

How To Protect Yourself Against Malicious Software (Windows XP users):

1) If you receive email notes from companies telling you that your anti spyware software license has expired and telling you to click on some link to deal with the problem then:

- **Do Not** click such links since doing so can result in the installation of a virus.
- Blocking the sender of such e-mails is recommended.

2) If a window pops up warning you that your computer may be risk and you need to download something to fix the problem then:

- **Do Not** click on anything in the pop-up window (i.e.: **don't click Yes, No or the Close button (x)**). Clicking on any control button on the pop up window can result in the installation of a Trojan worm.
- Hit **Cntl, Alt** and **Delete** on the keyboard (concurrently) to bring up the **Windows Task Manager (by pressing Ctrl+Alt+Del at same time)** then shut down the program in the **Application** window which has initiated the pop up window by clicking **End Task**. Alternatively, shut down your PC and restart.

3) If you keep getting pop up windows which you close only to have them pop up again a few minutes later and your PC has slowed down significantly then save your critical data (My Documents, email files, financial files, etc) as soon as possible. You may well have been infected and the virus has likely spread into most parts of your operating system. The only sure way to get rid of entrenched viruses is to format your hard drive then reload Windows, an up-to-date virus protection program and then reinstall your programs and your saved files.

Note: Scan your reinstalled files for viruses before opening them!

4) Any time an e-mail says forward this to 'X' number of your friends or you will get bad/good luck it almost always has an e-mail tracking program attached. Even when you get emails that try to make you ashamed if you don't send it on that e-mail is likely used for tracking! The host sender (the person who originated the e-mail) is getting a copy of each e-mail forwarded (including yours) for direct spamming or for reselling to other spammers. Ignore such e-mails and, if they are from friends then advise them to do the same in the future. If not from friends then block the senders.

5) Almost all e-mailed petitions that ask you to add your name to a list and forward it on to others are intended get names and 'cookie' tracking information for use by telemarketers and spammers. E-mail petitions are not accepted by legitimate organizations. To be acceptable, petitions

must be signed and show the full address of the signer. Stop adding your name(s) to these types of lists regardless how inviting they might sound even if the contents are designed to make you feel guilty if you don't. One example of such e-mails is about whales being killed on a beach in Denmark. Instead of supporting a great case you will receive tons of junk mail and will be helping spammers to get rich.

6) Delete other people's e-mail addresses on e-mails you forward.

7) Forward e-mails to your friends using BCC.

8) Viruses can be embedded in files and photos attached to an e-mail you receive. Save and scan all e-mail attachments with your virus software before opening. If you like a photo inside the e-mail you can save it by right clicking on it. If you want to do this then it is recommended that you scan the photo file first for viruses before opening it.

9) Do not provide your sensitive info to any third party based on claims that such information will be stored only for your use. It invariably gets mined by others. Some organizations offer such services with the implication that secure trade transactions (such as buying and selling gold/gold stocks) will be protected from the eyes of a prying public. In fact the intent is to gather info on persons who have something to hide.

10) Do not provide legal name, date of birth and place of birth to any internet based service providers. Even if the service provider does not voluntarily pass on this info hacker can obtain it (as was the recent case with Twitter). This information can be utilized by third parties to obtain your SIN number.

11) If you wish to prevent loss of important files/data then:

(a) Utilize a hardware firewall. This is typically a router which is connected between your modem and your PC. Routers can be purchased for about \$40.

(b) Utilize software firewalls (Windows based and/or one provided with your anti virus software).

(c) Utilize anti spam and virus protection.

(d) Back up your sensitive info (e-mails, addresses, documents, photos) at least one per month. A quick form of backup is an older PC connected via the router.

Note: Don't use your backup PC for internet surfing!!!

12) Check your PC's security against threats by going to the Symantec site and running their "Security Scan" and "Virus Detection" scans. These take time so be patient. You will receive comprehensive reports at the end of each scan.

13) Check your PC periodically with a test/benchmark program. Keep track of your PC's performance. A substantial reduction in performance could indicate that you have been "virus-ed".

14) If you suspect that you have been "virus-ed" then go to the MS Windows Security & Updates page and download the Windows Malicious Software Removal Tool. This tool may require other MS software to be first loaded before it can run on your PC. Follow the instructions as they pop up. Once the software is downloaded and installed it will take time for it to scan your PC for malicious software and to remove it.