All you need to know about Pc protection

Husanboy Bayern

Official Website

This Page Intentionally Left Blank

Keep Your Firewall Turned On

Firewall helps protect your computer from hackers. If you've been having troubles with Firewall, don't turn it off, rather, go into security options and make sure that it knows when to make exceptions. A Firewall can block important downloads and slow down online gaming and so on, but without the Firewall, you're going naked against hackers.

Install or Update Your Antivirus and Antispyware Software

Still don't have Anti-Virus and Anti-Spyware Software? Install one right away!
Anti-Virus and Anti-Spyware software work based on a database of known malware. In order to keep your data safe, you need to keep that database up to date. That being said, be careful that you only go with known, reliable security software. There a lot of programs out there that claim to be anti-viral software but are in fact Trojans and malware designed to create pop-ups and crash your computer under the guise of protecting you.

Keep Your Operating System Up to Date

Still using Windows 98? That may be why your computer acting funny. By keeping your operating system up to date, you can deal with two problems. First of all, you'll find that your anti-virus software is more compatible when you keep your OS updated. This means that you won't be experiencing system crashes and errors whenever the software tries to update. Secondly, you can more easily tell the difference between a real virus or hacking attempt, versus the issue of just plain having an outdated operating system that acts slow, isn't compatible with your software, and makes it hard to get work done on your laptop or PC.

Watch What You Download

Don't just download everything that comes your way in your email. Make sure that you know what it is, and that you scan it for viruses before right clicking and saving target as.

Turn Your Computer Off Now and Then

When your computer is always on, and always online, it's always open to an attack. Turn your computer off when you go to sleep or leave for work (or home, if it's your computer), and you'll not only stay safe, you'll save electricity.

10 Quick Tips:

1. Keep your web browser up to date.
2. Keep your security updates updated.
3. Keep all of your software updated, too.
4. See if your online bank offers free anti-virus software to their members.
5. Download software from official sources or known third parties (e.g microsoft.com).
6. Bookmark some forums, because most free software doesn't include technical support.
7. Keep your protection software up to date.
8. Scan for malware weekly.
9. Scan your plug-in devices, too.
10. If you don't know where an email link takes you, don't click it.

PC Protection Jargon:

1. **Adware** - Displays annoying advertisements on your computer, such as pop-ups etc.
2. **Malware** - A malicious software, which can harm your computer.
3. **Phishing** - Criminals attemptions to obtain users personal information, usually by directing victims to their fake websites.
4. **Rogueware** - Software designed to force you to pay for a useless fake anti-virus software, by falsely stating that your computer is on a risk.
5. **Rootkit** - Malware that hides deep in your computer; it's hard for antivirus software find.
6. **Spam** - Junk email that can include all the above.
7. **Spyware** - Collects private information from your computer and web browsing habits.
8. **Trojan** - Harmless-looking software that gives hackers an access to your computer.
9. **Virus** - A rogue program that infects and harms computers.
10. **Worm** - A program designed to automatically infect lots of computers with viruses or some of the above.

This Page Intentionally Left Blank

Computer, machine that performs tasks, such as calculations or electronic communication, under the control of a set of instructions called a program. Programs usually reside within the computer and are retrieved and processed by the computer’s electronics. The program results are stored or routed to output devices, such as video display monitors or printers. Computers perform a wide variety of activities reliably, accurately, and quickly.

Web Site, in computer science, file of information located on a server connected to the World Wide Web (WWW). The WWW is a set of protocols and software that allows the global computer network called the Internet to display multimedia documents. Web sites may include text, photographs, illustrations, video, music, or computer programs. They also often include links to other sites in the form of hypertext, highlighted or colored text that the user can click on with their mouse, instructing their computer to jump to the new site.

Computer Program, set of instructions that directs a computer to perform some processing function or combination of functions. For the instructions to be carried out, a computer must execute a program, that is, the computer reads the program, and then follows the steps encoded in the program in a precise order until completion. A program can be executed many different times, with each execution yielding a potentially different result depending upon the options and data that the user gives the computer.

Programming Language, in computer science, artificial language used to write a sequence of instructions (a computer program) that can be run by a computer. Similar to natural languages, such as English, programming languages have a vocabulary, grammar, and syntax. However, natural languages are not suited for programming computers because they are ambiguous, meaning that their vocabulary and grammatical structure may be interpreted in multiple ways. The languages used to program computers must have simple logical structures, and the rules for their grammar, spelling, and punctuation must be precise.

Virus (computer), a self-duplicating computer program that spreads from computer to computer, interfering with data and software. Just as biological viruses infect people, spreading from person to person, computer viruses infect personal computers (PCs) and servers, the computers that control access to a network of computers. Some viruses are mere annoyances, but others can do serious damage. Viruses can delete or change files, steal important information, load and run unwanted applications, send documents via electronic mail (e-mail), or even cripple a machine’s operating system (OS), the basic software that runs the computer.

HOW INFECTIONS OCCUR

A virus can infect a computer in a number of ways. It can arrive on a floppy disk or inside an e-mail message. It can piggyback on files downloaded from the World Wide Web or from an Internet service used to share music and movies. Or it can exploit flaws in the way computers exchange data over a network. So-called blended-threat viruses spread via multiple methods at the same time. Some blended-threat viruses, for instance, spread via email but also propagate by exploiting flaws in an operating system.

