La sécurité informatique

Article repris sur le site Forum d'entraide informatique. Il reprend certains points importants qu'il est bon de connaître, en particulier la partie IV.

Les liens repris dans le document ne fonctionnent pas.
Si besoin est, visitez le site du forum.

Ce dossier a pour but d'apprendre les bases de la sécurité informatique en s'informant sur les principales menaces, les méthodes permettant de se protéger et les réflexes à adopter pour utiliser un système informatique le plus sereinement possible.
Il est développé en 9 grandes parties, chacune d'entre elles comprenant plusieurs sous-parties. Bonne lecture !

Sommaire

I/ Introduction

Qu'est-ce que la sécurité informatique ?

La sécurité informatique désigne un ensemble de moyens (humains, logiciels, matériels, juridiques…) permettant de conserver la sécurité des systèmes liés à l'informatique.
La sécurité informatique vise principalement à garantir l'intégrité des données ainsi qu'à empêcher leur accès ou divulgation non-autorisés (confidentialité), empêcher un accès non-autorisé à des moyens informatiques (réseaux, ordinateurs…) et à assurer leur bon fonctionnement.

II/ Les menaces

1) Les escroqueries

Voici comment l'Article L313-1 du Code Pénal définit l'escroquerie : « le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende. »
Les principales escroqueries en ligne sont :
– Le phishing (hameçonnage en français) : pour piéger les personnes, le principe des pirates est simple : ils créent un faux site ressemblant le plus possible à un site officiel. Ensuite, ils vous demandent des informations personnelles, des coordonnées bancaires, mots de passe, etc. avec une fausse raison.
Cela peut également se passer par courrier électronique (e-mails).
En résumé, le procédé est le suivant : ils vous envoient un mail vous redirigeant sur un faux site officiel (de votre banque ou d'EDF par exemple). Ils vous fournissent une raison pour que vous renseigniez des informations personnelles (cette raison peut être, par exemple, que vous n'avez pas payé votre facture). Ensuite, ils exploitent vos informations à des fins frauduleuses.

– Les achats en ligne : produits ayant des prix anormalement élevés ou au contraire, des prix très bas. Généralement, le produit n'est jamais livré mais l'argent est bien prélevé sur votre compte bancaire. Les sites vantant de manière excessive les prix exceptionnels de leurs produits sont généralement des sites frauduleux.
– Les demandes d'argent : il n'est pas rare de recevoir un mail d'un individu réclamant de l'argent pour des raisons les plus souvent vitales. Ces personnes sont en réalité des escrocs.
– Le blocage de l'ordinateur : un message provenant prétendument de la police, gendarmerie ou interpol par exemple, bloque totalement l'accès à votre ordinateur. Il est demandé de payer une somme élevée pour retrouver l'accès à son PC. Ce sont des ransomwares. Nous allons développer ce point dans la prochaine sous-partie consacrée aux malwares.

2) Les malwares
Un malware (logiciel malveillant en français) est un programme développé pour nuire à un système informatique (ordinateur, téléphone, etc.). Ils sont très présents, plus particulièrement sur le système d'exploitation dominant : Windows. Contrairement aux croyances, leur arrivée a commencé à se faire depuis un certain temps sur Mac, mais aussi sur Linux.
Aujourd'hui, beaucoup d'ordinateurs sont infectés ou ont des restes d'infections sans que leur propriétaire ne le sache.
Les téléphones mobiles sont également touchés par les malwares.

Dans cette sous-partie, nous allons développer les fonctions des types d'infections suivantes : adwares, Logiciels potentiellement indésirables, pirates de navigateur, rogues, ransomwares, infections USB, keyloggers, spywares, rootkits, chevaux de troie, vers et virus.
Si vous pensez que votre ordinateur est infecté ou que vous souhaitez vérifier qu'il est bien sain, merci d'ouvrir un nouveau sujet sur le forum FEI dans la catégorie désinfection.

– Les adwares : un adware (publiciel ou logiciel publicitaire en français) est, comme son nom l'indique, un logiciel affichant de la publicité pendant son utilisation. Bien souvent, des fenêtres intempestives font leur apparition et affichent des publicités ciblées. Le développeur est donc rémunéré en incluant ces publicités dans son logiciel. Il est considéré comme un malware lorsqu'il n'est pas indiqué clairement dans les CGU (Conditions générales d'utilisation) que le logiciel affiche des publicités.
Les adwares s'installent généralement lors d'installations de logiciels, souvent gratuits.

– Les logiciels potentiellement indésirables : un Logiciel potentiellement indésirable (LPI) ou Potentially unwanted program (PUP) en anglais est simplement un logiciel non souhaité par l'utilisateur. Par exemple, un adware (explications ci-dessus). Ils installent simultanément régulièrement des barres d'outils (toolbars) indésirables et modifient les pages de démarrage et de recherche des navigateurs (explications ci-dessous : pirates de navigateur).

– Les pirates de navigateur : un pirate de navigateur (browser hijacker en anglais) est un logiciel modifiant la page de démarrage et les moteurs de recherches des navigateurs. Ils sont considérés comme des logiciels potentiellement indésirables.
Vous l'avez compris, les adwares, les logiciels potentiellement indésirables et pirates de navigateur sont très proches et sont généralement présents simultanément lorsqu'un PC est contaminé par ces types d'infections.

– Les rogues : un rogue, ou scareware, est un faux logiciel de sécurité tel un antivirus ou anti-spyware. Leur principe de fonctionnement est simple : le logiciel, ressemblant fortement à un antivirus ou à une protection Windows, effectue rapidement un scan de l'ordinateur. À la fin, un nombre élevé d'infections est détecté. Or, ces infections sont très généralement imaginaires. Il est demandé à l'utilisateur de payer pour désinfecter le PC. Or, même en payant, l'ordinateur ne sera en aucun cas désinfecté.
Ils s'installent le plus souvent via des bannières publicitaires ou via des cracks. Et parfois, lors de l'installation d'autres logiciels.

– Les ransomwares : un ransomware, ou rançongiciel, est un logiciel cryptant des données ou bloquant totalement l'accès à un ordinateur au démarrage avant l'affichage du bureau. En échange, pour retrouver un accès normal à l'ordinateur, il est demandé à l'utilisateur de payer une forte somme d'argent. Bien souvent, les données bancaires sont également dérobées si l'utilisateur décide de payer (chose à ne pas faire, bien évidemment).
Certains ransomwares bloquent également l'accès au mode sans échec. Ils se font souvent passer pour une institution officielle, comme la police, la gendarmerie, interpol ou le ministère de l'Intérieur.
Ils s'installent à l'exécution d'un fichier qui est censé avoir une autre fonction. Très souvent via des cracks, le P2P ou via les sites de streaming.

