

Tricks of the Trade: Cleaning up your PC in a few easy steps!

By: John R. Rohrbaugh, GISP
GIS/IT Analyst for the
Yakima Valley Conference of Governments
Newsletter – May 2010

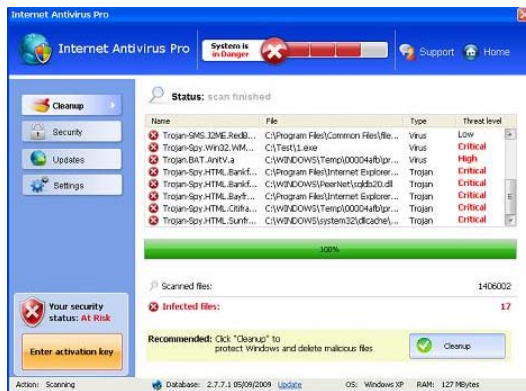
Nothing to me is more interesting than maps, mapping technologies, and location based or aware services, this is why I always write about them. However, unless my computer is running like a champ, my mapping software may not load and I'll be as directionless as a compass with needle! For this reason, I decided to offer up one possible solution to the myriad of issues that can crop up on a Microsoft Windows PC. If you happen to own and operate an Apple product instead, save this information and impress your Windows using friends with your Windows fix-it skills!

Have you recently been surfing the internet and had a window pop up that looks VERY much like a warning from Microsoft? Did this window tell you that your computer MAY be infected and you should click on the window to start a scan? Did you click the window and were then besieged by pop-ups that would not go away warning you of infections that would not go away unless you purchased one product or another? Have you let your children put a USB memory stick in your computer that they had been using on a school computer with limited anti-virus capability? Suddenly your own virus software runs amok telling you that you are infected? I have experienced this frustration on numerous occasions! There are MANY pathways by which your computer can get infected by nasties such as trojan horses, worms, and viruses. In addition, there are any number of methods to remove said infections and a large number of companies that will sell you a product to clean your system. In addition, there are many people, such as myself, who would gladly clean your system for you, or re-install Windows, for a fee. Thankfully, there is one method you can use on your own before you run out to spend great heaping wads of cash, the Microsoft Windows Live OneCare Safety Scanner. This scanner will diagnose and attempt to clean up infections and other operating system issues remotely!

I know what you are thinking: "But I already have a virus scanner that I've bought and paid for and paid a subscription fee to maintain! Why didn't it catch the problems I'm having now?" This question can be hard to answer. First: Are you making certain (even on a daily basis) that your anti-virus 'signature' files (those patches that give the software information about new viruses in the wild) are up to date? If you have then the likely explanation is that many pieces of software that will find or catch viruses simply are not made to find and fight other "malware" such as spyware, adware, Trojan horses, etc. In addition, the people writing these nasty programs are becoming just as skilled at 'coding' their software as most commercial software engineers. They will often buy copies of the latest anti-virus / anti-spyware packages to actually test their "software" out with to see if they can hide it from detection! One statistic I read actually stated that the most popular anti-virus software packages on the market have an 80 PERCENT miss rate!

So what is any self-respecting computer user to do? The first thing you can do is to obviously have one of the several anti-virus software packages installed and up to date

on your system. Although they DO miss SOME of the viruses, the DO catch plenty others. This is your ‘first line of defense’. The next thing that gets repeated as often as most bad jokes: do NOT click on attachments in your email messages if you are not expecting the attachment or do not recognize the user. When in doubt, delete the message, then contact the sender and ask them if they actually sent the message to you and ask what its purpose was. No one is going to fault you for keeping your system safe! The final key safety recommendation is to NOT click on any window that might pop up on your screen when you are surfing the internet that purports to be a Microsoft Windows notice from Microsoft. There are MANY rogue ‘security’ products that are in fact malicious software products which may look something like one of these:



So what are you to do if you ARE infected or believe you MAY be infected? Your first step is to open your anti-virus software and run a full scan. If that doesn't seem to be working, a method that has worked for me has been to run the Microsoft Safety Scanner that I mentioned earlier.

For the complete instructions to how to run this scanner for your system, go to the YVCOG web page for the full version of this column! This will provide you with step by step instructions and screen shots for how to use the scanner. Good luck and don't forget to practice safe computing!

