

Snelling Web Development

Phone: 702.341.5358

Website: <http://www.snellingwebdevelopment.com>

Email: info@snellingwebdevelopment.com

PC's and COMPUTER VIRUSES

By James E. Snelling

This article was originally published as:

"PC's and Computer Viruses", Snelling, James E., Win95 Magazine, Oct. 1997

What is a computer virus? What does a virus do? How does a virus work? How do I get a virus? Can I get a virus reading email? What can I do to prevent getting a virus? What can I do if I get a virus? How do viruses affect Windows 95?

In this age of unprecedented information exchange and communication, where millions of computers are hooked up over vast networks, and millions of files are transferred daily, these questions and more are being asked by an increasing number of computer users worldwide as the incidence of computer virus attacks continue to grow. No longer the rarity that they used to be, virus attacks now pose a real threat to nearly all computers worldwide. Viruses can infect, and spread from, computers used for games, online services, the Internet, business, networks, programming, and just about any other use. Not unlike biological viruses, computer viruses can replicate and spread from computer to computer. The effect viruses have can range from the non-damaging, yet annoying, display of messages on your computer screen, to serious damage such as corrupting programs, deleting files, or reformatting your hard drive. This article will concentrate on viruses in the Windows operating system environment, although the information here can also apply to other operating system environments. No assumptions are made about your prior knowledge of viruses, so you can sit back, relax, and enjoy the information you are about to learn.

NOTE: *At this time, there is no real standard for describing or classifying viruses. Many virus experts and research centers around the world have their own way of describing the various aspects of viruses. Although they agree on most topics, there are still some disagreements. For example, an expert may classify a virus a particular way, but another expert classifies it another way. Or a particular virus may have more than one name simply because of the lack of convention among experts. This article has drawn information from dozens of different sources and attempts to strike a balance between them. As a result, the information in this article may be perceived by virus experts differently. Also, this article concentrates on the basics of viruses and is meant to be understandable to the novice as well as to the expert.*

The graphics in this article have been designed and optimized for a display resolution of 800x600 at 16 bit color.

WHAT IS A COMPUTER VIRUS?

A computer virus is a self-replicating program that attaches itself to, overwrites, or otherwise replaces another program in such a way that the virus code is executed when the infected program is executed. Viruses are intentionally written to alter the way your computer operates, without your permission or knowledge. The intended effect that a virus has on a system is considered the "payload". Computer viruses can infect software applications, operating system software, system boot code

and records, device drivers, and just about any other software component. Their primary purpose is to infect, replicate, and spread. Viruses have not been known to damage hardware or destroy the physical components of computers. Viruses are simply programs, like the many other programs on your computer, except that they are designed to do things you and your computer don't like.

RISK OF VIRUS INFECTION

Before we get started, examine **Chart 1** to determine your risk of getting a computer virus:

<p>Low Risk Profile</p>	<ul style="list-style-type: none"> • Single user computer • No modem or network connections, such as to the Internet or online services • Don't trade files on floppy disk • Use only software from trusted sources, such as resellers. • Format all floppy disks before first use
<p>Medium Risk Profile</p>	<ul style="list-style-type: none"> • Trade files on floppy disk • Network connection • Buy software from unknown sources, such as computer swap meets • Use used, preformatted floppy disks • Use shared network programs • Use floppy disks from unknown sources
<p>High Risk Profile</p>	<ul style="list-style-type: none"> • Modem with connection to the Internet or online service • Network connection • Trade files or programs on floppy disk • Download many programs from online services or the Internet • Use pirated software • Other people use your computer • Use used, preformatted floppy disks • Use floppy disks from unknown sources • Use shared network programs

Chart 1

BOOT DISKS

To gain a better understanding of how viruses work, I'll first have to introduce you to some basic knowledge about disks and bootable disks. Every PC floppy disk and hard disk contains a boot sector. The boot sector contains information about the data on the disk, the disk's architecture, and formatting. On bootable floppy disks and hard disks, the boot sector also contains the boot record program, which is responsible for starting and loading the operating system during your computer's start up.

A computer's bootable hard disk also contains the Master Boot Record (MBR). This contains the Master Boot Program, which tells the computer to load the boot record program from the bootable hard disk, and also contains information about how a hard disk is partitioned.

