Ten Commandments for Your Computer Sanity and Safety

1. **Don't assume anything**. Make time to learn about securing your system and what predators do to trick you. Believing an email or a 'pop-up' warning that your computer may have a virus and that you need to click on a 'link' to remove or repair the problem may actually install a virus that takes over your system!
2. **Acquire and use a reliable antivirus program**. Select an antivirus program that has a consistent track record. Checkmark, AV-Test.org and T***U***V are among the most respected independent testers of antivirus software.
3. **Acquire and use a reliable firewall** solution. Again, independent reviewers are your best bet for reasonable choices. Some operating systems come with a firewall which only filters incoming traffic. Use a firewall that can control both incoming and outgoing internet traffic.
4. **Do not open e-mails coming from unknown or distrusted sources**. Many viruses spread via e-mail messages so **ask for a confirmation from the sender** if you are in any doubt.
5. **Do not open the attachments of messages with a suspicious or unexpected subject**. If you want to open them, first save them to your hard disk and scan them with an updated antivirus program.
6. **Delete any chain e-mails or unwanted messages. Do not forward them or reply to their senders.** This kind of message is considered spam, because it is unsolicited and it overloads the internet traffic.
7. **Avoid installing services and applications which are not needed in day-by-day operations in a desktop role, such as file transfer and file sharing servers, remote desktop servers and the like.** Such programs are potential hazards and should not be installed if not absolutely necessary. **Do not install 'toolbars'** even though the source may be well known!
8. **Update your system and applications as often as possible**. Some operating systems and applications can be set to update automatically. Make full use of this facility. Failure to update your system often enough may leave it vulnerable to threats for which fixes already exist. Use "Microsoft Update" rather than the basic "Windows Update" to update other (non Windows) MS software and hardware 'drivers'.
9. Do not copy any file if you don't know or trust its source. Check the course (provenance) of files you download and make sure that an antivirus program has already verified the files at their source.
10. Make backups of important personal files (correspondence, documents, pictures and such) on a regular basis. Store these copies on removable media such as CD or DVD. Keep your archive in a different location than your computer. Keep your original program application's installation discs in a safe place. If a Windows and software 'repair' can not be done, you will need these to rebuild your system.

!! PREVENTION IS MUCH EASIER THAN REPAIRS !!