

Factsheet 11, part 1 – You suspect your computer is infected with malicious software – what should I do?

Computers can be infected with malicious software (also known as malware) in a variety of ways. The Internet is by far the most popular medium such as attachments to spam email, served by malicious or compromised web sites or by self-propagating worms. However, some malware also spreads by removal USB devices (also called thumb drives and memory sticks) and writeable CDs and DVDs.¹ Care should be taken when using all computers, even if they are not connected to a network.

If you have reason to believe your computer might be infected with malicious software, what should you do?

Take action – don't ignore the problem

If you believe your computer may be infected with malware, it is important not to leave it, particularly if you or others rely on the computer to conduct online banking or other online financial transactions. At the very least, avoid using the computer for online banking or other important transactions until it can be properly checked and cleaned.


In determining the best course of action, you need to consider the potential risk. For example if the computer is used for conducting financial transactions online, then this poses a higher risk if malware is present on that computer. If the risk is high, then it is more likely to be worth spending time and money to ensure you stay malware-free.

Unless the computer is critical to your business operations, it would be wise to disconnect the computer from the Internet until it can be checked and cleaned.

As a general rule, if you have reason to suspect your computer is infected with malware, you should not use it to:

- conduct online banking
- access or submit personal information via e-government web site (such as Centrelink, Australian Taxation Office, Department of Foreign Affairs, Road Traffic Authority, etc).

¹ Writeable discs include those with the format CD-R, CD-RW, DVD-R and DVD-RW.



Even avoiding these activities will not protect information already stored on, or accessed by a computer infected with malware. Other risks remain as long as your computer is connected to the Internet or other networks.

How to detect and remove malware?

There are a few options available to you. Some options are easy to do yourself; others less so and may be more costly – and are likely to require the services of a computer professional with experience in malware removal.

This series of Factsheets (Factsheet 11, parts 1 -3) outline the steps that ordinary users can take to help detect and remove malware that might be on their computers.

These Factsheets should be followed in order – with the quickest and easiest first and later steps being more difficult but which have a better chance of detecting and removing “hard-to-find” malware.

Part 1 – Update and scan your computer with an installed anti-virus product (easy and quick)

Part 2 – Conduct an online (web-based) anti-virus scan with an alternative anti-virus product (easy and quick and when done after Part 1, more reliable than steps outlined in part 1 by itself)

Part 3 – Conduct a scan with a bootable CD-ROM (more difficult but more reliable than steps outlined in parts 1 and 2)

It is important to note that following all three steps does not provide a 100% guarantee that all malware that is on your computer will be detected and removed. It is recommended you seek professional assistance in helping detect and remove the malware if the risk is high and/or if you continue to experience problems after you have followed the steps outlined.

Updating your anti-virus software and scanning your computer

If you do not already have anti-virus software installed on your computer, then you should install it on your computer. **If you already have an anti-virus program installed on your computer, do not install a second program, this may cause your computer to stop working.**



Anti-virus software can be purchased from a computer store or purchased and downloaded online. The following anti-virus packages are free and can be downloaded online:

- Antivir, <http://www.freeav.com/>
- Avast, <http://www.avast.com/>
- AVG, <http://www.avg.com/product-avg-anti-virus-free-edition>
- ClamWin, <http://www.clamwin.com/content/view/18/46/>
- PCTools , <http://www.pctools.com/free-antivirus/>

Take care when downloading anti-virus software from the Internet as criminals often try and disguise malware as anti-virus or anti-spyware tools.

