



## PC Security checklist

Check the following point:

- Do not run Windows™ systems as 'administrator'
- Use non-trivial passwords for all accounts
- Disable 'guest' accounts
- Use the NTFS filesystem
- Turn on the Windows SP2 firewall unless you have good reason not to.
- Use a password protected screen saver
  
- Set Windows Update to run regularly
- Update other software (including Microsoft Office™) regularly
  
- Install anti-virus software and update regularly (preferably automatically)
- Scan regularly for viruses – preferably automatically
  
- Install anti-spyware software and ensure it automatically updates itself regularly
  
- Install a hardware firewall and check it is properly configured
- Change the router/firewall's default password and disable management from the internet
- Configure wireless routers to use high levels of security (you may need to take advice on this)
- Scan your own internet connection from time to time. Make sure you understand the use of any open ports. You may need help in interpreting the results
  
- Consider using another email client.
- Make sure your email preview pane is closed
- Configure Windows to show file extensions
- Never open file attachments unless you were expecting them. If necessary ask the sender to explain what they are and why they have been sent.
- Understand that Microsoft and many other organisations have a policy of never send information as email attachment
- Never open files with names ending in .exe, .bat, .cmd, .pif, .chm, .com, .hta, .ocx, .scr, .shs, .vbe, .vbs, or .wsf
- Never give your bank details or other sensitive information in response to an email
- Never, ever respond to SPAM. It only encourages them.
  
- Consider using a different browser
- Be careful how you surf, avoid sites of a dubious nature
- Never give sensitive information with seeing the yellow padlock or https: in the url bar
- Think before downloading
  
- Make sure the machine is physically secure from theft and from tampering
- Make sure backup media is physically secure
  
- Ensure your staff are trained to understand the above points
- Make your policy regarding computer use and mis-use clear
- Make sure your staff understand the value to your business of your data and the penalties for mis-use

---

™ Windows is a trademark of Microsoft Corporation

™ Microsoft Office is a trademark of Microsoft Corporation