You are browsing the web when a popup message box suddenly appears suggesting that you have been infected with something, or are at risk of something, or you are being offerred something unexpectedly (and suspiciously).

You don't know whether it's genuine or not and you may or may not be familiar with the website that you are visiting.

The options it seems to offer may be clear or ambiguous, attractive or unappealing, well-written or illiterate. Actually, none of that matters very much. What matters is whether you think that the message is genuine or is something you would prefer hadn't popped up and which you'd like to get away from as quickly as possible. If you think that the message is benign and you are prepared to go along with what it suggests then the rest of this article does not apply.

If you are still reading, then you are concerned about the situation and you do not trust the message.

What do you do?

My advice is straightforward:

DO NOT

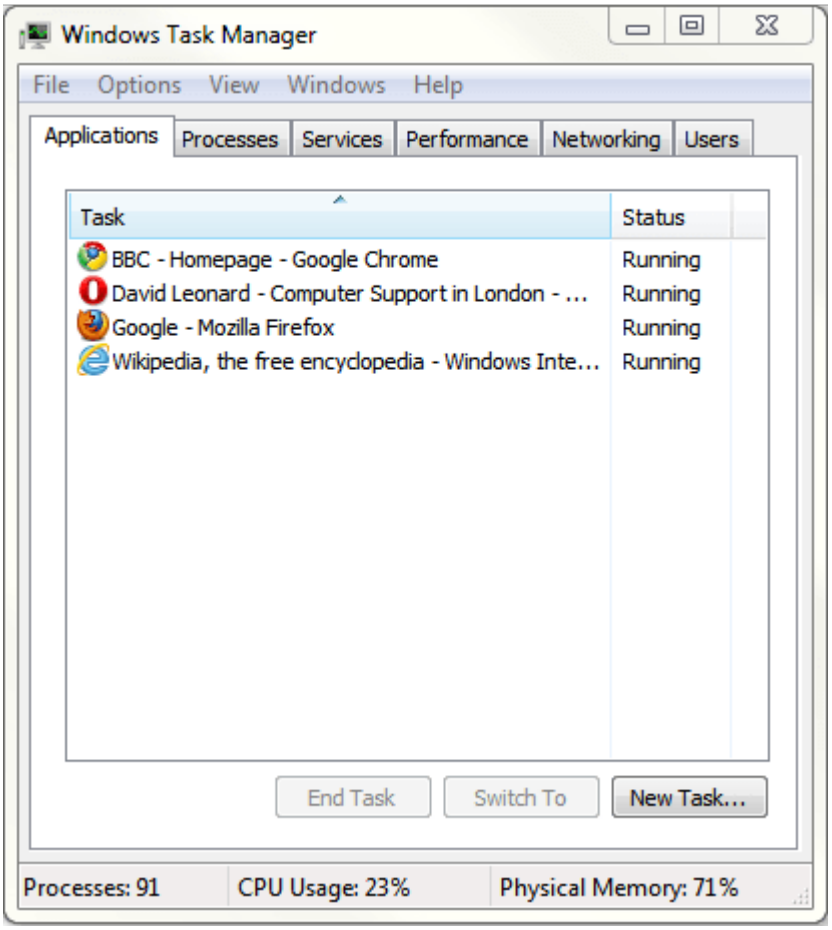
- Click on the option that seems to offer a solution to a problem you didn't have 30 seconds ago (and which you probably don't have now)
- Spend five minutes agonising over the potential consequences of the different options.
- Try to work out the motivation of the perpetrators
- Click on the "X" at the top righthand corner of the box to close it. Note: I just said DO NOT click on the "X" .....

DO

- Get out of the situation ASAP

  Clicking on any button in the box – even the "close" button – can have any consequence that the perpetrator has designed. All (s)he is interested in is getting you to click on something so that the master plan is triggered into action. I repeat, do not click on ANYTHING in the box – even the close button.

  Instead, close the browser (Internet Explorer, Firefox etc) immediately using the Task Manager. This is achieved as follows:



1) Right-click on the clock at the bottom right-handcorner of the screen.
2) Left-click on the “Task Manager” option.
3) Left-click on the “Applications” tab.
4) Look for the line(s) in the list that relate to your internet browser. In the example here I have four different browsers running – Chrome, Opera, Firefox, and Internet Explorer. Note that the description against each browser icon is the title of the web page that is being displayed in that browser window at the moment (eg I am looking at the BBC website in my Chrome browser). In this example, I have no programs loaded other than the four browsers. You would normally see the entry for your browser amongst entries for other open programs (eg Word, Excel).
5) Click on the line for the browser in which the popup has just occurred.
6) Click the “End Task” button.
7) If you happen to have that browser open in several windows, such that there are several lines for it in the Task Manager, then I would recommend closing all of them.
8) Close the Windows Task Manager by clicking on the “X” (top right-hand corner).

- Run the “on demand” scanner of your antivirus program to check whether you machine has been infected

  As far as I know, all antivirus programs have the ability to run a complete scan of your computer “on demand”. If you can find that option and run it then it will provide some peace of mind. If you can’t find this option then your antivirus program is probably set to run a complete scan automatically once a day anyway so you will probably know in 24 hours if you did, in fact, “catch” something.

- Consider downloading and running an antimalware program

  - Malwarebytes from http://www.malwarebytes.org/. Take the option to download the free version.
  - **Spybot** from http://www.safer-networking.org/en/mirrors/index.html
  - **AdAware** from http://www.lavasoft.com/single/trialpay.php

  Be very very careful if downloading any other antimalware program as some of the offerings are exactly the opposite – malware disguised as antimalware.

If you need more help, remember that my remote control support service is available – see http://www.davidleonard.net/remote-support/

Share this:

- Click to share on Twitter (Opens in new window)
- Click to share on Facebook (Opens in new window)