There exist many criminal gangs who attempt to extract money from you, or any unwary internet users. The ways and means which they attempt to do this, are many and varied.

The methods these criminals use varies from ransomware to hijacked websites, and everything in-between.

Recently, we've seen a considerable number of "browser session hijackers" appearing. These are when you hit a page in your web browser, or even an ad on a web page just "take over" the web browser. It doesn't matter if you use Internet Explorer, Microsoft Edge, Firefox, Chrome or Safari – these gangs have special code they detect the browser with, then send you to a page especially written to hijack that browser.

How do you know you've been hijacked?

Typically, the browser window opens to 100% of your monitor size and opens a dialog window with a message and can even start playing a looped audio file telling you that your computer has been "locked". Common tactics are to claim to law enforcement – often the FBI or the CIA. The screen will often claim that you've been caught visiting some nefarious website, downloaded some illegal pornography, or have engaged in criminal activities. More recent variations claim that there is a problem with your Microsoft Windows license and pretend to be from Microsoft.

A couple of examples of just such a browser locker can be found here:

Figure 1 FBI Browser Lock Screen

Figure 2 Interpol Browser Lock Screen

An annoying feature of these browser lock-screens is that it can come back even after a reboot of your computer. This seemingly adds weight to the claim that the authorities have taken over your computer, but instead it is just a feature within the browser. Most modern browsers will attempt to reload the page they were on if they crash or are terminated un-expectedly. This can include using the windows task manager to kill the process.

So now you know how to identify a fake browser hijacker, how do you get rid of one that might have taken over your browser?

You must kill your browser, but these crafty programmers have a way of making the page come back when you re-open the browser, so – how do I prevent this browser window from coming back?

First, you have to access the task manager. You can do this in one of two ways:

Method One:

1. Hold down CTRL and ALT and the Delete keys at the same time – sometimes called CTRL-ALT-DELETE. Select 'Task Manager'

Figure 3 CTRL - ALT - DELETE

2. Now select: “Task Manager”

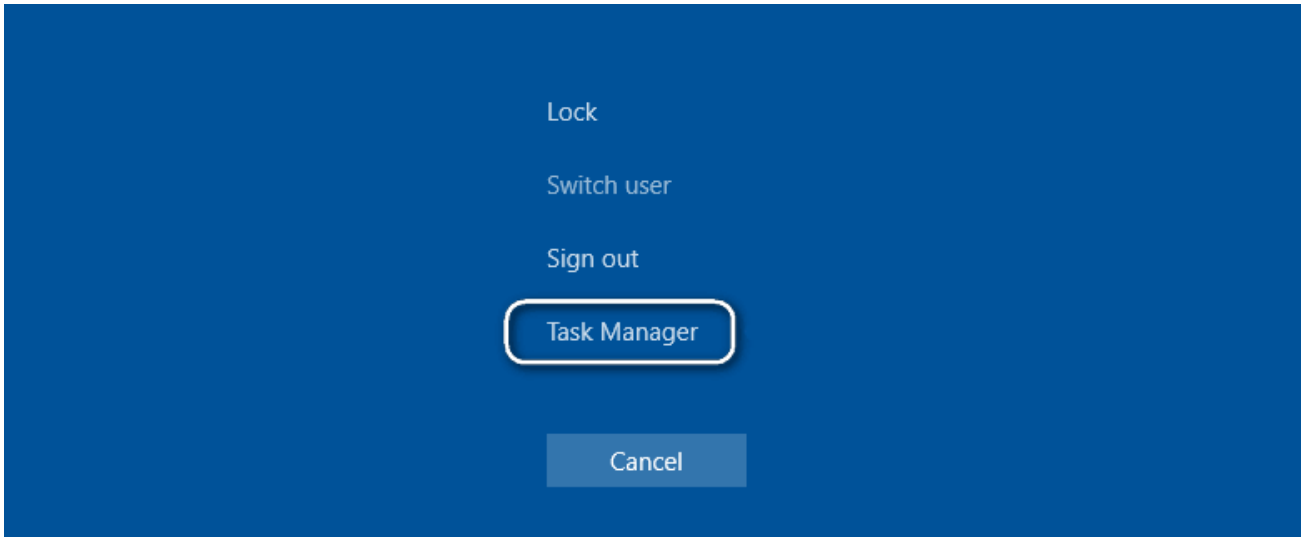

Figure 4 Select "Task Manager"

