



Factsheet 11, part 2 – You suspect your computer is infected with malicious software – what should I do?

The previous [Factsheet \(11, part 1\)](#) in this series explained how to perform a full malware scan of your computer using the anti-virus software installed on your computer. Some anti-virus software will detect certain pieces of malware when sometimes others won't. This is because they don't yet have a definition or signature for that particular piece of malware.

Also, if not detected at the time malware tries to infect your computer, many types of malware disable the anti-virus product installed, making it appear to work when it doesn't. Therefore, once a computer becomes infected, the ability of installed anti-virus products to detect malware on your computer is reduced. So, just because a full scan did not find malware, that doesn't mean your computer is not infected.

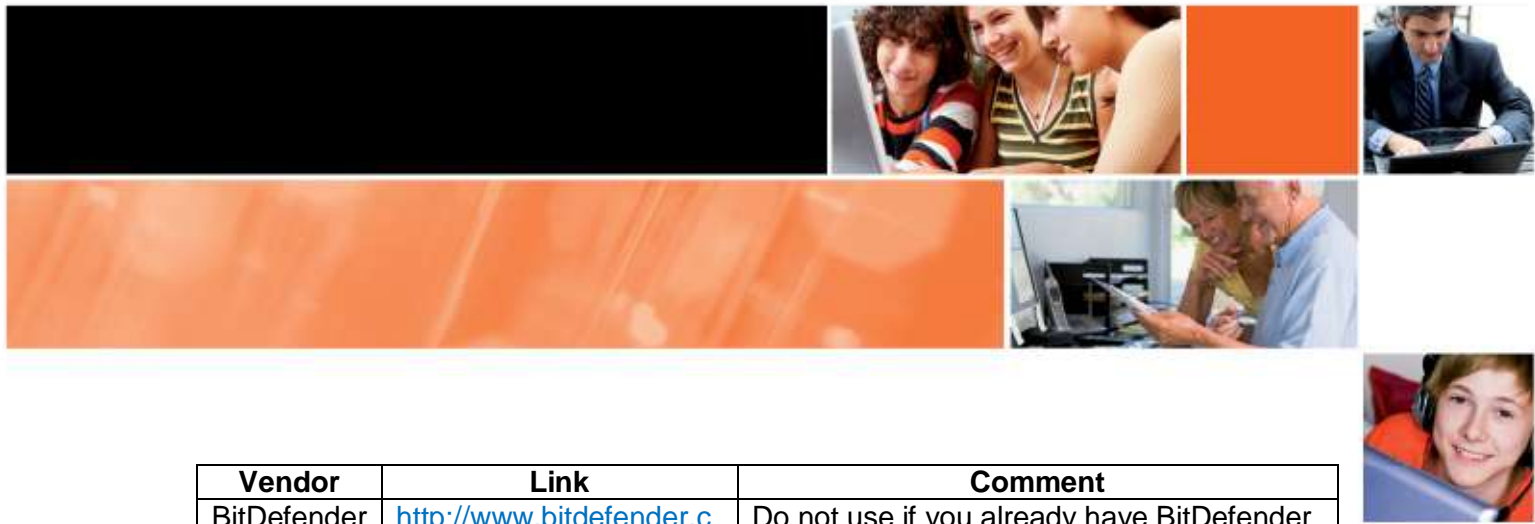
Installing multiple anti-virus software programs is not recommended because they can interfere with each other and the smooth operation of your computer. So how can you scan your computer with multiple anti-virus programs? You can do this, by using web-based scanning tools which are provided for free by several anti-virus companies.

Using an online web-based anti-virus scanner is not a substitute or alternative to installing and keeping up to date an anti-virus program installed on your computer. An anti-virus program installed on your computer will help detect and prevent infections from known threats. However, an online scanner cannot prevent malware infections – it can only potentially detect them, after the damage has occurred.

Using an online anti-virus scanner is recommended when you suspect you might have a malware infection which your existing anti-virus product has failed to detect.

