

NORMAN Contents

Introduction

[About this helpfile](#)

The Main Window

[Functions available from the Main Window](#)

Norman's Smart Behavior Blocker

[Smart Behavior Blocking](#)

[Loading the Smart Behavior Blocker](#)

[Configuring the Smart Behavior Blocker](#)

[What to Do When the Smart Behavior Blocker Warns](#)

The Scanning Process

[The Scanning for Viruses Dialog](#)

[Virus Found](#)

[Boot Sector Virus Removal](#)

Scanning Configuration

[About scanning](#)

Styles

[About Styles](#)

[The Edit Styles Dialog Box](#)

Scheduling

[Scheduling overview](#)

Virus Library

[Finding Out More About Viruses](#)

Display Function

[Display Files and System Area](#)

Appendix

[General information on installation/updates](#)

NORMAN About this helpfile

Norman Virus Control for Windows 95 is comprised of several modules. Some modules are DOS-based, meaning that they should be run from the command line.

This helpfile covers the Windows specific part of the product. For more detailed information on subjects not covered in this helpfile, please refer to the manual *NVC for Windows 95 - User's Guide*. This manual is available as a PDF file to be read with the Acrobat Reader, and - in some markets - as a printed manual.

NORMAN Functions available from the Main Window

Selecting areas to scan

The following toolbar buttons are shortcuts for selecting areas for scanning:



Selects all fixed local and network drives



Selects all fixed local drives



Selects all network drives



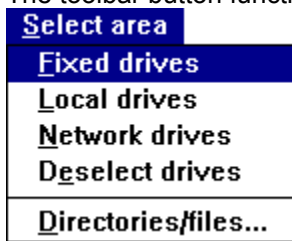
Deselects current selection



Selects directories, subdirectories, and files

From the menu options

The toolbar button functions are also available from the menu option Select area.



In the main window

You can also specify any combination of drives you want to scan by checking the relevant drive letters directly in the main window:

- A:
- C:
- D:
- E:
- F:
- G:

Other toolbar buttons



Scanning options, for configuring the virus scanner



Scheduler options, for entering scans at scheduled intervals



Scheduled scan on/off, for turning the scheduler on or off



Virus library, for information on known viruses



Online help



Exit NVC

NORMAN Smart Behavior Blocking

The Smart Behavior Blocker does not scan for specific virus patterns in files being run or in system areas. Instead, the Smart Behavior Blocker monitors all activities in the system and is able to recognize all program behavior that represents typical virus techniques. In this way, the Smart Behavior Blocker detects both known and unknown viruses and prevents viruses from infecting.

NORMAN Loading the Smart Behavior Blocker

The installation procedure automatically places the Smart Behavior Blocker (SBB) in the Startup group so that it is loaded automatically when Windows 9x starts.

If your Startup group contains multiple programs, and you wish to launch certain programs before the SBB, you can delay the SBB by entering the following command:

NORMISA /DELAY:10

The SBB will then wait for the specified number of seconds before it starts. SBB will wait for 5 seconds before it's loaded if you don't specify a number with the /DELAY command.

And if you don't want to display the Norman logo every time the SBB starts, enter:

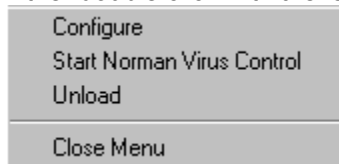
NORMISA /NOLOGO

If you unload the Smart Behavior Blocker and then want to reload it without restarting Windows 9x, simply run NORMISA.EXE from the C:\NORMAN\WIN95 directory.

When the Smart Behavior Blocker is active, you will see this icon in the notification area:



Either double click with the left mouse button or click once with the right mouse button, and you will see:



From here, you can configure the Smart Behavior Blocker, start the anti-virus scanner for Windows 95, or unload the Smart Behavior Blocker.

If you want to delete the Smart Behavior Blocker from your PC, use the Uninstall function in Control Panel in Windows 9x.

NORMAN Configuring the Smart Behavior Blocker

Buttons:

OK will accept all configuration settings and close the Configuration dialogs.

Cancel will cancel all configuration settings and close the Configuration dialogs.

Apply will accept all configuration settings and keep the Configuration dialogs open.

Reset all will reset all configuration settings to their default values and keep the Configuration dialogs open.

Help will display a short help file.

Unload will remove the Smart Behavior Blocker from memory. To activate it again, you must run NORMISA.EXE either manually or place it in the Startup group and then start Windows 9x again. See [Loading the Smart Behavior Blocker](#).

More:

[The Configuration Interface](#)

[Specifying Files](#)

[Boot Sector](#)

[Memory](#)

[Advanced Functions](#)

[The Configuration Files](#)

NORMAN The Configuration Interface

From the configuration screen you can access five different tabbed dialog boxes and specify your basic configuration. These fall into three categories:

1. What to do when a virus is found
2. Reporting
3. Including/excluding files

More:

[When a Virus Is Found](#)

[Reporting](#)

NORMAN When a Virus Is Found

[] Enable interactive mode

When you are running in interactive mode, you will be notified and prompted for action whenever the Smart Behavior Blocker detects virus-like activity. Normally, this will consist of two choices.

- A Clean and proceed
- B Ignore and proceed at your own risk

This warning pops up in “text mode” and not the interface that you are accustomed to seeing. The reason for using text mode here is that when an infecting process is stopped, we need to notify the user, wait for a response, and perform the desired action. The module in Windows 9x that handles this function is not a multitasking function and can therefore only handle one access at a time. You must therefore select an action in order for Windows 9x to resume control.