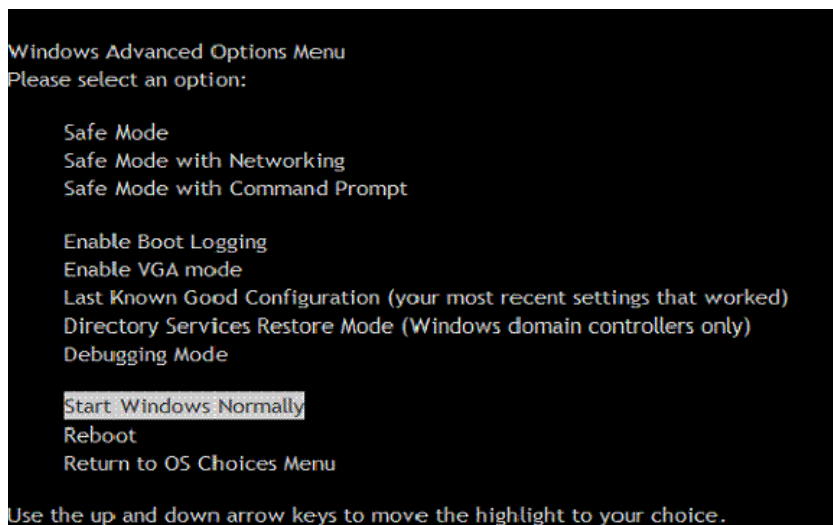
If you are still reading this, then you have come to this column through the web page link. As promised, below are the instructions for using the Microsoft One Care Live Safety Scanner, to review and hopefully fix your computer system.

The scanner mentioned above work while your computer is online. That said, you need to (preferably) have an active connection to the internet either through your office or a broadband connection at home. Here are the steps to take in order to scan and clean your system using the OneCare Safety Scanner:

- 1) Start up your computer 'cold' (from an off state).
- 2) When you see your computer manufacturer's 'splash' screen, hit the 'F8' key (I usually strike it a few times, often out of aggravation but logically to make certain that my selection is registered by Windows and the often finicky keyboard buffer! Here's an example of the 'splash' screen I'm referring to:

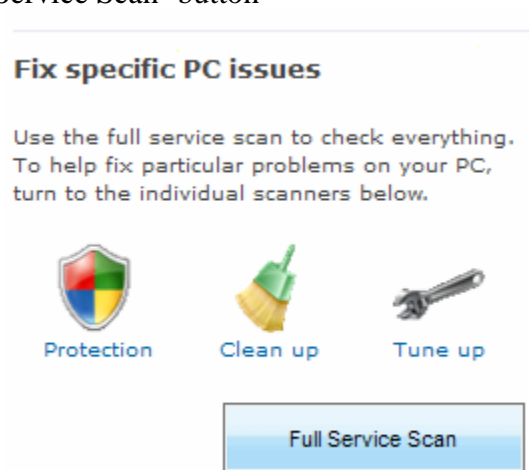


- 3) Hitting the 'F8' key brings up the Windows Boot Menu. At this point, select the option for 'SAFE MODE WITH NETWORKING'. Safe Mode allows Windows to function without a tremendous amount of operating system services that run in the background. In addition, many of the malicious programs also do not load in Safe Mode. Here is an example of the boot menu you will see after striking 'F8'.

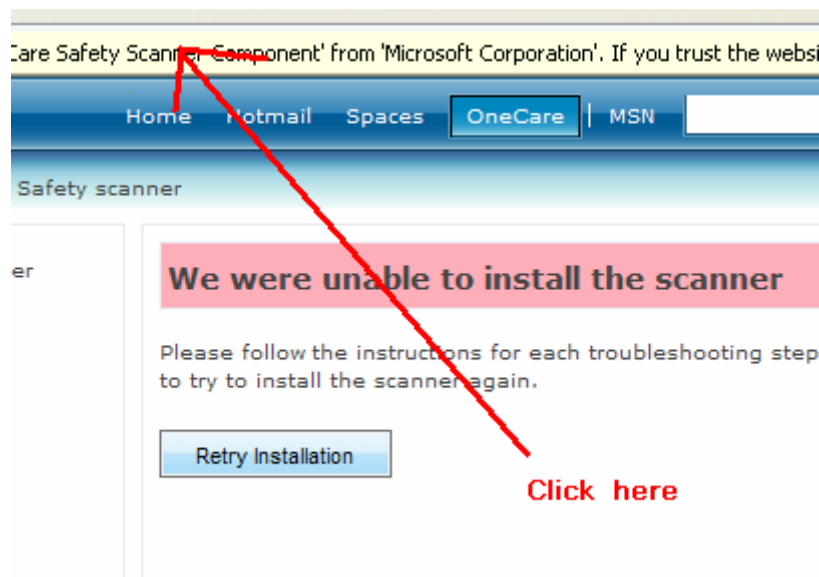


Your computer screen will then fill with computer gibberish as it loads the minimal version of Windows. You will then be required to log in with an administrator account. If this is your home system, your own personal account will do just fine as you are likely and 'administrator' on your own system! Windows will then warn you that you are running in 'Safe Mode' and ask if you want to proceed or use 'System Restore.' At this point, simply select 'YES'.