Method Two:

If you cannot access Task Manager using Method One – right-click on the task bar in a blank space (not on a program name) – alternatively right-click on the Windows Icon in the bottom left, or Cortana “type to search” box – again, select Task Manager.

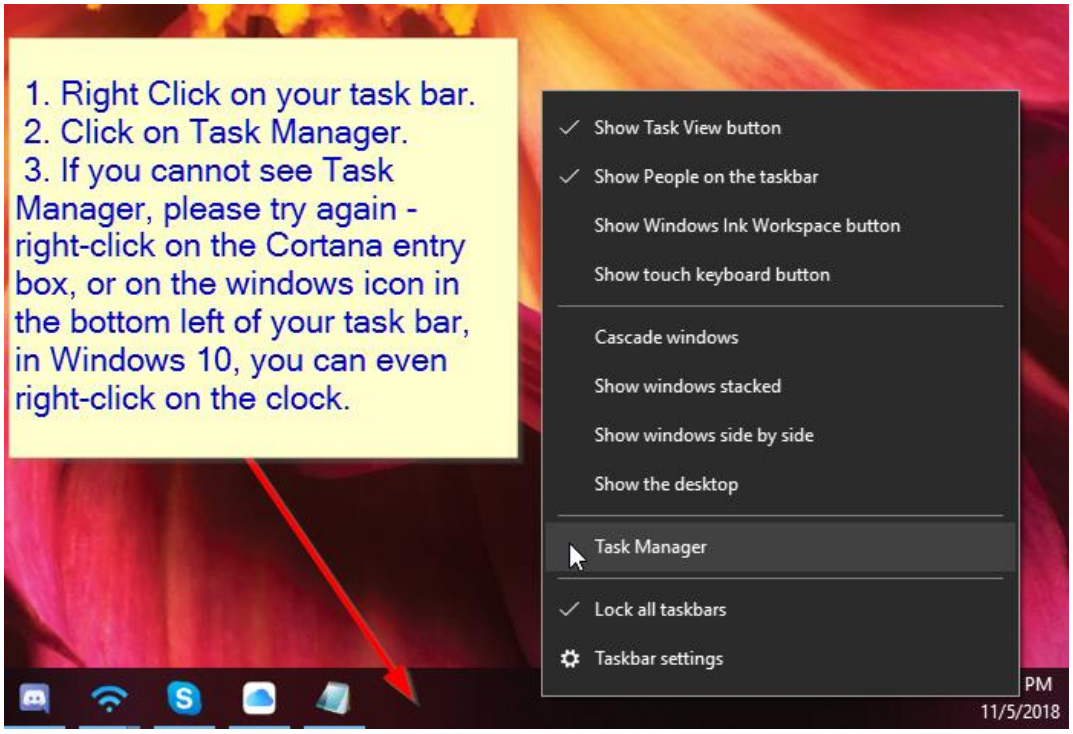

Figure 5 Select "Task Manager"

Now you have the task manager open – click on your browser program to select the task – then click “End Task”

