PUBLISHER'S EXPERT software CHOICE

New York, NY 10016

9 8 7 6 5 4 3 2

$19.95

Flu-Shot+

and

The Virus Protection Handbook

By Ross M. Greenberg & Software Concepts Design

The 5th Wave

The computer virus crept silently from network to network, until it found its way into the cafeteria vending machines.

Table of Contents

The Anti-Virus Handbook

Introduction:

Flu-Shot+ is an anti-virus program that can help to protect your valuable computer software and data from being "infected" by harmful viruses.

The program is designed for both novice and experienced IBM DOS users.

Flu-Shot + is provided with an installation program that makes it easy to configure the program. Every option in the installation has a default — that is an answer is provided for each question you are asked. The default is the most likely option that would be selected in most circumstances.

That means that if you do not have a technical understanding of your computer system, you can set up Flu-Shot + to work effectively by selecting the defaults during the installation.

However if you have a good understanding of the disk operating system, you can fine tune the program to work even more effectively.

Although Flu-Shot+ can detect most of the known viruses, we cannot guarantee that it is foolproof. A devious programmer could create another type of virus which could bypass Flu-Shot+'s security and infect your data.

For information on how to best protect yourself from harmful viruses, refer to the Anti-Virus handbook at the end of this manual.

Before you get started with Flu-Shot+, you may want to spend a few minutes reading the Anti-Virus Handbook for a full explanation about what viruses are, and what they do.

Preparation

Before you start the installation of Flu-Shot +, there are two things you must do. Start up your computer as you normally do.

#1: Check For a CONFIG File

Flu-Shot+ requires that there is a CONFIG.SYS file on the disk that you use to start the computer and the file must contain a line that says FILES=40.

If you have a hard drive the file is probably on there already. If you start up your computer by inserting a DOS disk or start up disk into your floppy disk drive, the CONFIG.SYS file is probably on there too.

You can check by looking at the disk directory. At the A> or C> prompt, type DIR and press Enter and the files will be displayed.

Automatically Create One

If you don't know anything about creating a CONFIG.SYS file, we've provided an easy way to do it.

a. Insert the Flu-Shot+ disk into drive A.

b. — If you are using a floppy disk drive as your start up disk, at the A> prompt type **A: CONFIG**

— If you are using a hard disk drive as your start up disk, at the C> prompt type **A: CONFIG**

c. The program will check your start up disk for a CONFIG.SYS file and confirm that it contains the line "FILES=40."

d. If there isn't a CONFIG.SYS file, the program will create one for you, automatically.

Once this is done, you will have to restart the computer before you can run Flu-Shot+.

#2: Creating A Directory For Flu-Shot+ (Hard Disks)

If you want to create a sub-directory specifically for Flu-Shot+ on your hard disk, you should create it before you run the Flu-Shot+ install program. To create a sub-directory:

a. Be sure the C> prompt is displayed on screen. (Most people designate their hard drive as the C device. If yours is different be sure the correct letter is displayed.)

You probably want to be at the root directory of the drive when you create a sub-directory. The root directory is the highest in the hierarchy. Sub-directories are used like file folders — to store related files together.

To get to the root directory type **CD** and press **Enter**. (You might already be at the root directory anyway.)

b. Type **MD\anyname**. ("anyname" can be a name, not already used, with up to eight letters.) Press **Enter** and the sub-directory will be created.

Later, when you use the Flu-Shot+ INSTALL process you can specify that the program is copied over to this sub-directory on your hard disk.

Getting Started

Hard disk users:
The C> should be displayed on screen. Insert the Flu-Shot+ disk into the A drive, type **A:** and press **Enter**.

Floppy disk users:
Insert a DOS disk in drive A and turn the computer on. When you see the A> take the DOS disk out and insert the Flu-Shot disk.

Running The INSTALL Program

Put the Flu-Shot+ disk into drive A, type **Install** and press **Enter**.

The Install program will allow you to configure Flu-Shot+ to your particular system by asking you a series of questions.

```
                FLU SHOT+ Installation

This is your initial installation of FLU SHOT+.
(For each question below, entering a return uses the
default entry as specified within the [ ]'s)
On what disk would you like to install FLU SHOT+? [C:]




Enter 'F1" at anytime for assistance.  <ESC> to exit.
```

Each questions has a default setting (the default will appear inside the [ ]s). To accept the default setting, press the Enter key. By choosing all the default settings, you create a very good protection scheme. To enhance protection, Flu-Shot+ lets you to tailor the options.

If, at any point, you are not sure about what to do, press the 'F1' key. A help window will appear which should point you in the right direction.

Installation Part I: File Information

1. Drive Selection

Select a drive to install Flu-Shot+ on. If you are using a hard disk, use the default setting (C:). If you are installing onto a floppy, type the letter of the drive and a colon (:). Then press Enter. If you are creating a boot disk, type **A:**. The program will use the B drive for installation. Insert your **boot disk** (not the Flu-Shot+ disk) into drive B. If you want to create a disk containing Flu-Shot+ which runs from the B drive type **B:** and proceed normally.

2. Specify A Directory

Specify a directory to install Flu-Shot+ onto. If you created one, type in that name or, if you want to use an existing directory, type in that name. If you want to install the program on the root directory, just press Enter. To specify a directory, type in a \ followed by the name of the directory, followed by another \. For example: \mydirectory\.

3. Give the Flushot.DAT file a name.

This is very important. Viruses could destroy Flu-Shot's ability to protect your files by attacking the Flushot.DAT file, if they knew what the file name was. By giving this file a new name, you hide it from anti anti-virus viruses. Type in a name (up to 8 letters) followed by a period and three letters, leaving no spaces in between. Do not use extensions such as SYS, COM or EXE as they are system extensions.

4. Give the Flu-Shot+ program a name.

As above, it's safer to disguise the Flu-Shot program under another name. Type in any name followed by a period and the letters COM . eg. ABC.COM. Note: Do not use the same names as the examples above.

5. Would you like Flu-Shot+ to run when you boot your system?

If you want Flu-Shot to run each time you start up your system (this option is strongly recommended) type Y here. If you don't want it to run, Type N. If you select "No" here, please remember that Flu-Shot+ will not be be able to protect you until you manually run the program.

This is the end of the first part of the installation. The screen displays the options and settings you selected. Press Enter to continue.

Installation Part II: Tailoring The Set Up

This section lets you tailor Flu-Shot+'s protection to your needs. The files that the program will automatically protect are shown on screen. If you press Y here, you will accept the default settings for this part of the installation and jump right to the next section ((Run Time Options).

However if you want to tailor the installation, press the N key here and you will be asked seven questions. They all have defaults so if you don't understand an option, choose the default. Explanations are below:

```
FLU SHOT+ Protection File

The default protections File (A:\FLUSHOT.DAT) shows:
You currently are write protecting:
*.bat, *.sys, *.exe, *.com

You are protecting these files from read access:
*AUTOEXEC.BAT

You are checksumming these files:
C:COMMAND.COM,C:\IBMBIO.COM,C:\IBMDOS.COM

OK? [Y]

 Enter 'F1" at anytime for assistance.  <ESC> to exit.
```

1. File Write Protection

The Flu-Shot default setting automatically write protects all files of the types BAT, SYS, EXE, and COM. These file types are rarely updated and are usually the files targeted by viruses.