- 4) Once Windows has finished loading, it's time to fire up Internet Explorer and head to the Scanner web site: <http://onecare.live.com/site/en-us/default.htm> You will note additional information on the site for FireFox users or users of Windows Vista or Windows 7.
- 5) Select the 'Full Service Scan' button

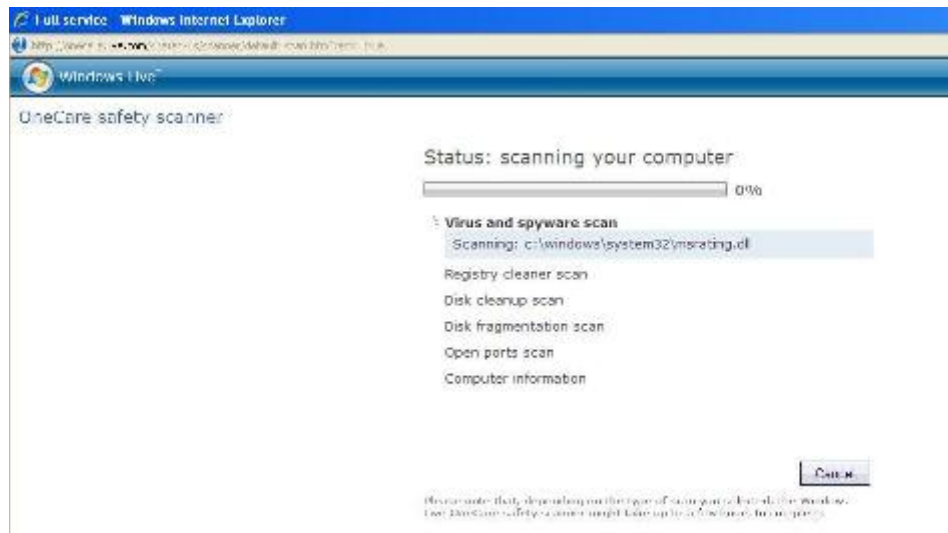


- 6) Of course, you will then need to accept the Agreement. Once you have done this another window will appear. Select to install the scanner. If you get an error stating that the scanner was not able to be installed, then you need to accept the install by clicking on the browser's 'notification bar' and choose to 'install the Add-on' as follows:



From here, another Security Warning dialog box will come ask whether you would like to install the software. Select 'INSTALL'. FINALLY, after much cranking on the part of your system, select the magic 'LAUNCH SCANNER' button which will once again, require you to click on the information bar and choose to run the Add-on (too much security is seldom a bad thing, right?).

- 7) After clearing all the security hoops, choose to run a 'Complete Scan' when prompted. Scan tools will then download and run. At this point, you can sit back and enjoy a cup of coffee, tea, or other beverage that could take a while to enjoy, due to the length of time the scanner takes to run. It may even take long enough to walk the dog or make dinner!



As you can see from this screen shot, the scanner is now doing a very thorough scan of your system to include virus and spyware scans, registry corruption, disk utility scans, and scans of potential network vulnerabilities.

When the preliminary scan completes, the software will return a window stating what it has done to clean up your system, and what it recommends. Note that in this example, the system is clean of infection! At this point, I strongly recommend selecting to complete whatever tasks it thinks are necessary to either clean your computer or improve its performance. Complete this task by checking all appropriate boxes and selecting NEXT. Note that this next step may also take a fair amount of time.





When the repair process is complete, the system will finally prompt you to share the information with Microsoft. Although I can think of no personal security information risk in doing this, I always elect not to share scan information with them. This is purely a personal decision.

Finally and at long last, close all the windows and reboot your computer. You should notice quite a change in performance and MOST problems you've encountered with malicious software should no longer plague you!

Please be aware that this may not cure ALL the ills your windows pc is having but it may certainly cure enough to get you back on your feet. When all else fails, be sure to contact your local favorite geek to diagnose any more serious problems!

If you have troubles running this scanner on your system or would like to ask a general computer related question, feel free to contact me at john.rohrbaugh@yvcog.org. I can't promise you that I'll have the time to answer ALL of your questions, but I'll certainly try. Now, back to our regularly scheduled mapping project, already in progress!