A bootable floppy disk is a disk that contains the necessary information for starting the computer. Most of the time, your hard disk is considered the disk you boot from, since it contains all the essential files necessary to start your operating system. A bootable floppy disk also contains these essential files, so that in case your hard disk encounters problems and cannot successfully load the operating system, you insert the bootable floppy disk into the floppy disk drive, then boot, or start, the computer and at least, in most cases, have access to your hard drive to figure out what went wrong. When you first turn on your computer, it looks at the floppy drive to see if there is a boot disk in it, before it goes to the hard drive. If it sees a floppy disk, it tries to find the boot information on it so that it can start the computer. Boot disks are essential to have in case your computer has problems loading the operating system from the hard drive. These problems can be caused by a hard drive crash, viruses, and missing, deleted, or corrupted files.

To create your own bootable floppy disk for Windows 95, click on "Start", "Settings", "Control Panel". In Control Panel, double click on the "Add/Remove Programs" icon. You will now see the "Add/Remove Programs Properties" sheet. Click on the "Startup Disk" tab. You will need one floppy disk that has no data on it. You may also need your Windows 95 program disks or CD. When you are ready, simply click on the "Create Disk" button and follow the prompts. After you are finished, store your new, bootable floppy disk in a safe place.

WHAT DOES A VIRUS DO AND HOW DOES IT WORK?

A virus infects executable program files such as spreadsheet programs, word processing programs, and just about any other program. Viruses can also infect the boot records and master boot records of floppy disks or hard disks, which contain the information your computer uses to start up. Some viruses don't infect other programs and simply replicate as many times as they can to take up space on the computer's hard drive.

A computer virus is inactive until you execute an infected program or boot your computer from an infected disk. When a virus becomes active, it loads into your computer's memory, or RAM, becoming memory-resident, and is ready to infect other programs you execute that become memory resident or floppy disks that you access. Most viruses stay memory resident until you turn off your computer. Turning off the computer removes the virus from memory, but it does not remove the virus from your computer's hard disk or the files it has infected. If the virus has infected a program, it will activate the next time you execute that program. Figures 1 - 4 below, show the typical computer virus infection process. If the virus has infected the boot record or master boot record of a disk, it will activate the next time you start up your computer.