If you want to write protect other files you can specify them in this section. To write protect a group of files of the same type, type in *.filetype where the file type is the three character code for that type. eg. to protect all system files, you would type in *.SYS and press Enter.

To protect specific files, type the full file name (eg. Customers.DBF) and press Enter. To write protect a file in a specific directory, type the name of the directory and file name. (Eg. \Database\Customers.DBF) using the back slash before and after the directory name.

When you finish entering file names to be write protected, press Enter. Please note. If you do not accept the default selections, you will have to re-enter the lines for ".BAT etc." to protect these files.

2. Except Files

In most cases you will not want to list any files under this option, however, if a need arises where you want to write protect all files of a particular type, but allow access to one particular file, you can use the except option. This will allow you to write to the file without triggering the Flu-Shot+ warning.

To exclude a file from protection, type in the full file name and press Enter. To include all files in a single directory, you can type in C:\directoryName*.* and press Enter.

3. Check boot record on drive

Boot records are programs that are read by computer to find out information such as the type of disk or where files are located. It's also a way that viruses can attack your disk. Unfortunately, this program is run before Flu-Shot+ can be run, making it a target for several viruses.

One way to protect against these viruses is to check if the "boot record" has changed since the last time you turned on the computer. When Flu-Shot loads, it automatically warns if there have been changes. This will not prevent infection, but it will let you know if there is a problem before your data files or programs are damaged.

If you choose to check, type N at the "Is this correct? prompt and enter the drive letter of the disk drive you boot from. A: for floppy disk users, C: for hard disk users.

4. The Execute Permission List

This is designed to allow trusted programs that would normally set off Flu-Shot+ to be allowed to work without interruption. As this allows a program to run without the supervision of Flu-Shot+, it is recommended that you use this sparingly. You might want to use it to allow DOS programs, such as FORMAT to run without interruption, however, it would be much safer just to live with the occasional interruption.

If you insist on using this option, type in the name of the file. Eg. FORMAT.COM and press Enter.

5. The Checksum File Option

This is an extremely useful option. It checks the current size of a file, and stores this information. Every time that Flu-Shot+ starts up, it will check the sizes of these files to make sure that they have not been altered in any way. Since many viruses attach themselves to existing files, they would show up immediately with the Checksum option.

Of course, this option should only be used with files that do not change in size (such as program files), and not with data files which are constantly being updated and consequentially changing in size.

To enter files into the checksum list, type in the full file name. Eg. Fred.EXE and press Enter. If the files are in a directory, include the directory name. Eg. \WORDS\Fred.EXE.

6. Setting Read Protect Files

In certain situations you may want to restrict access to a file by preventing it from being read by another program. This is useful if you have created some batch files. To set read protection of a file enter the name of the file, or for all batch files enter *.BAT and press Enter.

This still allows batch files to operate, but will prevent another program from reading them. Files can be READ and WRITE protected.

7. TSR Files

"TSR" programs (Terminate and Stay Resident) are loaded and stay in the computer's memory until you turn off the power.

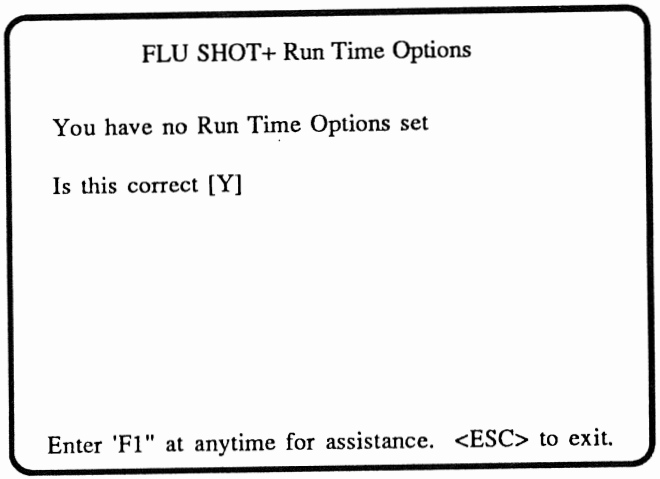
Programs, such as SideKick, leave sections in your computer's memory when they quit. This is necessary for the program's operation. Certain viruses operate the same way, but Flu-Shot+ has no way to distinguish between them. If the program is trust-worthy, you can enter its name into the TSR list. Type the full name of the program and press Enter. For example type \Util\SideKick.EXE. When a program goes "TSR" Flu-Shot+ checks the list , and if it is there, you won't be interrupted.

Installation Part III: Advanced Settings

This section of the install program allows you to set preferences as to when Flu-Shot+ warnings should be triggered and how messages are displayed. Although this is somewhat technical, the defaults for each question are the most commonly used settings.

FLU SHOT+ Run Time Options

You have a prompt on the first Run Time Options screen that indicates you have no run time options set. If you press Enter at the prompt "Is this correct?" you will accept all the run time defaults. If you press N at the prompt, you will be asked 11 questions about running the program. Explanations of those questions are detailed below.



1. Should Direct Floppy Access Cause Flu-Shot+ to Trigger?

Most programs, at one point or another, attempt to write to a disk. When they do this, they normally go through DOS. Viruses, in an attempt to evade anti-virus programs, may attempt to write to disk without going through DOS. This will trigger Flu-Shot+.

There are also some legitimate programs that may attempt the same function, again causing Flu-Shot + to put up a warning. If you know that you have programs like these, and you don't want the Flu-Shot+

warning to appear, you may want to disable this trigger by typing "N" here. We strongly recommend that you live with the interruptions of Flu-Shot+ rather than disable a valuable piece of protection.

2. Should Hard Disk Access Cause Flu-Shot+ to Trigger?

This is the same option as above, except for hard disk access. Again, we strongly recommend that you leave this protection enabled.

3. Use Standard Initial Sleep Period?

One idiosyncrasy of DOS is how a batch file is processed. DOS opens a batch file, reads the next command, closes the batch file, executes the command, and starts over again until the end of the file is reached.

This is normally not a problem, but can become one when you opt to put the Flu-Shot command line in your AUTOEXEC.BAT file and you've opted to Read Protect the AUTOEXEC file itself. You'll be advised that a program is reading this protected file. This is not a big deal, but certainly can be a hassle when you first start your system. That is why, protections within Flu-Shot+ are not turned on a certain amount of time.

The default is set to 10 seconds, or until you press a key. You can modify the "sleep" time by entering "N" and the number of seconds Flu-Shot+ sleeps before becoming active. Since Flu-Shot will be one of the final commands in the AUTOEXEC.BAT, the default setting should be fine.

4. Use The Standard Welcome Message?

When Flu-Shot+ is first run, it displays the standard "Welcome" message. There is another one built into the program which is longer. The default here is for the short message.

5. Allow "TSR" Direct Disk Interrupt Triggering?

"Interrupts" are where the computer actually interrupts the running of a program while it goes off and takes care of other functions (like updating the screen, or checking to see if it should write to the disk drive). The interrupts are quick, so you never notice them.

Most TSR programs "hook into" an interrupt vector before they go TSR. These hooks might intercept and process key strokes ("hotkeys"), or

they might hook and intercept disk writes themselves. Flu-Shot+ will do no more than advise you of the TSR'ing of the program. If you're suspicious, restart your machine immediately!

If a program attempts to write directly to the interrupts which are reserved for disk writes, Flu-Shot+ will also be triggered.

