Index to The Norton AntiVirus Help

Select one the following topics to obtain information on using The Norton AntiVirus:

Summaries

Repair Actions

Keyboard

Commands

Procedures

About The Norton AntiVirus

Credits

Product Management	Joe Fusco.
Project Management	Karen Black and Catherine Ruggles.
Development Team	David Chambers,Peter Dickinson, Craig Dickson, Kevin Flick, Larry Goldsmith, Mohan Gopalakrishnan, Brad Kingsbury, Mark Lawler, Mani M. Manivannan, Bruce McCorkendale, Keith Mund and Enrique Salem.
	With assistance from Tony McNamara and John Wilber.
Virus Definitions	Blair Brandenburg, Craig Dickson,Richard Pouncy and John Wilber.
Quality Assurance Team	Tom Burgess, George Chlentzos, Ian Colquhoun, Michel Roter and Mitchell Sanders.
Documentation Team	Tom Bergantino, Dan Borror, Craig Dickson, Denise Link, Joel Mallette, Donna Mosich, Allen Reed and Denise Weatherwax.
	Layout by Modern Design, Los Angeles.
Technical Support Team	Cory Haibloom, Bob Kirkland and Ray Waldin.
Engineering Support Team	Kim Johnston, Brian Foster and Bob Kirwin.
Additional Acknowledgements	Special thanks to our external testers and to our Norton AntiVirus customers who suggested product enhancements.

The Norton AntiVirus Keys

Use the following keys in The Norton AntiVirus.

Key(s)	**Function**
Alt or **F10**	Selects the first menu on the menu bar.
Alt+letter	Chooses the menu whose underlined letter matches the one you type.
	Or moves to the option or group in a dialog box whose underlined letter matches the one you type.
Letter Key	Chooses the menu item whose underlined letter matches the one you type.
Tab	Moves from option to option (left to right, top to bottom) in a dialog box.
Shift+Tab	Moves from option to option in reverse order.
	Moves up one item or line in a list or text box.
	Or moves among menu items in a selected menu.
↓	Moves down one item or line in a list or text box.
	Or moves among menu items in a selected menu.
→	Moves right one character in a text box.
	Or moves among menus.
←	Moves left one character in a text box.
	Or moves among menus.
Ctrl+→	Moves right one word in a text box.
Ctrl+←	Moves left one word in a text box.
Home	Moves to the first item or character in a list or text box.
End	Moves to the last item or character in a list or text box.
Ctrl+**Home**	Moves to the beginning character in a list box.
Ctrl+**End**	Moves to the last character in a list box..
Shift+→	Extends the selection one character to the right in a text box.
Shift+←	Extends the selection one character to the left in a text box.
Shift+Home	Extends the selection to the first character in a text box.
Shift+End	Extends the selection to the last character in a text box..
Enter	Executes a command button.
	Or chooses the selected item in a list box and executes the command.
	Or chooses the selected menu item.
Esc or **Alt**+**F4**	Closes a dialog box without completing the command (same as the Cancel button).
	Or cancels the selected menu.
Backspace	Deletes the character to the left of the insertion point.
	Or deletes selected text.
Del	Deletes the character to the right of the insertion point
	Or deletes selected text.
Shift+**Del**	Cuts the selected text to the Clipboard.
Shift+**Ins**	Pastes the contents of the Clipboard at the insertion point.
Ctrl+**Ins**	Copies the selected text to the Clipboard.
Alt+**Bksp**	Undoes the previous operation.
PgUp	Scrolls up in a list box, one window at a time.
PgDn	Scrolls down in a list box, one window at a time.
Alt+↓	Opens a drop down list box.
Alt+or↓	Selects an item in a drop down list box.
Spacebar	Selects or cancels a selection in a list box.
	Check or unchecks a check box.
F1	Displays a Help topic on the selected command, dialog box option, or system message. If a topic does not exist, displays the Help Index.

