Definition:

A virus is a program whose purpose is to reproduce itself through means of a computer without the knowledge ofthe user(s). Viruses are generallyalways malicious in nature, and can do anything from annoy users to destroy files. Viruses are not spontaneous creations of computers;they are written by people, for all the same reasons that people would want to annoy others inmore traditional manners.

The main purpose of a computer virus (like a biological one) is to duplicate itself. The results of this duplication tend to far outweigh the results of other damage it may cause.The duplication of viruses usually occurs through sending e-mail, which can clog networks to the point of crashes. Even if the virus has no other attack methods, it's using computer cycles that otherwise would not have been used, and without your permission.

How you would get them:

Viruses tend to come attached to files which can execute code. This includes actual programs (usually ending in".exe"), and files which contains script languages that can be runwithin other programs (such as Microsoft Word documents, or ".bat" or ".pif" files; they may also be embedded in ".zip" files). These viruses can begin executing their code in a variety of ways. They may start up immediately upon downloading and opening. Others may trigger when the clock reaches a certain date and/or time.

The majority ofpeople obtain these files downloading them as attachments from email.

How to recognize a virus - On the web:

Many viruses may masquerade as other programs, such as games, or other "freeware." If you are not sure about the authority or credibility of the site you would download said program from, your best bet isto not download from there at all. Or, use anti-virus software to scan a download before opening.

How to recognize a virus - In e-mail:

Viruses are generally "sent" by people you know, which may at first seem confusing. However, there are many indications that the e-mail contains a virus.

The first step is to look at the subject heading. Most viruses thatsend themselves via e-mail contain poorly worded subjects (with lots ofcapital letters in grammatically incorrect sentences). Be suspicious of poorly-worded or -spelled subject lines from people you know, inparticular.

If you have a message with an attachment in your inbox from someone you know, and theyhave not previously told you thatthey will be sending it,you should ask them if they knowthey have sent you such a message by sending them an e-mail before you open the e-mail of the attachment.

If you are using Microsoft Outlook Express as an e-mail client, click to highlight the message in question, and then click the right mouse button to bring up a menu. Choose "Properties," and click the "Details" tab. By clicking "Message Source" inthis area, you will be able to look back and see exactly who the e-mail is coming from without opening it; it's like peeking inside a sealed envelope. Look for something along the lines of "<iframe" . . . >"; this is the code that triggers the virus in Outlook-specific emails. By not even opening the mail, you have potentially saved yourself from further getting involved with a potential virus. If you see <iframe>, delete the mail.

On the other hand, if you receive a message with an attachment from someone you don't know, your best bet is to simply delete the message and be done with it. You can always use the above trick to "peek" inside the message first.

Anti-virus programs:

The most common method for dealing with viruses is the use of anti-virus programs. These programs actively "seek and destroy" viruses on your computers, and can be updated asoften as you wish (to add new viruses to their master list). Generally, these programs will also scan each new file as it is downloaded, to be sure nothing is infected. You can scan a hard drive, a floppy disk, etc. for viruses before anything is even opened from them! This is a great help in keeping viruses off ofyour computer.

Two of the most well-known (and proven effective) are Norton (www.norton.com) and McAfee(www.mcafee.com). Both offer their own anti-virus programs at a reasonable rate, and offer almost daily downloads and upgrades. For these programs to work, however, you MUST download upgrades and patches on a regular basis (these are available on the companies' respective websites).

Other Measures:

1. Turn off the preview pane in Outlook Express. The preview pane shows a message before you open it. Emails with code like <iframe> will execute in the preview pane before you can delete them. To turn off the preview pane, go to your inbox and click View >> Layout and uncheck "Preview Pane."

2. Switch e-mail clients. Outlook Express is a popular program for e-mail. It's also the most vulnerable for viruses. Consider switching to other free programs such as Netscape Messenger or Eudora. Alternatively, check for updates and patches for Outlook at: http://www.microsoft.com/windows/ie/downloads/critical/default.asp

3. Quarantine floppies. Public computers used by multiple users (such as in computer labs) often contain viruses. Designate one floppy to be used on public computers, and scan for viruses before transferring files to your home computer.

Not a virus?:

Not all data corruptionmay be the fault of a virus.Just like any other appliance, computers begin to wear down over time. It may be a sudden thing, but more than likely, it will be a gradual downward spiral.If you find data being corrupted, yet antivirus software finds noproblems, you may want to look into checking your hardware for problems.