You should leave this option at "Y", but if this message is appearing too frequently, and you know that it is being triggered by a trusted program, you might want to change it to "N".

6. Display Flu-Shot+ Status At All Times?

When Flu-Shot+ is running and active, you'll see a "+" at the top right corner of the screen. This may interfere with some graphics programs.

Therefore, you may want to turn this off by selecting "N" here. Or you can leave this turned on and, when you run a graphics application, you can depress the CTRL key three times to toggle the display on and off.

When you toggle this function, the '-' or '+' won't appear or disappear immediately. It changes the next time the screen is rewritten.

7. Use Fast Screen Drawing?

Some machines are not totally compatible with the IBM BIOS, which is the BIOS for which Flu-Shot+ was written. Because Flu-Shot+ has to deal with hardware in a direct manner in order to "pop-up" a screen, these machines may have difficulty running Flu-Shot+. If you select "N" here, then only the BIOS will be used for screen output.

This is slower than direct screen memory writes (the default), but at least it works. The "hit ALT and/or CTRL three times" options may not work in these machines — only experimentation will tell.

8. Trigger On File Open With Write Access?

When a program opens a data file to read information, there are several ways they can do it. If the program only needs to read data, it will only request read access. However, some programs may only intend to read from the file, but will request read and write access.

The default option warns you when this happens, but if it happens too often, you may want to disable it. Since a virus may try to write to read- only files, it is recommended that you leave this at the default setting.

9. Allow Interactive Disabling of Flu-Shot+?

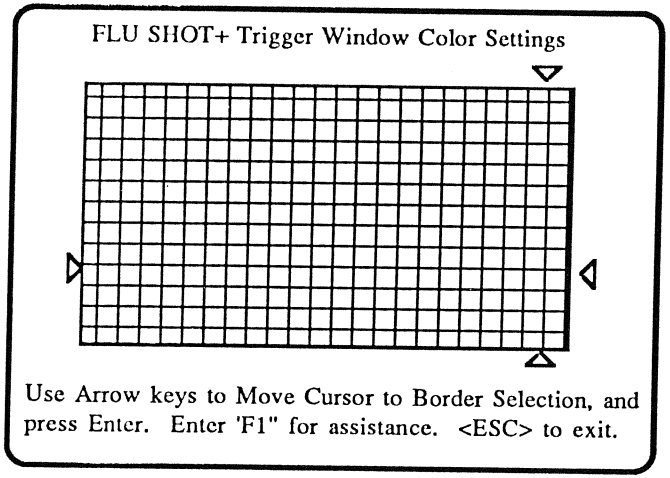
There may be times when you are about to do work that you know will trigger Flu-Shot+. You might want to avoid being bothered with all of the triggering, the pop-up windows and the required response.

When the program is installed and running, you'll see a '+' sign at the top right corner of the screen. This indicates that Flu-Shot+ is monitoring and attempting to protect your system. Depress the ALT key three times and the '+' sign' turns into a '-' which means Flu-Shot+ is disabled, and will not trigger on any event. If you depress the ALT key three more times, it will turn back on.

If you do not want someone to be able to turn Flu-Shot on and off, you can cause Flu-Shot to ignore the "strike ALT three times" function discussed above. By typing a "N" here, Flu-Shot will not be able to be disabled.

10. Use the Standard Screen Attribute Set?

Certain displays, particularly monochrome that try to emulate color displays, have a problem with the default color selection in the trigger window of Flu-Shot+. If you have problems, or, if you want to change the colors of warning messages, type "N" and this screen appears:



First select the border selection and press Enter. Next select the color or pattern for the text and press Enter.

11. Use the Standard Action Keys?

You can define your own "special keys" for turning Flu-Shot+ on and off (the defaults are the Alt and Ctrl keys). Press ENTER to continue.

This is the end of Installation Part III. You'll be asked to confirm all the Flu-Shot+ settings. The list of options set will be displayed along with an explanation of what they mean. If you selected the defaults, the list will be short. If you're ready to proceed, press the ENTER key.

The Installation

Enter your user name, and you'll be ready to install the program.

You'll see the message: "Install Flu-Shot+ as specified?" Press ENTER to start.

Make sure the Flu-Shot+ disk is in the A: drive when you install the program. The install program will copy the FSP.COM file and create a .DAT file on either your hard disk, or the floppy drive you specified.

When the installation is finished, the computer will return to the DOS prompt.

Running Flu-Shot+

Using A Floppy Disk Drive

If you selected the option "Would you like Flu-Shot+ to run each time you boot your system?" when you installed the program, then an Autoexec.BAT file was created to load and run Flu-Shot automatically when you start the system with the floppy you installed Flu-Shot on.

If you are manually running Flu-Shot+, insert the DOS disk you installed Flu-Shot+ on into drive A and turn on your computer Type the name of the Flu-Shot+ COM file. (This is the name you gave the file during installation). The default filename was FSP.

Using a Hard Drive

If you selected the option "Would you like Flu-Shot to run each time you boot your system?" when you installed the program, then an Autoexec.BAT file was created to load and run Flu-Shot automatically when you start up.

If you are manually running Flu-Shot+ turn on your computer and when the computer loads, type the name of the Flu-Shot+ COM file. (This is the name you gave the file during installation). The default filename was FSP.

Disabling Flu-Shot+

There may be times when you're about to do some work which you know will trigger Flu-Shot+. And you might not want to be bothered with all of the triggering, the pop-up windows and your need to respond to each trigger. If you look in the upper right hand corner of your screen, you'll see a '+' sign. This indicates that Flu-Shot+ is monitoring and attempting to protect your system.

Press the ALT key three times. Notice the '+' sign' turns into a '-' sign. Flu-Shot+ is now disabled, and will not trigger on any event. If you press the ALT key three more times, you'll see the '-' turn back into a '+' — each time you depress ALT three times, Flu-Shot+ toggles between being enabled and disabled.

Disabling Flu-Shot+ Toggle Display

There are graphics applications which will have difficulty displaying the '-' or '+' in the upper right hand corner of your display. Therefore, if you press the CTRL key three times, you'll be able to toggle the display capability of Flu-Shot+.

When you toggle this function, the '-' or the '+' won't appear or disappear immediately. It will change the next time the screen is rewritten.

Interpreting a Flu-Shot+ Trigger

So, you've run Flu-Shot+, and you're ready to try it out. Insert a blank disk which you don't care about into your A: drive and try to format it.

Surprise! Flu-Shot+ caught the attempt! You have three choices now: typing 'Y' allows the operation to continue, but the next one will be caught as well. Typing a 'G' (for Go!) allows the operation to continue, disabling Flu-Shot+ until an exit from the program is made. When Flu-Shot+ is in the 'G' state, a 'G' will appear in the upper right hand corner of your screen.

Any other key will prevent the operation from occurring.

When you've got Flu-Shot+ running and you get signaled that there is a problem, you should think about what might have caused the problem. Some programs, like FORMAT and Norton Utilities have good reasons for doing reads and writes to your hard disk. However, a public domain game doesn't. You'll have to be the judge of what are legitimate operations and which are questionable.

Copying a COM or EXE file if you have those protected will trigger Flu-Shot +. The program isn't intelligent about what is allowed and what isn't — it watches for everything that *could* be a virus. That's where you, the pilot, get to decide.