The Norton AntiVirus Menu Commands

Scan

Definitions

Tools

Options

Help

Scan Menu

Use the Scan Menu to start a scan of your files. You can start a scan at one of three levels:

Scan an entire drive (or drives).
Scan a directory
Scan a file

Scan Drive

Use this command to start a scan on the drive(s) you select. All files in all directories on the selected drive are scanned. The drives available for scanning are shown in the list box. Select the drive(s) by highlighting the drive letter(s) in the list box or use the Drive Type check boxes to select

All Floppy and removable disk drives.
All Local drives (including all RAM disks and SUBST drive names).
All Network drives.

Note: the All Network Drives check box is enabled only if network drives exist and Allow Scanning of Network Drives is selected in the Options menu.

GO TO:
Scan Menu
Scan Results

Scan Directory

Use this command to start a scan on the directory you select. Use the Drives drop down list box to select the appropriate drive, then select the desired directory from the directory tree and click the Change button. You can scan the files in the selected directory only or scan all the files in all subdirectories below the selected directory by checking the Include Subdirectories check box.

GO TO:
Scan Menu
Scan Results

Scan File

Use this command to start a scan on the file you select. Use the Drive and Tree list boxes to select the desired drive and directory. The Files list box displays the files in the selected directory. You can use wildcard specifiers in the Filename text box to selectively display filenames in the Files list box. Select a file by highlighting the filename in the Files list box or by typing the file's name in the Filename text box.

GO TO:
Scan Menu
Scan Results

Scan Results

Shows a scan's progress while the scan is in operation. The progress bar displays the percent completed during a scan. Any messages generated during a scan are displayed in the list box.

When a scan finishes (or you abort the scan by using the Cancel button), information about any infected file is displayed in the list box. This information includes the infected file's name, its full pathname, and the virus type. A scan summary is displayed for every scan. The summary lists the total files scanned and the total files infected.

Once a scan is completed, you have several options depending upon whether or not there are any infected files. If there are no infected files, you can select one of the following command buttons:

Scan Rescans the selected drives, directory or file that were scanned originally.
Print Prints the contents of the current Scan Results list box or saves them to a file..

If there are infected files, you have two additional options:

Repair Repairs the selected file (if the file is repairable). A Repair All option is available in the Repair Files dialog box.
Delete Deletes the selected file. A Delete All option is available in the Delete Files dialog box.

If you have Detect Unknown Viruses enabled, and a change is detected in an inoculated file, you have another option:

Reinoc Reinoculates the selected file. A Reinoc All option is available in the Reinoc dialog box.

Note: The Repair, Delete, and Reinoc options must be enabled in the Options menu.

GO TO:
Scan Menu

Print Scan Results

Use this command to print the Scan Results You may print either to the selected printer or to a file. If you print to a file, the Browse command button is enabled allowing you to select an existing file. To create a new file, type the desired filename in the text box.

GO TO:
Scan Menu
Scan Results

Definitions Menu

Use this menu to manage the virus definitions used by The Norton AntiVirus. The following commands are available in this menu:

Modify List
Load from File

Modify List

Use this command to

view the list of existing virus definitions
manually add a new definition
delete a definition
print a hard copy of the definition list.

The list of installed virus definitions is displayed in the list box. The definitions are arranged in alphabetical order.

To delete a definition from the list, highlight the name of the desired definition in the list and select the Delete command button. Although the definition name disappears from the list when you execute the command, the deletion does not take effect until after you reboot your computer.

Go To:
Definitions Menu

Add a Virus Definition

Use this command to manually add a new virus definition to the list of installed definitions.

New virus definitions are available by calling the Virus Newsline service of Symantec/Peter Norton Group. See "Appendix A, Updating Virus Definitions" in *The Norton AntiVirus User Manual*.

Important: The new virus definition must be typed exactly as given on the Virus Newsline.

Enter the appropriate information into the four fields:

the definitions name (up to 25 characters)
the definition's length in bytes (up to three characters)
the definition's checksum (up to four characters)
the actual definition (in hexadecimal)

The definition is entered as sets of two characters separated by a space. For example:

0K 0G 0L 0H 0G 8Q 0K 0J BK EZ 0R 2G ...

When a line is filled, click on the next line (or use the Tab key) to move the insertion point, then continue typing the definition.