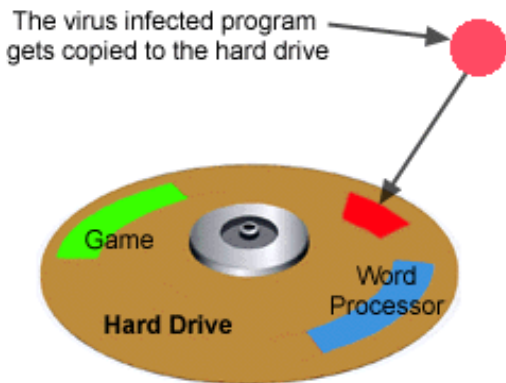


Figure 1

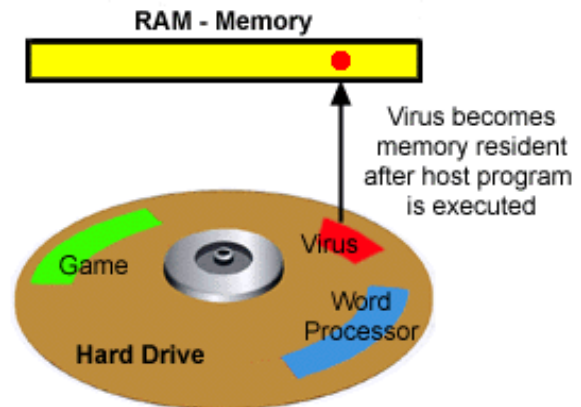


Figure 2

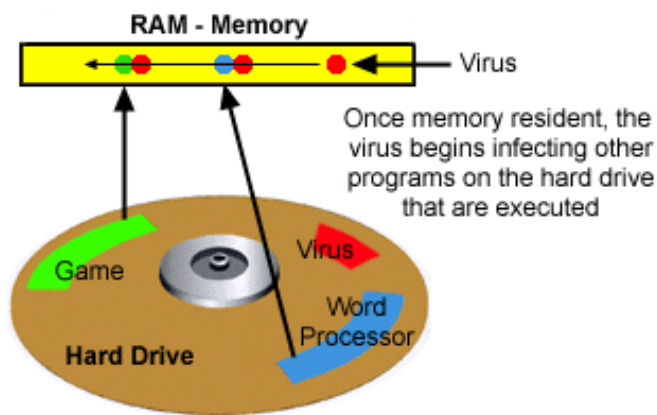


Figure 3

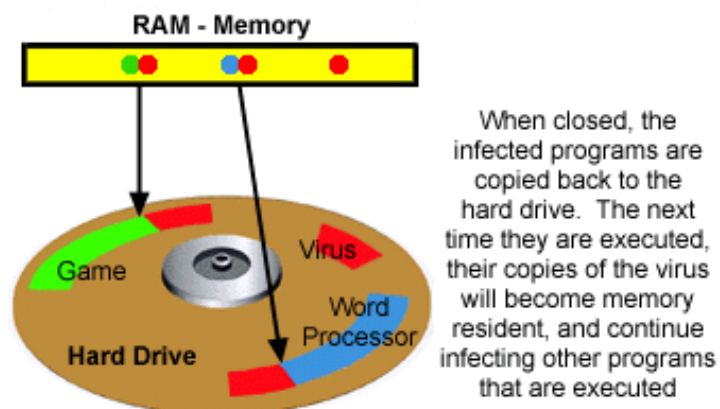


Figure 4

A virus can only activate if it is attached to a program file that is executed. By itself, a virus will not activate, because it relies on the execution of a host program to start it. Viruses typically do not infect data files, like a word processing document or graphic image for this very reason (this does not apply to the Macro viruses, which will be discussed shortly). Data files are not programs and do not execute; they are simply data, like a picture. Sometimes, viruses attach themselves to data files, but this is an accident, and usually results in only the data being damaged. Also, the virus can no longer spread because it is not attached to an executable file. However, viruses can infect the areas of a disk that don't currently have data saved to them, thereby permitting them to possibly infect other executable files and spread.

Most viruses are designed to simply replicate and spread, not damage software. At most, some will display a message from the virus's creator or play a sound. But some viruses are designed to intentionally damage the data on your computer, such as deleting files, corrupting programs, or reformatting your entire hard disk. These types of virus are the most dangerous.

THE CLASSIFICATIONS OF VIRUSES

Although there are well over 10,000 viruses in existence, many are simply modified copies of existing viruses. Most viruses fall into one of four classifications of virus:

- 1) Boot sector virus - This class of virus attaches itself to floppy disks, then copies itself to the boot sector of your hard drive when you turn on or reboot your system with the infected floppy disk in the disk drive. You can only get a boot sector virus from an infected floppy disk that your computer tries to boot from. The virus can infect any floppy disk, regardless of the data or programs on it and can continue to spread to other computers that are booted with the infected floppy disk in the drive. You cannot get a boot sector virus from using programs or files that are on an infected floppy disk. You must boot the computer with the infected floppy disk in the drive to become infected. If you boot a computer with an infected disk, the virus is copied to the computer's hard drive and goes memory resident, and continues infecting any floppy disks that are inserted into the floppy drive. Turning off your computer erases the virus from memory, but does not eliminate the virus from the computer, since it has been copied to the hard drive's boot sector or master boot record. The next time the computer is booted, the virus copies itself from the hard drive to memory and will continue to infect any floppy disks that are accessed.
- 2) Program file virus - This class of virus infects executable files, such as programs. They can infect files with extensions .EXE, .SYS, .OVL, .OVY, .BIN, .DLL, .DRV, .COM, .SCR, and .BAT. However, these viruses commonly infect .EXE and .COM files. Program file viruses work by attaching themselves to, replacing, or overwriting parts of, executable file types. When you start a program that is infected with this type of virus, the virus goes memory resident and continues to infect any other program files that are accessed.
- 3) Multi-partite viruses - This class of virus is a combination of the boot sector virus and program file virus. It will infect both program files and MBR's or both program files and boot sectors.
- 4) Macro virus - This is a fairly new class of virus and is considered by some experts to be a program file virus, although they are also considered the first viruses to actually infect data files. Macros, written in a

programming language like WordBasic, can be used in common office applications, such as Word or Excel, to automate complex or repetitive tasks. Once written, Macros are given a keystroke combination, toolbar button, or menu item which will activate the Macro. A knowledgeable person can use Macros for malicious means, thus the Macro virus. Macro viruses use office applications to replicate and spread. When a user opens a file, such as a word processing document, containing a Macro virus, the Macro will be either automatically run by opening the document or will be executed by the user by a certain key combination, a menu command, or toolbar button. Once run, the Macro virus will copy itself to the office application and will now infect other files that the user opens, creates, or saves. Some dangerous things a Macro virus can do include deleting or changing document contents, change settings in the office application environment, set a password, delete files, etc. Macro viruses are becoming extremely popular due to their simplicity and the widespread use of office applications.