Flu-Shot + Messages

Here's a list of messages you might see when you're using Flu-Shot+:

Checksum Warnings

Checking ===><filename>

This message is displayed as Flu-Shot+ checks the checksum on all files in the list when you first invoke Flu-Shot+. The files must be read from disk, the checksum calculated and then compared against the value the checksum should equal.

If the checksum does not equal what it was when you installed Flu-Shot+ (which means the file may have been written to and might be suspect), a window will pop up in the middle of your screen:

Bad Checksum on <filename>
Actual Checksum is: <checksum>
Press "Y" to allow, "G" to go till exit, any other key to exit.

This advises you there is a problem with the checksums not matching, shows what the checksum should be and waits for your response.

Except for the initial run of Flu-Shot+, if you type 'Y' or 'G', the program will load. Typing any other key will cause the program to abort and for you to be returned to the C> prompt. When Flu-Shot+ is in the 'G' state, a 'G' appears in the top right corner of the screen.

TSR Warnings

If you're running a program and you see a screen like:

? WARNING! TSR Request from an unregistered program!
Number of paragraphs of memory requested (in decimal) are:<cnt>
(Press any key to continue)

you're being advised that a program is about to go TSR. If this is a program you trust (such as SideKick), then you should consider adding it to the TSR list in the install program so that in the future this program will not trigger Flu-Shot +.

However, if you get this message when running a program you don't think has any need to go TSR, you should be suspicious. Having a TSR program is not something to be suspicious of. But having one you don't expect is a different story.

Flu-Shot+ will only advise you of the TSR'ing of the program. If you're truly suspicious, reboot your machine immediately!

Direct Disk Writes

If a program attempts to write directly to the disk, Flu-Shot+ will also be triggered and you'll see this:

====>Direct Disk Write attempt by program other than DOS! <====
Interrupt xx=> Drive: x Head: y Track: zzzzz Sector: zzzzz
By: <program>
Press "Y" to allow, "G" to go till exit, any other key to fail

where the <xx> represents either a 13, 26 or 40. Again, pressing a 'Y' or a 'G' allows the operation to continue, pressing any other key will cause the operation to return a failed status to DOS, and the operation will not take place.

Flu-Shot+ will attempt to let you know what program is actually attempting the write as well: this is not always reliable, though, so don't count on it as more than a hint.

Format Warning

If an attempt is made to format your disk, which may be a legitimate operation by the DOS FORMAT program, you'll see a message such as:

====>Disk being formatted! Are You Sure?<====
Interrupt xx=> Drive: x Head: y Track: zzzzz Sector: zzzzz
By: <program>
Press "Y" to allow, "G" to go till exit, any other key to fail

which follows similarly to the direct disk write operations. You should question whether the format operation is appropriate at the time and take whatever action you think is best.

Protected File Write Warning

If one of your protected files is about to be written to, you'll see:

Write access being attempted on:
<filename>
By: <program>
Press "Y" to allow, "G" to go till exit, any other key to fail

where <filename> represents the file you're trying to protect from these write operations. You should question why the program currently running should cause such an operation. You may also see the same type of message when one of your "Read-Protected" files is being accessed:

Read Protected File Access Warning

Read Access being attempted on
<filename>
By: <program>
Press "Y" to allow, "G" to go till exit, any other key to fail

You should be cautious, but it doesn't mean you're infected with a virus program. It could be harmless or intended. You'll have to be the judge.

Open File With Write Access Warning

Open File with Write access being attempted on
<filename>
By: <program>
Press "Y" to allow, "G" to go till exit, any other key to fail

If you see the above message, don't Panic! When a program opens a file, it may open the file for different types of access. One access method prohibits writing to the file. Another allows you to write to the file. However, programmers will often open a file for read and write access, even though they have no intention of ever doing a write into the file.

Flu-Shot+ isn't smart enough to be able to figure out what a program might do in the future, so it will alert you to an attempt to open the indicated protected file with write access allowed. Again, you'll have to consider whether the program opening the file is a "trusted" program or not and you'll have to then decide what action to take.

Handle Write Access Warning

Handle Write Access being attempted on:
<filename>
By: <program>
Press "Y" to allow, "G" to go till exit, any other key to fail

If you see this message, it means that some program is trying to write to a protected file through an access method known as "handle access". This should normally never happen, with the caveats raised above in the "Open With Write Access" section.

Renaming Warning

There are three separate messages you'll see if a program attempts to rename a protected file (only one messages is displayed at a time):

FCB Rename being attempted on source file:
FCB Rename being attempted on target file:
Handle Rename being attempted on:
<filename>
By: <program>
Press "Y" to allow, "G" to go till exit, any other key to fail

This indicates what type of operation is attempting to rename a protected file. It is possible that a trojan or virus writer will attempt to rename an existing protected file to some other name, then rename a trojaned or virused program in its place. Flu-Shot+ will alert you to this action: again, you'll have to decide what to do about it.

Delete File Warning

Delete being attempted on:
<filename>
By: <program>
Press "Y" to allow, "G" to go till exit, any other key to fail

This is pretty much self-evident as to what's happening here. There are very few reasons why one of the files you've decided to protect should be deleted. Unless you are trying to delete it yourself, this is most likely a virus attack.

Expert Level Configuration

For advanced users, the Flushot.DAT file can be edited manually. Options can be edited automatically using Install, but if you don't want to use the install program, here are the commands and what they do.

This data file contains a number of lines of text. Each is of the form:

<Command>=<filename><options>

Command can be any one of the following characters:

P — Write Protect the file named
R — Read Protect the file named
E — Exclude the file named from matching P or R lines
T — The named file is a legitimate TSR
C — Perform checksum operations on the file named

The filename can be an ambiguous file if you wish for all commands except the 'T' and 'C' commands. This means that:

C:\level1*.COM

will specify all COM files on your C: drive in the level1 directory (or its sub-directories). Specifying:

C:\level1.EXE**

would specify all EXE files in subdirectories under the C:\level1 directory, but would not include that directory itself.

You can also use the '?' operator to specify ambiguous characters as in:

?:\usr\bin\?.COM

is to specify files on any drive in the \usr\bin directory on that drive. The files would have to be single letter filenames with the extension of 'COM'. Ambiguous names are not allowed for 'T' and 'C' options.

Protecting files from Write Access

Use the 'P=' option to protect files from write access. To disallow writes to any COM, EXE, SYS, and BAT files, specify lines of the form:

P=*.COM
P=*.EXE
P=*.SYS
P=*.BAT

which protects these files on any disk, in any directory.

Protecting files from Read Access

Similarly, you can use the 'R' command to protect files from being read by a program (including the ability to 'TYPE' a file!). To prevent read access to all of your BAT files, use a line such as:

R=*.BAT

Combinations of R and P lines are allowed, so the combination of the above lines would prevent read or write access to all batch files.

Excluding files

Programmers should find a use for the 'E' command. This allows you to exclude matching filenames from other match operations. Assume you're doing development work in the C:\develop directory. You could exclude Flu-Shot+ from being triggered by including a line such as:

E=C:\develop*.*

Of course, you might have development work on many disks under a directory of that name. If so, you might include a line which looks like:

E=?:\develop*.* or
E=*\develop*

Checksumming files

This line is more complicated than others and involves some setup work. It's worth it though. A checksum is a method used to reduce a files validity into a single number. Adding up the values of the bytes which make up the file would be a simple checksum method. Doing more complex mathematics allows for more and more checking information to be included in a test. If you use a line on the form:

C=C:\COMMAND.COM[12345]

then when Flu-Shot+ first loads it will check the validity of the file against the number in the square brackets. If the checksum calculated does not match the number presented, you'll be advised with a triggering of FLUSHOT, which presents the correct checksum.

