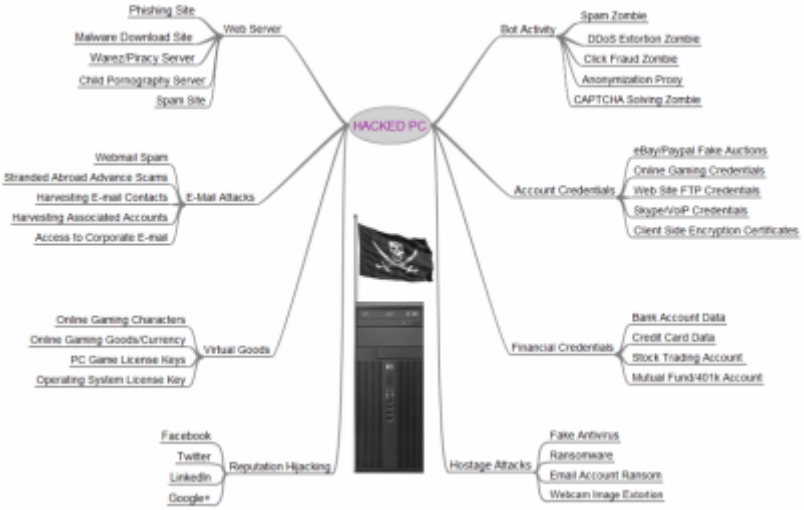
Vous trouverez sur cette pages des éléments de sécurité informatique destiné au non-initiés, dans le cadre d'ordinateurs personnels mais aussi pour des réseaux d'entreprises. Les explications seront simples et claires, n'hésitez pas à me faire part de vos remarques pour améliorer cette page.

Préambule

Un ordinateur non sécurisé est une proie facile pour les pirates informatiques. Même si vous n'avez “rien à cacher”, votre connexion peut être utilisé à votre insu pour faire des choses illégales. En effet, l'utilisation de votre ordinateur comme relai permet pour le pirate de se rendre anonyme (on ne pourra pas remonter jusqu'à lui) tout en vous mettant judiciairement sur la sellette.

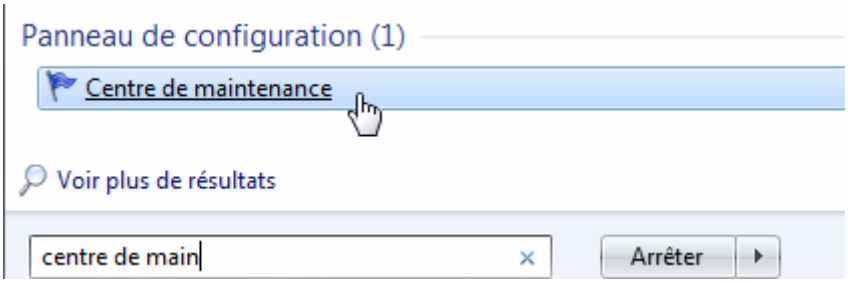


Il existe un certain nombre de choses simples à mettre en œuvre pour sécuriser son PC. Mais la meilleure des choses est encore de ne pas se retrouver infecté par un logiciel malveillant, et bien souvent cela peut être évité par certaines règles de bon sens : éviter les sites internet “louches”, ne pas télécharger et installer n'importe quel programme, ne pas ouvrir les pièces jointes suspectes de mail… Nous verrons cela en détail.

Hygiène informatique basique

Maintenez votre système d'exploitation à jour!

Windows est fournit avec l'utilitaire Centre de maintenance, qui permet en un coup d’œil de vérifier l'état global de la protection de votre système, et d'entreprendre le cas échéant des actions correctives. Pour démarrer centre de maintenance, Cliquez sur démarrer, et tapez “centre de maintenance”



Une fois sur la page, vous repérerez les éléments indiqués «importants». Ces points signalent des problèmes urgents, comme par exemple une mise à jour de sécurité majeure.

Il est également indiqué d'autres problèmes dont la résolution est suggérée.

C'est *via* le centre de maintenance que vous pourrez notamment exécuter Windows Update et télécharger les mises à jour de sécurité proposé par Microsoft pour résoudre les failles qui sont régulièrement découvertes.

A noter que Microsoft a cessé de donner des mises à jour de sécurité pour les systèmes d'exploitation antérieure à Windows 2000. Il n'est donc pas recommandé de continuer à utiliser ces systèmes d'exploitations.le support de sécurité Windows XP SP3 s'arrêtera lui en avril 2014.

Maintenez vos autres logiciels à jour

En mettant à jour vos logiciels, vous profiterez des dernières améliorations et bénéficierait des corrections de sécurité. Il s'agit de prendre les logiciels un par un et de vérifier sur le site officiel de l'éditeur s'il existe une version plus récente. il existe des logiciels pour vous aider à détecter les programmes qui disposent de mises à jour plus récente, tel que Secunia Software Inspector, Software Update Monitor Lite , Belarc Advisor ou FileHoppo Update Checker.

