

Viruses, adware, trojan horses, worms, spyware, spybot, nagware are names that can be referred to as a group as malware. Any computer connected to the Internet can easily be infected if not using a protection program and sometimes even then. This includes email as well as web browsing. PCs are especially vulnerable because they make up the vast majority of computers in use today. The bad guys apply their evil where they can do the most harm.

Although I sometimes face hardware problems, most computer problems here in Sun City are related to malware. Symptoms are slower and slower response and unwanted advertising popups. Some warn of computer problems and offer downloads to solve problems. Never, ever accept these offers because they lead to additional malware infection. Don't even click on a button to close the popup because the button may be labeled "Close" but it really means "OK". Instead, press Control+W or Alt+F4 to close the window.

The following will give some idea of what a technician will do to search for and destroy malware. Be very careful with these powerful methods so as not to delete something important to your system. If you do not know for sure what something is, do not delete it.

-- Go to the Control Panel and double click on the Add or Remove Programs to get a list of installed programs. Delete anything having to do with malware prevention except for your main antivirus program. Many of these are malware themselves in disguise. I hate the McAfee program and am not hot on AVG either although the Computer Club endorses AVG. Both of these antivirus programs consume huge amounts of CPU power. The Norton Company provides terrible user support. I usually delete Norton, AVG and McAfee.

-- Sometimes a malware program will not allow itself to be defeated because it is running a process to prevent such deletions. This is when I'll use the Windows Task Manager tool to stop the process and then again use the Control Panel to delete the trouble maker. Press Ctrl+Alt+Del keys at same time to bring up the Task Manager, but please be careful with its use.

The trick is figuring out which process from the displayed list belongs to a malware program. Many have cryptic, strange names. Some have names seemingly reasonable for Windows. If I do not recognize a process name, such as apdproxy.exe, I'll look it up on Google that shows apdproxy.exe belonging to an Adobe Photoshop Album organizer. Oops! Glad I did not delete that one. How about xpa.exe? Yes, that is a rogue security program.

-- Sometimes a malware program is smart enough to disable the Task Manager and disallow the installation of a virus checker. This is when I'll bring out tools such as Process Explorer <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx> or HijackThis [http://www.trendsecure.com/portal/en-US/tools/security\\_tools/hijackthis](http://www.trendsecure.com/portal/en-US/tools/security_tools/hijackthis). Be very careful to positively identify offending processes before using these powerful tools.

-- Lastly, I'll install the highly acclaimed free Avira antivirus program from <http://www.avira.com/en/pages/index.php>. It is fast without taking a lot of CPU power. I've been amazed at what Avira finds even after competitors have made their sweeps. On one client that had been attached to high-speed Internet four years without any kind of protection, the \$40 per year Norton found and removed 156 infected files. Then I ran Avira that found almost a hundred more and solved the original problem.

There are many more techniques for defeating malware, but I hope you get the idea.