You should copy down the "erroneous" checksum presented. Then, edit the FLUSHOT.DAT file and replace the dummy number with the actual checksum value you had copied down. If even one byte in the file is changed, you'll be advised the next time you run Flu-Shot+.

When a "checksummed" file is loaded by MS-DOS, it will, by default, be checksummed again. So, if you had a line such as:

C=C:\usr\bin\WS.COM[12345]

the venerable old WordStar program would be checksummed each time.

Of course, you might not want the overhead of that checksumming to take place each time you load a program. Therefore, a few switches have been added. The switches are place immediately after the ']' in the checksum line:

C=C:\usr\bin\WS.COM[12345]<switch>

These switches are:

- ,n will only checksum the file only 'n' times. Only one digit allowed.
- \- Only checksum this file when Flu-Shot+ first loads. ',1' and '-' are equivalent.
- \+ Only checksum this file when it is loaded and executed, not when Flu-Shot+ first loads

Therefore, if you wished to only check your WS.COM file when you first loaded the Flu-Shot+ program, you'd specify a line as:

C=C:\usr\bin\ws.com[12345],1 **or**
C=C:\usr\bin\ws.com[12345]-

If you wished to checksum your program called "MY_PROG.EXE" only when it was used, try:

C=C:\path\MY_PROG.EXE[12345]+

Registering a TSR program

Any unregistered TSR program which is run after Flu-Shot+ will cause a trigger when they "go TSR". You can register a program so no trigger goes off by specifying it in a line such as:

T=C:\usr\bin\tsr_s\sk.com

which will keep Flu-Shot+ from complaining about sk.com. Make sure to take a look at the '-T' option, specified in the next section.

Restricted Access

Normally, when access to a file causes Flu-Shot+ to trigger, the user is given the option of hitting a 'Y' to allow the access, or a 'G' to allow the access until program exit or a key is hit. However, in some cases,

access to a file should never be allowed. If you end a line in your FLUSHOT.DAT file with an '!', then the trigger will indicate that this is a restricted access file, and the user will be asked to press a key to continue. In any case, trigger accesses resulting from a line with a '!' at the end will not be allowed to go forth.

For example, if you never want anyone to be able to read an AUTOEXEC.BAT file on any of your disks, have a line of the form:

R=*AUTOEXEC.BAT!

in your FLUSHOT.DAT file. That's pretty easy! (Make sure, however, to take a look at the FSP command line arguments for the '--' switch.)

Protection Recommendations

Here's a sample FLUSHOT.DAT file, basically the same one included in the archive. Your actual checksums will differ, and you may want to modify what files and directories are protected. Obviously, your exact needs may different, so consider this a generic FLUSHOT.DAT:

```
P=*.bat
P=*.sys
P=*.exe
P=*.com
R=*AUTOEXEC.BAT
R=*CONFIG.SYS
E=?\dev\*
C=C:\COMMAND.COM[12345]-
C=C:\IBMBIO.COM[12345]-
C=C:\IBMDOS.COM[12345]-
```

Allowing "Dangerous" Programs to Run

In some cases, though, you'll want the ability to let "trusted" programs to run -- even if they are potentially dangerous. An example of this is DOS FORMAT. This is a program designed to overwrite the data on your disk in such a way that it would be difficult, at best, to recover. Yet, the program is a necessary part of your day-to-day computer usage.

Therefore, the 'X=' switch has been added in to allow a program such as FORMAT to run without interruption. THIS IS A POTENTIAL SECURITY HOLE. To prevent an 'X=' program from being corrupted, I

suggest you also include any 'X=' program as both a 'C=' and a 'P=' program as well: any writes to the file would cause Flu-Shot+ to trigger, and you wouldn't be able to run a modified program without first giving Flu-Shot+ permission. Use 'X=' sparingly.

Protecting Your Boot Track

Some of the virus writers out there are getting pretty devious: they are creating viruses which will replace your "boot record" with something of their own creation which will first create a virus upon a system boot, then will run your actual boot program. The "boot program" is a small program at the beginning of your disk, telling the system what to do when you first turn the system on. What makes these types of viruses particularly dangerous is that they are run before Flu-Shot+ can be run: by the time Flu-Shot+ is running, you're already infected!

Therefore, you might want to consider using the Boot Checksum option line in your FLUSHOT.DAT file. It takes the form of:

B=<disk><checksum>

where <disk> is a single character (no ':') indicating which disk drive you boot from, and checksum is the boot checksum. The boot checksum is checked each time you exit a program and when you first invoke Flu-Shot+.

First, create a sample boot checksum entry, as in:

B=C12345

then, run Flu-Shot+. You'll be advised of what the actual boot checksum is, and you should edit that checksum into the "B=" line.

You are now protected from some virus program somehow getting around the protections Flu-Shot+ offers and modifying the boot record. You'll also be advised if something changed your boot record while you weren't looking. Never boot from a floppy if you can avoid it. That's how a lot of viruses spread.

Commonly Asked Questions:

Q: Why doesn't Flu-Shot+ work with programs that use graphics capabilities, such as Microsoft EXCEL?

A: Flu-Shot+ is a TSR program, and uses up memory on your computer even when there is no suspicious action taking place. When such an action occurs, the current screen must be saved to bring up the trigger window. In graphics mode, this requires a great deal of memory to be set aside, and so we considered it not worth the loss of memory.

Q: What can I do if I use such graphics programs?

A: Turn the "faster screen display" off in the installer. You may lose a portion of the screen, but you'll see what is causing the trigger to occur.

Q: Certain programs lock up when Flu-Shot+ triggers -- I have to reboot the system. What can I do?

A: Try resetting the Action Keys with the install program. Chances are that your program is taking over the keyboard and not passing keys over to Flu-Shot+. Experiment with keys until you find a set that work.

Q: Certain programs, like WORDPERFECT, use temporary work files. When they are finished with them, it deletes them. This triggers Flu-Shot+. What can I do?

A: Try excluding the class of files causing the trigger. Look for the pattern of the target filenames in the trigger window, and enter them into the exclude list. Or, you could exclude that particular directory.

Q: Will Flu-Shot+ tell me if I have a virus on my disk and will it remove a virus if found?

A: No. Flu-Shot+ will check that files are what they appear to be when you run them, if you wish. And, it will interrupt the type of suspicious activity associated with a virus attack. At that point, you have to consider whether or not the program you're running is a virus or not, and take appropriate action if it is.

Q: What kind of appropriate action?

A: First thing to do would be to load a new copy of that program from your original distribution disk. Try using the program again. If the trigger window pops up, then chances are the program is violating one of the rules in your FLUSHOT.DAT file, but it isn't a virus. Alter the Flu-Shot+ configuration to accommodate this.

Q: What precautions should I take when reloading a program from my original distribution disks?

A: You should power off your computer for about ten seconds. Reboot with a clean, write-protected copy (stick a piece of black tape over the write enable notch on the disk) in your A: drive. Then, do a "SYS" onto your hard disk to play it safe (see the DOS manuals for an explanation of what SYS does and how to use it), then reinstall your software.

Q: I see copies of Flu-Shot+ on the Bulletin Board Systems I use. Are they the same as this version?

