Title:
Protect Your Notebook from Spyware and Viruses

Word Count:
616

Summary:
Notebook computers bring a tremendous convenience to personal computing. Just
sit within range of a wireless hotspot and you can connect to your office or
home network, access your email, and complete important projects for work.
However, roaming from one unsecured wireless network to another can leave your
computer vulnerable to malicious software attacks.

Keywords:
virus scan,spyware,virus protection,laptops,notebooks

Article Body:
Notebook computers bring a tremendous convenience to personal computing. Just
sit within range of a wireless hotspot and you can connect to your office or
home network, access your email, and complete important projects for work.
However, roaming from one unsecured wireless network to another can leave your
computer vulnerable to malicious software attacks.

Spyware and Viruses

If you are connected to a wireless network without its own firewall, hackers can
easily intercept the signals you send and receive across the airwaves.
Malicious individuals can also install spyware and viruses on your computer.

Spyware refers to an application designed to track a computer user's internet
activities, keep note of sites visited, and gather other information. The term,
"spyware," can also refer to any non-viral malicious software, including
software that takes over your internet connection, pops up unwanted
advertisements, or even blocks your internet connection. A tracking program is
technically labeled as spyware only if the computer user does not consent to the
download or installation.

Spyware collects information and sends it back to the spyware controller. The
owner of the spyware program usually sells gathered information to marketers.
For instance, spyware can get a computer user's email information, using that
information to bombard the user with advertisements and spam. Spyware is also

known as "malware" (Malicious Software), as it can be used to aid identity theft and fraudulent activities (some spyware programs mine credit card information and other sensitive financial information). Keylogging programs, used to steal credit card information and passwords by monitoring everything a user types, fall under the umbrella of spyware/malware.

Viruses are another type of malicious software. A virus is a piece of code that attaches itself to a program, a file, or your boot sector. These malicious programs are called viruses because they work much like a viral infection – they spread to other files, programs, and even computers, and they are designed explicitly to damage your files and destroy your applications.

Protecting Your Notebook from Spyware and Viruses

Protecting your notebook computer from spyware and viruses protects you against fraud and protects your privacy, too.

The first thing that you need to do is install a secure web browser. Internet Explorer is particularly vulnerable to unauthorized scripts which could be run and installed on your computer without your knowledge. Instead of using Internet Explorer, you can try using Mozilla Firefox, one of the most secure web browsers around. Firefox will always inform you about any download or installation, inform you about suspect sites, and update your browser automatically to continually improve security.

Aside from using Firefox, it is important that any computer user install a personal firewall to block unauthorized access attempts. For Windows XP users, Comodo Personal Firewall is a free option (there is an Alpha version of Comodo Personal Firewall Version 3, which adds Vista support, but this would not be a stable option until they reach the final release). Even the best firewall can sometimes allow spyware through, however, so scan your computer with a free program like Spybot: Search & Destroy or Ad-Aware SE, two of the very best anti-spyware programs available. You should not neglect to install anti-virus software, too. If you have an anti-virus program you already use, stick with it, but the free home edition of Avast and the open-source (free) anti-virus product ClamWin are two excellent options. Be sure to keep your security software updated (most programs will automatically update themselves, but they will sometimes prompt you for your permission) to give yourself the very best protection against malicious software.

This article may be republished freely as long as this copyright notice and box of resource links are included at the bottom.

Copyright © 2007 MALIBAL, lLc