If you choose to use interactive mode, you have the additional option of turning on the setting called

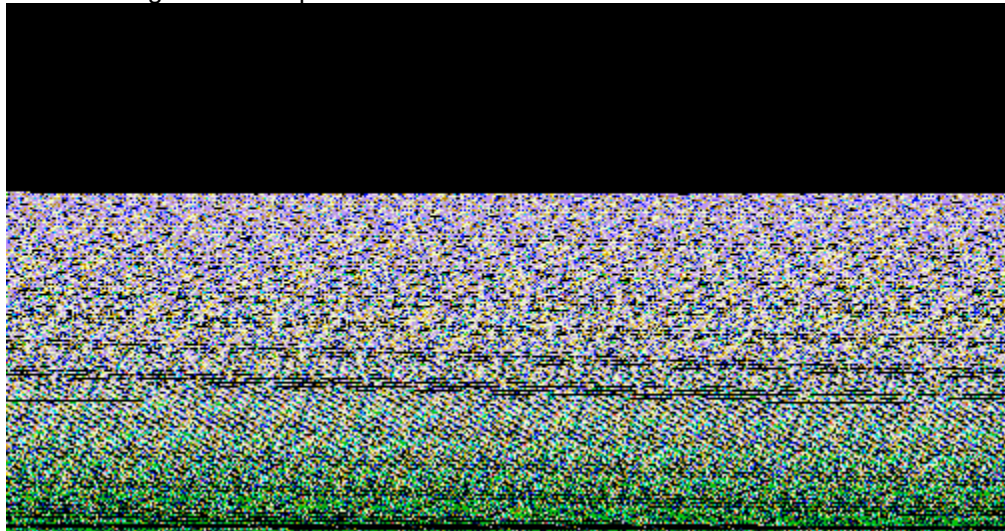
[] Force action on infection.

Normally, the user has the option to ignore the virus warning and continue with the task at hand without preventing the virus action. However, with [] **Force action on infection** turned on, the virus warning cannot be ignored.

See the [What to Do When the Smart Behavior Blocker Warns](#).

Note: In Automatic mode you will be notified if the Smart Behavior Blocker detects virus-like activity, but you will not be prompted for action. Instead, the Smart Behavior Blocker handles the problem in the background.

The following is an example of notification under Automatic mode:



In addition, you can choose to have an audible alarm sound when virus-like behavior is detected.

NORMAN Reporting

[] Log report to file

[] Dump boot sector to file

You can log both virus incidents as well as infected boot sectors to files. The default filenames are NORMISA.LOG and NORMISA.DMP, respectively.

If you so choose, you may view the most recent NORMISA.LOG from this menu.

Note that you can view NORMISA.DMP only if a boot sector virus has been detected. Dumping a boot sector to a file is not dangerous, and you cannot spread the boot virus in this fashion.

[] Enable user include/exclude lists

When this option is checked, then the following tabbed dialogs will be activated:

- Files
- Boot Sector
- Memory

Checking this option makes the “Files” tabbed dialog available. From here, you can specify files that you want to be closely monitored or excluded from monitoring altogether. These could be files that you know are exposed to virus infection, files vital to your system, or files that have produced false alarms.

Click on the Files tab.

We refer to all areas that the Smart Behavior Blocker monitors as “hot”. For example, we have “hot files”, “hot extensions”, and “hot areas”.

“Hot files” are files with the extensions of EXE (with MZ, NE, or PE headers), DLL, VBX, OCX, CPL, VXD, 386, COM, SYS, DRV, PDR and MPD. . The Smart Behavior Blocker monitors access to these files (activities that include file creation, deletion, rename and write).

Note: The files CONFIG.SYS and MSDOS.SYS are excluded from all monitoring.

We must take a little detour here and explain how the Windows 9x shell handles files so that you understand how the Smart Behavior Blocker will react.

Most users will not notice this, but when you press “DEL” in Explorer, the file is not deleted, but rather moved to the Recycle Bin under the same extension but different **filename**. The file will actually be deleted only when you empty the Recycle Bin.

If you have set the Smart Behavior Blocker to “strict” mode (see [Advanced Functions](#)), then emptying a Recycle Bin that contains hot file extensions will result in a virus warning.

Since files with these extensions are system properties, options are not provided for the user to include or exclude these extensions. Therefore, users should not name a data file ACCOUNT.EXE, for instance.

Note: If you are a programmer and are working on the file MYPROG.EXE, the following will happen when you link the file:

the Smart Behavior Blocker deletes the file and saves it as a temporary file. When the process is complete, the temporary file is renamed MYPROG.EXE and you may receive a false alarm. This will happen even if you have excluded the file.

If you are having this problem, then please call Norman Data Defense Systems for help.

From this dialog, there are three different groups of settings:

[] Include filenames

In this dialog box you can establish up to 16 specific filenames that should be included as “hot files”.

1. Enter a filename (even long filenames) in the Filename box.
2. If you do not specify the path, then ALL files found (even on remote drives) with this name are included.
3. Click the **Add** button to include the file in the list.
4. You may also **Remove** any files that are already in the list.

You may also include up to 16 sets of file types by specifying extensions. Click on **Include file extensions** to access the tabbed dialog ‘Files’.

NORMAN Specifying Files

Specify types by entering their file extensions. You do not have to include the leading dot (e.g., INI).

Note: If you include a filename and then try to delete the file using “DEL”, etc., the Smart Behavior Blocker will warn. To delete the file successfully, unload the Smart Behavior Blocker first or remove the file from the include list.

To navigate to the exclude filenames function from here, click on **Include filenames** and then click on **Exclude filenames**.

Exclude Filenames

From the “Include filenames” dialog, you can click on "Exclude filenames" from the Smart Behavior Blocker’s monitoring.

1. Enter a filename (even a long filename) in the Filename box.
2. If you do not specify the path, then ALL files found (even on remote drives) with this name are excluded.
3. Click the **Add** button to put the file in the list.
4. You may also **Remove** any files that are already in the list.

Note: You can specify a maximum of 16 files to be excluded, but unlike the “Include” functions, you may not exclude groups of files by their extensions.

Precedence of Checking Files

Since you have many options to include files/file extensions and exclude files, it is important to understand how the Smart Behavior Blocker processes these exceptions. The precedence for determining the status of a file is as follows:

1. User specified files for exclusion
2. User specified files for inclusion
3. System specified files for exclusion
4. User specified files by extension
5. System specified files by extension

NORMAN Boot Sector

We predict that this function will not be used by end-users but rather by administrators.

“Hot areas” are considered to be the Master Boot Sector, System Boot Sector, and extended partition table. All writes to these areas will be monitored by the Smart Behavior Blocker.

As with including and excluding files, you may also include and exclude certain strings within boot sectors. You can specify a maximum of 32 strings.

Note: This function’s purpose is not to exclude detection of certain boot viruses but rather to exclude monitoring of a stream of hex strings that cause false alarms.

As with including and excluding filenames, you can toggle between the include and exclude lists.

Note: You must enter a hex string in the text box marked “String”. All hex strings are to be provided by Norman Data Defense Systems to our customers. We do not recommend that customers define their own strings.