A: You'll have to check the version number to be sure — but there's no guarantee the version you see out on a BBS is going to be a clean copy of Flu-Shot+ (unless you get it from one of the BBS's the author uploaded it to himself). This commercial release has an installation program to help you install Flu-Shot+ and provides this printed manual.

Q: If I get a virus, what should I do with the infected program?

A: Just delete the infected program. A deleted virus can hurt no one.

Q: Will Flu-Shot+ stop every virus out there?

A: No. No software product can stop every virus attack, since there are a variety of ways a virus can attack your system and get around Flu-Shot+'s protection mechanisms. However, no virus can infect a program without changing the checksum of the program. Therefore, use the C= option in your FLUSHOT.DAT Protections File on all the programs you run. That way, you'll know if the program you're running has become infected since the last time you ran it.

The Anti-Virus Handbook

Section I: Viruses and Trojans

The Anti-Virus Handbook is designed to help you understand more about viruses and to help you to avoid being infected by one. If a virus does infects your computer and you've followed the guidelines in this handbook, you don't have to worry about losing any data or software.

What is a Trojan?

Back in the good old days, there was a bunch of soldiers who had no chance of beating a superior force or of even making it into their fortress. They had this idea: present the other side with a gift. Once the gift had been accepted, soldiers hiding within the gift would sneak out and overtake the enemy from within. Anyway, you're probably aware of the story of The Trojan Horse.

Now there's a modern day equivalent: getting a gift from your friends, BBS or user group which contains a little gem which will attack your hard disk, destroying whatever data it contains.

How Your Disk Works

In order to understand how a potentially useful program can cause damage when corrupted by some misguided soul, it's useful to know how a disk works, and how easy it is to cause damage to the data contained on it. This is brief technical discussion of the operation of a disk.

Data is preserved on a disk in different physical ways having to do with how the data is encoded in the recording of the data. The structure of that data, however, is the same among MS-DOS machines.

Each disk has a number of "tracks". Tracks can be thought of as the individual little grooves on an audio record. Each track is subdivided into a number of sectors. Each track has the same number of sectors. Tracks are numbered, as are sectors. Any given area on the disk can be accessed if a request is made to read or write data into or out of Track-X,

Sector Y. The read or write command is given to the disk controller, which is an interface between the computer itself and the hard disk. The controller figures out what commands to send to the hard disk, the hard disk responds and the data is read or written as directed.

The first track on the hard disk typically will contain a small program which is read from the hard disk and executed when you first power up your machine. The power up sequence is called "booting" your machine, and therefore the first track is typical known as the "boot track".

In order to read information from your disk in a logical sequence, there has to be some sort of index. An unusual index method was selected for MS-DOS. Imagine going to the card index in a library, looking up the title you desire, and getting a place in another index which tells you where on the racks where the book is stored. Now, when you read the book, you find that only the first chapter is there. To find the next chapter, you have to go back to the middle index, which tells you where the next chapter is. This process continues until you get to the end of the book. This is how MS-DOS does its "cataloguing" of files.

The directory structure of MS-DOS allows you to look up an item called the "first cluster." A cluster represents a set of contiguous or touching tracks and sectors. It is the smallest amount of information which the file structure of MS-DOS knows how to read or write.

Based on the first cluster number stored in a directory, the first portion of a file can be read. When information contained there is exhausted, MS-DOS goes to that secondary index for a pointer to the next cluster. That index is called the File Allocation Table, commonly abbreviated to "FAT". The FAT contains an entry for each cluster on disk.

If the directory or the FAT or other areas of the disk get corrupted you can't retrieve files. That's what Trojan programs do: they cause what appears to be a useful program to corrupt the important parts of a disk. This can be changing a few bytes of data, or wiping entire tracks clean.

Not all programs which write to your hard disk are bad ones, obviously. Your word processor, spreadsheet, database and utility programs have to write to the hard disk. Some of the DOS programs (such as FORMAT), if used improperly, can also erase portions of your hard disk. You'd be surprised what damage the simple "DEL" command can do with just a simple typo.

What is a Virus?

Trojan programs are just a delivery mechanism. They can be clever, so that they only trigger the malicious part on a certain date or when your disk contains certain information. However they're coded, they typically affect the disk only in a destructive manner once triggered.

A new breed of program has the ability of reserving malicious damage for a given event's occurrence,and replicating itself as well. This is what people refer to when they mention the term "Virus Program".

Typically, a virus will spread itself by replicating a portion of itself onto another program. Later, when that normally safe program is run it will, in part, execute a set of instructions which will infect other programs and then potentially, trigger the Trojan portion of the program contained within it.

The danger of the virus program is twofold. First, it contains a Trojan which will cause damage to your hard disk. The second danger is the reason why everyone is busy building bomb shelters. This danger is that the virus program will infect other programs and they in turn will infect other programs and so forth. Since it can also infect programs on your floppy disks, you could unknowingly infect other machines!

Kenneth van Wyck at Lehigh University first brought a particular virus to the attention of the computer community. This virus infects a program, which every MS-DOS computer must have, called COMMAND.COM. This is the Command Line Interpreter and is the interface between your keyboard and the MS-DOS operating system itself. Whatever you type at the C> prompt will be interpreted by it.

This virus subverts this intended function, causing the infection of neighboring COMMAND.COMs before continuing with normal functionality of the command you typed. After a certain number of "infections", the Trojan aspect of the program goes off, causing you to lose data.

Flu-Shot+ provides a certain amount of protection against viruses, but it is not foolproof. New viruses can be created which could bypass Flu-Shot's protection.

Section II:
Ten Steps To Virus Protection

The following steps can be used to minimize your risk of exposure to a virus and, if files become contaminated, limit the amount of damage. (Reprinted from PC Magazine April 25, 1989. Copyright © 1989 Ziff Communications Company.)

1. Make Frequent Back-Ups!

First and always: make frequent back-ups! One set is not enough - use several sets of backups in rotation. Setting up a regular backup system will help you recover from hard disk crashes, accidental formatting, and malicious programs.

2. Recovering From A Virus Attack

If you determine conclusively that a virus has infected your system and destroyed data, you can probably recover the information by using a recent backup. Shut off the system, then boot it from your original DOS disk (with a write protect tab on it). Format the hard disk using FORMAT.COM from the original DOS disk and do a selective RESTORE. You should restore only the data from your backups To restore the programs, get the original disks and reinstall them.

3. Write Protection

Always put write-protect tabs on floppy disks that don't need data written to them. If you get a "Write protect error writing drive A:" unexpectedly, something improper is going on.

4. Downloading Software From Bulletin Boards

Software downloaded from bulletin board systems hasn't been implicated in a major virus outbreak yet. Nevertheless, there are steps you can take to be safe. Use established BBS's in which the system operators check the software they post. If the sysop makes a point of getting programs directly from the authors, that's even better. Wait several weeks before downloading a new program to see if any problems are surfacing.

5. Read Only Files

Make all .COM and .EXE files read-only. Under DOS 3.3 you can do this with two calls to ATTRIB, one for .COM and one for .EXE. From the root directory, enter ATTRIB +R *.COM/S. The /S switch causes ATTRIB to execute the command in all subdirectories. Do the same for .EXE files. If your DOS is pre 3.3, you'll have to manually run ATTRIB in every directory or use a utility like PC Magazine's SWEEP.COM.