Using a web-based online anti-virus scanning tool

There are many free online anti-virus scanning tools to choose from such as:



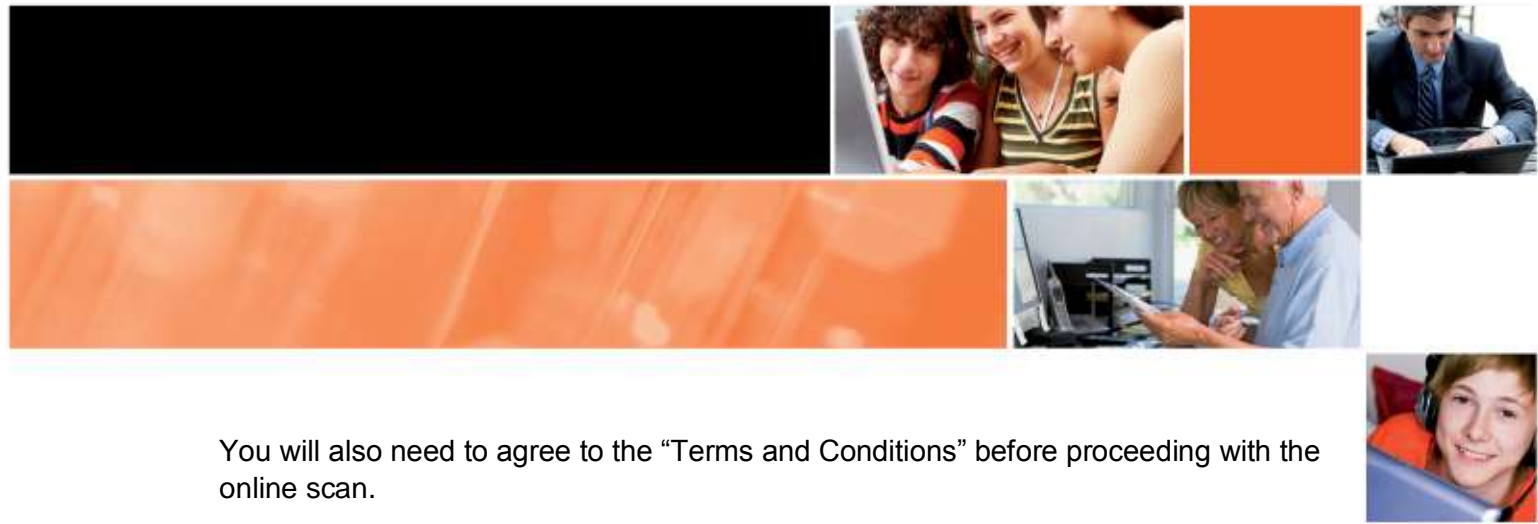
Vendor	Link	Comment
BitDefender	http://www.bitdefender.com/scan8/ie.html	Do not use if you already have BitDefender anti-virus software installed on your computer or network.
ESET	http://www.eset.com/onlinescan/	Do not use ESET if you already have NOD32 anti-virus software installed on your computer or network.
F-Secure	http://support.f-secure.com/enu/home/ols.shtml	Do not use if you already have F-secure anti-virus software installed on your computer or network.
Microsoft	http://onecare.live.com/site/en-us/center/howsafe.htm	The scanner is available for Windows operating systems only. Do not use if you have Microsoft Security Essentials anti-virus software installed on your computer or network.
McAfee	http://us.mcafee.com/root/mfs/default.asp	Do not use if you already have McAfee anti-virus software installed on your computer or network.
Trend-Micro	http://housecall.trendmicro.com/	Do not use if you already have Trend-Micro software installed on your computer or network.

Things to consider before beginning

When deciding which online scanners to use, select those brands which are different to the brand of anti-virus software already installed on your computer. For example, if you already have ESET NOD32 anti-virus software installed on your computer or network, do not use the ESET online scanner. Use another online scanner instead.

Most online scanners have a link to a section called "System requirements". Read these to make sure your system meets the requirements for the scan to run effectively. Generally, these requirements include connecting to the Internet from a user account with "administrator" privileges. See [Setting up a limited user account in Microsoft Windows XP \(Factsheet 3\)](#) which explains the difference between accounts with administrator and limited user privileges.

You need to connect to the online scanner web site with a web browser. It is recommended using Internet Explorer or any other browser included in the "System requirements" section.



You will also need to agree to the “Terms and Conditions” before proceeding with the online scan.