Virus Clinic checks for valid characters and format. If an error is found during entry, Virus Clinic beeps and does not let you continue until you enter a valid character or number. The OK command button is disabled until all errors detected by Virus Clinic are corrected.

The new definition does not take effect until you reboot your computer.

Go To:
Modify List
Definitions Menu

Print the Virus Definition List

Use this command to print the Virus Definition list. You may print either to the selected printer or to a file. If you print to a file, the Browse command button is enabled allowing you to select an existing file. To create a new file, type the desired filename in the text box.

Go To:
Modify List
Definitions Menu

Load from File

Use this command to add the most current virus definitions file into The Norton AntiVirus. This file is prepared by Symantec/Peter Norton Group and is updated whenever a virus is discovered. The updated file is available for downloading on the Virus Newsline. See "Appendix A, Updating Virus Definitions" in *The Norton AntiVirus User Manual*.

Select the appropriate drive, directory and file from the list boxes. Nav.def is the default filename for the definitions file.

Go To:
Definitions Menu

Tools Menu

This menu provides utility functions that support the operation of The Norton AntiVirus. The following commands are available in this menu:

Uninoculate

Uninoculate

Use this command to remove the inoculation file on a selected disk drive or drives.

The inoculation file stores the inoculation data for all the inoculated files on a drive. You can delete the inoculation file from a specific drive by highlighting the drive letter in the list box, or you can delete the inoculation files from all types of drives by checking the appropriate drive type check box.

GO TO:
Tools Menu

Options Menu

Use this menu to configure optional settings for both Virus Intercept and Virus Clinic. The following commands are available in this menu:

Clinic
Intercept
Global
Set/Change Password

Clinic

Use this command to set configuration options for Virus Clinic.

Options in the **Commands** group box select whether or not the following functions are active in the Scan Results Dialog box:

Repair
Delete
Cancel
Reinoc
Repair All
Delete All
Reinoc All

Check the appropriate check box to activate the command. If a command is not allowed (the check box is not checked), the corresponding command button is dimmed in the Scan Results dialog box.

Allow Scanning of Network Drives selects whether or not to allow scanning of networked drives. If network drive scanning is not allowed, the All Network Drives check box is dimmed in the Scan Drives dialog box and no network drive letters are displayed in the Drives list box.

Intercept

Use this command to set configuration options for Virus Intercept.

Options in the **Alert Options** group box select the activities that take place when a Virus Intercept occurs.

Beep Sounds the system bell when an intercept occurs.

Popup Alert Box Displays an alert box on the screen when an intercept occurs.

Seconds to display If Alert Box is enabled, specifies how long (in seconds) the alert box is displayed on the screen.

Log File Keeps a record of all Virus Intercept activity. This record is stored as an ASCII text file. To use an existing file, use the File Browser to locate and select the file. To create a new file, enter the desired filename in the text box.. The Norton AntiVirus creates the file the first time there is activity to log. The default file specification is C:\temp\nav.log

Options in the **Commands** group box select whether or not the following command buttons are active in the Virus Intercept Alert box:

Proceed Allows you to proceed after a virus intercept has occurred. Otherwise, you must stop the current file access.

Reinoculate If a file's inoculation data has changed, this option allows The Norton AntiVirus to recalculate new inoculation data for that file.

Global

Use this command to set configuration options for The Norton AntiVirus.

Detect Unknown Viruses adds the ability to check for potential viruses based upon a change to an inoculated file.

Auto-inoculate automatically calculates the inoculation data the first time an uninoculated file is accessed.

Note: Files must be inoculated before they can be scanned for unknown viruses. Scanning a drive with auto-inoculate enabled automatically inoculates all files on that drive.

Scan Executables Only limits Virus Intercept to checking and Virus Clinic to scanning only files with a extension that identifies the file as executable. The current list of valid extensions is .COM, .EXE, .VOR, .OVL, .DRV, .BIN, .SYS.

The **Network Inoculation Directory** is the directory where to store the inoculation file on a network drive. The inoculation file for local drives is stored in the root directory of each drive.

