

Rogue Security Programs

[caption id="attachment_1583" align="alignleft" width="248" caption="Spring has



sprung in Southern Oregon."]

[/caption] Had a client

come to me and tell me he had a bad problem with his computer. It was an easy diagnosis. It was a "rogue" security program. A program that installs itself from various websites and software and then runs itself, takes over your computer, and swears you have a virus and other various problems. Problem is, he didn't have a problem until this program came along. This particular client did not want his machine formatted and the system software(s) reinstalled. Which is ashame. It's the fastest and most cost efficient way to handle it. In my (not) so humble opinion the only proper way to handle the problem. However, yes, I was able to rid the machine of the software. It took many hours, lot's of scanning, and then some services needed to be turned back on, and corrupted files needed to be rebuilt. Literally, four days worth of work. Why this "rouge" security program is not classified as a virus is beyond me. It installs trojans, takes over the machine, and basically strong-arms the PC user into paying for services that were not needed until it came along. My client was most certainly willing to pay, as a lot of folks are, to just get his computer back. Problem is, after you pay, things don't usually go back to being normal. You still pay someone like me to get rid of the dirt! There are several ways to help keep this "rouge" (Vista Antispyware 2007, was the name, though it has many) from visiting you. Keep in mind that, good habits can help lessen the damage. 1. **Back up, Back up, Back up.** Regardless of anything that happens along the way, if you back up your files to a drive that it not attached to the machine (external, thumb, flash, etc.) then at least you've got those saved and you won't worry so much about loosing data. 2. When checking email only open attachments from someone or a company that **YOU KNOW and TRUST.** 3. **Always** run an Anti-virus program. There are a few good **FREE** ones out there available. Microsoft Security Essentials is **FREE!** ([download here](#)) 4. Run a program called **Malwarebytes** (an anti-malware program) on a regular basis. Depending on your usage, perhaps at least once per week. There is really no excuse, there is a **FREE** version. ([download here](#)) 5. **NEVER** use TORRENT (or other peer to

peer networking) programs. Look the truth is, if you are using this program there is a really, really GOOD chance you are downloading illegal software, music, or photos. It is a perfect way to get a virus. If you want a virus, just keep using it. If what you are doing is actually legal, then only download from known, & trusted people. Personally, I **NEVER** use them. 6. Only download software from known and trusted sources. I use CNET (download.com), Tucows, and a couple other places. Or I don't download. Games are notorious for containing viruses and malware. Think twice, and think about buying the game off the shelf where it is more than 99.9% chance it is virus free! Be prepared, that in the case this virus does catch up with you, that you are ready to have your hard drive wiped and all software reinstalled. If you are not ready for that, then you are not ready to have a virus. Have a great day!! Peg