

Removal of Malicious Software

Malicious software (malware) includes computer viruses, worms, trojan horses, spyware, rootkits, and other unwanted software. One common example is A360.

One of the latest types of malware is a fake anti-virus or anti-malware. An example is AV Security Suite. If you get a pop-up saying your PC is “infected” and suggests it can fix it be 100% sure the pop-up is from your anti-virus software or anti-malware software. Never go to a pop-up that wants you to purchase a fix!

The following instructions will work for A360, AV Security Suite and some other malware. As malware gets more sophisticated these instructions do not always work. Sometimes additional steps maybe needed. This example uses Malwarebytes' Anti-Malware but there are other good programs out there and the approach to clean the PC would be similar. For additional information on specific malware go to the Malwarebytes' Anti-Malware site (<http://forums.malwarebytes.org/>) and click on “Malware Removal Guides and Self Help Guides.” This will take you to a page with information on a specific malware.

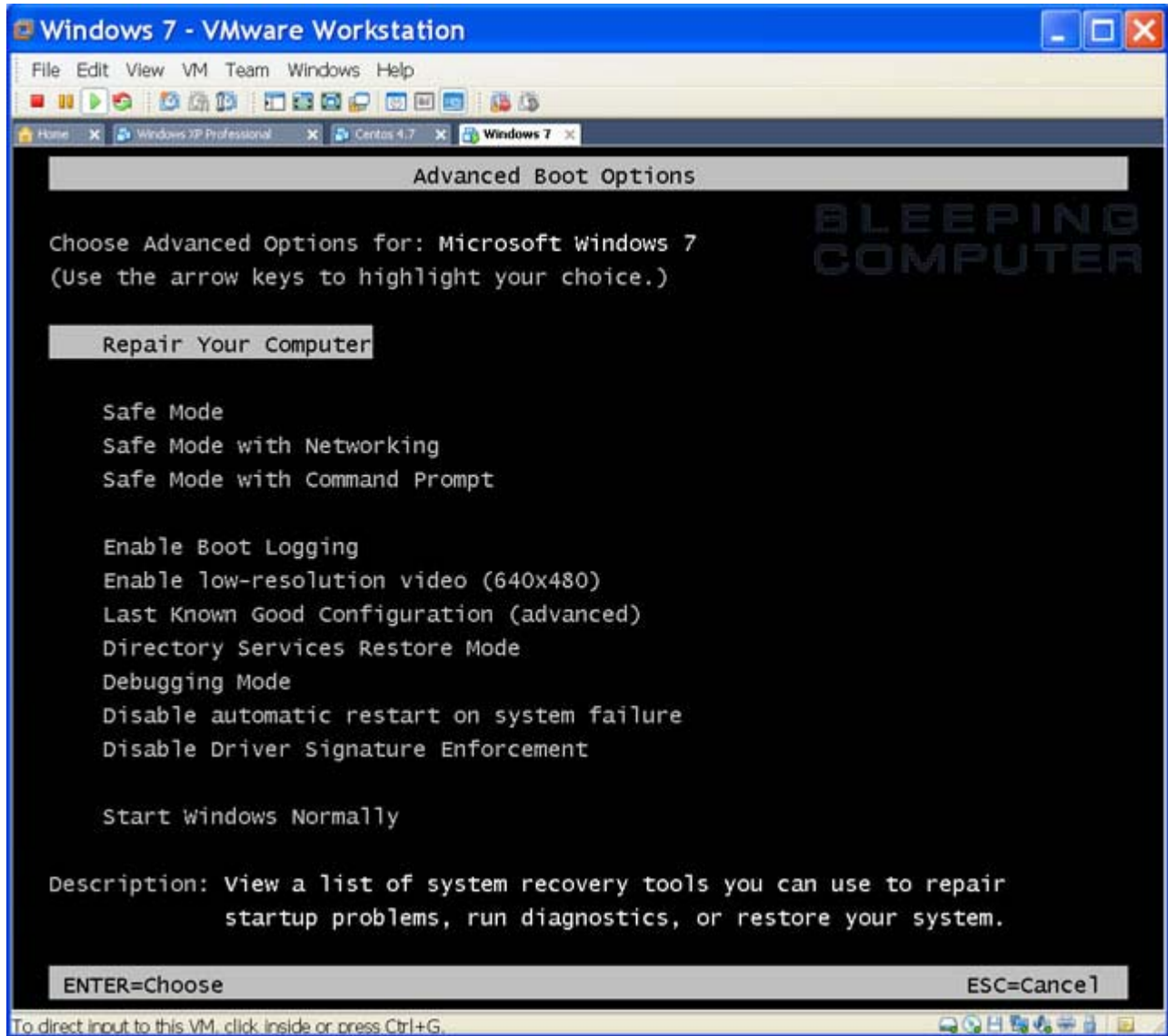
1. Download Malwarebytes' Anti-Malware on a good PC (known to be clean of infection) by entering www.download.com into your browser window.
2. Search for Malwarebytes and skip over the sponsored links until you get to it
3. Download the file (the file is an installation file so do not run it)
4. Rename the file to mph.exe. Some malware can detect programs that will remove it and will not allow anti-malware to be installed. Renaming the file prevents this.
5. Put mph.exe on a thumb drive or CD
6. Boot the infected PC in Safe Mode (see below on how to get into Safe Mode)
7. Copy mph.exe on to the infected PC
8. Run the program mph.exe (this will install Malwarebytes)
9. Once the install completes run Malwarebytes from the desktop icon
10. Do not update the program
11. Make sure the “Scanner” tab is selected
12. Select the “Perform Full Scan” radio button (see the picture below for how the menu should look)
13. Click on “Scan”

14. When the scan is complete click on “Show Results”
15. Make sure everything is checked and then click “Remove Selected”
16. Re-boot the PC in normal mode
17. Re-run Malwarebytes and select the “Update” tab
18. Click on “Check for Updates”
19. Once the update completes click on the “Scanner” tab
20. Click on “Perform full scan”
21. This scan should run without errors



Getting into Safe Mode

1. Turn on your monitor
2. Boot your PC.
3. As soon as you see characters on the screen tap F8 about once a second. On a few PCs you need to tap F5 not F8 (some older HP PCs use F5).
4. You should see a screen similar to the following (it will not be identical)



5. Use the arrow keys on your keyboard to move the highlighted area to "Safe Mode". Note that your mouse will not work.
6. Tap the "enter key"
7. After displaying many lines your PC should come up in Safe Mode. This is identified by the four corners having the words Safe Mode in them.
8. Some experts suggest you do not use msconfig (System Configuration Utility) to get into Safe Mode. The reason is the malware can corrupt the PC so that it can no longer be booted.