Virus Alert Custom Message is the message displayed in the alert box (or on the command line) when Virus Intercept detects an infected file.

Set/Change Password

Use this command to set a password initially and then to change an existing password.

If no password has been entered, the command reads **Set Password**. Type the desired password in the New Password text box and click OK. Type the new password a second time in the Confirm New Password text box and click OK. The new password is set. If you mistype the confirming password, an alert box pops up saying incorrect password. You must type the correct confirming password to set a new password.

If a password exists, the command reads **Change Password**. Type the existing password in the Old Password text box and click OK. If this is the currently valid password, the New Password text box is active and you can proceed to type your new password as described above.

Go To:
Options Menu

Help Menu

Use this menu to access The Norton AntiVirus help system. The following commands are available in this menu:

Index	The Norton AntiVirus help index.
Keyboard	Quick reference to keystrokes for this program.
Commands	Menu Commands. You can also get help on a particular menu item by selecting it and then pressing **F1**.
Procedures	Common procedures used in The Norton AntiVirus.
Using Help	How to use the Windows help system.
About	Product name, copyright, credits, and version of this program.

File Browser

Use the file browser to locate a file. Use the Drive and Tree list boxes to select the desired drive and directory. The Files list box displays the files in the selected directory. You can use wildcard specifiers in the File text box to selectively display filenames in the Files list box. Select a file by highlighting the filename in the Files list box.

Directory Browser

Use the directory browser to located directory. Use the Drive drop down list box to select a drive. Then select the desired directory from the directory tree and click the Change button.

Password Required

A password is required to perform the selected operation.

Type the password in the text box and select OK.
If you make a mistake, go ahead and select OK. An popup alert box is displayed. Exit from the alert box and type the correct password.

Welcome

Use this dialog box to personalize your copy of The Norton AntiVirus.

Type your name in the Name text box. Click on the Company text box (or use the Tab key) to move the cursor. Type your company name. Select OK (or use the Enter key) to complete the registration.

Note: You must type an entry in the Company Name text box to enable the OK button.

The Norton AntiVirus Procedures

Adding a Virus Definition Manually

Allows you to add a virus definition to the list by typing each part of the definition.

1. Choose Modify List... from the Definitions menu.
2. Select the Add command button.
   The Add Virus Definition dialog box is displayed.
3. Type in the definition's parameters in the appropriate text box:
   Name
   Length
   Checksum
   Definition.
   Note: Ensure that the definition is typed exactly as given by the Symantec Virus Newsline.
4. Select OK.

See also:
Add a Virus Definition

Assigning the Virus Intercept Log Filename

Assigns the name of the file used to log Virus Intercept alert messages.

1. Choose Intercept... from the Options menu.
2. Check the Enable Log to File check box.
3. Select the filename by:
   selecting the Browse command button and highlighting an existing filename,
   or
   typing the filename in the Filename text box. Use this option to type a new filename.
   The default filename is C:\temp\nav.log.
4. Select OK.

See also:
Intercept

Auto-inoculating Executable Files

Enables the calculating of inoculation data whenever an executable program is accessed for the first time.

1. Choose Global... from the Options menu.
2. Check the Auto-inoculate check box.
   Note: Detect Unknown Viruses must be selected for the Auto-inoculate check box to be enabled.
3. Select OK.

See also:
Global

Changing an Existing Password

Changes an existing password to a new password.

1. Choose Change Password... from the Options menu.
2. Type in the current password in the Old Password text box.
3. Select OK.
4. Type in the desired new password in the New Password text box.
5. Select OK.
6. Type in the new password again in the Confirm New Password text box.
7. Select OK.

See also:
Set/Change Password

Configuring the Virus Intercept Alert

Configures the action of The Norton AntiVirus when an intercept alert occurs.

1. Choose Intercept... from the Options menu.
2. In the Options group box, select the action to be taken when an alert occurs by checking the appropriate check box. There are two options:

   Beep - sounds the system's bell when an intercept occurs.
   Popup Alert Box - displays an alert box when an intercept occurs.

   If Popup Alert Box is selected, there is an additional option:

   Type the number of seconds the alert box stays on the screen in the Seconds to Display Alert Box text box.

