When you buy a new computer you must protect your investment from malicious software programs such as viruses, worms, spyware, and trojans. These programs can cause serious damage to your computer system by erasing data or providing your sensitive data to criminals. You can help protect your personal computer by installing antivirus software to remove and prevent nasty viruses and spyware.

There are various antivirus programs available on the market and while they all do the same job, there are several things to keep in mind when choosing a program.

First you will want to consider the ease of use of the software. The average computer user is not tech savvy so you will want your antivirus software to be very user friendly. Look for features such as easy configuration as well as scanning your system on demand. The software should also automatically check for updates.

A good antivirus program will also be able to remove dangerous viruses, trojans, and worms and prevent new ones from infecting your computer. If the program cannot completely remove these viruses, it should at the minimum be able to keep the virus from spreading.

It is also important to ask if the software is a system hog. Many antivirus programs can use up a lot of your computer’s resources slowing down your system. This can cause problems if you plan on running your antivirus software in the background while you continue to work. There are many good programs available that use resources more effectively. They run unnoticed in the background while you continue to work normally.

Some antivirus programs do include spyware prevention but in order to be fully protected, you may opt for purchasing separate spyware software as well. A separate spyware program can help ensure that your computer is safe from spyware issues that a combo program may not be equipped to catch.

It is quite possible you are inundated on a daily basis with spam mail and unwanted pop-ups which advertise the latest in spy-ware and antivirus protection. As un-amusing and counterintuitive as it may be, competition and the effective differences between competing antivirus application developers is so tight, that even the manufactures of antivirus programs are willing to exploit your computers weaknesses to advertise their solutions.

The sheer size and efficiency of the internet as well its billion-plus users makes new computer viruses more dangerous and virulent than ever. Viruses can literally spread around the globe in only minutes, effecting thousands of unprotected and unprepared users and businesses virtually instantly and simultaneously. The need for antivirus protection is of paramount concern for virtually all PC users.

First Things First: What IS a Computer Virus?

To be considered a true computer Virus, a program needs the ability to replicate itself and trigger its activity at specified events. A computer virus is just one of three types of programs known as "maliceware". "Maliceware" are applications designed to damage, delete or steal your information, hijack your computer and even damage or destroy your computers hardware. The three types of "maliceware" you need to concern yourself with are Viruses, Trojans and Worms. Most antivirus programs are designed to detect and defend your PC from all three threats.

What Does an Antivirus Program Do?

Antivirus programs take two common approaches to recognize threats to your computer.

1. Signature Detection: Via Signature Detection an antivirus application scans your computer, drives and storage devices for files that contain a code it recognizes as a virus variant.

2. Activity: An antivirus application will monitor the activity on your computer for suspicious behaviors i.e. modification of system files or folders and unauthorized connections to the internet to name two.

Signature detection generally requires the manufacturer of an antivirus application to obtain a copy of a specific virus and then reverse-engineer it to obtain markers relevant to its programming. These markers are then loaded into your antivirus software via updates. Signature detection is a sound methodology for detecting and protecting against computer viruses, however it can be rendered useless when faced with a virus for which is has no definition.

Antivirus applications that scan for potential computer virus activity can be more useful at detecting the latest threats than those reliant on signature detection. It is important to note that because many applications perform the same activities as a virus - writing and changing system files for example - a user can quickly become inundated with numerous and unnecessary warnings by antivirus applications that utilize this method for detection.

Most of today's "solid" antivirus programs utilize a combination of both signature detection and virus activity to protect your computer against threats.

How to Choose the Antivirus Program that is Right for You.

If you try surfing the web for insight into what is the best antivirus program or manufacturer, you will quickly find yourself neck deep in a sea of advertisements which profess themselves to be legitimate and impartial evaluators of the available programs. The truth is, of the major manufacturers, no one solution can provide for all of your potential needs. They all have instances where they are not as effective as the competition at detecting or eliminating a specific infection or threat. There are many good Antivirus applications and manufacturers all vying for your business, be it for personal or business use, and choosing the correct application or manufacturer for your computer security can generally come down to a few simple questions.

How at Risk are You?