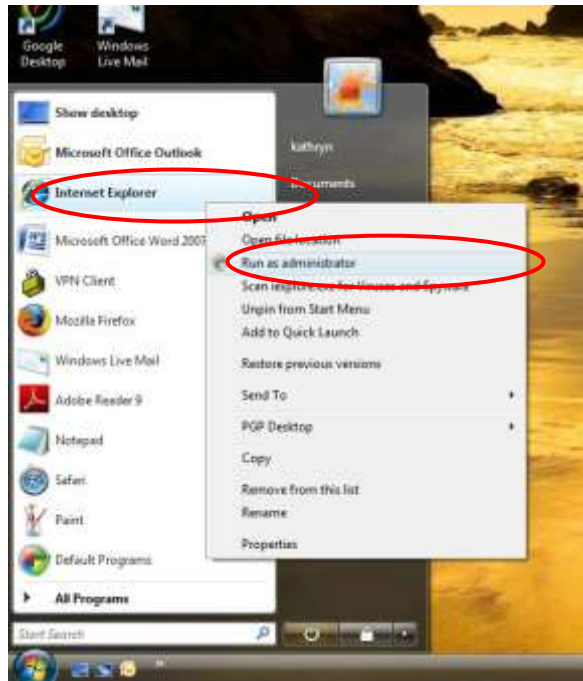
Many of these online virus scanners use ActiveX programs to scan your computer. You may need to install and run the ActiveX program in order to scan your computer using these tools.

Depending on the online scanner selected, there may be options for the type of scan that can be performed. Perform a full system scan, scanning all drives and attached storage devices. This may take a few hours to complete. **It is recommended that you do not continue to use your browser for other purposes while the scan takes place** – this is because the browser (Internet Explorer) is operating with ‘administrator’ privileges. Normally it should not be used in this mode.

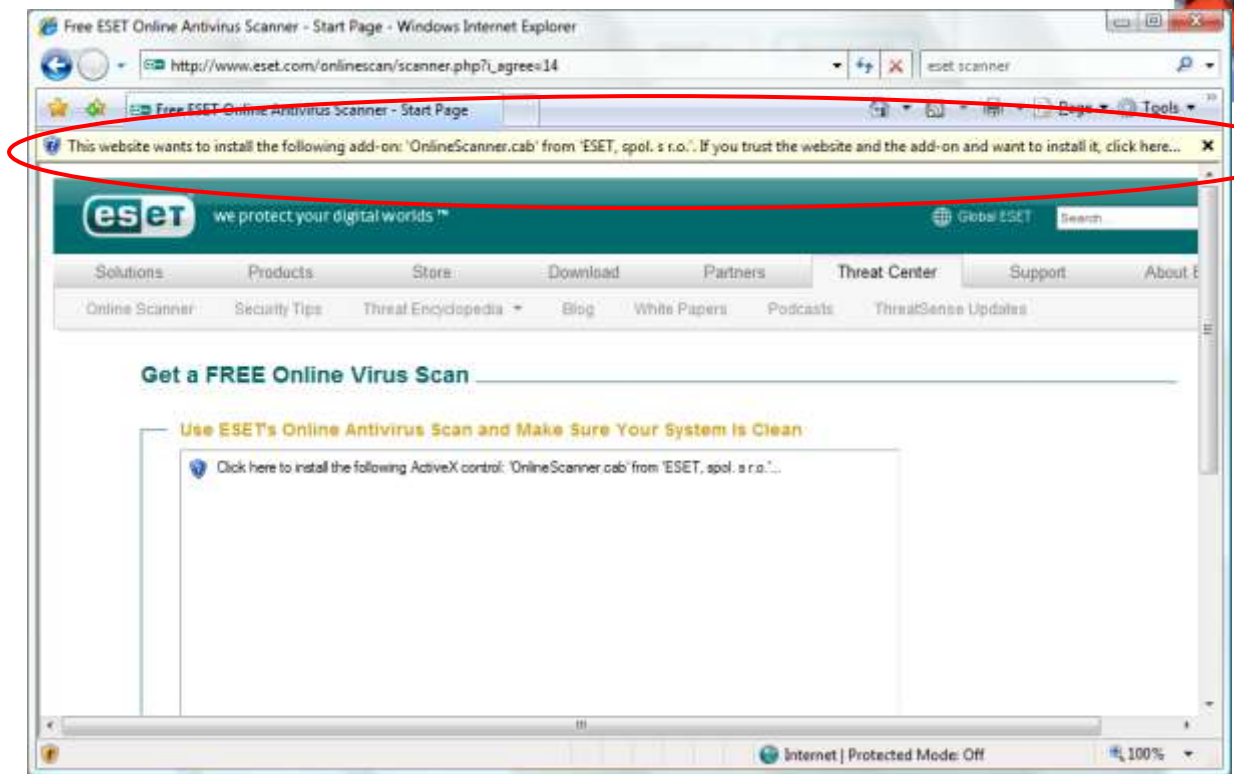
If the online anti-virus scanner detects malware it will generally ask you what action it should take. You should select options which “clean” and/or “delete/rename” any harmful files/threats found.