3. Select OK.

See also:
Intercept

Deleting a Virus Definition

Deletes a virus definition from the stored list of virus definitions.

1. Choose Modify List... from the Definitions menu.
2. Highlight the virus definition to delete in the Virus list box.
3. Select the Delete command button.
   An alert box is displayed prompting you to confirm the delete request.
4. Select OK.

See also:
Modify List

Deleting All Infected Files

Deletes all infected files detected during a scan.

Note: This procedure assumes that the scan is finished and infected files were detected.

1. Select the Delete command button.
   The Delete Files dialog box is displayed.
2. Select the Delete All command button.
   An alert box is displayed prompting you to confirm the delete request for each file to be deleted.
3. Select OK to delete each file.

See also:
Scan Results

Deleting an Infected File

Deletes a file from the list of infected files detected during a scan.

Note: This procedure assumes that the scan is finished and infected files were detected.

1. Select the file to be deleted from the list of infected files in the Scan Results dialog box.
2. Select the Delete command button.
   The Delete Files dialog box is displayed.
3. Select the Delete command button.
   An alert box is displayed prompting you to confirm the delete request.
4. Select OK.

See also:

Scan Results

Enabling Command Buttons in Scan Results Dialog Box

Configures which command buttons are active in the Scan Results dialog box.

1. Choose Clinic... from the Options menu.
2. In the Commands group box, check the appropriate check boxes to enable the command in the Scan Results dialog box:
    - Allow Repair
    - Allow Delete
    - Allow Reinoc
    - Allow Cancel
    - Allow Repair All
    - Allow Delete All
    - Allow Reinoc All
3. Select OK.

See also:
Clinic

Enabling Command Buttons in Virus Intercept Alert Boxes

Configures which command buttons are active in the Virus Intercept Alert boxes.

1. Choose Intercept... from the Options menu.
2. In the Commands group box, check the appropriate check boxes of the command buttons to activate in the Virus Intercept Alert boxes:
   Allow Reinoculate
   Allow Proceed
3. Select OK.

See also:
Intercept

Enabling Network Drive Scanning

Enables the display of network drive letters and the All Network Drives check box in the Scan Drives dialog box.

1. Choose Clinic... from the Options menu
2. Check the Allow Scanning of Network Drives check box.
3. Select OK.

See also:

Clinic

Increasing Virus Clinic's Protection Level

Increase the Protection Level to check also for unknown viruses.

1. Choose Global... from the Options Menu.
2. Check the Detect Unknown Viruses check box.
   Note: Files must be inoculated before they can be checked for unknown viruses. See Auto-Inoculating Executable Files
3. Select OK.

See also:
Global

Loading Virus Definitions from a File

Adds the virus definitions in the selected file to the existing virus definitions list.

1. Choose Load from File... from the Definitions menu.
2. Enter the filename to load either by:
   selecting the appropriate drive, directory and file from the list boxes,
   or
   typing the filename in the File text box.
3. Select OK.

See also:
    Load from File

Printing the List of Virus Definitions

Prints the names of the virus definitions in the list.

1. Choose Modify List... from the Definitions menu.
2. Select the Print command button.
   The Printing Virus List dialog box is displayed.
3. Select the Send to Printer option button.
4. Select OK.
   A print file is created and sent to the printer.

See also:
  Modify List

Printing Scan Results

Prints the results of the current scan.

Note: This procedure assumes that the scan is finished and the Scan Results dialog box is displayed.

1. Select the Print command button.
   The Scan Summary dialog box is displayed.
2. Select the Send to Printer option button.
3. Select OK.
   A print file is created and sent to the printer.

See also:
Scan Results

Repairing All Infected Files

Repairs all infected files detected during a scan.

Note: This procedure assumes that the scan is finished and infected files were detected.

1. Select the Repair command button.
   The Repair Files dialog box is displayed.
2. Select the Repair All command button.
   Each repaired file is noted in the Scan Results listing by "This item has been repaired" replacing the virus type label.

Important: Not all infected files can be repaired. If a file cannot be repaired, it must be deleted.

