la nature. Les emails destinés à vous hameçonner auront aussi quelques détails qui devraient vous mettre la puce à l'oreille (Faute d'orthographe, huissier ou directeur ayant une adresse e-mail yahoo ou gmail).
• Vous avez un doute, vous pensez que votre ordinateur ou votre boite e-mail est victime d'intrusion, changez immédiatement de mot de passe. Certains systèmes de messagerie permettent d'avoir un historique des accès et des connexions. L'analyse de cet historique pourrait bien vous donner une indication pour savoir si quelqu'un d'autre à accès à votre messagerie (alias, double diffusion, collecte d'un compte mail sur un autre compte etc).

Conclusion
Voila, vous avez maintenant toute une liste de recommandations qui peut vous rassurer (ou non) et vous permettre de prendre conscience de la complexité qu'est à ce jour la lutte de la #cybercriminalité.
Si maintenant tout ceci vous semble complexe, rassurez-vous, c'est notre métier. Nous seront donc en mesure de vous accompagner dans la sensibilisation des utilisateurs, la détection ou la protection contre ces « ennuiwares ».
Contactez-moi

Réagissez à cet article

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/usg12zkRD9I?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

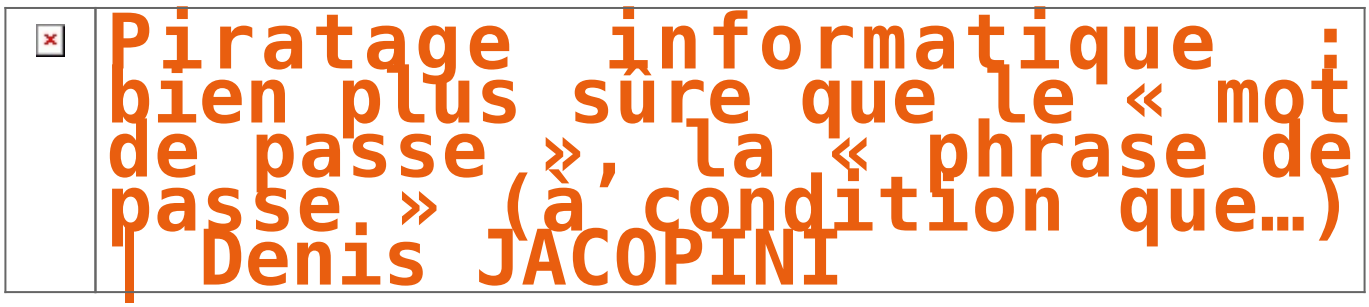
Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

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

Source : 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

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

	Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

1. CHOISISSEZ AVEC SOIN VOS MOTS DE PASSE

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

Comment bien choisir son mot de passe ?

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

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

Comment faire en pratique ?

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

Quelques recommandations supplémentaires

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

2. ENTRETENEZ RÉGULIÈREMENT VOS APPAREILS NUMÉRIQUES

En mettant à jour régulièrement les logiciels de vos appareils numériques

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

Comment faire ?

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

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

Comment faire ?

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

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

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

Voici quelques recommandations générales :

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

5. PROTÉGEZ VOS DONNÉES LORS DE VOS DÉPLACEMENTS

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

Précautions à prendre avant de partir en mission

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

Pendant la mission

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

6. SÉCURISEZ VOTRE WI-FI

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

Quelques recommandations générales :

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

7. SÉPAREZ VOS USAGES PERSONNELS DES USAGES PROFESSIONNELS

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

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

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

9. SOYEZ PRUDENT LORSQUE VOUS OUVREZ VOS MESSAGES ÉLECTRONIQUES

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

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

10. SOYEZ VIGILANT LORS D'UN PAIEMENT SUR INTERNET

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

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

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

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

Réagissez à cet article

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

---

Imprimante 3D : Comment ça marche ? | Denis JACOPINI

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/