– Les infections USB : une infection USB est une infection qui se propage par des supports amovibles (clés USB, disques durs externes, iPod, etc.). Une infection USB se propage très rapidement, étant donné qu'il suffit que le support amovible infecté entre en contact avec un PC sain et ce dernier sera infecté. Ce nouveau PC infecté infectera lui-même les futurs supports amovibles entrant en contact avec lui, et ainsi de suite…
Les écoles, cybercafés, bibliothèques ou autres lieux à forte influence sont régulièrement infectés par ce type d'infection.
Ces infections USB modifient régulièrement le fichier *autorun.inf*, fichier s'exécutant automatiquement lors de l'insertion d'une clé USB ou autre média amovible. C'est pourquoi le support amovible infecté contamine instantanément une machine saine lors de son insertion.
Les symptômes les plus courants : modification de la page de démarrage ou du titre d'une page internet, fichiers transformés en raccourcis, fichiers devenus cachés, accès au gestionnaire des tâches ou au registre interdits, UAC désactivé…
Si on affiche les fichiers et dossiers cachés sur une clé USB infectée, on pourra repérer rapidement l'infection (se mettant en fichier caché par défaut très souvent).
Parfois, il n'y a pas de symptômes et l'infection USB peut avoir une fonction de keylogger (explications ci-dessous).

– Les keyloggers : un keylogger, ou enregistreur de frappe, est considéré comme un logiciel espion (spyware). Un keylogger actif enregistre toutes les frappes du clavier à l'insu de l'utilisateur pour les envoyer à son développeur (pirate). Il porte généralement le nom d'un processus similaire à un processus légitime de Windows. Un keylogger peut être, dans de rares cas, un dispositif matériel (modification des branchements ou du clavier).
Il peut également enregistrer tout ce qui se passe à l'écran (mails ou sites web consultés…).
Le but premier d'un keylogger est de dérober des informations personnelles (mots de passe, coordonnées bancaires, identité,

adresse électronique) afin que le pirate les revende.
Ils s'installent généralement avec des cracks ou via le P2P.

– Les spywares : un spyware (logiciel espion, espiogiciel ou mouchard en français) est un logiciel malveillant installé sur une machine à l'insu de l'utilisateur récoltant un maximum de données confidentielles pour les envoyer à un tiers établissant des statistiques pour les revendre. Ils étudient le comportement de l'utilisateur afin de dresser son profil : c'est le profilage. Ils sont régulièrement développés par des sociétés de publicité sur internet.
Les spywares récoltent différents types de données : les achats effectués, les sites web visités, les recherches effectuées, voire les coordonnées bancaires et les mots de passe, ainsi que d'autres informations privées.
Eux aussi s'installent très généralement en même temps que d'autres logiciels, souvent gratuits, ainsi que les cracks, les sites pornographiques ou autre.

– Les rootkits : un rootkit est un logiciel malveillant tentant au maximum de masquer sa présence en modifiant le fonctionnement du système d'exploitation dans le but, généralement, de donner un accès à la machine à une tierce personne via une porte dérobée (backdoor). Ils peuvent également servir à envoyer des spams et peuvent désactiver les protections (antivirus, pare-feux). Les rootkits sont souvent relativement complexes à détecter et difficiles à désinfecter.
Il existe deux types de rootkits : les rootkits de type utilisateur (userland), caractérisés par un fichier .exe et une dll, actifs au niveau de l'utilisateur et souvent simples à désinfecter, car un outil qui travaille au niveau du noyau disposera de plus de droits que lui ; et les rootkits de type noyau (kernel-mode) fonctionnant donc au niveau du noyau de Windows, composés d'un driver et d'un service. Ce dernier type effectue des crochets (hooks) dans les fonctions de Windows pour fausser les résultats (par exemple si on souhaite lister les pilotes ou accéder au fichier) et est le plus complexe à éradiquer et généralement celui utilisé pour fournir un accès à l'ordinateur.
Ils s'installent en général via des cracks, les sites de streaming, etc.

– Les chevaux de Troie : un cheval de Troie (trojan horse en anglais ou troyen) est un logiciel d'apparence légitime effectuant des actions à l'insu de l'utilisateur, régulièrement sans que ce dernier ne s'en rende compte. Un cheval de Troie, en soi, n'est pas une infection, mais un logiciel contenant une infection. Généralement, il contient une backdoor (porte dérobée en français permettant de donner un accès à l'ordinateur) mais ils peut aussi servir à voler les coordonnées bancaires par exemple.
Parfois, le développeur inclut lui-même un trojan dans ses logiciels.
Les cracks et le P2P sont les principaux vecteurs de cette infection.

– Les vers : un ver, ou worm en anglais, est un logiciel malveillant capable de se reproduire à travers un réseau (internet, par exemple). Généralement, les vers spamment les courriels des utilisateurs ou bien les modifient avec des pièces jointes malveillantes.
Les vers sont généralement contenus dans des fichiers en VBScript ou .exe.
C'est donc principalement à travers les messageries que se propagent les vers.
Un ver peut ouvrir une porte dérobée, espionner le comportement de l'utilisateur, détruire des données, envoyer des requêtes sur un site internet (déni de service) tout en se reproduisant.

– Les virus : un virus, en soi n'est pas malveillant puisque c'est simplement un programme capable de s'auto-reproduire. Cependant, il contient souvent un code malveillant. Ses buts sont variés : par exemple, peut être considéré comme un virus un programme ouvrant sans cesse des fenêtres ou pouvant afficher un simple message, tout en ayant la capacité de se reproduire. Les virus peuvent également endommager le démarrage de l'ordinateur.
Son principal objectif est donc de se propager à d'autres ordinateurs via, par exemple, les courriers électroniques, les supports amovibles (clés USB…) dans un logiciel légitime « hôte ».
De nos jours, le terme « virus » est très régulièrement employé à tort à la place du terme « malware ». En effet, les virus sont devenus le type d'infection le moins développé actuellement et restent très rares.

