Malware/Virus removal

The Maintenance and Support Service Contract that covers your computer for manufacturing defects and certain software conflicts *doesn't* cover malicious infections. However, we will provide a free removal for the first time an infection occurs and explain the typical routes in how malicious software infects a computer, how to prevent it all whilst demonstrating on how to remove it and providing steps on how to stay diligent when browsing.

They are multiple types of malicious software, (typically referred to as malware) and the most common way of your computer becoming compromised is down the creators of these bits of software knowing how to exploit web browsers & working in conjunction with the companies that have/host websites and services. Internet Explorer is usually targeted over other browsers as it is bundled with all versions of Windows and is the lowest common denominator.

Due to licencing agreements we're unable to provide other browsers but we can and definitely do recommend others when assisting with malicious software infections.

Malware programs can come in the form of "freeware" or "adware" (advertisement software) and even be hosted/provided by seemingly legitimate sources. These bits infect your computer like a virus but don't have any malicious code in them so an anti-virus product will not be able to detect them. A lot of these programs are provided for free because the adverts within them (or during the installation) generate revenue when you click on them or they sell on the data that they can mine from your machine. This data is typically statistics about how you use your computer on the Internet and what hardware/software you are using, that sort of thing opposed to your own personal files.

An example of how your computer could be compromised is that you've opened a false link someone posted to your wall on Facebook and that site has had a funny video embedded to which you've had to install a "prerequisite" or to update something in order for it to work. In the background your browser is compromised and the next time you start your computer you're plagued with adverts and web-site redirects and programs you haven't installed.

Another example is opening an attachment within an e-mail you think is from a respectable source.

Below is a guide on how to install and use a piece of software that we use.

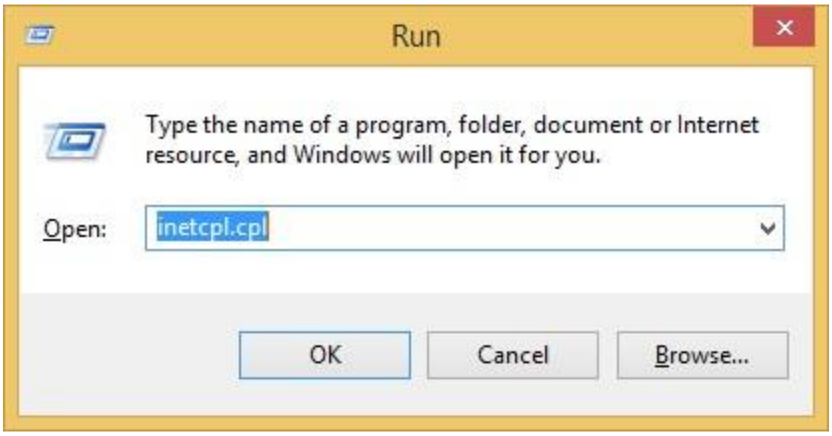
This will scan your machine for any malicious entities that are hidden, difficult and next to impossible to remove manually.

http://www.tomsguide.com/us/malwarebytes-how-to,news-18841.html

If you're unable to access the Internet correctly, it may be that one of the malicious programs has changed the settings to how your computer deals with an Internet connection.

Below are a few steps on how to change the settings that may have been changed by malicious software and prevent you from accessing the Internet correctly.

1.) On your desktop, if you press and hold down the Windows key and then press R it'll bring up a "Run" dialogue box illustrated in the image below…