Traditionally, even if a virus found its way onto a computer, it could not actually infect the machine—or propagate to other machines—unless the user was somehow fooled into executing the virus by opening it and running it just as one would run a legitimate program. But a new breed of computer virus can infect machines and spread to others entirely on its own. Simply by connecting a computer to a network, the computer owner runs the risk of infection. Because the Internet connects computers around the world, viruses can spread from one end of the globe to the other in a matter of minutes.

Preparation and Prevention

Computer users can prepare for a viral infection by creating backups of legitimate original software and data files regularly so that the computer system can be restored if necessary. Viral infection can be prevented by obtaining software from legitimate sources or by using a quarantined computer—that is, a computer not connected to any network—to test new software. Plus, users should regularly install operating system (OS) patches, software updates that mend the sort of flaws, or holes, in the OS often exploited by viruses. Patches can be downloaded from the Web site of the operating system's developer. However, the best prevention may be the installation of current and well-designed antiviral software. Such software can prevent a viral infection and thereby help stop its spread.

Virus Detection

Several types of antiviral software can be used to detect the presence of a virus. Scanning software can recognize the characteristics of a virus's computer code and look for these characteristics in the computer's files. Because new viruses must be analyzed as they appear, scanning software must be updated periodically to be effective. Other scanners search for common features of viral programs and are usually less reliable. Most antiviral software uses both on-demand and on-access scanners. On-demand scanners are launched only when the user activates them. On-access scanners, on the other hand, are constantly monitoring the computer for viruses but are always in the background and are not visible to the user. The on-access scanners are seen as the proactive part of an antivirus package and the on-demand scanners are seen as reactive. On-demand scanners usually detect a virus only after the infection has occurred and that is why they are considered reactive.

Antivirus software is usually sold as packages containing many different software programs that are independent of one another and perform different functions.

When installed or packaged together, antiviral packages provide complete protection against viruses. Within most antiviral packages, several methods are used to detect viruses. Checksumming, for example, uses mathematical calculations to compare the state of executable programs before and after they are run. If the checksum has not changed, then the system is uninfected. Checksumming software can detect an infection only after it has occurred, however. As this technology is dated and some viruses can evade it, checksumming is rarely used today.

Most antivirus packages also use heuristics (problem-solving by trial and error) to detect new viruses. This technology observes a program's behavior and evaluates how closely it resembles a virus. It relies on experience with previous viruses to predict the likelihood that a suspicious file is an as-yet unidentified or unclassified new virus. Other types of antiviral software include monitoring software and integrity-shell software. Monitoring software is different from scanning software. It detects illegal or potentially damaging viral activities such as overwriting computer files or reformatting the computer's hard drive. Integrity-shell software establishes layers through which any command to run a program must pass. Checksumming is performed automatically within the integrity shell, and infected programs, if detected, are not allowed to run.

Containment and Recovery

Once a viral infection has been detected, it can be contained by immediately isolating computers on networks, halting the exchange of files, and using only write-protected disks. In order for a computer system to recover from a viral infection, the virus must first be eliminated. Some antivirus software attempts to remove detected viruses, but sometimes with unsatisfactory results. More reliable results are obtained by turning off the infected computer; restarting it from a write-protected floppy disk; deleting infected files and replacing them with legitimate files from backup disks; and erasing any viruses on the boot sector.

VIRAL STRATEGIES

The authors of viruses have several strategies to circumvent antivirus software and to propagate their creations more effectively. So-called polymorphic viruses make variations in the copies of themselves to elude detection by scanning software. A stealth virus hides from the operating system when the system checks the location where the virus resides, by forging results that would be expected from an uninfected system. A so-called fast-infector virus infects not only programs that are executed but also those that are merely accessed. As a result, running antiviral scanning software on a computer infected by such a virus can infect every program on the computer. A so-called slow-infector virus infects files only when the files are modified, so that it appears to checksumming software that the modification was legitimate. A so-called sparse-infector virus infects only on certain occasions—for example, it may infect every tenth program executed. This strategy makes it more difficult to detect the virus.

By using combinations of several virus-writing methods, virus authors can create more complex new viruses. Many virus authors also tend to use new technologies when they appear. The antivirus industry must move rapidly to change their antiviral software and eliminate the outbreak of such new viruses.

VIRUS-LIKE COMPUTER PROGRAMS

There are other harmful computer programs that can be part of a virus but are not considered viruses because they do not have the ability to replicate. These programs fall into three categories: Trojan horses, logic bombs, and deliberately harmful or malicious software programs that run within a Web browser, an application program such as Internet Explorer and Netscape that displays Web sites.

A Trojan horse is a program that pretends to be something else. A Trojan horse may appear to be something interesting and harmless, such as a game, but when it runs it may have harmful effects. The term comes from the classic Greek story of the Trojan horse found in Homer's Iliad.

A logic bomb infects a computer's memory, but unlike a virus, it does not replicate itself. A logic bomb delivers its instructions when it is triggered by a specific condition, such as when a particular date or time is reached or when a combination of letters is typed on a keyboard. A logic bomb has the ability to erase a hard drive or delete certain files.