3) Les faux blogs de sécurité
Si vous pensez que votre ordinateur est infecté, votre premier réflexe est de taper sur un moteur de recherche le nom de l'infection dont vous êtes victime ou bien les symptômes. Or, en général, quasiment la moitié des résultats, dès la première page, sont des faux blogs de sécurité. Il est très difficile de les repérer pour un utilisateur lambda qui ne s'en doute pas.
Ces sites utilisent souvent le même genre de mots clés dans l'URL du site comme dans l'article : virus, removal, spyware, supprimer, remove, etc. avec, bien sûr, le nom de l'infection répété un nombre assez important de fois.
Leur principe est généralement le même : une introduction assez longue pour paraître sérieux qui exagère les dangers de l'infection pour effrayer le lecteur et le convaincre qu'il faut agir le plus rapidement possible, une image de l'infection, avec une solution assez complexe (qui peut parfois fonctionner même si, bien sûr, il y aura des restes de l'infection alors qu'elle ne sera plus visible) avec plusieurs boutons très visibles du type « *Télécharger outil de suppression pour …*« .
Ce logiciel téléchargé est en fait une arnaque. Il examinera assez rapidement votre ordinateur en détectant un grand nombre d'éléments (comprenant le nom de l'infection) mais, à la fin, lorsque vous passerez au nettoyage, il vous sera demandé de payer. Actuellement, SpyHunter est un logiciel type assez courant : il réclame, à la fin du scan, 72€ pour passer au nettoyage de votre PC.
Voici plusieurs exemples de faux blogs de sécurité : Exemple 1 – Exemple 2
N'allez pas sur ce genre de sites, mais suivez plutôt une désinfection complète et gratuite par des personnes compétentes sur des sites sérieux.

4) Les failles de sécurité
Une faille, ou vulnérabilité, est une faiblesse dans un système informatique due à un dysfonctionnement logiciel ou matériel. En général, il s'agit de bugs logiciels (logiciels installés par l'utilisateur ou bien le système d'exploitation lui-même). Une fois découvertes, ces failles sont comblées par les développeurs dans la mesure du possible.
Il n'est pas rare qu'elles soient exploitées par des pirates informatiques à des fins malveillantes pour forcer des opérations non prévues dans l'utilisation normale du logiciel. Des informations confidentielles peuvent être dérobées si une faille n'est pas comblée et le risque d'infection augmente donc considérablement.
Les codes malicieux inconnus du public permettant d'exploiter ces failles découvertes par les pirates sont fonctionnels le jour même de leur développement. C'est le principe d'une faille de type « Zero day » : les protections (antivirus, pare-feux…) ne les

détectent donc pas dans la plupart des cas.
Parfois, un utilisateur peut se faire infecter seulement en visitant un site web piégé exploitant une faille d'un logiciel (Java, par exemple).
Les programmes permettant d'exploiter une vulnérabilité sont appelés « exploits ».

5) Les achats en ligne
Le e-commerce est en pleine évolution depuis quelques années. En 2013, d'après la *Fevad*, le nombre d'acheteurs en ligne a progressé de 5 % ; le nombre de sites marchands répertoriés a dépassé les 138 000 (pour seulement 23 900 en 2006) et la fréquence d'achats en ligne est passée à une moyenne d'environ 18 transactions par an par acheteur (la moyenne étant de 16 en 2012). Tout cela pour un total de 51,1 milliards d'euros de dépenses et 600 millions de transactions en ligne par les Français en 2013. Une hausse de 13,5 % du total des ventes et de 17,5 % pour le nombre de transactions sur un an.
Vous comprenez donc que ce commerce attire massivement les personnes mal intentionnées qui regorgent d'astuces pour vous piéger.
Le phishing est l'un des principaux dangers des achats en ligne. Plus d'informations dans le point *II/ 1)*
Lorsque vous voulez effectuer un achat en ligne, ne vous jetez pas sur le premier site venu même s'il a l'air de répondre à vos besoins et surtout si vous ne le connaissez pas. Commencez par vérifier si le site est sérieux en vous assurant que le nom de la société, le téléphone et les conditions générales de ventes (CGV) sont facilement accessibles. Puis allez chercher des avis d'utilisateurs sur internet. Si vous n'en trouvez pas un certain nombre de positifs, évitez de passer commande sur ce site.
Vérifiez ensuite le descriptif détaillé du produit afin de vous assurer qu'il est bien neuf et que c'est bien le produit désiré, ainsi que sa disponibilité et le délai de livraison. Si le produit a un prix anormalement faible et que le site est rempli de propositions alléchantes envahissantes, il est probable que le site est frauduleux.
Soyez très vigilant lors de la fin de votre commande. Il est fréquent que les sites marchands proposent des services complémentaires (payants) à la fin de la commande. Veillez à que rien ne soit coché, au risque de payer plus cher. Relisez plusieurs fois le récapitulatif de votre commande avant de procéder au paiement. Vérifiez également que le site est bien sécurisé : pour ce, il faut que l'URL commence par https, avec un petit cadenas devant l'adresse.
Il est possible que certains sites demandent des justificatifs tels qu'une facture d'EDF, un RIB ou une photocopie de votre carte d'identité. En revanche, ne fournissez jamais la photocopie du recto-verso de votre carte bancaire.
Si vous avez un doute sur le sérieux du site sur lequel vous comptez passer votre commande, la plupart des banques mettent à la disposition de leurs clients un système de « carte virtuelle ». N'hésitez pas à profiter de ce service pour plus de sécurité.
Sachez que si un achat en ligne frauduleux a été effectué sans preuve de votre identité, votre banque doit vous rembourser dès lors qu'une somme a été débitée de votre compte.

6) Le spam
Le spam, courrier indésirable ou pourriel, est un envoi massif non sollicité par les destinataires de courriers électroniques envoyés par des spammeurs. En général, ces courriers sont envoyés à des fins publicitaires pour vendre divers produits.
On ne peut pas faire grand-chose face au spam. Si votre adresse est répertoriée par les spammeurs, difficile d'y échapper à moins de configurer les paramètres de votre messagerie pour faire en sorte que la plupart des courriers aillent automatiquement dans le dossier des courriers indésirables. Cependant, évitez au maximum de déposer votre adresse électronique dans des endroits publics (blogs, forums…). C'est souvent comme cela que les spammeurs en profitent pour répertorier votre adresse. Par ailleurs, si une personne a votre adresse et que son ordinateur se fait infecter : selon l'infection, votre adresse électronique peut être volée.
Si vous recevez un spam, n'y prêtez pas attention et supprimez le courrier sans y répondre au risque d'entrer dans le jeu du spammeur.
Il y a également :
– Le scam : généralement une personne originaire d'Afrique qui demande un service pour une transaction financière importante.
– Le hoax : un hoax est un canular. Le courrier demande de le transmettre à un maximum de personnes avec souvent des motifs grossiers (problèmes de santé, menaces, etc.).
– Le Fear, Uncertainty and Doubt (FUD) : Peur, incertitude et doute. Cela consiste à lancer diverses rumeurs (sur la santé ou la sécurité, par exemple).
- Le phishing : explications ci-dessus dans la première sous-partie.
Il existe aussi le spam mobile : c'est l'envoi répétitif et abusif de SMS non sollicités par leurs destinataires. Ces messages tentent d'attirer votre attention, demandant généralement de rappeler à un numéro 08 97 ou 08 99. Le but est donc que vous appeliez ce numéro, surtaxé bien évidemment, ou que vous répondiez au SMS.
Tout comme les spams de messagerie classiques, ne prêtez pas attention à ces messages et supprimez-les.
Toutefois, il est possible de signaler ces spams à la plateforme multi-opérateurs qui se chargera d'analyser votre signalement afin de désactiver le numéro de spam en fonction de sa récurrence et de sa gravité. Pour cela, transférez le message tel que vous l'avez reçu au 3700. Ensuite, envoyez un second message contenant seulement le numéro de l'expéditeur du message indésirable.
Si vous souhaitez rappeler un numéro douteux, n'hésitez pas à regarder auparavant sur le web s'il y a des informations le concernant et mettez *#31#* au début du numéro du destinataire afin de masquer votre numéro.