Example – online malware scan using ESET free online scanner

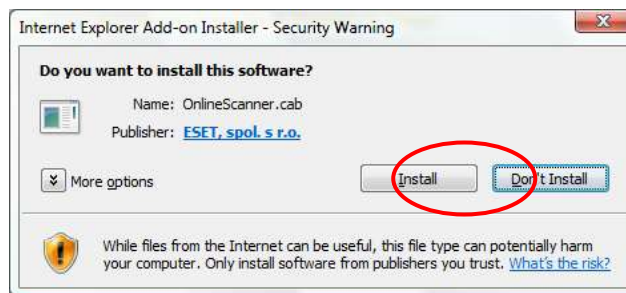
1. If using Windows Vista, open the web browser, Microsoft Internet Explorer “as an administrator”. Do this by going to the “Start menu”, select “Internet Explorer” in the start menu (but do not open it yet), right-click the mouse to bring up a new menu. Select “Run as administrator” from this menu. This opens Internet Explorer with “administrator privileges” which will be necessary to run the scanning software.



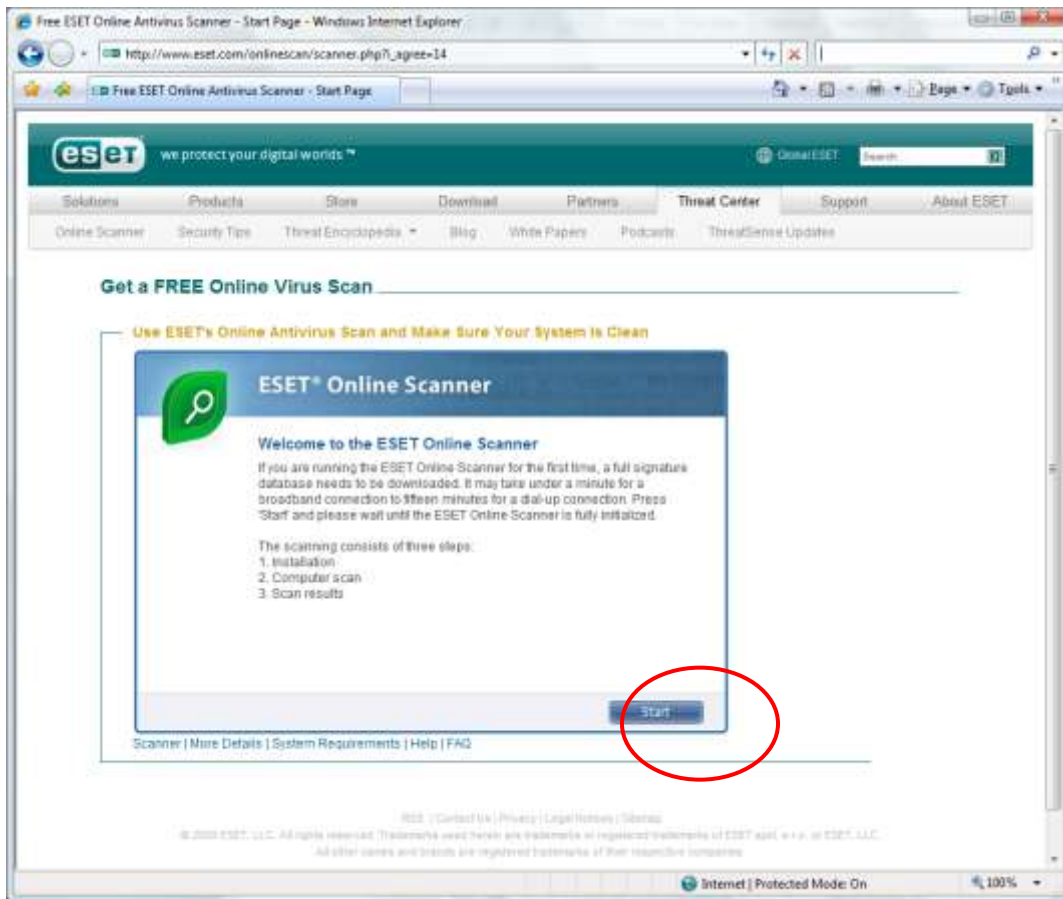
2. Or if using Windows XP, log into an account with administrator privileges and open Internet Explorer.
3. Click on the link below to open the ESET free online scanner web page:
<http://www.eset.com/onlinescan/>
4. Agree to the terms and conditions of use.
5. If your browser is set to “prompt” before installing ActiveX controls or other scripts, it will display a warning in a yellow strip above the web page. Click on the yellow bar and agree to install the ActiveX control for this web site.



