

AUDIENCE

This document is for TAG Helpdesk staff and customers.

Note: For TAG Helpdesk staff, the software downloaded below can be accessed using library domain credentials at the following shared drive.

[\\146.229.4.80\utility\\$](\\146.229.4.80\utility$)

If you are experiencing any of the following issues, follow the associated steps to troubleshoot.

COMPUTER IS EXPERIENCING FAKE POP-UPS AND ALERTS

1. Download the free version of Malwarebytes' [Anti Malware](#).
2. Double-click on mbam-setup-[version].exe and follow the installer directions.
3. When the Anti Malware application launches, accept the defaults and click Scan.
4. Wait several minutes. Show Results and remove any found files and close.
5. Restart the PC.
6. Download the free version of Safer Networking's [Spybot Search and Destroy](#).
7. Double-click on spybot[sd][version].exe and follow the installer directions. You can use a wizard to walk through steps before the scan. You will be prompted to back up your registry, search for updates, and immunize your PC.
8. Click Check for Problems.
9. In the results window, click Fix selected problems and close.
10. Download the free version of [Super Anti Spyware](#).
11. Double-click on SUPERAntiSpyware.exe and follow the installer directions. Download any updates.
12. Perform a Complete Scan and wait.
13. Click Next and Finish to quarantine and remove any problems.
14. Restart the PC.
15. If you have not solved the problems, to scan the computer for rootkits and registry infections, download the free version of [ComboFix](#) (You may need to register).
16. To prevent McAfee from blocking any scans performed by ComboFix, disable McAfee On-Access Scanner:
 - a. Right-click the McAfee icon in the system tray.
 - b. Select VirusScan Console.
 - c. Right-click Access Protection and select Disable.
 - d. Right-click On-Access Scanner and select Disable.
17. Double-click ComboFix.exe and click Run
18. The PC will beep twice and a message displays. Make any necessary changes and click Yes or OK.

19. ComboFix may install Microsoft Recovery Console if the computer does not already have it. When the computer prompts you to install it, agree to the EULA by clicking Yes. ComboFix will install the Recovery Console and resume scanning.
20. When the scan is complete, a log report is created for your reference.
21. If Combofix does not automatically restart the PC before preparing the log, close the report and reboot the PC.

COMPUTER IS RUNNING SLOWLY

1. To free up disk space by removing temporary Internet files and cleaning up other unnecessary files, download the free version of [CCleaner](#).
2. Double-click on ccsetup[version].exe.
3. Accept the defaults and click Run Cleaner.
4. To group files together so the computer does not have to look for them, use Windows Disk Defragmenter:

For Windows XP

- a. Click Start > Accessories > System Tools > Disk Defragmenter
- b. Click 'Defragment' (this process may take several minutes).
- c. When process is complete, click Close.
- d. If you see error message "Some files on the volume could not be defragmented," simply click Close.

For Windows7/Vista

- a. Select 'C:' drive.
- b. Click 'Defragment disk' (this process may take several minutes).
- c. If you see error message "Some files on the volume could not be defragmented," simply click Close.

Note: If the PC is still running slowly, follow steps above for running Malwarebytes' Ant-Malware and Spybot Search and Destroy to scan for spyware or viruses that could be slowing down the computer.

COMPUTER HAS BLUE SCREEN OF DEATH (BSOD)

Note: If BSOD gives an error message, search the message in Google to identify solutions. If this is not successful, follow these steps to reboot from the system disk.

1. Use the following steps to access Microsoft Recovery Console and check the disk:

For Windows XP

- a. Insert XP disc and boot the disc.
- b. When the setup screen appears, type R for repair on the keyboard.
- c. When the command prompt has appeared, selected the C: drive by typing 1 on the keyboard.
- d. When the command line appears, type the following to check the disk.

chkdsk C: /r

For Windows7/Vista

- a. Insert the Vista/7 disc and boot the disc.
- b. When the setup screen appears, select English and click command prompt when the setup options appear.
- e. When the command line appears, type the following to check the disk.

chkdsk C: /r

Note: If the disk check does not fix the issue, fixboot and fixmbr may be used as a last resort to rewrite the boot record.

FAKE ANTIVIRUS SECURITY SOFTWARE IS INSTALLED

1. Delete the following files from your computer.
 - a. %UserProfile%\Desktop\Antivirus Security.Ink
 - b. %UserProfile%\Start Menu\Antivirus Security
 - c. %UserProfile%\Start Menu\Antivirus Security\Antivirus Security.Ink
 - d. %UserProfile%\Application Data\Microsoft\Internet Explorer\Quick Launch\Antivirus Security.Ink
 - e. c:\WINDOWS\system32\scui.cpl
2. Click Start and Run.
3. Type regedit and delete the following registry entries.
 - a. HKEY_CURRENT_USER\Software\9178374C66E059CC11C19DCD899FD538
 - b. HKEY_CURRENT_USER\Software\Microsoft\Windows\
 - c. CurrentVersion\Uninstall\AV9