See also:
Scan Results

Repairing an Infected File

Repairs the selected infected file detected during a scan.

Note: This procedure assumes that the scan is finished and infected files were detected.

1. Highlight the file to be repaired from the list of infected files in the Scan Results dialog box.
2. Select the Repair command button.
   The Repair Files dialog box is displayed.

3.. Select the Repair command button.
When the file is repaired, the virus type label is replaced with "This item has been repaired"

Important: Not all infected files can be repaired. If a file cannot be repaired, it must be deleted.

See also:
Scan Results

Rescanning Files

Executes another scan using the same specifications as the just completed scan.

Note: This procedure assumes that the scan is finished and the Scan Results dialog box is displayed.

1. Select the Scan command button.
   A scan is executed and the new scan results are displayed.
2. Select OK.

See also:
Scan Results

Saving Scan Results to a File

Prints the results of the current scan to a user-specified file.

Note: This procedure assumes that the scan is finished and the Scan Results dialog box is displayed.

1. Select the Print command button.
   The Scan Summary dialog box is displayed.
2. Select the Send to File option button.
3. Select the filename to print to by:
   selecting the Browse command button and highlighting an existing filename,
   or
   typing the filename in the Filename text box. Use this option to type a new filename.
4. Select OK.

See also:
Print Scan Results

Scanning a Directory

Scans all files in a directory (and its subdirectories, if selected) for viruses.

1. Choose Directory... from the Scan menu.
2. Select the desired disk drive from the Drives drop down list box.
3. Select the desired directory from the directory tree and then the Change button.
4. Check the Include Subdirectories check box to scan all files in all subdirectories under the selected directory.
5. Select OK.

See also:
Scan Directory

Scanning a File

Scans an individual file for viruses.

1. Choose File... from the Scan menu.
2. Select the desired disk drive and directory from the list boxes.
3. Select the file to scan from the Files list box (or directly type the filename in the Filename text box).
   Note: You can use wildcard patterns in the Filename text box to selectively display certain file types in the Files list box.
4. Select OK.

See also:
   Scan File

Scanning All Drives

Scans all files in all directories of all drives on the system.

1. Choose Drive... from the Scan menu.
2. Check all three Drive Types check boxes:
   All Floppy Drives
   All Local Drives
   All Network Drives (if enabled, see Enabling Network Drive Scanning)
3. Select OK.

See also:
  Scan Drive

Scanning Floppy Drives

Scans all files in all directories on the selected floppy drive(s).

1. Choose Drive... from the Scan menu.
2. Select the letter of the floppy drive(s) to scan from the Drives list box.
   or
   Check the All Floppy Drives check box. All floppy and removable drives are highlighted.
3. Select OK.

See also:
Scan Drive

Scanning Hard Drives

Scans all files in all directories on the selected hard drive(s).

1. Choose Drive... from the Scan menu.
2. Select the letter of the hard drive(s) to scan from the Drives list box.
   or
   Check the All Local Drives check box. All hard drives, RAM drives, and SUBST drive names are highlighted.
3. Select OK.

See also:
  Scan Drives

Scanning Network Drives

Scans all files in all directories on the selected network drive(s).

1. Choose Drive... from the Scan menu.
2. Select the letter of the network drive(s) to scan from the Drives list box.
   or
   Check the All Network Drives check box. All network drives are highlighted.
   Note: Scanning of network drives must be enabled, otherwise network drive letters and the All Network Drives check box are dimmed. See Enabling Network Drive Scanning
3. Select OK.

See also:
Scan Drive

Setting the Password for the First Time

Creates the initial password.

1. Choose Set Password... from the Options menu.
   Note: If a password has already been set, this command reads Change Password.
2. Type the desired password in the New Password text box.
3. Select OK.
4. Type the new password again in the Confirm New Password text box.
5. Select OK.

See also:
    Set/Change Password

Uninoculating a Drive

Removes the inoculation file on the specified drive(s).

1. Choose Uninoculate... from the Tools Menu.
2. Select the drive(s) to uninoculate.
3. Select OK.

See also:
Uninoculate

Viewing the List of Virus Definitions

View the list of currently defined virus definitions.

