Comment protéger son PC ?

Internet est une technologie formidable dont on peut difficilement se passer, mais c'est aussi un endroit que tout le monde fréquente (y compris les pirates), et qui contient son lot de dangers. Cheval de Troie, virus, spyware, malware[1], spam... On peut se faire pirater de centaines de façons différentes, en ouvrant un mail, en cliquant sur une pièce jointe, en consultant une page Facebook se faisant passer pour une autre, en utilisant un réseau wifi public, en utilisant sa clé usb sur un ordinateur infecté, en introduisant ses données sur un site frauduleux qui ressemble à s'y méprendre à un site légitime, etc. Autant de menaces qui risquent de nuire à votre ordinateur et à vos données personnelles. Ces invasions peuvent aussi être à l'origine d'usurpation d'identité ou de fraude bancaire. Face à la multiplicité de ces risques, il existe de nombreuses solutions pour surfer en toute tranquillité. Du paramétrage de son ordinateur jusqu'à une certaine prudence lors de la navigation en passant par la protection via des logiciels spécialisés, découvrez comment **protéger au mieux votre ordinateur** et votre vie privée..

La meilleure manière de protéger son pc, quoi qu'il arrive, est de prendre conscience soi-même des dangers et des techniques pour s'en défendre : Utiliser une **protection logicielle (antivirus et pare-feu)** est indispensable, mais pas suffisant. Il faut également…

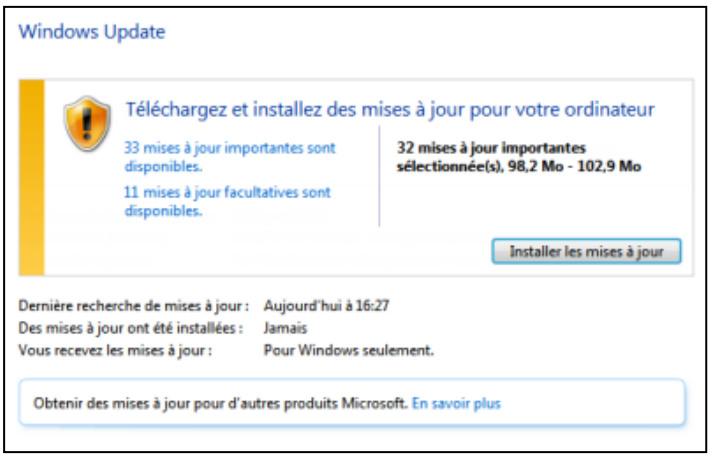
- mettre à jour vos systèmes et programmes (pour éviter les failles systèmes et logicielles).
- restez attentif, observez avant de cliquer ou de télécharger.
- protéger vos données personnelles (en ne les partageant pas, par exemple).
- utiliser des mots de passe forts, différents pour chaque site, et que vous changez régulièrement.
- faire des sauvegardes régulières sur un support de stockage externe (clé usb, disque dur externe ,…que vous ne laissez pas branchés sur votre pc)

Étape 1 : La protection logicielle

Il est *indispensable* d'utiliser un antivirus. Il existee n de nombreux fiables : AVG, Bitdefender, Eset Nod32, Kaspersky, Malwarebytes, Macafee,… Cette liste n'est pas exhaustive Les prix varient selon la durée, le nombre de PC protégés, le type de protection,… comptez au minimum 25€ pour un an pour un PC. Un petit prix pour éviter de se faire crypter tous ses fichiers musique, vidéos, documents et images par un ransomware[2] !

Étape 2 : Mettre à jour les systèmes et les programmes

Un antivirus qui n'est pas à jour est peu efficace : les programmes malveillants évoluent chaque jour, votre antivirus doit en faire de même. Les mises à jour du système et des programmes en général ont également pour but de corriger les failles de sécurité. En quelques mots, une faille de sécurité est un bug ou une erreur dans l'implémentation d'un logiciel qui permet à un attaquant de prendre avantage de cette faille pour mener à bien des attaques.



