Title:
Computer Viruses - the basics

Word Count:
595

Summary:
This article is intended for the new or casual computer user who wants to know about man made viruses (aren't they all?) that may plague system files, internet files, hard drives and e-mails and what to do about it.

Keywords:
Computer viruses,pc viruses,system crashes,drive crashes,anti-virus protection,virus definition list,data crashes,spyware,adware

Article Body:
In its simplest terms a virus is a disruptive computer code period!
A computer virus almost always repeats itself and spreads by attaching itself to other files. Viruses can be made to host a number of harmful things on any computer from disrupting files to crashing networks. It can even be laying dormant, without you knowing it's there and then attack when least expect it, like right in the middle of downloading a large file or typing a long report.

It can even be made to open at a certain date, sitting like a timebomb until it's time arrives. As you can see it can be annoying at the very least.
I do not want go into all the different types of viruses here because there are so many and more are being made everyday in some dank basement by the Dark Lord.
However, since so many viruses came from unknowingly opening e-mails I would like to mention some basics here:

Never open e-mail attachments unless you know for sure who it's from and that it's safe.
Some mail programs will even ask if you trust the attachment and if you're sure this you want to do. Your computer software can also scan attachments for viruses.
The danger is that when the attachment is opened the virus can attach itself to your hard drive and damage files. Not only that, it can search your saved e-mail addresses and send itself out to your friends, business partners and whoever is on the list, masking the message to look like a legitimate one from you. It will probably have an attachment too and when opened will infect other

computers.

Many people like to download music, video, games or other programs from different sites. If it is a site you dealt with before and trust it may be safe ok, but if you're not sure you can always run a virus scan on the download before installation. (You will need to check the anti-virus program that came with your system on procedures). This security measure is necessary because some downloads may contain virtues, spyware or adware – these last two can collect personal information, note your browsing habits and spam your e-mail with unwanted ads. Some software sites will offer a readme file that shows technical information on the download (if you like tech talk) as well as contact info.
The better sites that offer downloads will test and scan all there software programs before going online with it. As a last resort you can do an internet search for reviews on that particular company to see if others got burned.

This may sound scary to some but the fact is in this world anyone who owns a computer will have to look over there shoulders for hidden attacks when working with online.
That said there are some things should do to prevent viruses from attacking your computer:

* Download the latest virus definition lists (files that tell your computer what to scan for) that's used for your anti-virus program.

* Check to see if your internet service provider has tools to stop viruses before they can reach your mailbox.

* Always back-up your computer on CD-R disks or other media in case you loose some or all your data.

* You can scan software for viruses before installing it. (See system manual for procedure)

* Set your security settings at the highest level.

* Check your web browser and e-mail settings.

Doing these things at least every week will help keep your computer up to date on Virus protection and running safely.