Protect Your Computer

Everyone had heard of Viruses, Worms and Trojans. The general term used is Malware. This term is derived from the words **Mal**icious Soft**ware.**

For some details on the differences between them visit: http://technet.microsoft.com/en-us/library/dd632948.aspx

How to help protect your computer from malware

There are several free ways to help protect your computer against malware:

- Make sure automatic updating is turned on to get all the latest security updates.
  - Start > Programs > Windows Update
  - When the Windows Update window opens Click on the link to Automatically Update
  - It may take a while depending on how long it has been since your computer was updated
  - Once the Windows Update is complete it will notify you if you need to restart your computer to finish installing updates, and give you the opportunity to restart right away or postpone the restart. If you're away from your computer for an extended period of time, Windows will automatically restart your computer. Windows does this to help make sure all the latest security and other important updates are applied in a timely manner to help keep your computer more secure.
- Never turn your firewall off. A firewall puts a protective barrier between your computer and the Internet.
  - Click on Start > Control Panel > Windows Firewall > Click on Turn Your Firewall On
- Don't open spam email messages or click links on suspicious websites.
- Download a free antivirus program. I use Microsoft Security Essentials, (see the warning below).
- Scan your computer with the Microsoft Safety Scanner.

Warning: Cybercriminals sometimes try to trick you into downloading rogue (fake) security software that claims to protect you against malware. This rogue security software might ask you to pay for a fake product, install malware on your computer, or steal your personal information.
Don't click links in email messages and avoid websites that offer free software—especially free antivirus software. For more information, see Watch out for fake virus alerts .

- Be very cautious about opening attachments or clicking links even if you know the sender. Call to ask if a friend sent it. If not, delete it.
- If an email has **F**W in front of the Subject that means it has been forwarded to others and it could have picked up a virus from those other computers.
- Avoid clicking Agree, OK, or I accept in banner ads, in unexpected pop-up windows or warnings, on websites that may not seem legitimate, or in offers to remove Spyware or viruses.
- Instead press CTRL + F4 on your keyboard. If that doesn't close the window, press ALT + F4 on your keyboard to close the browser. If asked, close all tabs and don't save any tabs for the next time you start the browser.
- Only download software from websites you trust. Be cautious of 'free' offers of music, games, videos, and the like. They are notorious for including malware in the download.
- Use strong passwords, of at least 14 characters and include a combination of letters, numbers, and symbols.
- Don't share passwords with anyone.
- Don't use the same password on all sites. If it is stolen, all the information it protects is at risk.
- Create different strong passwords for the router and the wireless key of your wireless connection at home.