[1] un **malware** est un logiciel malveillant

[2] un **ransomware** est un logiciel malveillant prenant en otage les données. Vous récupérerez (soi-disant !) vos données seulement après avoir payé une rançon. Bien sûr, ne payez surtout pas, vous ne reverrez quand même pas vos données. Une seule solution si votre PC est bloqué par un ransomware, formatez le disque dur et réinstallez tout.

Imaginez que vous ouvrez un fichier .PDF dans *Adobe Reader*, et que ce dernier exécute un programme malveillant caché dans ce fichier *PDF.* C'est possible si *Adobe Reader* contient une faille de sécurité critique et qu'il n'est pas aussitôt mis à jour.

Vous trouverez les mises à jour disponibles dans Windows Update qui se trouve dans votre panneau de configuration (sous Windows 8.1, cliquez-droit sur le bouton Windows et vous verrez le panneau de configuration dans la liste qui apparaît), sous « Système et sécurité ».

Étape 3 : Protéger ses mots de passe et données personnelles

Utilisez un mot de passe fort (mélange de lettres, chiffres et symboles), et changez-le régulièrement. N'utilisez pas le mot de passe de votre PC ou de votre adresse mail quand vous vous créez un compte sur un autre site : si la banque de données de ce site se fait pirater, ils auraient ainsi le mot de passe de tous vos comptes en un coup ! Cela vous fera donc plusieurs mots de passe différents, faites-vous par exemple un petit carnet des mots de passe si vous avez du mal à les retenir.

Ne donnez le mot de passe de votre PC à personne. Le fait de donner soi-même son mot de passe paraît absurde ici, mais les techniques de manipulation sont prévues. Exemple : si quelqu'un vous demande "Donne ton mot de passe s'il te plait, je regarde juste un truc rapidement…", cela vous met la puce à l'oreille, vous ne donneriez pas votre mot de passe. Mais :"Bonjour, je suis le responsable informatique de l'entreprise SuperMegaAntiVirus, j'ai besoin de votre mot de passe pour mettre votre système à jour et vérifier vos coordonnées client, celui-ci ne sera pas partagé et vous pourrez le changer ensuite." C'est une approche typique pour le phishing[3]. Que ce soit dans vos emails ou sur les réseaux sociaux, dès qu'un lien vous paraît louche, ne cliquez pas, peu importe qu'il vienne d'une personne que vous connaissez bien ou non. Les cybercriminels utilisent souvent de faux emails, prenant le nom de banques ou autres organismes, où il faut cliquer sur un lien pour réaliser une opération importante. De plus en plus de cas d'infections via des liens partagés par les réseaux sociaux sont observés, restez donc très vigilants.

Comment discerner ces attaques par usurpation (« spoofing attack »)? Soyez attentifs. Avant de cliquer sur un lien ou d'ouvrir un fichier joint, regardez l'adresse utilisée par l'expéditeur. Si vous recevez un email soi-disant de votre banque, mais que l'adresse est « hickso567@chip.mal », il est certain que c'est un spoof. Faites également attention aux extensions des fichiers. L'extension d'un fichier, c'est une sorte de suffixe, que l'on trouve après le nom du fichier, afin de définir son type. Ainsi, les images ont des extensions .jpg, .gif, .png, les fichiers d'installation sont en .exe, .msi, etc. En activant la fonction "Afficher l'extension des noms de fichiers", vous pourrez mieux percevoir si un fichier est malveillant. Souvent, l'extension ne correspond pas à la description du fichier (par exemple, un mail prétend vous envoyer une image, mais le fichier porte l'extension d'un fichier d'installation, comme .exe). Dans tous les cas, méfiez-vous des extensions .exe, .vbs et .scr si vous n'avez pas demandé l'installation d'un programme. Vigilance constante !