There are also the unknown viruses. These are the newly created viruses that have not yet been officially identified by the anti-virus (AV) communities of the world. On average, about 3 new viruses are discovered everyday. Once isolated, they are researched, and a defense is developed. New viruses are usually based on existing ones, and do not pose a great threat. In addition, active viruses are considered "in the wild", which means that they have been tracked and identified by virus experts to have caused infections outside of laboratory environments. A virus that has never been seen outside of the laboratory is considered "in the zoo."

VIRUS CHARACTERISTICS

All viruses have certain characteristics that fall into pre-defined groups. These characteristics are:

- 1) Trojan - The Trojan is not really a virus, but instead a means of virus delivery. The virus masquerades as a legitimate program, so that the user will not realize that it is a virus. For example, you've downloaded from an online service what you thought was a game program, but when you execute it, it turns out to be virus that infects your computer.
- 2) Polymorphic - The polymorphic virus is one that has been designed to change segments of its own code so that it looks like a different virus from one infection to another. This technique is employed by virus creators to make it harder for anti-virus (AV) software to detect them, since detection software has a harder time of comparing the changing virus to its inventory of known viruses.
- 3) Encrypting - This technique allows the virus to transform itself into something that doesn't look like a virus, in order to avoid detection by anti-virus software. It does this with special code that allows the virus to convert, or encrypt, itself into program code that is non-infectious. But in order to infect, the virus must re-convert, or decrypt, itself into the original virus code, also making it visible to anti-virus software.
- 4) Stealth - This technique gives viruses another tool to make their detection even harder. This characteristic gives a virus the ability to actively conceal itself from being discovered by AV software. There are two types of stealth viruses:
 - a) Size stealth - Once it infects a computer and becomes active in a computer's memory, a virus with size stealth capabilities monitors the opening and closing of all files. If it sees that a file it has infected earlier is about to be opened, it races to the file and uninfected it, so that the AV software doesn't know it's been infected. Once the file is closed, the virus then re-infects it. Another means these viruses have for hiding from AV software is by altering the disk directory data of a file to hide the additional bytes of an infecting virus. When possible, the virus may continue to infect any other files that are accessed on your hard drive.
 - b) Full stealth - Like a size stealth virus, a full stealth virus is memory resident and monitors all file activity. When it sees that an infected file is about to be opened, it redirects the call to an uninfected copy of the file that it made before infecting it. The virus stores the uninfected copy of the file at some other location on the hard drive for just this purpose.
- 5) Triggered Event - A virus can be programmed to activate based on some event. This event is known as a

"trigger event", hence the characteristic name. An event can include a date, a certain keyboard action, or the opening of a particular file. The effect depends on the virus.

6) Memory Resident - A memory resident virus copies itself to the computer's memory when its host program is executed. It no longer relies on the host program to remain active. It stays active in memory, infecting other files, until the computer is turned off.

7) Non-memory Resident - A non-memory resident virus becomes memory resident when the host program is executed. It stays active in memory, infecting other files, until the host program is closed. It can only remain active while the host program is running.

8) Combination - A virus can include one or more of the above characteristics, thus having a combination of characteristics. For example, a particular virus can be a polymorphic encryptor, which means that it combines both polymorphic and encryption characteristics.

HOW DOES A COMPUTER CATCH A VIRUS?

There are many ways that a computer can become infected with a virus. There are also many misconceptions about how a computer becomes infected with a virus. Due to public awareness, AV software, precautions taken by online services, and other efforts, the chances of catching a virus are actually very low. But there are still many entry points to a computer that a virus looks for when looking to infect. By being aware of the various ways a computer can catch a virus, a computer user reduces the chance of infection. Below are descriptions of the myriad of ways that a computer can become infected with a virus.

1) Booting a computer with an infected floppy disk, as described earlier, is one of the most common ways of infecting a computer.

2) Trading data or program disks with other people opens a very ugly door and is one of the most common ways of catching and spreading viruses. Once a disk leaves your hands, you have no idea what it may encounter, especially if the other person does not practice good AV techniques. This also applies to any disks someone gives you. Do you know where that disk has been? As an analogy, you may have caught the common cold from a friend who shook hands with another friend that had a cold. Can you see how computer viruses spread like common cold viruses?

3) Files downloaded from the Internet or online services can also contain viruses. This has been, and is continuing to be, one of the most popular ways of spreading viruses due to many reasons. With millions of downloads occurring daily from the Internet, online services, and BBS's (Bulletin Board Services), it's a virtual open season on unsuspecting users. Since viruses can masquerade as legitimate programs, or be attached to legitimate programs or executable files, catching a virus by this means is very easy. A virus creator simply uploads his or her creation to an online service or Internet site and hopes that the virus is not detected. For example, a person using an online service, or Internet site, finds a simple program, such as a screen saver, that they want to download and install on their computer. This particular program is infected with a virus. Once the user downloads and executes the program, the virus becomes active and sets out to perform its damaging mission.