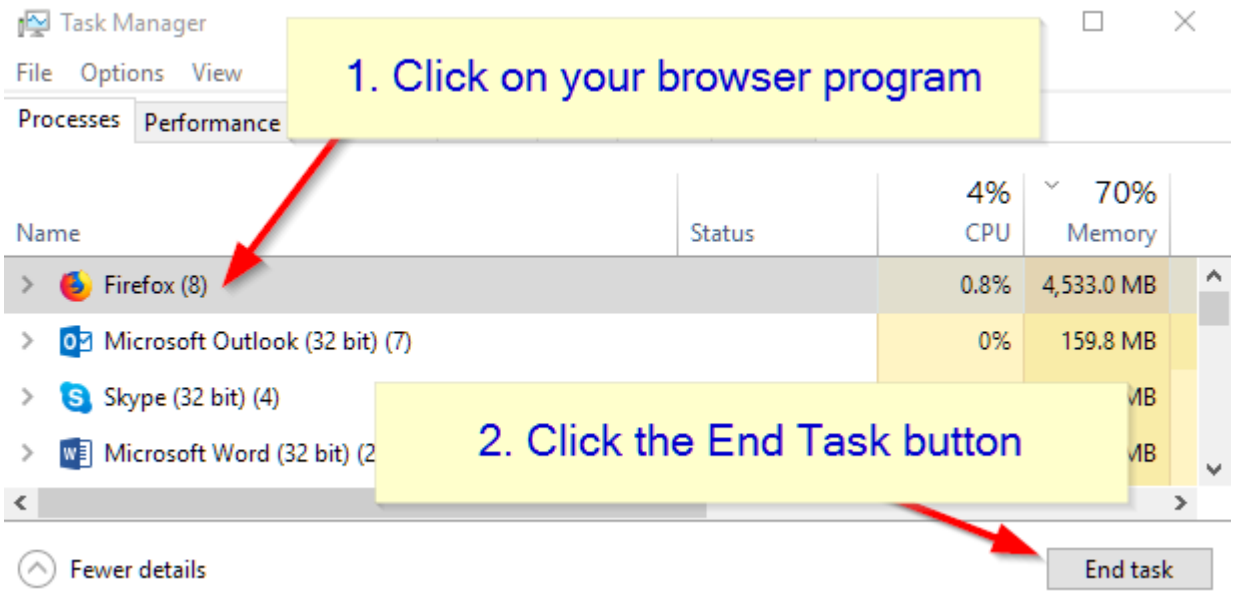

Figure 6 Click on your Browser (Edge, Firefox, Explorer) - then click "End Task"

Once your Browser has been closed, you need to open a clean browser

To restart your browser into a clean session – you do this by clicking your browser icon while holding down either the SHIFT key, or the CTRL key. Each browser is different. If you get the wrong one, repeat the task manager kill process, try again with the other.

Finally – for Microsoft Edge, there is a foolproof method of starting it with no pages loading. Hold the Windows Key and R – Win-R.

When the ‘Run’ menu opens – type: *explorer.exe microsoft-edge:about:blank*

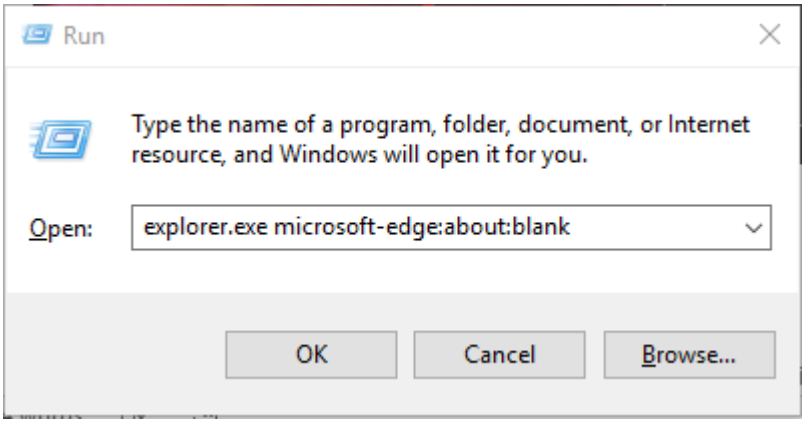

Figure 7 Hit CTRL-R to open the Run box, then type explorer.exe microsoft-edge: about:blank

Once your blank windows is opened – close the window, and then open edge once more. It will open without the problem window.