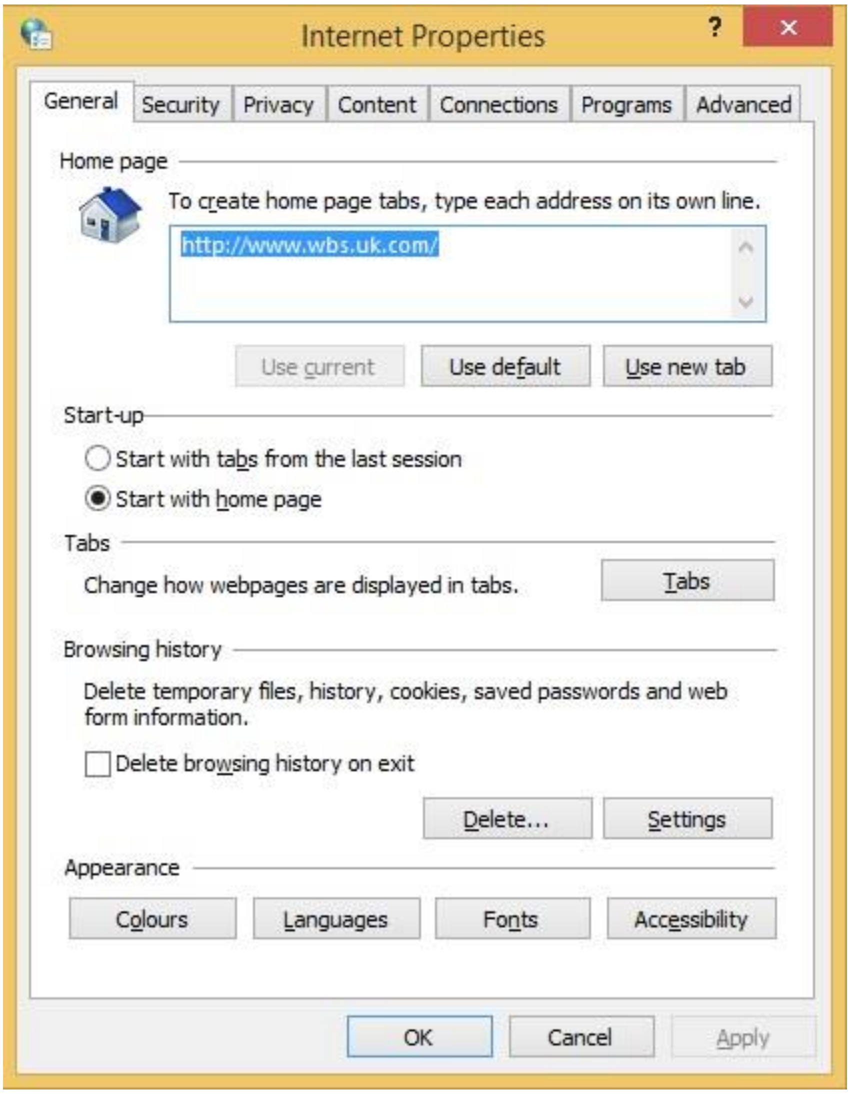


Run

Type the name of a program, folder, document or Internet resource, and Windows will open it for you.

Open: inetcpl.cpl

2.) If you can then type in “inetcpl.cpl” (without the quotation marks) this will then open up Internet Properties…



Internet Properties

Home page

To create home page tabs, type each address on its own line.

http://www.wbs.uk.com/

Start-up

○ Start with tabs from the last session

● Start with home page

Tabs

Change how webpages are displayed in tabs.

