How to protect from Malicious Software

People use the term "virus" for any piece of software that make harm to their computer. But a computer "Virus" is only one form of harmful software among many others which are purposely prepared to do harm to computers or computer networks. Some of them are worms, spy ware, ad ware, etc. The common term used to define all of this harmful software is "Malicious software" and short term is "Mal ware".

A Mal ware can destroy your data in the computer, shut down networks/services by creating enormous amount of data traffic and it may cost considerable amount of money and time to recover. Also sometimes it may not be able to recover the systems back to the original condition with a permanent loss of your valuable data.

To protect your computer from this harmful software you need to get some basic understanding on the behavior of each type of Mal ware and how to defend.

Virus

A Mal ware can be called as a "Virus" only when if it fulfills the following 3 requirements.

- It should make harm to the computer or its information
- It propagates with the support of another file (host file)
- It can add or send a replica of itself to its selected targets

Worm

It is a self spreading malicious piece of software. It uses the network connection of the existing computer to propagate and infect other computers. It doesn't need a host file to spread as a "virus".

Spy ware and Ad ware

There are malicious web sites that distribute this type of Mal ware. If you access those web sites this software will be installed secretly on your computer.

The intent of these programs is to collect your interests so that some web sites can tailor their advertisements to those interests. They send the list of web sites (URLs) that you are visiting to a Internet connected computer or store them in your computer itself in small files known as "Cookies".

Spy ware may also collect your personal information; Credit card numbers etc. and send them outside without your knowledge.

Spy ware and Ad ware may also degrade the performance of your computer, steal confidential data, capture passwords, destroy data etc.

Let's see how we can defend against those Mal ware. Most of the Anti Virus software has the ability to detect viruses and other forms of Mal ware. So make sure that you have installed an anti virus software in your computer and it is running.

These anti virus software are looking for specific command sequences used by known viruses called "Signatures" in the files on your computer to detect Mal ware. So it is very important to update the data base of known signatures by updating the anti virus software. Otherwise the installed anti virus software may not be able to detect newer mal ware and your computer is vulnerable to them. There are both free and commercial anti virus software available for selection.

Following tips will also help you to keep your computer Mal ware free.

- Use strong password to each and every computer user accounts
- Keep all of the installed soft ware , operating system up to date
- Configure your installed applications considering security
- Don't copy or open files from USB drives, diskettes, CD ROMs received from untrusted sources.
- Don't open emails or email attachment received from suspicious sources
- Surfing / downloading from unknown web sites is dangerous

It is impossible to protect any computer system interacting with outside world with a 100% guarantee even though you are using the world best anti virus and security practices. But the above tips will help you to protect your computer to some extent by making harder the job for Mal ware since your data and information is very important to you.