Avira : Comment mieux protÃ©ger son ordinateur en 10 Ã©tapes
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 31/10/2013 14:00:00

L'expert en sÃ©curitÃ© Avira promulgue ses conseils aux acquÃ©reurs de nouveaux ordinateurs afin de les aider Ã mieux se protÃ©ger. Voici donc quelques recommandations pour sÃ©curiser son ordinateur et pouvoir commencer Ã l'utiliser et Ã y stocker des informations personnelles sans craindre l'espionnage informatique.

1. (RÃ©)Installer le systÃ¨me d'exploitation de son choix

Si l'ordinateur provient d'une source inconnue, d'un revendeur local par exemple, il est vivement conseillÃ© de rÃ©installer le systÃ¨me d'exploitation. Au dÃ©but de la procÃ©dure d'installation, l'utilisateur est invitÃ© Ã formater le disque dur. Il faut le faire ! Ainsi, aucun programme furtif, rootkit cachÃ© ou logiciel de surveillance ne risque plus d'Ãªtre exÃ©cutÃ©.

2. Installer un logiciel de sÃ©curitÃ©

En installant dÃ¨s le tout dÃ©but un antivirus ou une suite de sÃ©curitÃ©, on est certain qu'aucun logiciel malveillant ne s'infiltrera sur le tout nouvel ordinateur.

3. Installer et configurer un pare-feu adaptÃ© Ã ses besoins

Si le logiciel de sÃ©curitÃ© qui vient d'Ãªtre installÃ© n'inclut pas un pare-feu, il faut en installer un. Il en existe plein de gratuits, mais commencer par Windows Firewall est tout aussi bien. Si le pare-feu propose de bloquer toutes les connexions entrantes (gÃ©nÃ©ralement le plus haut niveau de sÃ©curitÃ© mais qui reste accessible), choisir cette option. Cela permettra d'Ã©viter que quelqu'un se connecte Ã des services ouverts du systÃ¨me d'exploitation potentiellement vulnÃ©rables.

4. Actualiser son systÃ¨me d'exploitation et tous les logiciels

L'installation des derniÃ¨res mises Ã jour permet de renforcer le systÃ¨me d'exploitation. En installant les correctifs disponibles, cela empÃªche que les vulnÃ©rabilitÃ©s connues puissent Ãªtre exploitÃ©es et corrige aussi les bugs constatÃ©s dans les versions antÃ©rieures. C'est Ã faire systÃ©matiquement pour tous les logiciels installÃ©s.

5. DÃ©sinstaller tous les services ou fonctions du systÃ¨me d'exploitation et des logiciels qui ne sont pas utilisÃ©s

Cette Ã©tape s'inscrit aussi dans la procÃ©dure de renforcement du systÃ¨me d'exploitation. Ce faisant, la potentielle zone d'attaque de l'ordinateur est rÃ©duite. En effet, moins il y a de logiciels qui tournent, moins il y a de points d'infiltration pour des attaques.

6. Utiliser un mot de passe compliquÃ© Ã deviner

Toutes les mesures prises jusqu'ici ne servent Ã rien si n'importe qui a librement accÃ¨s Ã l'ordinateur, ou si le mot de passe est facile Ã deviner.

7. Utiliser un compte non administrateur

En utilisant un compte sans autorisations, ni droits particuliers, les risques d'endommager les logiciels installÃ©s sur l'ordinateur, y compris le systÃ¨me d'exploitation, sont limitÃ©s.

8. SÃ©curiser le navigateur

Le navigateur est probablement le programme que l'on utilise le plus sur un ordinateur, suivi par le client de messagerie. Pour renforcer sa sÃ©curitÃ©, le mieux est d'installer la derniÃ¨re version disponible et d'en changer les paramÃ¨tres par dÃ©faut. Voici une liste non exhaustive de recommandations :

Â· DÃ©sactiver l'exÃ©cution de code/contenu actif.

Java, les applets ActiveX, Silverlight, Flash, etc. sont des exemples de contenu actif. Ils peuvent Ãªtre dÃ©sactivÃ©s pour tous les sites Web (paramÃ¨tres globaux) ou activer pour quelques sites de confiance uniquement.

Â· DÃ©sactiver le suivi ou tracking

Les navigateurs modernes incluent des fonctions qui signalent aux sites Web que l'internaute prÃ©fÃ¨re ne pas Ãªtre traquÃ©. Si le navigateur ne propose pas ces options, il existe des extensions qui le font. Le module additionnel DoNotTrackMe de la sociÃ©tÃ© Abine est un bon dÃ©but.

Â· DÃ©sactiver les cookies

Mieux vaut ne pas accepter de se faire espionner par des sites Web sans avoir donnÃ© son autorisation. LÃ encore, il y a des paramÃ¨tres appliquÃ©s par dÃ©faut Ã tous les sites ou au cas par cas. Il existe aussi des modules additionnels pour tous les navigateurs.

9. VÃ©rifier que la connexion au rÃ©seau Wi-Fi est sÃ©curisÃ©e

MÃªme si ce sujet mÃ©rite un article Ã lui seul, voici quelques rÃ¨gles de base pour protÃ©ger son ordinateur et tous ses autres terminaux :

Â· ProtÃ©ger le rÃ©seau par un mot de passe

Â· Changer l'identifiant SSID par dÃ©faut

Â· Changer les paramÃ¨tres par dÃ©faut pour renforcer le degrÃ© de sÃ©curitÃ©

Â· Choisir un algorithme de chiffrement, comme WPA2-AES ou TKIP.

10. Ne pas perdre de vue la sÃ©curitÃ© pendant l'utilisation de l'ordinateur

Ce sujet est aussi suffisamment complexe pour qu'on lui consacre un article, voici cependant quelques rÃ¨gles de sÃ©curitÃ© de base :

Â· Ne pas installer de logiciels provenant de sources inconnues ou en qui la confiance n'est pas totale

Â· Ne pas exÃ©cuter les piÃ¨ces jointes aux e-mails

Â· Ne pas visiter de sites Web inconnus ou suspects

Â· Ne pas installer de codecs, visionneuses ou autres programmes qui font des promesses sortant de l'ordinaire. La plupart du temps, ce sont des programmes malveillants.

Plus d'informations.