Pensez également à mettre à jour flash et Acrobate PDF Reader. le site Internet Ninite.com peut vous aider.

Installer un pare-feu

Sur Internet, votre ordinateur envoie et reçoit des informations. Un pare-feu permet de contrôler les connexions entrantes et sortantes et de bloquer les connexions non autorisées. si un programme tente d'établir une communication avec l'extérieur, le par-feu va vous alerter, vous donnez le nom du programme, et vous demandez si vous voulez le bloquer. C'est vous qui choisissez quels programmes sont autorisés à communiquer ou non vers l'extérieur. Si vous utilisez Windows XP, Windows Vista ou Windows 7, un pare-feu est déjà pré installé et configuré.

Si vous utilisez un système d'exploitation plus ancien, vous pouvez choisir un pare-feu tel que Online Armor ou Zone Alarm . Lisez sa documentation pour le configurer et le maintenir à jour.

Installer un anti-virus

Des millions de virus circulent en permanence sur internet. Ces programmes malveillants causent divers problèmes sur votre pc, vvieolent vos fichiers et certaines données sensibles (Mots de passes, numéros bancaires) et/ou les effacent, ouvrent des accès pour que des pirates prennent le contrôle de votre ordinateur, envoient des spams... Ces virus cherchent également à se diffuser à d'autres personnes *via* votre ordinateur. Pour vous en prémunir, vous avez besoin d'un anti-virus.vous pouvez prendre un antivirus gratuit : il en existe plusieurs,tel que Avast! Antivirus ou Avira Antivirus.

Quel que soit l'antivirus que vous choisissez, n'oubliez pas que, pour que celui-ci soit efficace, il est vital que vous effectuiez les mises à jour des “définitions de virus” très régulièrement, les menaces sur Internet évoluant en permanence. La plupart des antivirus possèdent une fonction de mise à jour automatique.

Installer un anti-spyware

Votre anti-virus vous protège de nombreux virus, mais il existe d'autre formes de nuisances tels que :

- Les trojans (Chevaux de Troie), qui occtroie au hacker le contrôle total de votre ordinateur et vole vos mots de passe et informations sensibles;
- Les spywares (Logiciels espions) qui collectent des informations sur vos habitudes d'utilisation de votre ordinateur (Sites web consultés, centre d’intérêts, adresses mails...) et revendent ces informations;
- Les adwares (Logiciels publicitaires), qui vous harcèleront de publicités intrusives sur votre écran;
- ... et, malheureusement, bien d'autres formes de logiciels indésirables.

La plupart de ces programmes malveillants peuvent être détectés et éradiquer avec l'aide d'un anti spyware à jour. Ces programmes ne rentrent pas en conflit avec votre antivirus. Ils ne se lancent que lorsque vous leur demandez de procéder à une analyse de votre ordinateur. L'un des anti spywares gratuits les plus efficace se nomme Malwarebytes Anti-Malware. Il existe également HitmanPro, SuperAntiSpyware ou encore TDSSKiller.

Hygiène informatique supplémentaire

Un navigateur plus performant qu'Internet Explorer

WOT

OpenDNS

Quelques règles générales de bonne conduite

- Windows update est activée
- Mon antivirus est installé, en fonctionnement, et à jour
- Le pare-feu Windows est en fonctionnement

Choix de mot de passe

Comment les pirates tentent de trouver votre mot de passe?

Malwares

Social Engineering

Brute Force

Entropie d'un mot de passe

Comment choisir ses mots de passe?

Les mots de passes à ne surtout pas utiliser

Les astuces pour choisir un mot de passe fort

xkcd : “Après 20 ans d'effort, nous avons réussi a entrainer les gens à utiliser des mots de passes qui sont complexes à mémoriser pour les humains, mais faciles à deviner par les ordinateurs.”

Pour aller plus loin

Authentification forte

- Facteur mémoriel : “Ce que je sais”
- Facteur pratique : “Ce que je sais faire”
- Facteur biométrique : “Ce que je suis”
- Facteur matériel : “Ce que je possède”

La sécurité en entreprise

Les bonnes recommandations de l'ANSSI

Crédit :

- http://sebsauvage.net/safehex/
- Aide de Microsoft Windows
- www.techsupportalert.com/best-free-anti-virus-software.htm
- http://www.selectrealsecurity.com/best-free-security-software/
- http://pctech.invisibill.net/wp-content/uploads/2008/09/checklist_full.html
- http://www.selectrealsecurity.com/security-checklist
- http://xkcd.com/936/
- http://www.ssi.gouv.fr/
- http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html