NORMAN Memory

This is an extremely advanced feature that end-users will not utilize.

In the event of false positives or false negatives on memory addresses, you may include or exclude up to 32 memory addresses.

Note: As with Boot Sector hex strings, memory address strings must be provided by Norman Data Defense Systems.

NORMAN Advanced Functions

These functions are not intended for end-users but rather for administrators.

You can choose settings from two groups:

1. Areas to monitor

By default, all of these options are turned on.

When **Enable File Protection** is checked, then the Smart Behavior Blocker will monitor both the default and user-defined hot files and extensions.

When **Enable System Area Protection** is checked, then the Smart Behavior Blocker will monitor modifications to any system area on hard drives and diskettes.

Note: We do not recommend that these two options both be turned off at the same time.

When **Enable IO port protection** is checked, then the Smart Behavior Blocker will monitor all attempts to access the diskette drive or the hard drive from the outside (i.e., protecting the software that is handling such activities).

When **Enable DOS Integrity Protection** is checked, then the Smart Behavior Blocker will monitor activity on all critical DOS files.

Windows 9x still very much depends on DOS for some of its internal system housekeeping. Whereas Win32 programs run in their own address space safely hidden in the System Virtual Machine, and all DOS boxes are Virtual Machines which are not supposed to threaten the stability of the Windows 9x system as a whole, all the Win32 programs and DOS boxes still share one copy of DOS. Although this copy of DOS is shared, the TSRs (“terminate and stay resident programs) loaded from the DOS boxes are not. In brief, it is still possible for a virus to modify this one copy of DOS in a way that it will affect all the Win32 programs and DOS boxes. Therefore, it has a system-wide impact. The Smart Behavior Blocker watches for this, but you can turn off DOS integrity protection.

2. Level of protection

You may choose between two levels of protection: Normal and Strict.

Normal security is the default provides protection for all default hot areas (files, file extensions, and boot areas).

Strict security is the “paranoid mode” in which no modifications to any hot areas — files, file extensions and boot areas — are allowed.

Note: Regardless of mode, all hot files are treated with strict security.

Following are charts that describe both modes in more detail.

Normal Mode Chart

User action

Delete hot files and hot extensions

Smart Behavior

Blocker action

Tracks

Rename hot files and hot extensions

Create new COM file

Replace existing hot files, hot extensions,
and hot areas

Write to hot files, hot extensions,
and hot areas

Tracks

Alerts if EXE exists

Tracks/amends

Tracks if MZ, NE,
COM or SYS.

Alerts if PE, LE or
W3.

Note that “track” means that the Smart Behavior Blocker will allow modifications to occur until the point at which they are deemed to be as a result of virus-like activity.

Strict Mode Chart

User action

Delete hot files and hot extensions

Rename hot files and hot extensions

Create new COM file

Replace existing hot files, hot extensions,
and hot areas

Write to hot files, hot extensions,
and hot areas

Smart Behavior Blocker action

Alerts

Alerts

Alerts if EXE exists

Alerts

Alerts

NORMAN The Configuration Files

It is also possible to configure the Smart Behavior Blocker from the configuration interface as described above, but you can also edit the configuration files manually, if you wish.

- `ISAMON.CFG` This is the default system wide configuration file and is not meant to be edited.
- `ISAMON.INI` This is the default system wide **user** configuration file. The file contains what has been specified in the configuration interface and can be edited from here as well.
- `ISAMON.UPD` This file supplements `isamon.cfg` and should normally not be edited. If necessary, Norman Data Defense Systems may issue updates to this file between official releases of NVC.

NORMAN What to Do When the Smart Behavior Blocker Warns

When the Smart Behavior Blocker warns, you will either be presented with choices appropriate to the situation or the Smart Behavior Blocker will prevent the destructive action automatically, depending on whether Interactive or Automatic mode is turned on.

In Interactive mode, we recommend that you always choose option “A” in order to prevent the destructive action from occurring.

When the Smart Behavior Blocker warns, it does not provide the name of the virus. If you want the name, you must run the Windows 95 scanner. Start the scanner from the Smart Behavior Blocker’s menu, or click on the icon in the Norman Virus Control folder.

To remove the virus from the original infected file or boot area, you must first unload the Smart Behavior Blocker and then run the Windows scanner or the command line scanner against it. If you do not unload the Smart Behavior Blocker first, the Smart Behavior Blocker might warn when the scanner attempts to remove the virus.

NORMAN The Scanning for Viruses Dialog

In the uppermost part of the dialog box, NVC95 displays information, updating it as the scan progresses.

In the “Infected areas” list box at the bottom of the screen, you will receive information on infected files. The scanner reports the path and name of the infected file, the virus name, and the status of the infected file. There are four possible status types:

Status:	Reason:
Repaired	You checked the <input type="checkbox"/> Repair file when possible option, and the scanner automatically removed a virus.
Deleted	You did not check the repair option, and/or the infected file could not be repaired. You also specified that infected files should be deleted.
Moved to...	You did not check the repair option, and/or the infected file could not be repaired. You also specified that infected files should be moved.
Infected	You did not check the repair option, and/or the infected file could not be repaired, and/or you specified <input type="checkbox"/> No action when virus found .

If the status is “Repaired” or “Deleted”, the virus is already taken care of. You can check the details in the scanning report.

See [Managing Infections Options](#) for details about options for handling infected files.

If the status is “Moved to” or “Infected”, you still have one or more infected files on your machine. Remove the virus(es) by running the scanner with the option **Repair file when possible** ON, or highlight the virus in the list box and click the Repair button.

If NVC cannot remove the virus(es), you should delete the file(s) altogether.

Note: If an infected file resides on a write-protected diskette, a CD-ROM, or a protected area on a server, the scanner cannot repair, move, or delete the file. When this is the case, the status for the file will always be listed as “Infected”.

You can highlight entries in the “Infected areas” list box, and then click on one of the following buttons:

Repair file, **M**ove to, or **D**elete file. Note that:

- A repaired file cannot be highlighted to ensure that it’s not accidentally deleted.

Buttons:

Help Gives direct access to the NVC95 help system.

Cancel/OK This button will appear either as **Cancel** or **OK**, depending on the status of the scanning

While NVC95 is scanning, the button will appear as **Cancel**. When you click on the **Cancel** button, you instruct NVC95 to abort the scan.