III/ La confidentialité / les réseaux sociaux
1) Les dangers des réseaux sociaux
Un réseau social est un groupe d'individus regroupés par un lien social.
Commençons par quelques statistiques de l'*Ifop* datant de fin 2013 afin de montrer l'ampleur des réseaux sociaux à ce jour :
– 86 % des internautes français sont inscrits sur au moins un réseau social.
– 60 % sont inquiets pour leurs données personnelles.
– 63 % sont inscrits sur Facebook ; 32 % sur Google+ et 17 % sur Twitter.
– 46 % des membres Facebook se connectent sur le réseau social chaque jour.
– Un internaute a en moyenne un compte sur 1,9 réseau social.
Les réseaux sociaux les plus connus sont : Facebook (1,189 milliard d'utilisateurs actifs par mois à travers le monde (UA / M)),Google+ (300 millions d'UA / M), Twitter (231,7 millions d'UA / M), LinkedIn (184 millions d'UA / M), et enfin Instagram(150 millions d'UA / M).

À travers ces réseaux sociaux, les utilisateurs partagent un grand nombre de données différentes les concernant, mais aussi concernant d'autres personnes : photos, vidéos, profession, situation amoureuse, activités, lieu de résidence, vacances, courriel, numéro de téléphone, etc.
Un grand nombre des utilisateurs pensent que leurs données sont protégées selon les différents réglages de confidentialité. Cependant, une minorité d'entre eux se soucie que ces données soient exploitées par des tiers (les applications ou les annonceurs par exemple) mais surtout que la plupart des réseaux sociaux conservent un certain temps toutes les données même celles censées être supprimées.
Vous pouvez d'ailleurs faire une demande à Facebook pour qu'ils vous envoient toutes les données qu'ils détiennent sur vous (voir ici).
En effet par exemple, vous ne l'avez peut-être pas constaté, mais les applications (jeux…) Facebook demandent votre autorisation pour accéder à votre profil et toutes les données qu'il contient. Donc, même si les paramètres de sécurité sont réglés au plus strict possible, ces applications pourront accéder à vos données censées rester dans un cadre restreint. Évidemment, il est fréquent que ces données soient revendues à d'autres sociétés.
Même les discussions instantanées ne sont pas réellement privées et sont parfois examinées par Facebook, notamment.
Un réseau social est donc un outil divertissant présentant toutefois des dangers selon l'utilisation que l'on en a.
Et ces dangers sont nombreux. Les jeunes en particulier sont des proies faciles, pour les pédophiles entre autres. D'après les statistiques du ministère de la Justice, chaque année en France, une quinzaine d'enfants sont victimes de violences sexuelles par une personne rencontrée sur internet.
D'autres utilisent les réseaux sociaux pour insulter leurs amis, parfois pour plaisanter, ou pas. La discrimination et le racisme sont donc deux phénomènes assez courants sur les réseaux sociaux malheureusement.
Certaines personnes utilisent les réseaux sociaux pour faire de l'usurpation d'identité. Le principe est simple : la personne se crée un faux profil avec de vrais noms trouvés sur le réseau social lui-même ou ailleurs, accompagné régulièrement de vraies photos ou autres. Cela sert souvent pour diverses escroqueries (prétendu déblocage de téléphone portable par exemple), ou tout simplement pour s'amuser à semer le désordre un moment.
Parfois même, les cambrioleurs utilisent les réseaux sociaux avant de passer à l'action. En effet, les utilisateurs ne font pas toujours attention aux paramètres de confidentialité lors de la publication d'une information, celle de départ en vacances plus particulièrement. Ensuite, il leur suffit de taper votre nom sur les pages blanches, s'il est répertorié, pour savoir où ils pourront faire leur travail « tranquillement » durant vos vacances…

2) Le comportement à adopter sur les réseaux sociaux
Pour éviter tous les ennuis décrits ci-dessus, il n'existe pas des dizaines de solutions, il ne faut tout simplement pas publier de données confidentielles. Gardez toujours à l'idée que, lorsque vous publiez quelque chose sur un réseau social, même supprimé cela restera probablement plusieurs années et cela pourra être revendu à d'autres sociétés extérieures. Ce n'est pas parce que vous êtes derrière votre écran que vous êtes en sécurité, même si vous en avez le sentiment.
Évitez surtout de fournir votre lieu de résidence, votre numéro de téléphone, des documents (photos, vidéos…) à caractère trop « osé » et privé. Et n'exposez pas toute votre vie en disant constamment ce que vous êtes en train de faire et ce que vous allez faire.
Respectez également vos proches ou d'autres personnes : ne publiez pas d'éléments (photos et vidéos en particulier) les concernant sans leurs accords (de préférence écrits).
Il peut vous arriver de constater des comportements irrespectueux ou hors-charte envers d'autres personnes. Dans ces cas-là, n'hésitez pas à avertir la personne ayant publié l'élément posant problème et si besoin ou en cas d'impossibilité, de signaler le comportement au réseau social afin que les modérateurs puissent l'examiner et prendre une décision.
Par ailleurs, essayez de ne pas passer trop de temps sur les réseaux sociaux.
Ces règles ne s'appliquent pas uniquement aux réseaux sociaux, mais à tout internet (forums, blogs, etc.).