6. Hiding COMMAND.COM

Move COMMAND.COM out of the root directory. Edit your CONFIG.SYS to include a line like

SHELL=C:\HIDDEN\COMMAND.COM /P

replacing HIDDEN with whatever directory you choose to keep it in. Add the line

SET COMSPEC=C:\HIDDEN\COMMAND.COM

to your AUTOEXEC.BAT. You can even hide COMMAND.COM and the directory it's in by using PC Magazine's ATTR.COM.

7. Protect Your Software

Don't loan out program disks - they may come back infected. If you have a legitimate reason to loan a disk, make a DISKCOPY and format the disk when you get it back.

8. Boot Disks

On a floppy disk system, use only one boot disk. Write protect it and never boot from any other. If you have a hard disk, don't boot from a floppy.

9. Other Users

Don't let anyone else use your system. If that's not feasible, at least don't let them bring their own program disks.

10. Illegal Copies Of Software

Don't use illegal copies of programs that have been "hacked" to remove copy protection. In one instance, a hacked version of a game program contained destructive code that was triggered by winning the game.

Section III:
How Does A Virus Work?

A computer virus is actually a very simple program to write. First, a little bit of terminology can help you understand what they are:

A computer virus has a number of different parts. Some viruses have a 'pre-trigger'. If the pre-trigger does not go off, then the infected program will work normally, as if not infected.

What makes a pre-trigger go off? Almost anything the virus writer wants. It can be made to go off when the disk is more than a certain amount full, or when more than a certain amount of memory is in use by a program. Or, when a certain date comes or has past.

Once the pre-trigger goes off (not many viruses have them, by the way), the next phase, the 'replication aspect' phase, gets initiated. Viruses seem to come in two flavors: the transient virus, which is only active when you're running your code, and the Terminate and Stay Resident kind, which stay active from the time initiated until you reboot your computer. There's a third kind, called a 'boot sector' virus which will be discussed below.

When you invoke a program, infected or not, your computer will read the image of the program from the disk into the computer's memory, do a little bit of futzing with the program. The computer's operating system, in this case MS-DOS, is really stupid: it gives total control to the running program from that moment until the program exits and you get back to your command line prompt.

When you invoke an infected program, it runs just as any other program. The virus portion of that program will typically be run first. After passing the pre-trigger (if any), the replication aspect will consider what types of files to infect. For the standard transient virus, this usually means that a given directory will have one or more of its .COM or .EXE files infected.

Some viruses will infect only one program each time they are run, some will infect many. Each virus has some characteristic about it which is unique, and often the virus writer will examine the target .COM or .EXE

file for this characteristic to see if it is already infected. If it is, then the program will be passed over and the next one examined and potentially infected.

Since the computer passes control onto the program once it is loaded into memory, and then basically forgets about it, if the first few instructions of the program can be changed to cause the computer to execute some new instructions, it will blindly do so.

And that's what a virus does. It takes the first few instructions of the program, saves them someplace, and replaces those instructions with a call to jump to the virus code.

When the virus infected program executes later, it will first run the virus code, then restore the original code (unless the virus "goes off", discussed below), and finally will jump to the beginning of the reconstructed program. The infected program executes as if nothing had happened at all.

When a virus infects another program, it must add code to it. And it must replace at least a few instructions at least temporarily, with some of its own.

Typically, a virus will add to the end of a program, although not all viruses work that way. This is how almost all transient viruses work.

TSR Virus

Another, more sophisticated virus, is called the "TSR virus". This infects a program like the transient virus, but its "action" involves leaving a little piece of itself behind (those in the anti-virus field seem to call that part left behind the "worm trail," or the "slime"). This piece becomes an active, and permanent, part of your computer's operating system. Typically, it will look for instructions your computer sends in response to you entering a run command. When you do, it infects the program you've requested to run before it is actually executed.

Going back to the phases, the third phase is called the "trigger aspect". Like a pre-trigger, it depends on how devious the virus writer is when he or she creates a trigger, and can go off on just about anything.

When it goes off, the final (and most dangerous) phase of the virus is

reached: the "Trojan aspect". This is the part that deletes files, trashes your hard disk, or otherwise makes your life miserable.

Boot Sector Virus

When you turn your computer on, a small program is run before anything else. It's called the Boot Sector, and it loads up important software your computer needs in order to work, like the operating system. Without the operating system (MS-DOS), your computer is an expensive paperweight. Without the Boot Sector, and the program thereon, you have an expensive paperweight with an inoperable operating system on it.

A Boot Sector Virus replaces the current boot program with itself, and sticks the original boot sector onto an unused portion of your disk. After the Boot Sector Virus has run, leaving behind a little worm trail of its own, it will execute the original boot program. You'll have an infected system even before an anti-virus program is run!

When you access some other disk, the worm trail of the Boot Sector Virus will examine the boot sector of that disk. If not infected, it will infect it. And the infected diskette waits for you to pass it on to one of your friends, who will then (by booting on that disk) infect their own drive. The moral here: never boot up your system on anyone else's disk and you'll be a much happier person.

Section IV:
Computer Virus Myths

by Rob Rosenberger, with Ross Greenberg

A number of myths have popped up recently about the threat of computer "viruses." There are myths about how widespread they are, how dangerous they are, and about what a computer virus really is.

We'd like the facts to be known. The first thing to understand is that a virus is a programming technique in the realm of "Trojan horses." All viruses are Trojan horses, but few Trojan horses can be called a virus.

To understand more about viruses it helps to know the terminology.

Terminology

BBS Bulletin Board System.
If you have a modem, you can call a BBS and leave messages, transfer computer files back & forth, and learn a lot about computers.

Bug
An accidental flaw in the logic of a computer program that makes it do things it shouldn't be doing. Programmers don't mean to put bugs in their program, but they always creep in. The first bug was discovered by pioneer Grace Hopper when she found a dead moth shorting out a circuit in the early days of computers.

Hacker
Someone who loves computers and who wants to push them to the limit. Hackers don't release Trojan horses onto the world, it's the wormers who do that. Hackers have a healthy sense of curiosity: they tinker with a piece of equipment until it's "just right."

Shareware
A distribution method for software available on a "try before you buy" basis. You pay for the program if you find it useful. Shareware can be downloaded from BBSs. There are few advertising & distribution costs, so many shareware applications can rival the power of off-the-shelf counterparts, at just a fraction of the price.

Trojan horse
A set of computer instructions purposely hidden inside a program. Trojan horses tell a program to do things you don't expect it to do.

Virus
A term for a very specialized Trojan horse that can spread to other computers by secretly "infecting" programs with a copy of itself. A virus is the only type of Trojan horse which is contagious, like the common cold. If it doesn't meet this definition, then it isn't a virus.

Worm
A term similar to a Trojan horse, but there is no "gift" involved. An example is an unauthorized program designed to spread itself by exploiting a bug in a network software package. Worms are usually released by someone who has normal access to the computer or network.

Wormers
The name given to the people who unleash destructive Trojan horses. These people aren't angels. What they do hurts us. Viruses, like all Trojan horses, are purposely designed to make a program do things you don't expect it to do. Some viruses are just an annoyance. The viruses we're worried about are the ones designed to destroy your files and waste the valuable time you'll spend to repair the damage.

Myths

All purposely destructive code comes as a virus.

Wrong. Remember, "Trojan horse" is the general term for purposely destructive code. Very few Trojan horses are actually viruses.