Most online services and reputable web site servers now scan all files being uploaded to them and downloaded from them for their own protection as well as their customers. Also, popular web browsers now include various levels of safety and warning features to alert the user of a suspect site. AV software has also been adapted to scan files for viruses as they are downloaded. Although the chances of catching a virus from a download is very small due to these measures, the explosive rate of the Internet's growth, technology, and functionality, not to mention the tenacity and ingenuity of virus creators, does lead to oversights and unintentional developments that allow viruses to sneak into computer systems. For example, Microsoft's Internet Explorer web browser was a recent target because of a security "hole" that was the result of its cutting edge ActiveX technology. Although the security "hole" was not a virus, it demonstrated how new technologies can expose unknown weaknesses that malicious programmers may take advantage of. Microsoft quickly released an update to the browser that fixed this problem.

4) Email attachments sent via the Internet or online services are yet another popular way of contracting a virus. This particular subject does require special attention, since many people do not fully understand how viruses and email are related. First off...to shatter a widespread myth...A VIRUS CANNOT BE CAUGHT BY

JUST READING THE TEXT OF AN EMAIL MESSAGE. Email text cannot contain or execute a virus, since the text is not an executable program. Even if a virus writer were to embed the code of a virus into the text of an email, nothing would happen. Where viruses are caught from, though, are the attachments to email that are downloaded and executed. These attached files usually have an .EXE, .COM, or .BAT extension, indicating that they are executable files.

For example, you receive email with an attached file from company "XYZ" that is advertising how to make a million dollars in ten days. The email says to download and execute the attached file, because it has more information on how to make money. So you do. Once you execute the attached file that you have downloaded, you suddenly find your computer doing strange things and that you no longer have control. After running your AV software, assuming that you can, you find that you were just infected with a nasty little bug that's causing havoc on your computer system. Since you haven't read this article to learn more about viruses, you think that the email was infected with the virus, when in fact, it was the email attachment that was downloaded and executed that was the virus. The email was simply an enticement to download and run the attached software.

Also, certain viruses, like the Word Macro viruses, are embedded in Word documents that can be sent as attachments via email. If your email reader is configured to automatically launch Microsoft Word when you receive such attachments, you could infect your computer without knowing it.

5) Surprisingly, brand new, shrink-wrapped software has been known to be infected with viruses. This usually happens when the software, or application, is produced at the factory. A disgruntled employee might insert a virus into the final production code of an application, before he or she quits. Thousands or millions of copies of the application head to market and it's not till customers buy the product and install it that the virus is discovered. This is very rare.

6) In the corporate environment, viruses can spread via networks or corporate intranets. This is becoming more and more common, since networks are becoming very popular. Typically, a network can consist of a few or several thousand computers hooked up to the company's network servers, which allow the sharing of company data and programs to anyone with access. All it takes for a virus infection to happen is just one of those computers becoming infected with a virus. Whether it's one of the computers attached to the network, or one of the network servers itself, once infected, it's only a matter of time before the infection spreads to every computer on the network. This problem is usually avoided, though, by stringent disk access policies, AV software on the network, and limited access to the network.

7) Pirated software is also a popular means of spreading a virus. A person with malicious intent gets a hold of a popular application, infects it with a virus, and either makes it available for illegal download or makes illegal copies of it on disk, to distribute to anyone who wants what they believe are simply pirated copies of the popular software.

PREVENTION OF VIRUSES

With all the possible ways that a computer can become infected with a virus, it's surprising how simple it is to avoid them. By following the guidelines below, you will greatly reduce your chances of encountering a virus, as well as minimize your computer's downtime in the event you do encounter one.

1) Anti-virus software (AV software) - Installing anti-virus software on your computer could be the most important thing you do to protect your system and data. Make sure to use a highly recommended brand of AV software. Check to make sure that it has the capability to scan file downloads and email attachments. Also, choose one that has monthly updates available for free download, so that you can keep your virus scanner up-to-date with the latest AV virus definitions. There are many different methods that AV scanners use when monitoring for viruses. Without going into too much depth, AV scanners can analyze and record basic information about the files on your computer system, such as file size. Anti-virus scanners work by constantly monitoring your system for changes, such as unauthorized hard disk access and file size changes. AV scanners go to work by analyzing every file on the computer, looking for strings of code that match it's library of known virus signatures, or comparing it's recorded information about a file with the current information to see if there has been a change. When a virus is found that matches a known virus, or a file has changed because of a virus infection, the AV software can go to work to disinfect the infected files. Another function of scanners is to remain active in memory at all times, watching all file accesses for possible virus activity and taking appropriate action if virus activity is suspected or found. Advanced AV scanners can also search for

and repair most polymorphic, encryptor, and unknown viruses.