3) Le cyberharcèlement
Le cyberharcèlement est un acte malveillant répété par une ou plusieurs personnes envers une autre par le biais des nouvelles technologies (réseaux sociaux, téléphones portables, chats, jeux en ligne, courriers électroniques, etc.).
Cela peut se traduire par des insultes, des rumeurs, des menaces, des intimidations, publications de photos ou vidéos compromettantes, voire des usurpations d'identité, pour porter atteinte à la personne et d'autres choses encore.
Les jeunes sont les plus touchés par le cyberharcèlement et les conséquences peuvent être graves. Derrière son écran, l'adolescent est seul et personne n'est là pour le protéger. De plus, s'il en est également victime dans son établissement scolaire, il subit ce harcèlement sans cesse.
Son bien-être et son mental sont directement atteints.
Et si les harceleurs se cachent, cela augmenter davantage le stress.
Si la situation est constatée, il est important que les parents et membres de l'établissement scolaire gèrent la situation ou un autre adulte, tel qu'un psychologue. Le harcèlement peut être puni par la loi d'un an d'emprisonnement et de 15 000€ d'amende.

IV/ Sécuriser et sauvegarder ses données

1) Comportement à adopter avec son ordinateur
Il est important de savoir quel comportement adopter avec son ordinateur, particulièrement sur le web.
Tout d'abord, concernant la confidentialité et la protection de sa vie privée, reportez-vous au point *III/ 2)*
Ensuite, le téléchargement de logiciels infectés est fréquent. En fait, la plupart du temps, ce sont les sites proposant le logiciel qui repacke les logiciels en ajoutant leurs propres installateurs contenant principalement des adwares et LPIs, pré-cochés lors de l'installation. À chaque installation réussie, le site est rémunéré par l'éditeur de l'infection.
Pour éviter cela, il faut toujours essayer de télécharger sur le site de l'éditeur. Ce n'est pas parce qu'un site est gros qu'il n'a pas ce genre de pratiques (je pense surtout à 01Net et Softonic qui ne s'en privent pas). Et soyez vigilants lors des installations des logiciels : décochez les modules complémentaires proposés.
Il faut également être vigilant avec le streaming. Il arrive régulièrement que les sites de streaming ouvrent de fausses pages de mises à jour de sécurité (concernant Java et Adobe le plus souvent). L'utilisateur, pensant que c'est une vraie alerte, procède à la mise à jour. Or, le logiciel n'est absolument pas actualisé et le PC se fait infecter.
Les publicités incluent aussi ce genre de choses, de temps à autre.
C'est exactement la même chose pour les sites pornographiques (ou autre).

Le P2P (pair à pair) est également un vecteur important d'infections, à travers des logiciels comme Emule, Vuze, BitTorrent…
Les fichiers téléchargés à travers ces logiciels sont assez fréquemment des infections et non le fichier attendu. C'est pourquoi il est déconseillé d'utiliser ces logiciels, qui, de plus, sont communément utilisés pour des actions illégales (crack principalement).
L'utilisation du P2P se fait donc à vos risques et périls.
Pour éviter que certaines infections puissent s'activer, il est préférable d'utiliser une session utilisateur et non administrateur.
De même, évitez de sauvegarder les mots de passe dans les navigateurs comme ils le demandent, car ils peuvent être dérobés en quelques secondes.
Vous pouvez aussi désinstaller les logiciels de sécurité comme Java ou Adobe Reader pour réduire les risques d'exploitations de failles.
Soyez prudent lorsque vous naviguez sur le net. Ne cliquez pas sur n'importe quoi et réfléchissez à ce que vous faites. N'hésitez pas à interroger Google si vous avez un doute sur un élément. Adoptez un esprit critique : ce n'est pas parce qu'un site vous garantit à 100 % qu'un logiciel (ou autre) est légitime qu'il l'est réellement. Si un doute persiste, posez la question sur un forum spécialisé ou abandonnez ce que vous souhaitez faire.

2) Logiciels de sécurité conseillés

Il existe différents logiciels de sécurité pour tenter de protéger davantage votre ordinateur et ses données.
Bien sûr, la meilleure sécurité reste votre comportement.
Même en ayant beaucoup de sécurités et logiciels efficaces, si le comportement n'est pas adapté, il y aura forcément un moment où votre ordinateur se verra infecté ou vulnérable.
Voici certains logiciels recommandés :
– Un antivirus : gratuit ou payant. Par exemple, Avast (gratuit), BitDefender ou Kaspersky sont des antivirus relativement efficaces.
N'installez jamais plusieurs antivirus simultanément. Ils risquent d'entrer en conflit et faire planter votre machine.
Aucun antivirus n'est infaillible. Ce n'est pas parce qu'il considère un fichier comme sain qu'il l'est réellement.
– Malwarebytes' AntiMalware : un scanner généraliste visant à éradiquer toutes sortes de malwares. Il est efficace et régulièrement mis à jour. Il est disponible gratuitement, mais une version pro est également disponible pour disposer de la protection en temps réel en particulier. Il peut être utilisé en complément avec un antivirus. Plus d'informations sur le forum.
– Secunia PSI : un logiciel permettant de s'assurer que les logiciels tiers installés sur votre ordinateur sont à jour. Cela permet notamment de bénéficier des corrections des failles de sécurité sur différents logiciels et donc d'être moins vulnérable. Plus d'informations sur le forum.
– Update Checker : c'est exactement le même principe que Secunia PSI. Vous pouvez le tester également si jamais Secunia PSI fonctionne mal ou simplement si vous le préférez. Plus d'informations sur le forum.
– UsbFix : cet outil permet de vacciner vos supports amovibles en empêchant les infections de modifier le fichier *autorun.inf*pour se lancer automatiquement. Plus d'informations sur leforum.
– WOT (Web of trust) : une extension qui indique la fiabilité d'un site basé sur les avis des utilisateurs. Idem, ce n'est pas parce qu'un site est considéré comme fiable qu'il l'est réellement et vice-versa. Plus d'informations sur le forum.
– HTTPS Everywhere : une extension pour Chrome, Firefox et Opera servant à crypter les données échangées entre l'internaute et le site parmi plus de 1000 sites majeurs. Extension disponible sur le site FEI.
– AdBlock Plus : une extension permettant de bloquer les publicités malveillantes. Gardez à l'esprit que certains sites internet vivent grâce à la publicité et donc qu'il ne faut pas bloquer toutes les publicités, mais uniquement les plus intrusives. Plus d'informations sur cette extension sur le site.
– VirusTotal : un site internet regroupant plus de 40 antivirus pour scanner divers fichiers. Cela permet, en cas de doute, sur un fichier de savoir s'il est infecté ou non. Comme pour le reste, il ne faut pas s'y fier à 100 % même si cela reste assez fiable : si un fichier a un ratio de 0 de détection, cela n'assure pas forcément que ce fichier est sain. Plus d'informations ici.
Il existe aussi l'outil VirusTotal Uploader permettant d'afficher un bouton « Envoyer vers => VirusTotal » pour gagner du temps si vous utilisez l'outil régulièrement. Outil disponible sur le site
– Unchecky : logiciel permettant de décocher automatiquement les cases des modules complémentaires souvent indésirables lors des installations de logiciels. Si vous êtes un peu tête en l'air, cet outil peut vous être très utile. Plus d'informations ici.
– Ccleaner : ce logiciel est plus un logiciel de nettoyage et d'optimisation de Windows qu'un logiciel de sécurité. Cependant, il peut être utile pour effacer les données sauvegardées (fichiers temporaires, mots de passe sauvegardés dans les navigateurs, etc.). Plus d'informations à propos de ce logiciel sur le site.
– Concernant le pare-feu, il est conseillé de conserver celui de Windows si vous n'avez pas de connaissances en réseau et ports. Sinon, vous pouvez en installer un tel que Comodo.

