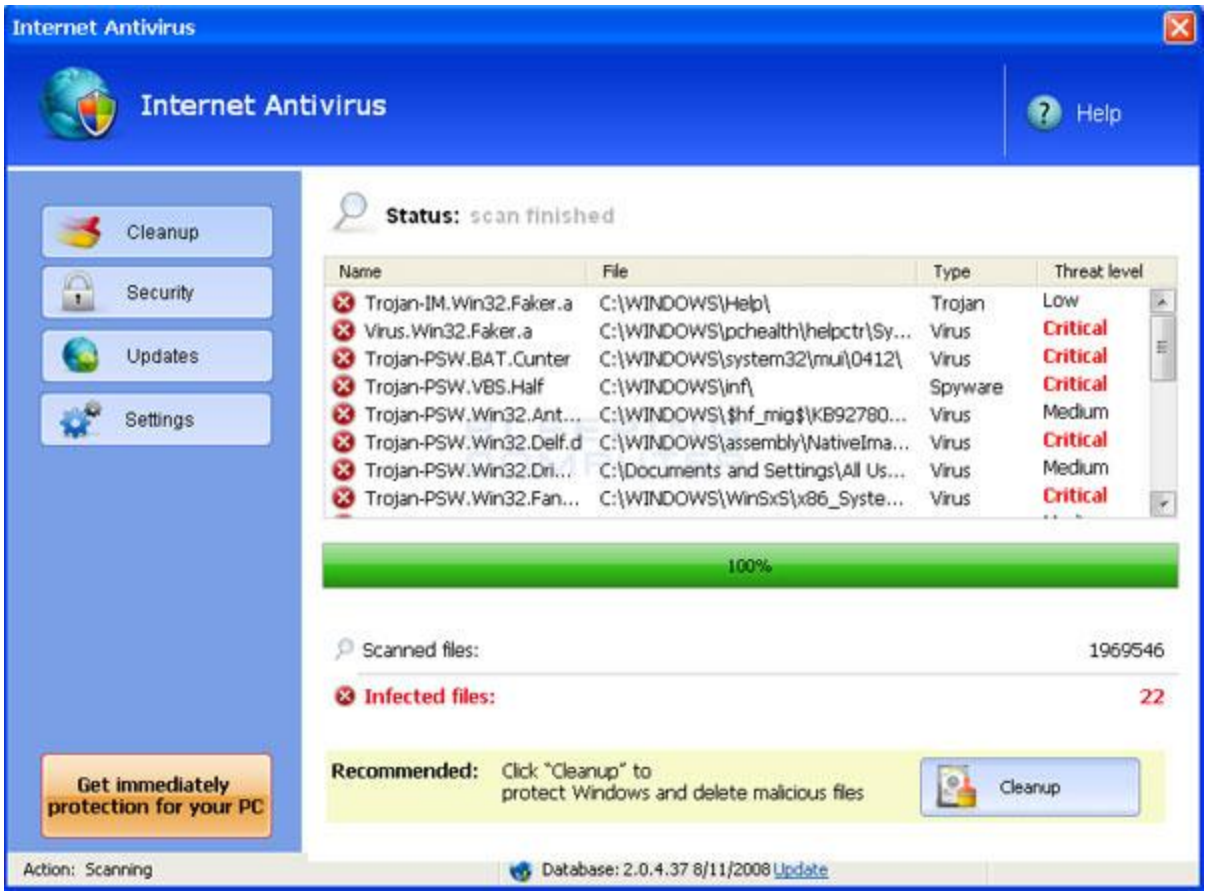
# Scare Ware Virus Infection

Scareware infections are malicious pieces of software which pose as legitimate anti virus programs. As such they look like anti virus programs that you would often use. Do not let their appearance fool you. These programs will attach themselves to infected web sites and will ask you to scan your computer to remove potential infections. If you choose to scan the machine the virus will activate and will appear as below. There are many different strains of the virus and the appearance will often vary. However, the basic look will be similar and you should be able to spot the infection. You should **only ever** run Anti Virus which you have chosen to install on your computer. Anything trying to access your machine from the internet should not be allowed to run.



## How to Prevent Scareware Infections

1. You should ensure that you have an active anti virus program before accessing the Internet. The University recommends Microsoft Security Essentials

2. When browsing the web you may receive a message from the web page saying something like “Internet Anti Virus” “Security Tool” ( etc ) “would like to scan your computer, click here to scan” This is how the Scareware installs itself. Do not click on the pop up box as this will install the Scareware. Instead Press **Ctrl Alt Del** keys on your keyboard to access the Task Manager > click Task Manager > Application > highlight the offending web page in the Task Manager > click End Task. This should shut the web page down. If this does not work you can try and log off, or restart the machine. **Do Not** click the pop up box at any time as the Scareware may install.

## How to Remove the Scareware Infections

Unfortunately, unless you know what to look for you may have already been infected by the Scareware Viruses. If this is the case, the following removal guide will work for many but not all infections. (Please note the links are external links located on the Bleeping Computer’s web site) We cannot control these links, if they do not appear to be working please let us know on Helpdesk@exeter.ac.uk

1. Firstly, you may notice that you are unable to access the Internet. This is because the Scareware, changes the Proxy settings on the web browser. To resolve this, go to internet explorer > tools > internet options > connections > lan settings, ensure that there is no tick in the auto config script or use a proxy server for your lan. The only tick should be in the top box (auto detect settings) Click okay and okay again to accept the changes.

2. Secondly, we need to stop the virus from running in the current Windows session, a useful program is very good at doing this. It is called RKill and is available from the Bleeping computers web site here. **http://www.bleepingcomputer.com/download/anti-virus/rkill**

3. It is a simple program that runs when double clicked and automatically terminates many (not all) of the malicious processes associated with the Scareware.

4. Finally, you should download Malwarebytes, install and update it, and run a full scan. Malwarebytes is free and can be downloaded here: **http://www.bleepingcomputer.com/download/anti-virus/malwarebytes-anti-malware**

5. Malwarebytes will usually do the job but only when the Virus processes have been terminated. Malwarebytes will take around 40 mins to scan the computer.

## Additional Steps

If you are unable to download the files above because the Scareware will not let you connect to the Internet, (and step 1 has not resolved this) you can download them from a clean machine and copy them across using a USB stick or other portable media.

You may also need to start the machine in Safe Mode if you find you cannot stop the Virus in Normal Mode. Restart the computer and tap the **F8 key** repeatedly as soon as the machine starts to boot. This will bring up a Startup Menu. One of the options will be **Safe Mode with Networking**, use the **Arrow keys on the Keyboard** to navigate to **Safe Mode with Networking** and press the Enter key to select. Repeat the steps above to try and remove the Scareware once the machine starts in Safe Mode.