When you abort an ongoing scan or when the scan is completed, the button will appear as **OK**. Clicking on the **OK** button closes the dialog box and returns you to the main window.

You may also abort a scan by pressing the [Esc] key.

View report: If you have chosen either of the report options from the "Reporting" tabbed dialog box in the Scanning options dialog, you have the opportunity to view the report on the screen.

This button appears grayed until the job is done or if the report option is not selected.

After NVC95 has created the report, you can click on the **View report** button, and Notepad will display the report.

You can scroll through the report by using either the scroll bar or the [PgUp] and [PgDn] keys. You can also save it as a different filename, print it, and so on.

Information during the scan:

The following information is also useful during a scan:

Files: the number of files that have been found in the specified location so far in the process.

Scanned: the number of files that have been scanned so far in the process.

Note: The number of files found in the specified directory will almost always be different than the number of files scanned because NVC95 only scans files with certain (default) extensions in addition to the user-specified extensions you specify. Please refer to the Read Me file for more information on which extensions NVC95 scans.

COM:, EXE:, SYS:, OV?:, DLL:, Others: how many files of these different extensions that have been found and scanned for viruses. The total of all these will be equal to the total number of files scanned.

Infected: the total number of infected files that NVC95 has found so far in the process.

Scanning: this shows the area that is currently being scanned.

The dialog box also contains a **progress bar** which shows the percentage of the scan that has been completed.

The list box at the lower part of the screen displays the path and filename of possibly infected files and/or boot areas along with the name of the virus that has infected these areas.

If the list of infected files is long, you can scroll through the list box by using the scrollbar or the [PgUp] and [PgDn] keys.

At the bottom of the dialog box is a status line, which summarizes three pieces of information:

Variants: shows the number of viruses and variants this version of NVC95 is able to recognize. See [Finding Out More About Viruses](#).

Log: shows you whether or not the report function is activated. This field can have the values **Y** or **N**.

Selected areas: displays the areas that you have selected for the scan.

NORMAN Virus Found

Highlight the infected area by clicking on it **once**. The buttons **M**ove file and **D**elete file are now activated, and you are allowed to delete or move the infected files.

The **R**epair file button is activated when you highlight an infected file or area.

1. First, try to remove the virus by highlighting the infected file in the list box and then click on the **R**epair file button.
2. If the virus can be removed, it will appear in the “Infected areas” list box with status “Repaired”.

Note: Remember that automatic removal of boot sector viruses is not possible. If you’re infected by such a virus, follow the instructions on the screen.

The option of automatic removal of known viruses is implemented in the scanning function. During on-demand and scheduled scans, the scanner will check for known viruses and try to remove possible infections on-the-fly.

Viruses cannot be removed automatically by the scanner in the following situations:

1. The file resides on a write-protected diskette or CD-ROM
2. The file resides on a network drive and is write-protected,
3. The file is in use (i.e., you do not have write access).

Note that the infected file(s) appears in the “Infected areas” list box with details about the virus and where it’s located.

Note: If you highlight several infections, click on **R**epair file, and receive the message "Cannot repair file", try to highlight and repair one infection at the time.

NORMAN Boot Sector Virus Removal

The core technology in all NVC components is the scanning engine. The scanning options reflect the capability of the engine. In addition to detect viruses, the engine can also remove them (repair the file or boot sector, and thereby clean the machine). This process is technically more complicated than detection.

If anything goes wrong, repairing a file is less hazardous than repairing a boot sector. A corrupted boot sector may render the system useless. To ensure that a failed boot sector repair will not put you in an awkward situation, we do not allow automatic repair of boot sectors.

If a boot sector virus is detected, you will see a dialog box that recommends that you back up the necessary data to a diskette. If the repair fails, you can boot your machine from the restore diskette.

More:

[Boot Virus On Hard Drive Detected](#)

[Boot Virus Removed And Restore Diskette Created](#)

[Boot Virus Removed But Restore Diskette Was Not Created](#)

[Boot Virus Repair And Restore Diskette Creation Failed](#)

NORMAN Boot Virus On Hard Drive Detected

A boot sector virus was detected on the hard drive. The scanner is not allowed to remove a boot virus automatically. Repairing a boot sector virus is not risky, but in case something goes wrong, we recommend that you back up the replaced sectors.

If repair fails, you will most likely discover it on next reboot. If this happens, boot from the restore diskette. Note that in such a situation, your system is still infected.

NORMAN Boot Virus Removed And Restore Diskette Created

It is important that you label the restore diskette properly and keep it in a safe place. If repair fails, you will most likely discover it on next reboot. If this happens, boot from the restore diskette. Note that in such a situation, your system is still infected.

NORMAN Boot Virus Removed But Restore Diskette Was Not Created

The boot virus was removed from the hard drive, but no restore diskette was created. The reason for not succeeding in creating a restore diskette is most likely a damaged diskette.

However, the virus is removed.

NORMAN Boot Virus Repair And Restore Diskette Creation Failed

Repair failed, but your boot sector is most likely intact. This is a rare situation, which could have been caused by a write-protected medium, for example a Jaz disk.

When repair fails, a restore diskette will never be created.

Note that your hard drive is still infected.

NORMAN About scanning

Scanning is a way to identify viruses that already exist in memory, files, or boot areas. Identifying these by name requires that the scanner recognizes the virus, which means that scanners must be frequently updated for information about new viruses.

We recommend that you visit Norman's Web site for free downloading of updated versions of the virus definition files.

See [Appendix](#) for more information.

Note: Options checked like this: [x] are default settings.

More:

[Scanning Options](#)

[Reporting Options](#)

[Managing Infections Options](#)

[Additional Options](#)

[User-Specified Extensions](#)

[Scan Directories or Files](#)

[Specify Directories in Styles](#)

NORMAN Scanning Options

Don't stop on virus

Click on this option when you do not want to sit and watch the scanner working. This is especially useful when scanning a network. Usually, when the scanner detects a virus, it asks for keyboard input, but in this mode, the scanner does not require keyboard input when a virus is found and proceeds until the scan is done.

Ignore locked files

During normal use, the scanner will stop processing if it cannot open a file. You will see a dialog box showing you which file is locked. At this point, you may press **Cancel** in order to continue the scan but ignore all subsequent locked files.

