

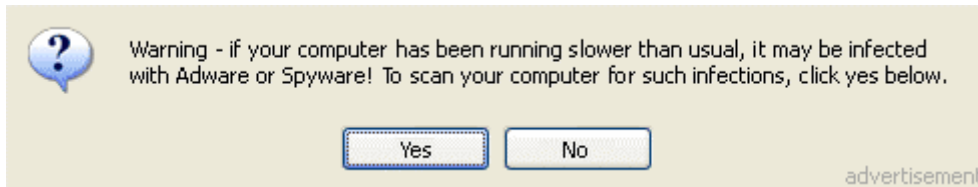
Spyware, Keep It Out

One day you innocently click on the Internet Explorer icon and a search page comes up on the screen that you have never seen before. You try to change it back to your regular home page but it won't let you. Or, your front office person is trying to check in a patient and pop-ups keep opening on her computer that cannot be closed essentially preventing her from typing. Or, all of the sudden your billing computer won't connect to the Internet or network at all. Most people have experienced one of these scenarios either at the office or at home or know someone who has as they are becoming more and more common. The cause behind most of these issues is a type of software called spyware or malware. This software has loaded itself onto your computer, usually without your knowledge, and sets itself up to run in the background any time your computer is started up, or booted up. Generally, its intent is to track your browsing habits and report back to a "mother" server, however it can sabotage your computer to the point that your only option is a complete reload of the operating system.

Spyware can embed itself on your machine using a variety of techniques, but the most common ones are: free offers, peer-to-peer file sharing networks, email, and flaws in your operating system.



The Olsen Twins starred in which show?
Answer to get **FREE** movie tickets for a year!
 [Step by Step](#) [Full House](#) [Family Ties](#)
©2005 EveryFreeGift.com © 2005 AnyFreeGift.com



? Warning - if your computer has been running slower than usual, it may be infected with Adware or Spyware! To scan your computer for such infections, click yes below.

advertisement

Every time you click on a banner ad on a webpage, you are accepting the End User License Agreement for whatever software is attached to that ad, which, of course, is not disclosed to you. Examples of peer-to-peer file sharing networks are mostly music based – KaZaa, Morpheus, gnuella, Grokster. Spyware programs generally pay to bundle themselves with these networks. Free email cards may seem innocuous but in reality they too are not really "free". In essence the receiver has to go to a website to open the card, thus accepting the EULA and opening the door for the spyware. Typosquatting works in conjunction with unpatched operating system flaws and is the practice of preying on misspelling and mistyping on website names such as googkle.com or firstnationa1.com. All you have to do is open the site for a split second and code will run to check your machine for particular flaws where the programs can enter. It is a fact of life that all software is released with flaws, and Microsoft operating systems are no exception. Unscrupulous software developers are continually testing operating system code for new ways to exploit it. Also, Internet Explorer is built into the operating system itself so it is the vehicle of choice for hiding downloads.

Antivirus companies have traditionally shied away from scanning for spyware programs because there are big advertising dollars that fund its

WINNER!
WINNER!
WINNER!

You just
WON
FREE*
gas for
a year!

[Click here
to claim!](#)

*See offer details.
© 2005 EveryFreeGift.com

existence and pay to bundle it with legitimate sites. Those antivirus companies that have added a few spyware programs to their scans have generally been served threatening legal letters from the spyware firms. Computer Associates has been a leader in the anti-spyware front, having developed scanning and removal software as well as an extensive spyware database – with over 28,000 spyware programs listed. Microsoft has also entered into the fight against spyware with its free download of a beta anti-spyware tool.

Since spyware is so ill-defined, there are more bogus spyware removal tools than legitimate ones, so it is important to purchase anti-spyware tools from a reputable brand name such as Trendmicro, Computer Associates, Panda, or Webroot. There are only a handful of free tools that actually work such as Spybot (www.safer-networking.org) and Ad-aware (www.lavasoft.com). It is also important to remember that you may need to run at least 3 different tools since each company defines spyware slightly differently. Keep in mind that spyware developers are continually updating their software to make it more difficult to uninstall just as fast as anti-spyware developers are writing tools to remove it.

A few tips to keep unwanted software out of your machine: 1) always run security patches for your operating system when they come out, 2) upgrade old machines to Windows XP (old operating systems such as Windows 98 are no longer patched by Microsoft), 3) consider using an alternate browser such as Mozilla, Opera, or Netscape, 4) don't be a sucker for "free offers" – remember if it sounds too good to be true, it probably is, and 5) always have a good, complete, removable backup copy of your data.

For more information regarding spyware prevention and removal, please contact Carin Slader at cslader@mdserv.com or 864-297-8889.