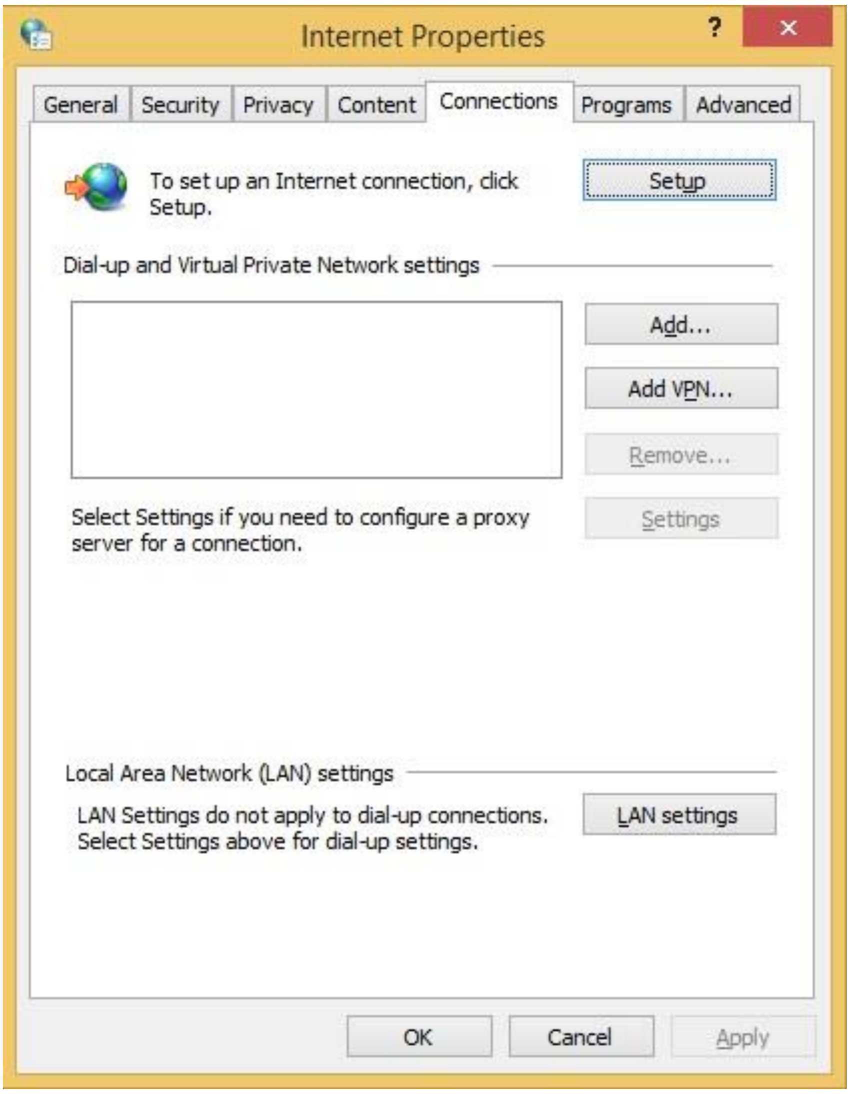
Browsing history

Delete temporary files, history, cookies, saved passwords and web form information.

□ Delete browsing history on exit

Appearance

3.) … along the top of this window, if you click on the Connections tab.



To set up an Internet connection, click Setup.

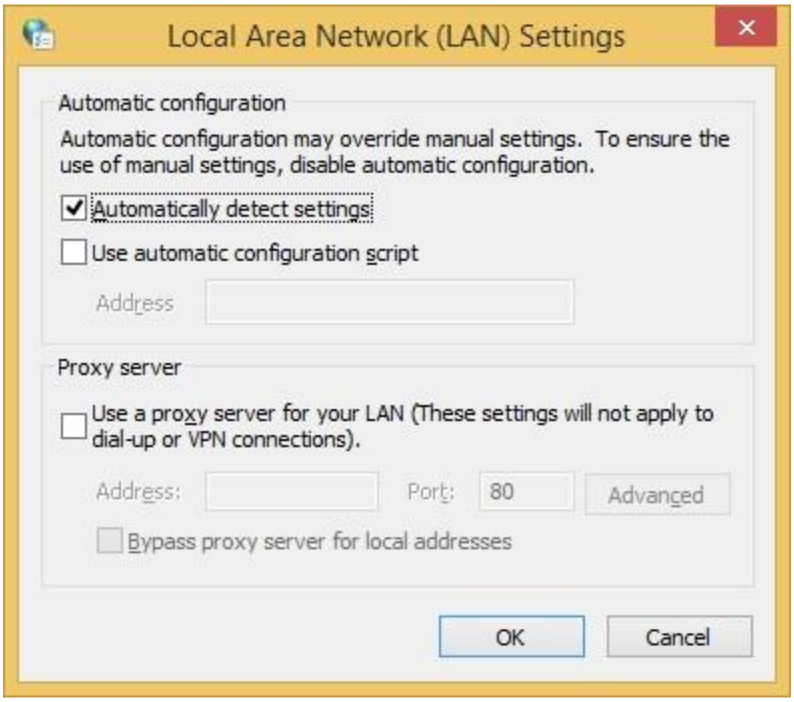
Dial-up and Virtual Private Network settings

Select Settings if you need to configure a proxy server for a connection.

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Select Settings above for dial-up settings.

4.) Then at the bottom of the window if you click on “LAN settings”…



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

□ Bypass proxy server for local addresses

5.) .. we need to make sure the settings are the same as in the image above. With “Automatically detect settings” ticked and nothing else.

If you follow these steps and you’re still unable to connect to the Internet, download the Malwarebytes Anti-Malware software on another computer, copy it over to a USB stick and follow the instructions provided within the guide. If you are unsuccessful from there, then we need to make arrangements to have your computer collected for assessment.