

# Dealing with Disguised Malware Pop-ups

*"A study by Google researchers analyzing fake AV distribution found that up to 90% of all domains involved in distributing fake antivirus software used social engineering techniques." [en.wikipedia.org/wiki/...](http://en.wikipedia.org/wiki/...)*

If you suspect a malware infection, **DISCONNECT your computer from the internet!** Malware uses your internet connection to install more malware and further compromise your privacy and security. For what follows, if there are any steps you don't know how to do or something doesn't go as planned, shutdown your computer (if shutdown is disabled, power off your computer) and call tech support immediately! If you are a small home office or larger business and don't have expert support, call Personal Systems Services, Inc. at 770-485-8954 or 770-587-9095 for assistance.

## How to Recognize Disguised Anti-Malware Pop-ups

Any list of internet malware and their techniques changes constantly. Their socially-engineered, disguised appearance gets better all the time. At this time, there are a few ways to spot disguised spyware infection attempts:

1. Typically, the fake anti-malware has an official looking pop-up window displaying information about multiple infections, such as "XXX serious infections detected". It requires payment (i.e. blackmails you) to fix problems.
  - Legitimate security software usually detects and alerts one possible threat at a time, such as "Suspicious file XXX.exe is attempting to access the internet", and offers options such as "Delete, quarantine, or allow."
2. False security software tries to panic you into entering a credit card for payment to remove the fictitious infections. It'll say things such as "extremely high risk threats detected" or "potential identity theft detected."

## What-Not-To-Do! Tips for Fake Anti-Malware Pop-ups

- DON'T interact with the software at all! **Don't click on anything in the window, including the X in the top right corner of the Window.** Any click in the window may allow the malware to install itself.
- DON'T delay dealing with it; don't even wait an hour. Once you are infected, it quickly gets worse.

A malware infection may disable Safe Mode and corrupt your computer if you try to remove it. It will likely disable security settings and provide an open door for additional malware. If you delay dealing with a malware infection, your computer will eventually stop working and become much more difficult and costly to repair. If you immediately follow the suggestions below, there is a good chance you will be able to avoid a catastrophic infection and continue to use your computer without risk from this threat. If you delay or are unsuccessful and continue to use your computer, the only economical solution the computer expert will probably have is to format the boot drive and reinstall Windows, applications, and data. Although data is usually recoverable, there is no guarantee. **Always have a separate backup of your data before the crisis or disaster!** If the computer is more than 3 years old, the typical 3-5 hour expense is usually better invested in a new computer rather than starting from scratch with your existing computer.

- DON'T waste time searching the web for solutions. During the time you're browsing the internet, infections are getting more deeply entrenched and disabling the tools you could use to remove them.
- Download and install the free version of [MalwareBytes](http://www.malwarebytes.com) now. The free version does not interfere with your primary anti-malware and provides additional options for removing an infection that bypasses your primary anti-malware's defenses. Once infected, you may not be able to access the internet or install anti-malware tools.

## What-To-Do When Anti-Malware Pop-ups Appear

As recommended above, the first line of defense is spotting a security threat and dealing with it immediately. **The objective is to stop it as quickly as possible!** Some threats are very resistant to termination. Some can't be closed from Task Manager because they will restart themselves or prevent Task Manager from loading. Every second counts; don't delay doing the following steps:

1. **Promptly disconnect from the network and save all open files.**
2. Right-click the malicious pop-up **icon in your taskbar** and click on "Close (Window)". Close all applications, shutdown your computer, and if successful, go to step 5.
3. Use Task Manager to kill the pop-up (Ctrl-Shift-Esc, right click on the malicious icon in the Applications tab, and click End Task). Close all applications, shutdown your computer, and if successful, go to step 5.
4. If you can't shut down your computer any other way, as a last resort, press and hold the power button until the computer turns off. You usually have to continue to press the power button in for at least 5 seconds.
5. **Do the following steps only if you know how to Restart in safe mode!** Otherwise, call tech support now.
6. Use System Restore to go back **two restore points** (the infection may have occurred before pop-ups started).
7. After the System Restore finishes, reconnect the network, and boot into Safe Mode with Networking.
8. Turn off System Restore. If your current anti-malware software works, update your virus definitions and do a deep/full scan (memory, all files on the hard drives, etc).
9. Even though the threat may appear to be gone, (download/install) update and run [MalwareBytes](http://www.malwarebytes.com).
10. Once the computer is cleaned, restart Windows in normal mode, and verify operation.
11. If anything is abnormal, shutdown/power-off the computer and call tech support.
12. Turn on System Restore. If anything was changed by returning to a previous restore point (e.g. Windows updates), fix what was lost.