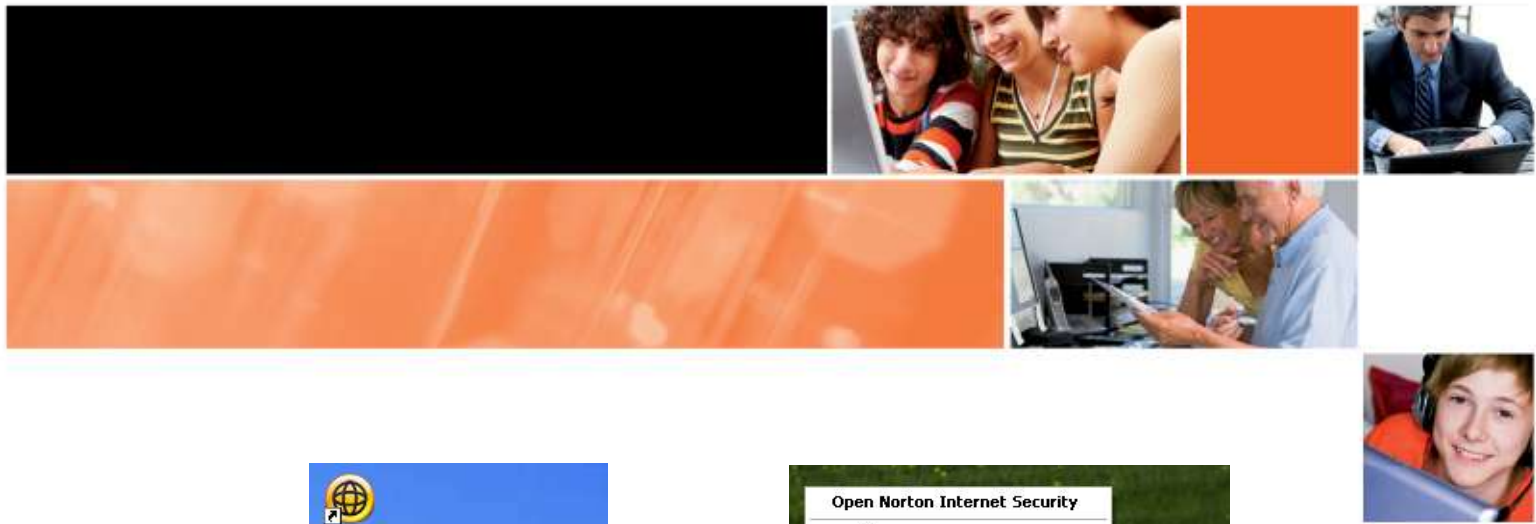
1. Ensure the anti-virus definitions (or signatures) are current. Most anti-virus software packages use a set of signatures or definitions to help recognise what files are malware and what are not. These packages will often be set to automatically check for updates to these definitions but it is worthwhile manually checking to ensure that you have up to date definitions.
2. Perform a full system scan, scanning all drives and attached storage. This may take some time to complete, but scanning can normally occur in the background while you continue with other activities.
3. When the scan is finished, check the results of the scan report to see what was found. If malware (or “threats”) are found, the AV software product will ask what action it should take. You should “clean” or “quarantine” any infected files, according to the AV product instructions.

Example: Updating and scanning using Norton Internet Security

The following example works through these steps, using Norton Internet Security 2009, running on Windows XP as an example. It assumes that you already have this installed and operating on your computer, so we’ll start at step 1 of those listed above.

Checking and downloading updated anti-virus definitions

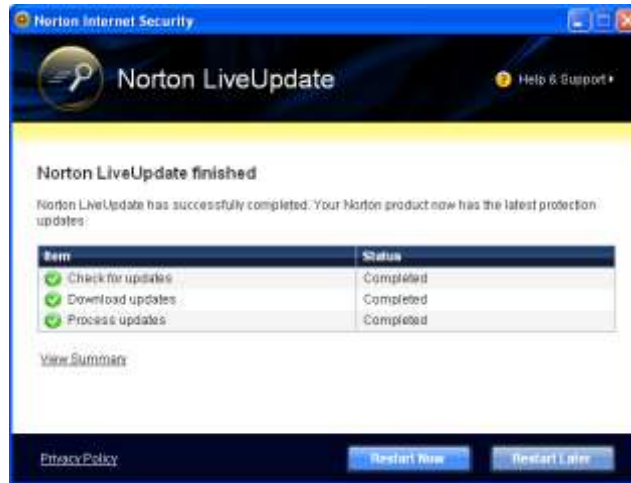
1. Open the main control panel of Norton Internet Security. This can be most easily be done by double clicking on the icon on the desktop, or by right clicking on the icon in the task bar and selecting “Open Norton Internet Security”:



2. Examine the control panel to see when the last definition update occurred:



3. In this case, the last definition was 112 days ago and a definition update should be performed before scanning. You can update the definitions by clicking the “Run Live Update” link. You will need to be connected to the Internet for this to work. The example should not be regarded as ‘best practice’ and is used for illustration purposes only. **Definitions should be updated at least daily to provide the most effective protection.**
4. Once the update is complete, depending on the type of update, you may need to restart your computer:



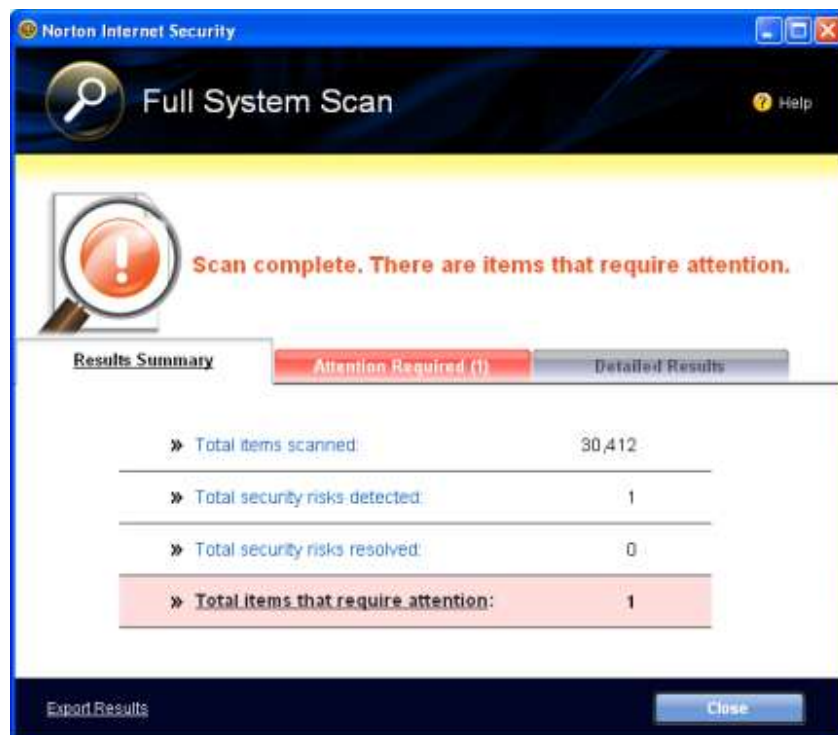
- Once you have restarted your computer (if necessary), open the main control panel and click the “Scan Now” button, this will give you several options, in this case, you should select “Run Full System Scan”:



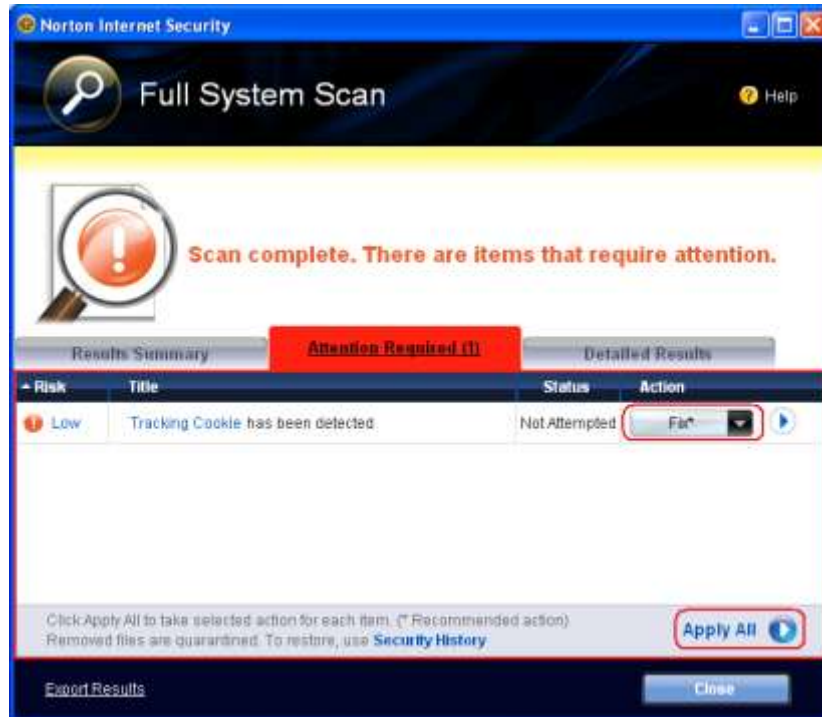
- You should then see a scanning window showing the progress of the scan:



7. Once the scan completes, you should see the results:



8. In this case, the scan found something that requires attention.
9. Click on the “Attention Required” tab to find out more information and fix the problem:



10. In this case, the scanner has discovered tracking cookies. Tracking cookies are used by web sites to track your visits, to see which parts of the site you visit, store your preferences and deliver you personalised content. While cookies may be seen as a privacy concern by some, they are generally not a security risk. However, for the purposes of this example, we'll remove them by setting the action to "Fix" and clicking the "Apply All" button.
11. Finally, you should see that all the detected items have been resolved:



12. You can now close this window and this completes the full system scan.

What next?

If you followed these steps and you have not yet detected malware, but still have reason to suspect your computer has an infection, then we recommend you follow the steps in [Factsheet 11, part 2](#). The steps in part 2 are easy and will provide greater ability to detect if your computer is infected. Part 2 should as a rule not be attempted until part 1 is completed.

If you do find malware and have followed the instructions to remove or quarantine it, then it is still recommended you proceed to part 2 because there could still be further malware on your computer which your existing anti-virus product has not yet detected.

Prepared May 2009