To avoid error messages when locked files are found, turn this option on.

If you have logging turned on (either report to file or report to printer), then the log will contain the name(s) of the locked file(s).

Look for OLE2 header

Files generated in MS Word and Excel can be renamed and thus receive file types other than .doc and .xls, for example, which the scanner is always looking for. However, these files can be identified by their header, which will be OLE2. To detect camouflaged Word and Excel files, which are possible macro virus carriers, this option instructs the scanner to scan files with OLE2 headers.

Exit upon completion

This is handy when you wish to terminate the scanning session when the scan is complete.

For maximum efficiency, use this option along with the "Minimize while scanning" and "Report only if infection" options. With **all** these options turned on, the scanner will appear as a minimized icon while the scan progresses, a report will be generated only if a virus is found, Notepad will display the report (if it exists), and the scanner will exit when the scan is complete.

Multiple diskettes

If you have several **diskettes** that you want to check during one scanning session, check this option. You may click on **Cancel** any time you wish to stop.

Any reporting done when this option is checked will result in one report for all diskettes scanned instead of separate reports.

Scan archive files

Archiving files is an efficient way to transfer files as well as freeing up space on your hard drive, a diskette, or a server. Since many viruses attach themselves to programs, it is possible to archive an infected file. We provide this option to temporarily uncompress an archived file and scan the files within.

When archived files are being scanned, the **Cancel** button is unavailable.

Note: When a file is archived, the scanner can only tell you whether or not it is infected. It cannot take any action on the infected file while it is archived.

The scanner will scan .ZIP and .ARJ files **internally**. This task is performed by the scanner's internal decompression system. The .ZIP and .ARJ files will therefore not be decompressed into "TMP" or

“TEMP”.

If the archived files are other types than .ZIP and .ARJ, then the scanner automatically reverts to **external** decompression, assuming that you have the archive system necessary for decompressing the archive files you want to scan. It also assumes that these programs are available in your path. If they are not in your path, then the scanner cannot decompress the files.

[] Compressed program files

Many users apply PKLITE, DIET, LZEXE or ICE, for example, to compress executable files. A compressed executable is better protected against viruses because the compression works almost like encryption. Still, if the compressed executable contains a virus, then the virus is activated whenever you run the executable. Even though you can scan for and detect the virus externally, the virus is still there and will be activated the next time you run the program.

This option makes use of a decompressor emulator to open and scan the file in memory. Scanning compressed program files is more time-consuming than scanning archive files. This is a good reason for not choosing this option unless you have strong reason to believe that a compressed executable is infected.

[x] Enable memory scan

When you scan the memory area, NVC95 looks for resident viruses. You should always make sure that no viruses exist in memory, and this option is therefore the default.

See the topic [Additional Options](#) for more information.

NORMAN Reporting Options

If you want NVC95 to give you a status report after a scan, you must choose the **Report to printer** and/or **Report to file** option(s).

Report to printer

The scanner will send its report right to the default printer that is set up through Windows 95.

Report to file

This default option will create the report NORMAN.RPT in the directory where the scanner resides. You may, however, specify another report name and directory.

Note: NVC now allows the use of UNC (Universal Naming Convention) names and environment variables wherever file and directory names can be entered. Please refer to the Administrator's Guide for details.

Overwrite previous

By default, the previous report is overwritten. If you want to keep track of previous scans on your PC, you should uncheck this option. The report will then be appended to the previous report(s).

If you are running several unattended scheduled scans, you should specify different report names for the different styles or uncheck this option.

See also [Scheduling Several Unattended Scans](#).

Note: If reporting to a file is disabled, then the **Overwrite previous** option will be grayed.

Report only if infection

The report will only be generated if an infection is found. If this is turned on, then the only reporting level available is **Log infected files**. See the list below for more details on reporting levels.

You may choose among three reporting levels:

1. **Log infected files**

This level will only report the infected files that are found. The report is short and concise.

2. **Scanned directories**

This level will make a list of all the directories that were scanned *in addition to* all the files that were found to be infected.

3. **Scanned files**

This level generates a list of all scanned directories and files. Infected files will be specifically marked. Of course, if you scan many files, this report will be quite long.

The "plus" signs between these reporting levels means that when you choose higher levels of reporting, the characteristics of the lower level(s) will be included.

You will see that the reporting level choices on the right side of the dialog box are only available if reporting to file or printer is turned on.

Note: Provided that you selected one of the reporting options, you may at any time view the last report that the scanner generated. Click on [View|Report](#) from the main window.

NORMAN Managing Infections Options

The option of automatic removal of known viruses is implemented in the scanning function. During on-demand and scheduled scans, the scanner will check for known viruses. If a virus is found, the scanner will try to remove it on-the-fly.

Viruses cannot be removed in the following situations:

1. The file resides on a write-protected diskette or CD-ROM,
2. The file resides on a network drive and is write-protected,
3. The file is in use (i.e., you do not have write access).

Repair file if possible

This option ensures that viruses detected during on-demand or scheduled scans are removed on-the-fly, if possible. If this option is checked, you are well protected against all viruses known to NVC.

The present version of the scanner detects and removes known file and macro viruses, as well as boot viruses. The 32-bit scanner can also detect and remove unknown macro viruses using heuristic methods. When the scanner detects an unknown Word 6/7 macro virus, the virus name will be reported as WM/GENERIC. If this option is ON, all macros in the document are removed.

Through internal testing it has been established that the detection rate for unknown macro viruses is about 80%.

Note: If you select the repair option, the remaining options in this dialog box are valid only when repair is not possible.

No action

If you wish to leave infected files alone at the time they are detected, check this option (default).

Note: Even if you choose not to delete or move infected files in this dialog, you can highlight infected files and delete or move them from the Scanning for viruses display.

Delete infected files

If you wish to delete infected files as they are discovered, select the **Delete** radio button.

Move infected files to

If you want to move all infected files as they are detected, you must specify the full path name of the destination. Otherwise, the scanner will move infected files into the directory C:\NORMAN\INFECTED.

To do this, click the **Move to** radio button and specify the path of the destination in the accompanying text box.

Note: NVC now allows the use of UNC (Universal Naming Convention) names and environment variables wherever file and directory names can be entered. Please refer to the Administrator's Guide for details.

If the specified directory does not exist, the scanner will create it for you automatically.

