Most computer users know what antivirus software is, but have no idea how it works. Knowing how it works is key to choosing the right virus protection for your system.Following is an overview of how antivirus software works.

Antivirus software is basically computer programs that protect your system from malicious or damaging software. The name antivirus software has its genesis in the fact that it was originally designed to fight computer viruses. Now, it has evolved into a more sophisticated, all encompassing virus protection program. It targets phishing attacks, destructive worms, Trojan horses and a host of other malware that can destroy your system.

**The 2 Methods Used by Antivirus Software to Protect Your System**

Antivirus software uses two different approaches to protect your system:

**(i) scanning files and**

**(ii) targeting suspiciously behaving files from computer programs that may be infected.**

Scanning: Scanning can be explained by the law enforcement analogy of police lineups. Basically you match a perp (a suspect) to a photo. To explain, when antivirus software scans a hard drive, for example, it is referred to as the virus dictionary approach.

It is so named because it is looking for a match between a file on your hard drive and comparing it to a dictionary of known viruses. If any piece of code in a file on your hard drive matches the known virus in the dictionary, then the antivirus software swings into action, taking one of the following three actions:

Repair the File: The antivirus software will try to repair the infected file by removing the virus; or

Isolate the File: The antivirus software will attempt to provide virus protection by making the file inaccessible programs. This keeps the virus from spreading; or

Delete the File: The antivirus software will delete the file, which is arguably the most drastic form of virus protection.

The dictionary approach requires computer users to constantly download updated versions of their virus protection software. This is because new entries (ie, viruses, malware, etc.) are constantly being added to the dictionary.

Dictionary based antivirus software usually starts working when a computers operating system either opens, closes, emails or creates them. However, a user can set up their system to be constantly monitored by scheduling the antivirus software to scan files on a consistent basis. This can be daily, weekly, monthly, etc. In short, however often they want.

The Suspicious Behavior Approach: The suspicious behavior approach to virus protection is different from the dictionary approach. It monitors all of the programs on a system instead of attempt to identify known viruses.

For example, if one program tries conduct a suspicious activity like writing data to an executable program, the antivirus software will alert the user to this and inquire about what steps it should take, if any.

One of the advantages often cited of using the suspicious behavior approach for virus protection is that it offers protection against new viruses. Remember, with the dictionary approached, the virus has to first be identified and listed.

To use another law enforcement analysis, this is like staking out a suspect because of his behavior. Even though he hasn't done anything yet, the actions he has taking alerts you to the fact that he might be up to something.

telefon dinleme