Computer Virus Identification and Prevention

Even though new computer viruses are created almost daily, there are practical steps you can take to prevent these viruses. This article will define a computer virus, identify the most common virus sources, highlight the three virus protection steps, and finally explain your role in virus protection.

A computer virus is a software program written to damage other computer programs; some viruses will actually erase everything on your computer, and others will randomly pick a document in your computer and email it to everyone in your address book. Viruses self-replicate and attach themselves to files such as documents, presentations, and system files and can be spread by email, CDs, and floppy disks. Viruses may also infect hardware such as system memory and hard drives.

There are several warning signs associated with viruses. Files that increase in size randomly, the appearance of unknown files, lost files, the inability to save files, corrupted files, sudden lack of hard drive space, the inability to access programs, your system not starting or closing correctly, or strange messages appearing on your screen are all telltale signs that you might have a virus.

Protecting Your Information: There are three basic steps to virus protection: prevention, detection, and eradication.

Prevention—You must install virus protection software in order to detect, eradicate, and report viruses. There are several programs out on the market, and all are very reasonable in price. It is much cheaper to buy virus prevention software than it is to fix a computer once it's infected. Of course, you also need to update your virus definitions frequently; new viruses are created every day, and it's up to you to make sure that your software is up to date by checking with your anti-virus software's website or running updating software, which will automate the task for you. A final and important step in prevention is to delete email attachments without opening them and to refrain from downloading files from the Internet.

Detection—Installing the program is not enough to prevent viruses. It's up to you to make sure the program is run on a regular basis—twice weekly is usually enough. It's also a good idea to run the program manually on occasion to make sure it is doing its job.

Eradication—When a warning is given about a virus being detected on your computer, you must act quickly and quarantine the virus, delete it, and repair the compromised program; most virus protection programs do this for you.

Following these three simple rules is the best way to prevent your information system from being attacked by viruses. Virus protection software can handle most threats from viruses as long as the software is regularly updated. Anti-virus software relies on people like you to provide information on new viruses so antidotes can be created quickly, and with new viruses being generated daily, it is essential that your virus definitions are up to date.