If you don't already have AV software, seriously consider purchasing one. These companies, as well as many others, offer free, downloadable, trial versions of their AV software:

Symantec Corporation: <http://www.symantec.com>

Dr. Solomon's Software: <http://www.drsolomon.com>

McAfee Associates, Inc.: <http://www.mcafee.com>

2) Don't trade floppy disks with other users - Although it sounds like a simple way to prevent viruses, it's not practical in today's world of massive information exchange. But the important point to keep in mind is to reduce the amount of information you exchange with others via floppy disks. A regular habit of exchanging disks with friends or co-workers can lead to a possible virus infection. Keep this type of exchange to a minimum. If you do give your floppy disks to others, make sure to write-protect them by sliding the black tab to the "open hole" position (*see Figure 5 below*). Write-protecting a floppy disk prevents others from writing files to them, such as programs that may have viruses, unless they undo the write-protection. Also, if you have AV software, always scan floppy disks you receive before using them.

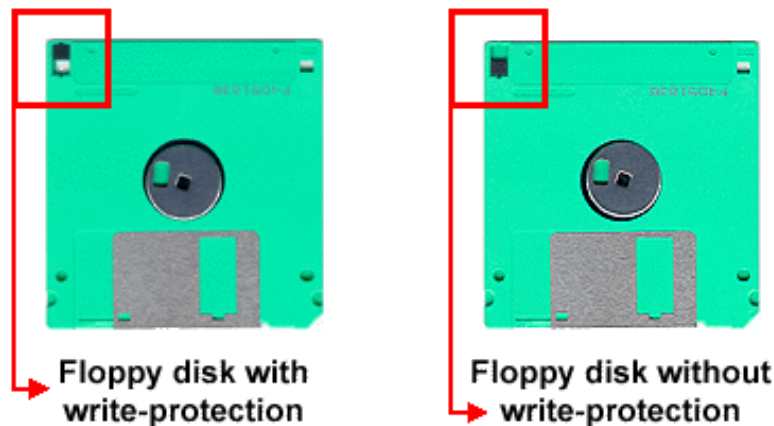


Figure 5

3) Be wary of file downloads and email file attachments - Since the downloading of files from the Internet and online services is very popular, it's possible to encounter a virus from a download. You can minimize the chance of infection by being cautious of what files you download. From the Internet, try and download files only from legitimate or respected sites, such as known companies or organizations. It is rare for such a site to be infected. From online services, the files available for download are usually virus free, since services actively monitor for viruses. However, this does not include file attachments sent to you via email. File attachments are not monitored by online services for viruses, so you're on your own. If you are sent email with a file attachment from someone you don't know, don't download it. Also, do not configure your email reader to automatically launch office suite applications when you receive such office type documents as file attachments, since you could infect your computer with a Macro virus without knowing it. If you do download any files, always scan it with AV software before executing it. Outside of file attachments, online services do their best to avoid viruses.

4) Back-up everything - This doesn't prevent viruses, but does reduce your computer's downtime in the event you lose data because of one. By maintaining regular back-ups of all your data, you stand a better chance of recovering your system in case of a nasty virus infection. If you encounter a virus that damages the data on your hard drive, or find that you have to reformat your hard drive, having all your important data backed up beforehand will make the damage and computer downtime you suffer much less. One note though...it is possible to have a virus infection that goes unknown for a long period of time, thus your back-ups may be

infected since the virus was circulating on your system for days, weeks, or months. AV software usually prevents long term viruses because it is always monitoring your system.

SOME SYMPTOMS OF A VIRUS

The following examples may be indications that a computer has been infected with a virus. Although these problems can be caused by a non-virus problem, they are the most reported symptoms of an infection.