3) Sécuriser et sauvegarder ses données

Sauvegarder ses données est une tâche importante pour minimiser les risques de pertes de données définitives.
Car il n'est pas rare qu'un disque dur lâche et qu'il soit impossible de récupérer les données qu'il contenait. Il faut donc prévenir ce phénomène.
Pour cela, il vous faut identifier les données les plus importantes : photos, souvenirs, documents professionnels ou personnels, archives… ?
Ensuite, il faut plusieurs supports pour pouvoir sauvegarder ces données : disques durs, clés USB, CD / DVD, etc.
Le cloud est également un moyen de sauvegarde, développé dans la prochaine sous-partie.
Puis, il vous faut effectuer des sauvegardes régulières sur ces supports.
Il est conseillé d'avoir au minimum deux autres supports de sauvegarde en plus de son ordinateur, pour les données les plus importantes. Il est également recommandé d'en avoir à plusieurs endroits différents, car il serait dommage, en cas d'incendie par exemple, de tout perdre alors que vous effectuez des sauvegardes régulières depuis plusieurs années.
Ne négligez pas ce point en pensant que ce type de soucis n'arrive qu'aux autres et que, quoi qu'il en soit, vos données seront récupérables. Ce sera peut-être le cas mais, dans certains cas, les fichiers sont endommagés et inexploitables.
Établissez des ordres de priorité pour les types de données à sauvegarder. Et, en fonction de l'utilisation de votre ordinateur et de la fréquence de modification des fichiers les plus importants, mettez en place un planning pour savoir quand sauvegarder vos données.
Une fois l'habitude prise, cela deviendra un réflexe et cela ne vous gênera plus.
Et le jour où un de vos disques rendra l'âme, vous verrez que vous serez très fier de vous d'avoir effectué des sauvegardes régulières, ce qui vous encouragera encore davantage à continuer.

4) Le cloud

Le cloud, ou nuage, est un moyen de stockage de données en ligne. C'est un terme dont vous avez sans doute entendu parler récemment, car il est en pleine expansion ces dernières années.
C'est un moyen de sauvegarde pratique, puisqu'il permet d'accéder à ses données n'importe où sans avoir à transporter de matériel avec soi : ces données étant stockées sur des serveurs distants.
Il est également possible de synchroniser ses données sur plusieurs appareils simultanément.
Le cloud est un moyen de sauvegarde plutôt fiable si l'on prend des précautions (voir la prochaine sous-partie sur les mots de passe). Les données sont généralement sauvegardées dans plusieurs pays différents, en cas d'incendie des serveurs par exemple, et pour accéder aux données plus rapidement selon l'endroit où l'on se trouve.
Désormais, il existe des dizaines de services proposant le cloud. Parmi les plus connus (sans ordre particulier) :
– iCloud : permet de partager ses données sur ses différents appareils Apple.
– Dropbox : un service connu mondialement pour accéder où que vous soyez à vos données.
– Google Drive : le cloud de Google, proposant 15 Go de stockage gratuits et jusqu'à 16 To en payant.
– OneDrive : le cloud de Microsoft lié à la messagerie, proposant jusqu'à 7 Go de stockage gratuits.
– Archive-Host : un autre moyen de stockage de données en ligne, assez proche de Dropbox.
– Et bien d'autres comme le cloud d'Orange, d'OVH, Amazon Cloud Drive, …

5) Les mots de passe

« Les mots de passe » est un sujet qui revient fréquemment. Un mot de passe est un moyen d'authentification permettant d'accéder à un service protégé.
Pour une sécurité optimale, il faut utiliser des mots de passe forts, difficiles à deviner et différents pour chacun des services.
Un mot de passe est considéré comme fort si :
– Il comporte au moins huit caractères.
– Il comprend des majuscules, minuscules, chiffres et caractères spéciaux.
– Il est unique.
Un moyen de créer un mot de passe est de prendre les premières lettres de tous les mots d'une phrase en y ajoutant des chiffres et caractères spéciaux.
Exemple : *Je dois avoir un mot de passe fort sur FEI => 15Jdaumdpfs F/*
N'utilisez pas les mots de passe les plus courants tels que : 123456, password, 12345678, azerty, qwerty, 0000, etc.
N'utilisez pas des mots présents dans le dictionnaire ni des suites de chiffres ou de lettres.
Certains outils permettent de vérifier le niveau de sécurité d'un mot de passe, tel que celui d'Intel. Ces outils sont à utiliser avec précaution et sont un petit plus par rapport aux règles générales qui restent bien plus importantes que les indications de ce genre d'outils, à utiliser avec un certain recul, car ils ne sont pas toujours très fiables.
N'hésitez pas à changer vos mots de passe les plus importants assez régulièrement. Vous pouvez également les noter afin de ne pas les oublier, mais si possible dans un endroit différent d'un endroit numérique susceptible d'être piraté. Vous avez la possibilité de les noter sur un petit carnet par exemple, placé dans un endroit sûr où seules des personnes de confiance auraient la possibilité d'accéder.