Étape 4 : Faire des sauvegardes régulières

L'idée est simple : toutes les données que vous ne voudriez jamais perdre ou qui sont importantes à vos yeux doivent être sauvegardées en dehors de votre ordinateur. Sauvegarder dans le Cloud est une possibilité, à condition de chiffrer votre contenu avant de l'envoyer (via une archive protégée par mot de

[3] Le terme **phishing** désigne une technique utilisé par des escrocs sur internet pour obtenir des informations personnelles. Les escrocs se font souvent passer pour un organisme de confiance (organisme bancaire, Paypal, eBay, Amazon ...), dans le but d'obtenir des données confidentielles. Selon les données récoltées (informations bancaires, identifiants de connexions ...), les escrocs peuvent par exemple réaliser des virements bancaires sur leurs comptes ou se connecter à un site pour envoyer du spam (*emails non sollicités*).

passe par exemple). Une autre possibilité, fortement recommandée, est de sauvegarder sur un disque dur externe. Au moment où cet article est écrit,

Étape 5 : adopter un comportement prudent en général

Effacer votre cache Internet et votre historique de navigation
Lors de vos passages sur Internet, vous êtes amenés à livrer des informations personnelles comme votre état civil ou vos coordonnées postales et téléphoniques. Les navigateurs conservent par défaut ces données. Il est alors bon de savoir effacer ses traces sur Internet et notamment, lorsque vous utilisez l'ordinateur portable d'un proche ou l'ordinateur de votre entreprise par exemple.

Éviter de télécharger sur les réseaux P2P
Le peer to peer, ou pair-à-pair permet de partager divers contenus. Musique, films, logiciels, jeux... Autant de fichiers téléchargeables qui peuvent renfermer des virus. Toute une panoplie de logiciels malveillants peut ainsi envahir l'ordinateur des utilisateurs de ce type d'application. Un seul moyen pour réduire cette vulnérabilité : proscrire l'usage des réseaux P2P !
Utiliser les paramètres de confidentialité de son navigateur Internet
Les hackers peuvent, pendant votre navigation sur le net, faire en sorte de récupérer vos données personnelles et ainsi vous envoyer des messages ciblés, voire usurper votre identité. Afin d'éviter l'exploitation de vos informations, vous devrez utiliser les paramètres de confidentialité inclus dans votre navigateur.

Clés USB

Si vous utilisez votre clé USB sur un autre PC, faites d'abord un scan, une analyse de votre clé avec votre anti-virus avant de l'ouvrir (pensez aussi à désactiver si nécessaire l'ouverture automatique des clés USB sur votre PC).

Que ce soit dans vos emails ou sur les réseaux sociaux, dès qu'un lien vous paraît louche, ne cliquez pas, peu importe qu'il vienne d'une personne que vous connaissez bien ou non. Les cybercriminels utilisent souvent de faux emails, prenant le nom de banques ou autres organismes, où il faut cliquer sur un lien pour réaliser une opération importante. On appelle cela le phishing. De plus en plus de cas d'infections via des liens partagés par les réseaux sociaux sont observés, restez donc très vigilants.

Prendre le temps de rechercher sur Internet lorsque vous n'êtes pas sûr(e) : une simple recherche Google permet parfois d'éviter une attaque inopinément !

Ne pas se connecter à des **réseaux Wi-fi publics** ou sur un ordinateur public pour effectuer des transactions importantes (bancaires)

Malgré toutes ces précautions, le risque 0 n'existe pas…

Si vous constatez un comportement bizarre (affichages de fenêtres non-désirées, ralentissement considérable, programmes inconnus qui se lancent), coupez immédiatement la connexion à internet et lancez l'antivirus. Il arrive qu'une fois le virus installé sur la machine, l'antivirus ne puisse plus le bloquer. Le plus simple est alors de chercher un point de restauration, afin de revenir à un état antérieur, non-infecté du PC. Si cette opération est impossible, rendez-vous chez l'informaticien du coin, ou faites une remise à zéro de l'ordinateur, si votre back up est récent.

Sources :

https://www.leblogduhacker.fr/comment-proteger-son-pc/
http://glossaire.infowebmaster.fr
http://pratique.leparisien.fr/conseils-high-tech/informatique/ordinateur/comment-proteger-son-ordinateur-des-virus
https://www.rtbf.be/info/medias/detail_comment-proteger-au-mieux-son-ordinateur-des-ransomwares-et-autres-virus?