- 1) Programs take longer to load than normal.
- 2) Computer's hard drive constantly runs out of free space.
- 3) The floppy disk drive or hard drive runs when you are not using it.
- 4) New files keep appearing on the system and you don't know where they came from.
- 5) Strange sounds or beeping noises come from the computer or keyboard.
- 6) Strange graphics are displayed on your computer monitor.
- 7) Files have strange names you don't recognize.
- 8) Unable to access the hard drive when booting from the floppy drive.
- 9) Program sizes keep changing.
- 10) In Windows 95, 32-bit errors keep occurring or Windows refuses to use 32-bit file or disk access.
- 11) Conventional memory is less than it used to be and you can't explain it.
- 12) Programs act erratically.

WHAT TO DO IF YOU GET A VIRUS

If your computer becomes infected with a virus, don't panic. You need to remain calm and clear headed in order to eradicate the virus. If you don't feel comfortable dealing with the situation yourself, contact a trained technician to help out. If you have AV software installed, consult the documentation that with came with it. It should guide you step-by-step through the process of identifying the virus and eliminating it. If you don't have AV software, purchase one, or download a free, functioning trial version from an AV manufacturer, if possible. Before installing itself, the AV software will scan your system to identify the virus, then complete it's install and attempt to eliminate it.

Many AV software companies encourage users to submit to them the viruses that were caught by their software. You can also submit what you suspect is a virus. This gives the AV software company a closer look at the virus, to determine if it's a new strain of an existing one, or a completely new, unknown virus, so that they can provide a solution for it in the next monthly update to their virus signatures.

Remember...if at anytime you feel you're in over your head, call a trained AV technician to help. The technician may or may not charge, but it's worth not losing your data and getting your computer back to a productive state.

VIRUS HOAXES

Virus hoaxes are almost as common as real viruses. There are generally two sources for hoaxes. The first one is misinformation and misunderstanding. This is caused by a computer user who executes a non-infected program, but because of other problems with the computer or a bug in the program, it begins to act like it has been infected with a virus. The user panics, thinking that the program he/she just installed is a virus. They post warning messages to online service bulletin boards, tell their friends, send email to others, thus propagating the whole situation.

The second source for hoaxes are pranksters. For amusement, a prankster will make up a story about a virus and begin to circulate a story about what it did to his/her computer. As word spreads, the hoax takes on a life of it's own, to the point where no one really knows if it exists or not, until it is researched by the AV community and declared a hoax.

An interesting footnote in the history of viruses is the AOL4FREE program/virus/hoax. This popular event began as a real program, written by a student, that allowed the user free access to the online service, America Online. This was a real

program, not a virus. After the programmer was arrested and the program's effect eliminated by AOL, someone decided to capitalize on the AOL4FREE name and created a simple program that, when executed, would erase the files on a computer's hard drive. He spread this program around, and users, thinking it was the "real" AOL4FREE program, downloaded and executed it. Needless to say...the program erased files from their hard drive. This is an example of a Trojan Horse...a malicious program masquerading as something else. Other users got into the fray and spread the message, through AOL's email system, that the AOL4FREE program was really a virus that destroyed hard drives, driving the program to such heights that it gained media coverage and a special spot in AOL's backside. From what is known, very few people were ever infected by the Trojan.

WHO WRITES COMPUTER VIRUSES?

Most people imagine computer virus writers as shadowy, underground figures that have complete mastery over computers and programming, whose sole intent is wreaking mass havoc on society. Most of this is not true. After dissecting thousands of viruses, experts have come to the conclusion that most virus writers are average or poor programmers that have a basic understanding of the subject. Many viruses are poorly written and have bugs that cause them to malfunction, preventing them from doing what the writer intended. Also, most viruses are simply copies of existing viruses with minor modifications. The typical virus writer is a student, or computer hobbyist that wants to test his/her programming skills. One of the first things an aspiring programmer wants to create is a virus, due to the lore surrounding them. Thus with barely enough knowledge, they create a virus that is poorly written, a copy of an existing virus, or is too simple to cause appreciative damage. But, there are world class programmers who do create lethal viruses that are considered excellent, and respected, work. It is these viruses that most aspiring virus writers copy. They add their own twist to them and screw them up.

WINDOWS 95 AND VIRUSES

Prior to Windows 95, most PC viruses targeted DOS and earlier versions of Windows. Without AV software protection, they were at the mercy of the virus, since built in protection was very limited. With the introduction of Windows 95, though, the game has changed considerably. Without getting into a technical discussion, I'll explain the various aspects of viruses versus Windows 95.

Although there is no direct virus protection built into Windows 95, it does include several features that make it very difficult for a virus to infect it. These features include blocking direct hard disk access, identifying unknown device drivers, and recognizing modifications to the MBR.