6) Sécuriser son smartphone

Les smartphones sont des « téléphones intelligents » possédés par des millions de français : plus de 50 % d'entre eux avaient un smartphone en 2013, et ce chiffre ne cesse d'augmenter. Mais, malheureusement, le vol de smartphones est lui aussi en pleine croissance.
Il faut donc, tout comme son ordinateur, sécuriser son smartphone pour plus de sécurité.
Tout d'abord, évitez de laisser votre smartphone traîner n'importe où : sur les terrasses des bars, sur le dessus de votre sac à main, sortant à moitié de votre poche et évitez aussi de l'avoir tout le temps dans vos mains. Placez-le de préférence dans des poches qui ferment et difficilement accessibles.
Les malwares font aussi leur apparition, notamment sur le système d'exploitation Android. C'est pourquoi il faut aussi avoir un bon comportement lorsque vous utilisez votre mobile. Vous avez la possibilité d'installer un antivirus : plus d'informations ici.
D'autres réflexes sont également à adopter :
– Mettez un mot de passe pour pouvoir déverrouiller l'appareil, en évitant les plus connus et utilisés du style : 1234, 0000, 1111, 2580, 5683, 2222, 1212, 0852, 1998, 5555, etc.
– Mettez également en place un code PIN (pour accéder à votre carte SIM), lui aussi sécurisé et différent.
– Chiffrez vos données les plus importantes en installant des mots de passe (différents également) pour accéder aux applications.
– Sauvegardez régulièrement les données de votre smartphone sur votre ordinateur, grâce au cloud par exemple.
– Dès qu'une mise à jour est disponible, installez-la afin de corriger les différentes failles de sécurité pour que votre smartphone soit moins vulnérable.
– Installez une application de géolocalisation, en cas de perte ou de vol (si jamais le voleur n'a pas l'idée de retirer la carte SIM…).
– Soyez vigilant sur les applications que vous installez. N'hésitez pas à aller chercher des avis sur le net avant de procéder à un téléchargement.
– Ne rappelez pas les numéros que vous ne connaissez pas, notamment les 08 97 ou 08 99 (numéros payants). N'hésitez pas à vous reporter au point *II/ 6)* abordant le spam sur mobile.
– Lorsque vous ne vous en servez pas, désactivez le Wifi et le Bluetooth : certains hackers s'en servent pour accéder à votre appareil.
– Connectez-vous à des réseaux Wifi sécurisés. Évitez les Wifi publics disponibles dans les restaurants, aéroports…
– Notez le numéro IMEI en cas de perte ou de vol : il permettra de rendre l'appareil inutilisable.

V/ Sensibiliser et protéger ses enfants

1) Le contrôle parental

Un contrôle parental, ou filtrage parental, est un système installé par les parents permettant de contrôler et limiter l'activité de leurs enfants sur l'ordinateur dans le but de les protéger.
Les contrôles parentaux permettent notamment d'assurer la sécurité de l'enfant sur le web en cas d'absence d'adulte. Ils offrent la possibilité de surveiller l'activité de votre (ou vos) enfant(s), d'établir des tranches horaires pour autoriser ou interdire l'utilisation de l'ordinateur, etc.
Il est nécessaire pour un bon fonctionnement du contrôle parental, que l'ordinateur comporte au moins deux sessions : une dédiée

aux parents où le contrôle parental sera géré par ces derniers et une autre session sans pouvoir administrateur dédiée aux enfants sur laquelle le contrôle parental prendra effet.
Le site internet *Filtra* a établi une liste de 28 contrôles parentaux testés, gratuits ou payants, classés par ordre (en fonction des notes attribuées). Les différentes fonctions de chacun des contrôles parentaux sont présentes pour vous aider à choisir la solution qui vous convient la mieux selon vos souhaits. La liste est disponible ici.
N'hésitez pas à chercher des avis sur le web avant d'installer un logiciel de filtrage parental.

2) Informer ses enfants des risques d'internet

Informer ses enfants des différents dangers d'internet est un élément primordial avant de leur donner la possibilité de naviguer seuls sur le web, que ce soit avec un ordinateur ou d'autres supports numériques (tablettes, smartphones, télévision, consoles de jeux…).
Car, de nos jours, étant donné l'ampleur que le numérique a pris, il faut sensibiliser les enfants avant qu'ils ne soient entourés de ces nouvelles technologies avec la nécessité de les utiliser.
Il n'est pas rare de croiser des contenus indésirables sur le net susceptibles d'être vus par vos enfants.
Il est important, pour vous parents, d'établir un dialogue constant et durable avec votre enfant sur l'utilisation qu'il a du web.
Essayez de faire en sorte qu'il vous prévienne dès qu'il croise un contenu indésirable ou suspect : conseillez-le en fonction.
N'hésitez pas à regarder ce qu'il fait et, en fonction, à le prévenir des risques rencontrés. Tentez de garder un œil sur son activité : installez l'ordinateur dans un endroit que vous fréquentez régulièrement et non dans un endroit isolé.
Expliquez-lui que beaucoup de faux contenus se trouvent sur internet et qu'il ne faut pas croire tout ce que l'on y lit. Essayez de développer son esprit critique.
Si un site ou une autre application informe qu'il y a une limite d'âge (pour les mineurs notamment), utiliser un autre service similaire approprié.
Prévenez-le qu'il peut croiser des faits, images ou vidéos choquants et de vous en parler si cela arrive.
Lorsque vous naviguer sur le web de votre côté, dès que vous rencontrez un contenu indésirable que votre enfant pourrait lui aussi rencontrer (arnaques, publicité mensongère, courriel indésirable, etc.), montrez-le-lui et expliquez-lui clairement pourquoi ce contenu est indésirable. Profitez-en également pour lui demander s'il a déjà vu ce type de contenu et ce qu'il a fait à cet instant-là.
Autre élément très important : il ne faut jamais qu'il fournisse d'informations personnelles (identité, adresse électronique ou postale, numéro de téléphone, mots de passe…) en raison des nombreux faux sites et personnes mal intentionnées exploitant ces données personnelles. N'importe qui peut se cacher derrière un pseudo.
Informez-le également qu'il ne doit pas fournir de photos de lui ou autres photos personnelles sans votre accord.
Ne jamais, dans la mesure du possible, fixer de rendez-vous à travers internet, en particulier avec un inconnu, car nombreuses sont les personnes ayant de mauvaises intentions. Si tel est le cas, qu'il vous prévienne et accompagnez-le, dans un endroit public fréquenté.
Ne jamais non plus accepter de quelconques invitations d'inconnus.
Si jamais il fait quelque chose qu'il n'aurait pas dû faire (cela arrive), expliquez-lui les conséquences que cela aurait pu avoir. Il est important qu'il apprenne à respecter les conseils et qu'il se dise, lorsqu'il fait demi-tour face à un contenu indésirable : « Je risque telle ou telle chose, c'est peut-être un pédophile ou une arnaque… » et non pas : « Je risque de me faire engueuler par mes parents. » Efforcez-vous de lui faire acquérir cette réflexion.
Il est important également qu'il n'utilise la webcam qu'avec des proches et des personnes de confiance qu'il connaît bien.
Il lui faut adopter un bon comportement, et respectueux, sur le web, car les autorités peuvent vous retrouver à tout moment grâce à votre adresse IP en particulier. Ils ne sont pas anonymes et sont sur un lieu public, c'est-à-dire à risques.