In a network environment, the area that you specify for storing infected files should be off-limits to everyone but the Supervisor.

If you have more than one instance of an infected `COMMAND.COM`, for example, and you choose to move each copy into the same directory, then the scanner will rename each instance of the file.

NORMAN Additional Options

There are a handful of options that need not be used by everyone, and so we have placed them here:

[] More specific virus names

This option allows NVC95 to use secondary virus signatures when it finds a virus, resulting in a more specific name for the virus.

This option does **not** increase the number of viruses detected but does increase scanning time.

[] Scan all files

One of the goals a virus has is to infect other files. The most efficient way of doing this is to infect executables. Normally, you do not have to scan files other than the defaults. However, when you use this option, NVC95 will scan all files it finds on the specified drive(s). This is a helpful feature if you suspect you have a virus and want to check all files.

Scanning time increases when you use this option.

[] Ignore system areas

By default, NVC95 scans the system areas (see below for definition) of a diskette or a local hard drive.

In cases where system areas have been severely corrupted, scanning them may cause NVC95 to fail with an error. This option instructs NVC95 to skip these areas and simply scan files.

The system area includes the Master Boot Sector (MBS) and System Boot Sector (SBS).

Master Boot Sector (MBS)

The MBS is located on all physical hard drives.

The MBS contains, among other data, information about the partition table (information about how a physical disk is divided into logical disks), and a short program that can interpret the partition information to find out where the System Boot Sector is located. MBS is independent of type of operating system.

System Boot Sector (SBS)

The SBS is located on all diskette and physical hard drives that are formatted, and it is created with FORMAT.COM. The SBS contains, among other data, a program whose purpose is to find and run an operating system (DOS, UNIX, or OS/2, for example). If the program does not find an operating system to run, the user will be prompted for a diskette with an operating system on it.

[] Look for EXE header

More and more often, we encounter viruses that keep track of all activities in individual files. Many look for signatures in .EXE files and make their decision on whether or not to infect based upon what they find (instead of simply looking for a file extension). To detect such viruses, this option instructs the scanner to scan files that have EXE headers.

Note: If you check this option, the scanner will look for the EXE header in **all** files and therefore increase scanning time considerably.

[] Delay between files

If you instruct NVC95 to scan many files, you can use this option to minimize the I/O (read/write from/to disk) load by pausing between each scanned file.

[x] Beep upon infection

By default, NVC95 beeps each time it detects an infected file or boot area. Clicking on this check box toggles between turning the beep on and off.

[] Minimize while scanning

If you wish to have NVC95 minimized while it performs a scan, then click on this option. When the scan starts, NVC95 will appear as an object on the Windows 95 taskbar.

If NVC95 is minimized and you wish to view the results, then you may double click on the icon, and you will see the Scanning for viruses dialog box.

NORMAN User-Specified Extensions

By default, NVC95 scans files with certain extensions. Please refer to the Read Me file for more information on which extensions NVC95 scans.

If you wish to add files with other extensions for scanning, you may use this dialog box to instruct NVC95 to look for up to 20 additional extensions.

To add a new user defined file extension:

1. Click on the **New type** check box
2. Type the file extension in the accompanying text box. All file extensions are limited to 3 characters.
3. Click on the **Add** button.

New file extensions will be saved in NVC95's Registry.

If you would like to have these extensions included in all of your scans, specify them as a setting within the **<NORMAL>** style.

If you would like these extensions to be used during only some of your scans, specify them as a setting within a style other than **<NORMAL>**.

For more information about styles, see [Saving Your Configurations as Styles](#).

To remove a user defined file extension, click on the extension you wish to remove and then click on the **Remove** button.

NORMAN Scan Directories or Files

If you choose "Directories/files", then you can:

- type in the name of the directory or file that you wish to scan
- clear the [] **Scan subdirectories** checkbox if you do **not** wish to scan directories underneath the directory you specify. This option is turned on by default.
- find the file or directory to scan by clicking on the **Find dir** button:

When you click on **Start scan** back in the "Scan directory or file" display, then the scan will start with the current configurations. These may not be the settings that you wished for this scan. Therefore, when you wish to use the "Directories/files" feature, be sure to set all configurations **before** you select "Directories/files".

NORMAN Specify Directories in Styles

You can identify drives for scanning by specifying the target areas with scanning options from the Edit styles dialog. You cannot specify individual files or directories in the same manner.

You can, however, use the DOS command `subst` to solve this problem.

Task: to scan directory `c:\data\internet` only.

1. From the command prompt, type:

```
subst z: c:\data\internet
```

where `z:` is a virtual drive. If a 'z:' drive exists on your system, you must select another drive letter.

2. Select Options|Styles and add the new style INTERNET:



3. Note that the virtual drive `z:` now appears in the Select drives list box.
4. Highlight the new style.
5. Select the `z:` drive from the box.
6. Click on **C**onfigure to determine the scanning options.

You have now created a style for scanning a specific directory. Like all styles, it is eligible for scheduled scans.

Note: You must run the `subst` command again to create the virtual drive again if after you have turned off or rebooted your PC.

NORMAN About Styles

You can save yourself time by saving your configurations as styles. For example, if your goal is to run scans in certain combinations (scan diskettes and delete infected files; scan local drives and move infected files to a specific location, for example), then you can simply configure both types of scans as different styles and have NVC95 use the appropriate style at the appropriate time.

To access the styles function, click on Options|Styles. You will then see a dialog box titled "Edit styles".

NVC95 is shipped with one style called the **<NORMAL>** style. It contains all the configuration settings that you have made thus far. The **<NORMAL>** style will always be available. You can customize it in any way you wish as well as create up to 20 additional styles, but you cannot delete the **<NORMAL>** style.

NORMAN The Edit Styles Dialog Box

From this dialog, you can add, delete, and modify styles.

Add a Style

1. Click on the check box marked [] **New**.
2. A new style is always based on the factory default settings.
3. Give the new style a name.
4. Do this by entering the new name in the text box located to the right of the control box. The name can be up to 8 characters long.
5. Click your mouse on the **Add style** button.
6. Your style's name is added in the list box "Styles" and is now available as an alternative to the <NORMAL> style.
7. Highlight the new style by clicking it once. Select drive(s) from the "Select drives" list box by highlighting the drive letter(s).
8. Click the **Configure** button.
9. Enter your choices in the tabbed dialog "Scanning options". When you click on **OK**, a pop up dialog box will inform you that the style has changed.
10. Click on **Update**.
11. If you wish to make this new style current now (i.e., to activate the settings of the style in this session of NVC95), then click on the **Make current** button.