In versions of Windows earlier than Windows 95, a virus, being a program performing it's mission, could make normal DOS operating system calls, or access the hard disk directly, with little trouble. Windows 95, however, has changed the way calls are made to the operating system, including hard disk access, therefore rendering 16-bit viruses impotent when trying to assault Windows 95 or 32-bit applications. If a program or virus attempts to bypass the operating system and write directly to the hard disk, Windows 95 will prevent it from doing so and alert the user with an error message:

["Windows has disabled direct disk access to protect your long file-names. To override this protection, see the LOCK /? command for more information.](#)

[The system has been halted. Press CTRL+ALT+DELETE to restart your computer."](#)

In the case of unknown device drivers, Windows 95 maintains a list of all the real-mode device drivers that it can safely replace with its own protected-mode drivers. If a new device driver is added that hooks the INT13h or INT21h chain, and the driver is not on the list of drivers that can safely be replaced, Windows 95 presents a warning dialog explaining the situation and gives you the chance to remove the suspect driver/virus before it can do any damage.

MBR infector viruses have a hard time with Windows 95, as well. Viruses that infect the MBR also hook the INT13h chain, which allows the virus to monitor hard disk access and damage the data on your hard disk. Each time you start your computer, Windows 95 checks to see which programs are monitoring the INT13h chain, and then compares this list of programs with the list that it recorded the last time Windows 95 started. If any new programs that Windows 95 does not recognize hook the INT13h chain, the following message is displayed:

["WARNING: Your computer may have a virus. The Master Boot Record on your computer has been modified. Would you like to see more information?"](#)

Windows 95 will then present you with a series of steps to troubleshoot the suspect file. This type of infection is most likely to occur when you start your computer using a bootable floppy disk. If the floppy disk is infected with a virus, the virus will likely modify the MBR on the hard disk and hook the INT13h chain. When the floppy disk is removed and the computer is booted normally, Windows 95 recognizes that the MBR has been modified and that the INT13h chain has been hooked by an unknown program. The warnings you receive give you an opportunity to remove the virus before it can damage your data.

Despite these features, viruses may be able to infect via other aspects of the operating system. Viruses may run just fine in a DOS session under Windows 95 or when the computer is booted to MS-DOS instead of Windows 95. Also, there is no protection for floppy disk access. So a virus that could not infect Windows 95 could infect an accessed floppy disk, therefore allowing the virus to spread.

Although Windows 95 is a full-fledged operating system that, technically, does not rely on DOS, it does contain and exhibit several attributes of its ancestor in order to maintain backwards compatibility with the thousands of DOS and 16-bit Windows 3.1 applications still in existence and still being produced.

As a result, 16-bit viruses can still run within a DOS session provided by Windows 95, since Windows 95 is providing a virtual 16-bit environment for them to run within. In addition, to remain backwards compatible with older drivers and devices, Windows 95 starts out in real-mode, reads the AUTOEXEC.BAT and CONFIG.SYS files, and loads any TSR's (terminate and stay resident programs). In this mode, it is possible for a boot-sector virus to infect the MBR or boot sector of a Windows 95 hard disk, since Windows 95 has not yet technically taken control of the system.

Since Windows 95 is a 32-bit operating system, older 16-bit AV software will not work properly due to Windows 95's new file structure, including long filename support. Although they may run and appear to be working, they are not, due to the changes in Windows 95. The user's only option is to upgrade to 32-bit versions of AV software if they wish to prevent infection from 16-bit and 32-bit viruses.

32-bit, Windows 95 specific viruses arrived on the scene shortly after Windows 95 was released, the first being the infamous "Boza" virus discovered in 1996. Several more exist and as the popularity of Windows 95 grows, more virus writers are going to introduce more potent threats to the operating system and 32-bit applications. Speculation on the future of 32-bit Windows 95 viruses centers around exploiting VxDs (Virtual Device Drivers), COM objects (Component Object Model), and further development around the WordBasic and Visual Basic Macro languages, to introduce viruses to the operating system. A more in-depth discussion about viruses in the Windows 95 environment may be the topic of a future article.

CONCLUSION

It's safe to say that computer viruses, like biological viruses, are here to stay. As better methods of detection and repair of viruses are developed, virus writers develop new ways to defeat them. As new computer hardware and software technologies arise, viruses are developed or adapted for them. In some cases, the new technologies assist in the creation of viruses, such as the easier to learn and powerful visual programming languages and environments. Expanding technologies, like the Internet and online services, also help them to survive and spread. As operating systems become more and more advanced, so do viruses to meet the challenge or face extinction. As they evolve, replicate, survive, and spread...it's easy to see that viruses were aptly named.