Malware Defence

1. Always set automatic updates for Operating System, Anti-Virus and Applications. (My Computer -> properties -> automatic updates select Automatic and time)

2. Enable hidden file & system file view to find any unusual or hidden files. (My computer -> tools -> folder options -> view -> select enabled with "Show hidden file and folders" option and disable "Hide protected operating system files")

3. Turn off auto play (Start -> Run -> type gpedit.msc -> Computer Configurations -> Administrative Templates -> Windows Components -> Select "AutoPlay Policies" -> Double Click at "Turn off Auto play" -> Select Enabled -> Set "Turn off Auto play on:" to "All drives" and Click OK.)

4. Type: %temp% in "run" and delete all entries after opening any suspicious attachments.

5. Type cmd in run and type netstat –na. Checkout foreign established connection and IP addresses. Check the IP address for its ownership.

6. Type “msconfig” in “run" and check for any unusual executable running automatically.

7. Check Network icon (for packets received and sent) I ADSL lights for data in non-browsing mode. If the outgoing is unusually high, it is very likely that the system is compromised.

8. Type "ipconfig/displaydns" in cmd prompt and look out for any URLs which you have not accessed recently.

9. Always be cautious while opening attachments even from the known sources. Try to use non-native applications for opening attachments. Example for word document use, WordPad to open the attachment.

10. When in doubt, better to format the Internet connected computer rather than doing some "patch works".

11. Prohibit any remote logon to the system (RDP, SMB, RPC) for local administrators.

12. Enforce application whitelisting 'Software Restriction Policies on all endpoint workstations. This will prevent malware droppers or unauthorized software from gaining execution on endpoints.

13. Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages.

14. Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.

15. Disable Macros in Microsoft office documents (doc/docx, xls/xlsx, ppt/pptx and mdb/accdb), by default, Microsoft products come with VBS Macro disable.

    Office Button-> Word Options Trust center-> Trust Center Settings -> Macros Settings.

16. Disable Java Scripts or similar scripting functions in Adobe Acrobat Reader for PDF files.

17. Configure built in feature for "Protected View" settings in Microsoft Office 2010 to open the Microsoft Office word documents in Protected view:

    Office Button -> Word Options -> Trust center -> Trust Center Settings -> Protected View