Pahdi Yadav

Professor Milton

English 101

Antivirus Program

Today, people rely on computers to create, store, and manage critical information, many times via a home computer network. Information transmitted over networks has a higher degree of security risk than information kept in a user’s home or company premises. Thus, it is crucial that they take measures to protect their computers and data from loss, damage, and misuse resulting from computer security risks. Antivirus programs are an effective way to protect a computer against viruses.

An antivirus program protects a computer against viruses by identifying and removing any computer viruses found in memory, on storage media, or on incoming files. When you purchase a new computer, it often includes antivirus software. Antivirus programs work by scanning for programs that attempt to modify the boot program, the operating system, and other programs that normally are read from but not modified. In addition, many antivirus programs automatically scan files downloaded from the Web, e-mail attachments, opened files, and all types of removable media inserted in the computer.

One technique that antivirus programs use to identify a virus is to look for virus signatures, or virus definitions, which are known specific patterns of virus code. According to Shelly and Cashman, many vendors of antivirus programs allow registered users to update virus signature files automatically from the Web at no cost for a specified time. Updating the antivirus program’s signature files regularly is important, because it will download any new virus definitions that have been added since the last update.

Methods that guarantee a computer or network is safe from computer viruses simply do not exist. Installing, updating, and using an antivirus program, though, is an effective technique to safeguard your computer from loss.

Bulowski points out that most antivirus programs also protect against words and Trojan horses.