All Trojan horses are bad.

Believe it or not, there are a few useful Trojan horse techniques in the world. A "side door" is any command not documented in the manual, and it's a Trojan horse by definition. Some programmers install side doors to help them locate bugs in their programs.

Viruses and Trojan horses are a recent phenomenon.

Trojan horses have been around since the first days of the computer. Hackers toyed with viruses in the early 1960s as a form of amusement.

Computer viruses are reaching epidemic proportions.

No. Viruses may be spread all over the planet but they aren't taking over the world. There are only about fifty or so known virus "strains" at this time and a few of them have been completely eliminated. Your chances of being infected are slim if you take proper precautions.

Viruses could destroy all the files on my disks.

Yes, and a spilled cup of coffee will do the same thing. If you have backup copies of your data, you can recover from a virus/coffee attack. Backups mean the difference between a nuisance and a disaster.

Viruses can be hidden inside a data file.

Data files can't wreak havoc on your computer -- only an executable program can do that. If a virus were to infect a data file, it would be a wasted effort.

Most BBSs are infected with viruses.

Here's another scary myth drummed up in the big virus panic. Few BBSs are infected. (If they are infected, they won't be around for long!) It's possible a dangerous file could be available on a BBS, but that doesn't mean the BBS itself is infected.

BBSs and shareware programs spread viruses.

"The truth," says PC Magazine publisher Bill Machrone, "is that all major viruses to date were transmitted by commercial packages and private mail systems, often in universities." The Peace virus, for example, made its way into a commercial software product sold to thousands of customers. Machrone goes on to say that "bulletin boards and shareware authors work extraordinarily hard at policing themselves to keep viruses out."

Many reputable sysops check all new files for Trojan horses; nationwide sysop networks help spread the word about dangerous files. You should be careful about software that comes from friends and BBSs, that's definitely true -- but you must also be careful with the software you buy at computer stores.

My computer could be infected if I call an infected BBS.

BBSs can't write information on your disks — that's handled by the communications software. You can only transfer a dangerous file if you let your software do it. (In rare cases, a computer hooked into a network could be sent a dangerous file or directly infected, but it takes special software to connect a computer into a network. BBSs are NOT networks.)

My files are damaged, so it must have been a virus attack.

It could also have been caused by a power flux, or static electricity, or a fingerprint on a floppy disk, or a bug in your software, or perhaps a simple error on your part. Power failures and spilled cups of coffee have destroyed more data than all the viruses combined.

My backup disks will be destroyed if I back up a virus.

No, they won't. Suppose a virus does get backed up with your other files. Backups are just a form of data, and data can't harm your system. You can recover the important files from your backups without triggering the virus.

Anti-virus software will protect me from viruses.

Anti-virus packages offer some good front-line protection, but they can be tricky to use at times. You could make a crucial mistake in deciding whether to let a "flagged" event take place. Also, Trojan horses can be designed to take advantage of holes in your defense.

Copy-protected software is safe from an attack.

No. Copy-protected software is the most vulnerable in a Trojan horse attack. You may have big problems trying to use or re-install it, especially if the master was attacked. Copy-protection schemes rely on extremely tricky techniques which have occasionally "blown up" on users. Some people believe they were attacked by a clever virus.

We hope this dispels the myths surrounding the virus scare. Viruses DO exist, many of them will cause damage, and all of them can spread to other computers. But you can defend yourself from an attack if you keep a cool head and a set of backups.

Section V:
How To Protect Yourself From Viruses

These guidelines can shield you from Trojan horses and viruses. They lower your chance of being attacked and raise your chance of recovering from one.

1. Download files only from reputable BBSs where sysops check every program for Trojan horses.

2. Let a newly uploaded file "mature" on a BBS for one or two weeks before you download it (others will put it through its paces).

3. Set up a procedure to regularly back up files. Follow it religiously!

4. Rotate between two sets of backups for better security .

5. Consider using a program which will create a unique "signature" of all the programs on your computer. Once in a while, you can run this program to determine if any of your applications have been modified.

6. If your computer starts acting weird, don't panic. It may be a virus, but it may not. Immediately reboot from a legitimate copy of your master DOS disk. Put a write-protect tab on that disk. Do NOT run any programs on your regular disks (you might activate a Trojan horse). If you don't have adequate backups, try to bring them up to date. You might be backing up a virus as well, but it can't hurt you as long as you don't run any of your normal programs. Set your backups off to the side. Then can you safely hunt for the problem.

7. If you can't figure out what's wrong with your computer, and you aren't sure of yourself, just turn it off and call for help. Consider calling a local computer group before you hire an expert to fix your problem.

8. If you can't figure out what's wrong with your computer, and you are sure of yourself, execute a low-level format on all of your regular disks, then do a high-level format on each one of them. Next, carefully re-install your software from legitimate copies of the master disks, not from the backups. Then, carefully restore only the data files (not the executable program files!) from your backup disks.

Index

Expert Software License Statement

Some states do not allow limitations on how long an implied warranty lasts or the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions might not apply to you.

Copyrights:
The manual and the software described in it are copyrighted with all rights reserved. The manual or software may not be copied in whole or part, without written consent of Expert Software. You may not sell, rent, lease nor transfer copies of the manual or software in any other way with out the prior written consent of Expert Software.

Trademarks
All trademarks are acknowledged.

Service Policy

Replacement Policy
If the disk or disks should fail within 90 days of purchase, please return the original disk with proof of purchase for FREE replacement. After 90 days from date of purchase, include $9.50 for replacement.

You can obtain a replacement disk of the program by returning the defective copy, with your proof of purchase to Expert Software, Attention: Customer Service, P.O. Box. 1911, Murray Hill, New York, NY 10156.

Product Support
All of Expert Software's products are thoroughly tested and come with a comprehensive User Guide. However, if you have a problem using the product, we recommend you doing the following:

1. Review the User Guide - it answers most questions and problems. Also, check your computer system to make certain the program works with the operation system, interfaces, peripherals, and overall configuration.

2. If you still have a problem, contact Expert Software at the address above (be sure to include your telephone number for a faster response). Describe the problem as detailed as possible including error messages, and the sequence of steps leading up to the problem. Also, describe your hardware - including manufacturer, type and number of drives, printer, expansion boards, etc.

3.5" Disk Offer

Your program is now available in 3.5" format. To receive your disks return the original system disk, a check or money order for $9.50 to Expert Software, P.O. Box 1911, Murray Hill, New York, NY 10156

Free Software Coupon

Select either PC Protection, Disk Tools, or Personal Skills (see catalog). Enclose Two (2) Expert Software Coupons (photocopies not accepted) along with Proof of Purchase (the actual box top with the product code number) and a photocopy of your sales receipt, for your free Expert Software product. Enclose $3.00 to cover shipping and handling (US funds, payable to Expert Software).

Free Product requested: (circle) **PC Protection Disk Tools Personal Skills**
Specify computer type: IBM PC Apple II Commodore 64/128

Name: .....

Address: .....

City: ..... **State** ..... **Zip** .....

Offer expires December 31, 1990. Offer not valid with any other offers or discounts. The certificate has no cash or refund value. Offer void where taxed, restricted or prohibited by law; good only in the United States and Canada. Allow 4-8 weeks for delivery of the free software program. Limit two (2) free products per household/customer. Schools and institutions not eligible. If your selection is not available when order is received, we reserve the right to substitute a similar product.