



Fake Anti-virus and “Scareware”

If you own a Windows PC, and have connected it to the internet, we can say with relative certainty that you have had a virus at one time or another. Recently, the most common type of infection that we have seen is the Fake Antivirus, or “Scareware” infection. This is software that appears to be beneficial by popping up alerts alerting you that you have a virus infection and offering to clean your PC. In actuality, this software is a virus, and in most cases is responsible for the infection itself. The designers of these rogue security software packages create legitimate looking alert windows that pop up and tell you that your PC is infected, or at risk. Some other symptoms may include:

- 1) Alerting a user with the fake or simulated detection of malware or pornography.
- 2) Displaying an animation simulating a system crash and reboot.
- 3) Selectively disabling parts of the system to prevent the user from uninstalling them. Some may also prevent anti-malware programs from running, disable automatic system software updates and block access to websites of anti-malware vendors.
- 4) Installing actual malware onto the computer, and then alerting the user after “detecting” them. This method is less common as the malware is likely to be detected by legitimate anti-malware programs.
- 5) Altering system registries and security settings, then “alerting” the user.

The underlying purpose of these viruses is to generate revenue. So, once installed, most of these rogue security software packages will try to scare you into thinking your PC is severely infected, and offer to fix it for you if you simply upgrade to the paid version. Of course, once you have paid them, the infection actually does nothing but get worse.

There are several ways to get infected with one of these rogue security packages, and the methods continue to evolve as time passes. Browser toolbars, email attachments, multimedia codecs, P2P software downloads, and free online scanners are just some of the ways to get infected. More recently, malware distributors have been using Search Engine Optimization (SEO) poisoning techniques to push infected URLs to the top of search engine results about recent news events. People searching for such articles are redirected to a series of sites before arriving at a page that says their machine is infected and pushes a download to a “trial” of the rogue security software. Some distributors may actually claim to give a portion of their proceeds to a charitable cause to ease the mind of the potential victim.

Once you are infected, the symptoms tend to get progressively worse, slowing your PC down and interfering with normal operations until the PC is completely un-useable. For the most part, this type of infection is not easily cleaned, and generally requires advanced tools and techniques to completely remove the virus. Sometimes a system restore will make the PC accessible, and then further scans can remove the infection. However, most of the time the hard drive has to be removed from the PC and hooked up as a slave drive to another clean PC to be scanned and cleaned fully. If you suspect you have this type of infection, the best course of action is to stop using the PC and immediately call the 4IT Helpdesk for assistance.

By: Brian Small, Helpdesk Manager

4IT, Inc.

305-278-7100

<http://www.4it-inc.com>