VI/ Les pirates informatiques

1) Les fonctions des pirates informatiques

Un pirate informatique est une personne spécialisée dans la sécurité informatique. Il dispose donc des moyens permettant de déjouer les différentes protections.
Un pirate informatique est un hacker, mais la réciproque n'est pas forcément vraie.
En effet, un hacker est un passionné par le fonctionnement des systèmes informatiques.
Il existe plusieurs catégories de hackers :
– Les chapeaux blancs : professionnels tentant d'accéder à un système en détournant les sécurités, avec l'accord du propriétaire du système. Cette pratique est donc légale.
– Les chapeaux gris : ils ne sont pas autorisés à pénétrer dans les systèmes mais n'ont pas d'intentions malveillantes. Souvent, seulement pour prouver, à eux-mêmes ou à d'autres, qu'ils en sont capables.
– Les chapeaux bleus : même principe que les chapeaux blancs, sauf qu'ils sont chargés de vérifier les vulnérabilités d'un système d'exploitation.
– Les chapeaux noirs : eux, sont des pirates informatiques, ou crackers. Ces personnes agissent dans le but de nuire, en pénétrant et parfois en endommageant des systèmes informatiques. Ils peuvent le faire pour des raisons financières, politiques, pour le plaisir de d'être hors-la-loi, etc.
– Les hacktivistes : personnes endommageant un système dans le but de défendre une cause. Cette pratique est, bien sûr, hors-la-loi.
– Les script kiddies : souvent des jeunes qui exploitent des codes trouvés sur le net pour pénétrer dans un système. Ils font cela généralement pour se faire remarquer, en pensant qu'ils sont compétents et en se prenant pour des hackers alors qu'ils ne le sont pas réellement. Ils ne font que suivre des tutoriels très généralement.

2) Les risques encourus par les pirates informatiques

Voici ce que dit la loi à propos du piratage informatique :
« *Article 323-1*
Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002
Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30000 euros d'amende. »
– Le fait de fausser un système de traitement de données automatisé : trois ans d'emprisonnement et 30 000 euros d'amende.
– Pour supprimer ou modifier frauduleusement des données : trois ans d'emprisonnement et 45 000 euros d'amende.
Une synthèse des peines encourues est disponible ici.

VII/ Savoir quoi faire si vous pensez que votre PC est infecté

1) Les forums de désinfection

Les forums proposant des services de désinfection, tel que celui-ci, sont gratuits.
Selon les forums, des personnes compétentes et spécialisées dans la désinfection vous prendront en charge afin de vous faire bénéficier d'une désinfection complète et la plus efficace possible.
Si vous pensez que votre ordinateur est infecté ou si vous souhaitez procéder à une simple vérification, vous avez la possibilité d'ouvrir un nouveau sujet ici.
N'hésitez pas à utiliser et à partager ce moyen, qui, pour moi, est celui qui convient le mieux à une personne se débrouillant un minimum avec son ordinateur. Sinon, vous pouvez toujours faire appel à une personne un peu plus compétente qui se chargera d'effectuer les manipulations demandées par les helpers (personnes compétentes aidant à la désinfection).
Les manipulations sont détaillées au maximum.

2) Les magasins informatiques

Généralement, les personnes font appel à des prétendus « professionnels » de l'informatique. Or la plupart de ces personnes, ou « informaticiens » ne connaissent pas grand-chose à la désinfection et ne font que passer certains antimalwares ou antivirus pour désinfecter la machine (mauvaise méthode). Mais, la plupart du temps, lorsque cela les ennuie trop, ils réinstallent entièrement le système.
Et pour ce travail, mal effectué, vous devez payer : cela ne revient presque jamais à moins de 50€ et cela monte régulièrement à plus d'une centaine d'euros.
Alors que vous pouvez simplement vous débrouiller vous-même sans sortir de chez vous et sans payer, en suivant les instructions que les helpers vous donnent.
Bien sûr, certains informaticiens savent tout de même désinfecter correctement. Même s'il est vrai que c'est assez rare selon les nombreux retours que j'ai reçus ces dernières années sur les forums à propos des manipulations effectuées ou recommandées par les « informaticiens » aux différents internautes…

VIII/ Se former à la sécurité informatique

Les centres de formation en sécurité informatique en ligne

Actuellement, il est possible de suivre une formation gratuite en ligne pour apprendre la sécurité informatique, c'est-à-dire :
– Apprendre à maîtriser correctement Windows.
– Comprendre le fonctionnement des différentes infections et apprendre à les éradiquer efficacement.
– Savoir se servir des outils de désinfection et interpréter les rapports qu'ils fournissent.
– Sécuriser son ordinateur.
– Savoir désinfecter et faire de la prévention.
Il faut une motivation importante pour suivre une formation, car elles durent généralement plusieurs années. Il est nécessaire d'être patient et avoir un esprit autodidacte pour y arriver facilement.
Voici les trois centres de formation actuellement disponibles :
– Helper Formation (HF) : accessible à tous, la formation proposée sur ce site commence par traiter les bases du fonctionnement de Windows et de la sécurisation d'un ordinateur, puis devient plus poussée afin de vous rendre capable de désinfecter. Inscriptions limitées.
– Security-X (SX) : une formation plutôt complète permettant d'obtenir de bonnes connaissances sur la désinfection et Windows. Les inscriptions sont aussi limitées.
– Sécurité Académie (SA) : formation plutôt dédiée aux débutants. Ce sont surtout les bases de la désinfection qui sont enseignées dans ce centre. Idem, les inscriptions sont limitées et pas toujours ouvertes.

IX/ Conclusion

1) Principaux réflexes à adopter

Pour terminer et pour rappel, voici les principaux réflexes à adopter lorsque vous êtes sur votre ordinateur :
– Téléchargez sur les sites des éditeurs.
– Soyez vigilant, lorsque vous installez des programmes, sur l'existence de modules complémentaires.
– Maintenez vos logiciels à jour.
– Évitez les cracks et le P2P.
– Évitez au maximum les sites pornographiques et de streaming (et autres sites déconseillés).
– Cherchez des avis sur internet en cas de doute, ou posez la question sur un forum spécialisé.
– Ne cliquez pas n'importe où et soyez critiques.

2) Diffuser le message

Si ce dossier vous a permis d'adopter un comportement plus sécurisé avec votre ordinateur et de comprendre les différentes menaces, n'hésitez pas à le partager autour de vous.
Merci à tous d'avoir lu cet article.
Si vous souhaitez plus de détails sur un élément ou si vous avez une remarque, n'hésitez pas à laisser un commentaire.