

## Beware of Fake Anti-Virus at Work and Home!

Users should be aware of what antivirus they have installed and what the alerts look like. That way, impostors such as this one will be more obvious.

### For UT owned computers -

1-1. Never, ever click on such an alert. Simply shut down the computer and wait a minute before turning it on again. Chances are if you do this, the problem will go away.

1-2. Notify the helpdesk that you just got a fake antivirus popup.

1-3. Email the Information Security team at [its@uth.tmc.edu](mailto:its@uth.tmc.edu) with the following details: your IP address, what website you just visited before the popup, and the time the event happened.

1-4. After rebooting your computer, you notice anything odd in its performance or you see the popup again, contact the helpdesk and Information Security team again.

### For personally owned computers -

Follow steps 1-1, 1-3, and 1-4 as above.

If you see the pop-ups again, or notice any odd behavior or slowness, do the following AFTER creating a 'restore point' and backing up any important data.

2-1. Download Malwarebytes Anti-Malware: <http://www.malwarebytes.org/mbam.php>, and/or Superantispyware: <http://www.superantispyware.com/>.

2-2. Reboot your computer into "safe mode". This is done as your computer is starting up. Begin tapping the F8 key until the Windows Advanced Options Menu appears.

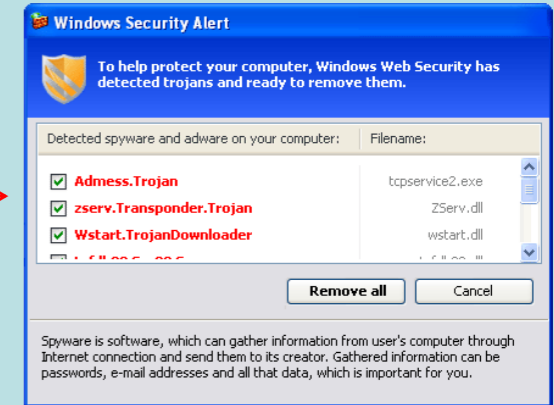
Note: If you begin tapping the F8 key too soon during reboot, you might see "keyboard error". To resolve this, either press a 'resume' key or restart the computer and try again.

2-3. Ensure that the Safe mode option is selected and wait until Windows starts completely.

2-4. Install Malwarebytes and/or Superantispyware and do a full scan. You may want to do a scan with one, then the other just to be safe.

2-5. Reboot to safe mode again and repeat the scan.

2-6. If you see any malware detections that mention "restore" in the file path or keep getting re-infected after cleanup, you will probably need to turn off system restore, then go back to step 2-2 above. Don't forget to turn system restore back on when you're done.



Turning system restore on and off is discussed here:

XP: <http://support.microsoft.com/kb/310405>

Vista:

<http://windowshelp.microsoft.com/Windows/en-US/help/f0688925-5abe-4caf-b49a-018f8cfcaf4d1033.mspx>

Possible network connection loss after malware cleanup is discussed here:

<http://support.microsoft.com/kb/811259>

2-7. Lastly, once your PC appears to be clean, be sure to update your current antivirus and make sure it's running, then catch up on any Windows system patches.

Remember, the Information Security team [its@uth.tmc.edu](mailto:its@uth.tmc.edu) will always be happy to answer any emails about computer security.