When you make a style current, the scanner will be configured with the options that are associated with that style until you choose different options for that style or until you make another style current.

Delete a Style

1. Choose the style you wish to delete from the "Edit styles" dialog by clicking it once.
2. Click on the **Delete style** button. Before the style is deleted, you will be asked to confirm the deletion of the specific style.
3. To complete the operation, click on the **Update** button.

You cannot delete a style if it is current. You must first make another style current, select the desired style name from the list box, and then click on **Delete style**.

If a style is specified for a scheduled scan, you'll receive an error message if you try to delete it.

Modify the <NORMAL> Style

You cannot change the <NORMAL> style from the "Edit styles" dialog box. To change this style:

1. Make sure that <NORMAL> is the current style.
2. Make sure that Options|Save on exit is on. This is the default setting.
3. Configure your scanning options from the Options|Scanning options tabbed dialog boxes.
4. Click on **OK** when you've made your choices.
5. You have now changed the <NORMAL> style permanently.

Remember that all new styles are based on the original, factory default <NORMAL> style.

Note: When no other style is specified, the <NORMAL> style will be used. You may specify styles for both on-demand scans and scheduled scans. See [Scheduling overview](#) for more information on scheduled scanning.

More:

[Save as Style](#)

NORMAN Save as Style

There will always be a current style. Unless you have specified otherwise, <NORMAL> is current. The name of the current style is displayed in the Style name box.

When you are working with the scanning options, you are therefore editing the current style. If you want to keep the current style as it is **and** save the present changes as a separate style, you should enter a new name in the "Style name" combo box and click on **OK**.

Check the [] **Make saved style current** option if you want to apply the new style right away.

Save on Exit

The menu option Options|Save on exit is on by default. If you change the settings for the current style, they are permanently saved when you exit the scanner.

If Options|Save on exit is OFF, changes to a style are only valid for the present scanning session.

Unless you specify otherwise, the <NORMAL> style is the default style. Any configuration changes that you make while the <NORMAL> style is current will become part of the <NORMAL> style, regardless of whether or not you make the configuration changes from the "Edit styles" dialog box.

When a style other than the <NORMAL> style is current, the name of the style will appear in the title bar of the main window, in the title bar of the "Scanning for viruses" dialog box, and right under the title bar in the "Edit styles" dialog box.

NORMAN Scheduling overview

Not only does NVC95 perform on-demand scans, it can also scan at scheduled times. You can set the following:

- the time a virus scan will begin
- how often the process is to be run
- what type of style to use

You can schedule up to 20 scans, ranging from once, hourly, daily, weekly or monthly.

More:

[Schedule a Scan](#)

[Scheduling Several Unattended Scans](#)

NORMAN Schedule a Scan

To schedule a scan, first set the frequency of the scheduled scan from the “Add scheduling task” section of the display. Click the [] **When** combo box and choose from:

- **Once**
- **Hourly**
- **Daily**
- **Weekly**
- **Monthly**

When you select **Once**, **Hourly**, or **Daily**, today’s date is automatically selected.

If you select **Weekly**, then you may choose the day of the week on which the scan should occur.

If you click on **Monthly**, the combo box changes to list the numbers 1 through 31. If you choose "5", for instance, then the scheduled scan will occur on the 5th of each month at the time you have specified. If you choose "31", and there are only 30 days in a particular month, then the Scheduler will begin the scan on the 1st of the following month.

Then:

1. Click on the [] **Hour** combo and select the hour you wish. Hours are listed in 24 hour format.
2. Click on the [] **Minutes** combo and select the minutes you wish. Minutes are given in 15 minute increments.
3. Click on the [] **Styles** combo and select the style you wish to use for this particular scheduled scan.
4. Click on the **Add** button, and the scheduled scan appears in “Scheduled tasks” list box.
*Once you have set 20 daily scans, the **Add** button becomes inaccessible.*
5. When you add a scheduled scan, it pops up in the “Scheduled tasks” list box and activates the scheduler.
6. You cannot change a scan after it’s been scheduled. You must highlight the scheduled task by clicking it once, then click the **Remove** button and enter a new scan.
7. The first scheduled scan to be run appears at the top of the list in the “Scheduled tasks” list box, as well as at the top of the display in the list box “Next scan at:”.
8. The “Scheduled tasks” list box provides information on future scans. The watch to the left of the scheduled scan tells you that a scan is scheduled:



9. Click on the OK button when you have entered all your scheduled scans.

Make sure that the scheduler is active. The scheduled scan is on by default. You can turn the scheduler on and off from the Options menu or from the scheduler status button on the toolbar.

Note: In order for a scheduled scan to occur, scheduled scanning **must** be ON, and the scanner must be

active.

When scheduled scan is **on**, the toolbar button is depressed and looks like this:



When scheduled scan is **off**, the toolbar button looks like this:



If no scans are scheduled, the toolbar button is grayed out:



If a scan failed to run at the scheduled time, you'll be notified the next time you access the scheduler.

NORMAN Scheduling Several Unattended Scans

Like on-demand scans, scheduled scans require user action when the scan is complete. A scan will either inform you that no infected areas were found, or that a possible infection is detected. In either case, you need to take some action to remove the messages.

However, if a message that has not been closed is blocking an upcoming scheduled scan, NVC will remove the message 30 seconds before the scheduled scan is due to run.

There are nevertheless a couple of options you must be aware of when you're scheduling more than one scan to run unattended at night, for example:

1. In the styles being used, do **not** check the **Exit upon completion** option in the tabbed dialog "Scanning options". If you do, the scanner will close and consequently not run the remaining scheduled tasks.
2. In the styles being used, you **must** check the **Ignore locked files** option in the tabbed dialog "Scanning options". If you don't, the scan may be blocked by messages about locked files that could not be opened.
3. Make sure that you specify different names for the reports for the various styles. Alternatively, uncheck the **Overwrite previous** option in the Options|Scanning options tabbed dialog Reporting for each style being used. If you use default setting, you'll only get the report from the last scan.

NORMAN Finding Out More About Viruses

Computer viruses can be categorized in two distinctly different classes: binary and macro viruses.

