

How to Protect Yourself from Malware

Malware is the broad term that computer security experts use to describe any type of software created to cause specific damage to a computer system or circumvent the security of a computer system. This includes the wide array of software types that we occasionally hear about in the press such as viruses, worms, Trojans, spyware, etc. Because these programs can cause damage to your computer system, infect other computer systems and possibly leave your personal information at risk, it is important to know how to identify and get rid of potentially dangerous programs before they can cause too much damage. There are three things most computer security experts would recommend you do in order to protect yourself from malware.

First, you should invest in a good firewall for your computer, especially if you use a broadband connection (cable modem, DSL, fiber optic or satellite connection) and have a computer that is always connected to the internet. If you use WindowsXP, you likely already have the Windows Firewall already built in. A good firewall will keep unauthorized users from gaining access to your computer from the outside and will keep programs on your system from communicating through to the outside without your permission. Most anti-virus programs come as a suite of programs, including a firewall so you should check to see if you have one of those in lieu of the Windows firewall. Finally, you can download free firewall software such as ZoneAlarm or, if you have a broadband router, it probably has a firewall feature built into the hardware.

Second, you'll need to be sure you're running an anti-virus program and that it is kept up-to-date. Yes, this means you will probably have to pay for a new license each year in order to keep getting the updates, but this really comes out to be about a few cents a day. In order to keep it updated, you should schedule automatic updates to occur at a set time or whenever the program detects new updates available. While it's important to keep your system up-to-date, it's better if it doesn't have to be one more thing on the to-do list. Automatic updates will take care of that so you can set it once and just move on.

Third, you should get a good spyware remover program. This might be a feature of your current anti-virus program but check that out and don't assume that's the case since many don't have this feature. A dedicated spyware remover will either detect/remove potential spyware whenever you run it or will also add the feature of monitoring programs as they run to prevent future installations of spyware. This is called real-time protection and is the best option for most users, again focusing on a set-it-and-forget-it type of solution. The spyware remover should also have the ability to auto-update, similar to what we recommended for anti-virus programs in the previous section.

With these three items, you should be well protected against malware of all sorts. The last piece is getting a better understanding of spyware, adware and other malware threats. With a good understanding of the threats and by knowing good security practices and computing habits, you can likely avoid coming into contact with malware and rely on your software tools as a backup (hey, we all make mistakes, right?).

Source: <http://www.articlecircle.com>

About the Author

For a limited time, get exclusive access to our anti spyware mini-course - protect yourself from this growing threat. A \$29.00 value, yours free if you sign up now. Visit: <http://www.fastspywarehelp.com/minicourse>