6. You will then be asked to “Install” the ESET software again. Click “Install”.



7. The following window will be displayed. You will then be able to start the scan. Press the “Start” button.

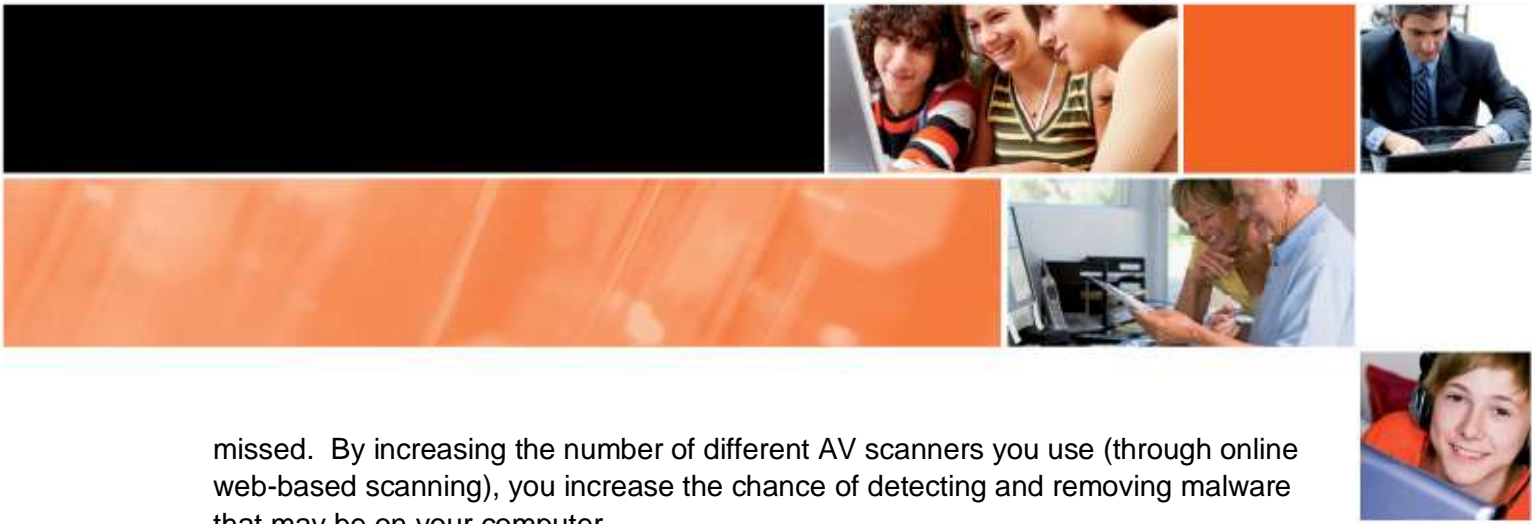


8. The scan will take one or more hours to complete, depending on how many files you have on your computer.

Greater variety improves your chance of detecting malware

If you think your computer has a malicious software infection, it is important to be as thorough as possible to detect and remove it.

It is desirable to repeat these steps again using a different online scanner. In fact if you suspect you have a malware infection and the first scan did not detect malware, then it is recommended running at least two other online scans – each with a different product. Even if the first scanning tool detected and removed malware, it is still desirable to try another scanning tool. The reason is that it is common for infected computers to have more than one malware infection because the initial infection degrades the computer's overall security and makes it more vulnerable to subsequent infections. Secondly, because different anti-virus products detect different sets of malware, you may still find additional malware other products



missed. By increasing the number of different AV scanners you use (through online web-based scanning), you increase the chance of detecting and removing malware that may be on your computer.

Don't run online web-based anti-virus scans simultaneously. Wait until one scan has completely finished and take the recommended action before starting another scan.

Conclusion

Taking the steps in this factsheet is relatively easy and within the ability of most ordinary computer users. While the scans may take some time to conduct, the effort is worthwhile if there is a chance your computer may be infected with harmful malicious software.

Computers are complex systems and require a level of care and maintenance to make them run effectively and securely. Following the steps in this factsheet will help keep your computer secure and recover from potential malware infections.

What next?

If you followed these steps and you have not yet detected malware, but still have reason to suspect your computer has a malware infection, then read [Factsheet 11, part 3](#). The steps in part 3 require intermediate computer skills but will provide greater ability to detect if your computer is infected.

If you do not have intermediate skills then it is recommended that you seek professional assistance from a reputable computer technician to help you detect and remove the malware which may be on your computer.

Report prepared May 2009

For more information go to www.staysmartonline.gov.au