Asking yourself this question is perhaps the first and most important step toward choosing what degree of protection you need, and how much money you are willing to spend, on Antivirus protection. Risk generally equates to your computers exposure to outside applications, files or connections. If you were to operate a computer that would never come into contact with any program or file not manufactured by a secure source, then you have virtually no need for an Antivirus application. Simply put, if you never plan to connect your computer to the internet, download files with it or upload "at risk" files from outside data sources, you should have no need for Antivirus software.

If you are a casual user who perhaps connects to the internet on occasion through a temporary or dial up connection and only download or upload files and programs from reasonably secure sources, your need for an antivirus program is clear, however, your risk may be minimal. In this situation the types and range of protective applications can be kept to a minimum; a basic antivirus program designed to regularly scan your hard drive for infections should offer you the protection that you need. There are many good antivirus programs that will fit this need available as shareware - a free download - throughout the internet.

Now, if you are like what I would consider to be the majority of today's computer users, you are a high risk user and need a wide variety of the most up to date antivirus programs available. If you have a broadband internet connection which keeps your computer connected to the internet 24/7. If you regularly upload and download files and applications from random and un-trusted sources, you need to invest in very thorough security for your computer. High risk users should invest in an antivirus program that offers real time scanning of all incoming and outgoing connections or files, a firewall to prevent unauthorized access to your PC via an open broadband connection, a pop-up blocker that prevents your computers web browser from being hijacked and adware scanners that detect pop-up, spy-ware, tracking and redirection software.

Are you Purchasing for Business or Home?

Antivirus software manufactured for business and home can be two very different applications both in cost and effectiveness. Home versions generally cost less and come with fewer options than business based antivirus programs. Generally the home user does not need the added functionality built into business versions and as such, I would not recommend that a home user invest in an antivirus solution designed for business.

Good antivirus software designed for business is focused on security, both from external and internal threats, as well as ease of maintenance. Most corporate versions of antivirus applications allow for a central point of control over entire networks. Protection can be divided between internet or application servers and individual PCs. New software updates are generally "pushed" from a central application server through the entire network, allowing for simplicity and assure-ity of a network's protection. Most times, corporate versions of antivirus applications do not allow individual users within a network to make changes to their protection settings; this is of key importance when considering overall network security and stability.

As a business purchasing a corporate class antivirus suite, it is important that your protection extends to each individual user that will access your network. Exchange/mail and internet server protection is a must, as well as protection for mission-critical file and application servers. It is a good rule of thumb for IT managers within corporate environments to assume that all their users will do everything within their power to infect corporate equipment with viruses and threats. Though this most certainly is not true, assuming that users know how to protect themselves or their corporate computer environment from infection is in most cases professional suicide for the IT manger in charge.

Antivirus software for business is generally loaded with more options than software built for home, and as such is often times much more expensive on a whole. Usually business antivirus programs come as a server based application. Clients, or additional licenses, are purchased for each computer or user that connects to the antivirus server.

With Regard to the Antivirus Program Itself:

Determining the true quality and effectiveness of an antivirus program can sometimes come down to how often the manufacturer releases updates to the program. New viruses are introduced to the web on most certainly a daily, if not hourly basis. The best antivirus manufacturers release updates on a daily basis and often offer updates to their programs on a real-time, as needed basis. The ability for an antivirus software manufacturer to release constant, and relevant, updates to their programs should be of great concern to the user. Not having the latest updates can almost be as dangerous as having no protection at all.

Other Important Factors to Consider:

1. The programs compatibility with your current set up and operating system? - If you are still using Windows 98 and you are purchasing an antivirus software manufactured in 2006, chances are it is not compatible with your computer.

2. How much in the way of system resources does the program use? - Just like all applications and operating systems, antivirus applications will use your computers processing power, memory and storage space to function. Keeping this use to a minimum will help to keep your computer operating at peak performance.

3. What kind of protection does the software offer? - Does the program offer protection against multiple threats such as Worms and Trojans? Will the program scan incoming and outgoing

text messages and e-mails?

4. Cost - How much will the protection cost you over the life of your usage? - Most antivirus programs require that you subscribe to their service and then purchase updates on a yearly basis. The costs of these updates can vary widely between manufacturers and should be considered when making your final decision.

Answering these questions truthfully though an honest assessment of your PC usage will help to guarantee that you invest the proper amount of money and time into ensuring your PC and data are safe and secure.

telefon dinleme