Binary viruses contain executable code, i.e. program instructions. Binary viruses can infect program files (frequently referred to as executables), boot sectors, or other executable code on your PC.

Macro viruses do not contain executable code. They employ the macro programming language used in most word processors and spreadsheets. Macro viruses will infect Word or Excel files, for example, and replicate when infected files are accessed. Macro viruses do not depend on specific microprocessors or operating systems.

The virus library contains two tabbed dialogs, one for binary viruses and one for macro viruses. Here you will find key information for every virus in this list.

Because of its comprehensive nature, it may be time-consuming to use the arrow keys to navigate through the list.

Therefore, you can:

- Click or drag the scrollbar to the right of the list box to browse quickly through the list. Then set the focus on the list box and highlight the desired virus name.
- Enter the first letter of the virus you are looking for. The first virus whose name starts with this letter will appear as the first item in the box. Continue pressing the same key until the desired virus appears highlighted.
- If you know the full name of the virus you are searching for, you can use the [Tab] key to set the focus on the text box to the right of the list box. Then type the name of the virus and press [Enter].
- Narrow your search by clicking the check boxes in the two columns under the combo box. The left hand column displays viruses by what they infect, while the right hand column allows you to sort viruses by how they perform.

If you check the **List all**, or checkboxes, the other options in that column are grayed out.

There are many viruses that are known by several names. Hence, a virus you are looking for under one name may be in this list under another name. Call us if you can't find the virus for which you are searching...

More:

[Binary Viruses](#)

[Macro Viruses](#)

NORMAN Binary Viruses

These are the possible attributes for binary viruses:

It has a destructive payload

While most viruses are relatively harmless, this virus will perform destructive acts such as delete critical files, format your hard drive, or destroy other data.

It is a fast propagator

The virus stays in memory (goes resident) and hooks the services used by other programs to open, read, write and/or close files. Whenever any program opens a file, this will start the virus code, infecting the opened file, or look for another file to infect.

Uses encryption

The virus code itself is encrypted to avoid detection. It can be detected anyway.

Uses stealth techniques

The virus tries to hide itself to avoid detection. It is normally detected anyway.

Overwrites original file

The virus code overwrites parts of the infected file. Files infected this way cannot be cleaned, but must be replaced from backups in order to get rid of the virus.

Boot Sector

Infects boot sectors on diskettes and/or hard-drives. Will in most cases infect the hard drive if left in the diskette drive when the PC is booted.

EXE, COM files

Infects mainly EXE or COM files or both.

COMMAND.COM

Infects COMMAND.COM.

OV? files

Infects overlay files. An overlay file is a part of a program split in separate, overlaid, files.

Other files

Infects other files.

Goes resident in Low, High, UMB, Video RAM

The virus stays in memory when first activated.

NORMAN Macro Viruses

These are the possible attributes for macro viruses:

Can be repaired

Documents or template files infected by macro viruses can in most cases be repaired. Technically, this involves removal of the viral macros, while legal, user defined macros are left intact.

However, some macro viruses "snatch" user defined macros while replicating, making each infection unique. The user defined macros will in most cases be changed to call the main macro in the virus. The WM/CAP family of macro viruses is an example of viruses with this capability. Files infected by this kind of virus are repaired by removing all macros.

It has a destructive payload

While most viruses are relatively harmless, this virus will perform destructive acts such as delete critical files, format your hard drive, or destroy other data.

Is polymorphic

The virus changes itself from infection to infection.

Is a Virus

This is a true virus, able to replicate itself. Opening this document will trigger the macros, probably infecting other document files.

Is a Trojan

This is not a virus, meaning that it doesn't replicate. Contains other forms of malicious code.

Drops binary virus

This macro virus contains a binary virus. See [Binary viruses](#).

Is a joke, non-infectious

This document file contains macro code that performs harmless, sometimes visible, actions. Opening this document will trigger the macros, but no other document files will be infected.

Contains garbage

Is inactive or damaged

This document file contains remnants of macro viruses, or other macros that don't work as intended.

Infects Word2 documents

This document file contains a macro virus that requires Microsoft Word version 2 to replicate.

Infects OLE2 documents

Virus needs Word6/7 (Office '95)

Virus needs Excel6 (Office '95)

Virus needs Word8 (Office '97)

Virus needs Excel6 (Office '97)

This document file contains a macro virus that needs one of the specified Microsoft applications to replicate.

NORMAN Display Files and System Area

The **Display** feature displays data from files and system areas as hexadecimal values and printable characters.

You can access this function from the File menu.

If you want to take a look at the contents of a file (presented as hexadecimal values and printable characters), or if you wish to look at the contents of the system areas on your boot drive, you may choose the "Display" menu option.

More:

[Display File](#)

[Display System Areas](#)

NORMAN Display File

If you choose **Display file**, you will be prompted to choose a file from within a file window.

When you have chosen to display a file, this dialog box appears.

The dialog box shows you the file contents as hexadecimal values (left) and text (right). To maneuver up and down within the file, use the scrollbar along the right edge of the dialog box.

This function is especially useful when technical personnel want to look inside a file or sector for signs of a virus infection.

The buttons at the bottom of the dialog box:

Close quits from the function and returns you to the main window. **Print** permits you to send the displayed file to the printer that is set up through Windows.

NORMAN Display System Areas

You chose the **Display system area** menu choice, which displayed this his screen.

The System area includes the Master Boot Sector (MBS) and System Boot Sector (SBS).

You have a choice of viewing the MBS area of the first physical hard drive as well as the SBS on drive C:.
In addition, you can view the SBS on all diskette drives.



General information on installation/updates

Any virus scanner is only as effective as its most recent update, so obtaining frequent virus signature updates is critical to maintaining a secure computing environment

There are two different kinds of updates for NVC:

Version update: actual program changes for one or more of the modules in the package. To install a version update, run a regular install as described in the setup procedure.

Definition file update: change to the files `nvcbin.def` and `nvcmacro.def`. These files hold the virus signatures (fingerprints of known viruses) and are used by the scanning engine.

Normally, a version update will be shipped with a setup program that handles the installation. However, in some situations we'll make certain modules available for downloading from our Web site.

Definition file updates are available from our Web site on a regular basis. We recommend that you pay us a visit at:

<http://www.norman.no/update.htm>