1. Choose Modify List... from the Definitions menu.
   The list of current virus definitions is displayed in the Virus list box.
2. Use the scroll bar to scroll through the list.
3. Select OK.

See also:
Modify List

Virus Clinic Summary

Virus Clinic is the part of The Norton AntiVirus that scans files for viruses. If a virus is found, Virus Clinic then gives you the option of repairing the file (if the file is repairable) or deleting the file. You may scan complete disks, specific directories, or individual files.

A virus is known to The Norton AntiVirus by having an entry in the virus definition file that is maintained by Virus Clinic. Virus definitions are provided by Symantec. See Appendix A, "Updating Virus Definitions" of *The Norton AntiVirus User Manual* for more information.

To check for unknown viruses, The Norton AntiVirus first must inoculate a file. Then, whenever that file is accessed, the file is checked against the stored inoculation data, and if the file has changed, you are alerted to the fact that the file has changed and that there is a possibility of an unknown virus.

Virus Clinic also provides commands to configure both Virus Clinic and Virus Intercept and to manage the list of virus definitions in Virus Clinic

Virus Intercept Summary

Virus Intercept is the component of The Norton AntiVirus that constantly monitors your system for viruses. Virus Intercept is loaded into memory when you boot your computer. Whenever you copy a file, copy a disk, or start an application, Virus Intercept first checks the file(s) for any virus defined in the virus definition list.

If an infected file is found, an alert is sounded and the action is stopped. At this point, you would start up Virus Clinic and scan for the infected file. Once clinic has identified the infected file, you can then repair (or delete) the file. See Repairing versus Deleting Infected Files for more information.

Another feature of Virus Intercept is the ability to "inoculate" application files. With this feature enabled, the first time you run an application program, Virus Intercept calculates inoculation data for that application and stores it in the inoculation file. Whenever you run that application again, Virus Intercept checks the inoculation data to verify that the application's code has not changed. If the code has changed, there is a possibility of an unknown virus. In this case, Virus Intercept alerts you to the change and gives you the option to reinoculate the file. Use this option only if the code changes are valid.

application

software designed to do certain tasks, such as word processing, accounting, or telecommunications.

back up

Copying and storing all or some files on another disk for archival purposes.

boot

To start or restart the computer. A "cold boot" means to turn off the computer's power and then turn it back on, instead of pressing Ctrl-Alt-Del, known as a "warm boot.."

boot disk

Any disk that contains the DOS files your computer needs to start up. The boot disk may also be called the system disk.

boot sector

The first sector on every logical DOS drive is designated as the boot sector when the drive is formatted. The boot sector contains parameter DOS uses to manage data storage on the drive and the boot strap program.

boot sector virus

A virus the substitutes itself for the boot-sector information (See boot sector)

checksum

The "signature" created and stored for each application. The checksum is verified each time the application launches. The checksum is stored in a separate file. If the checksum has changed, this may mean that a virus infected the file.

choose

To select an option on a menu. Position the pointer on the name of the menu title, then click. The menu opens. Drag the selection cursor to the menu item you want, then click. Or, type the underlined letter in the item name.

device driver

An application that DOS uses to communicate with hardware devices.

dialog box

A box on the screen that provides information or requests information..

download

Copying a file from an on-line service to your computer. This is normally accomplished using a modem to transmit the file over a telephone line.

infection

A virus is triggered when the host program it resides in is executed. When the virus is triggered, it tries to target another program by copying itself into the target program and infecting the target program.

inoculate

Creating a checksum for an application. See checksum .

interception

Detecting virus activity in real time to prevent viruses from attempting to infect other application programs.

known virus

A virus that The Norton AntiVirus has a definition for.

partition

A segment of a disk treated as a separate drive with its own letter designation.

partition table

A table that records the partition assignments for a disk.

repair

Cleaning up a file by extracting the known virus from the infected file.

scan

The process of checking a file for infections.

virus

A program (executable code segment) designed to attach itself to other applications and code resources. The virus copies itself into an application and is activated when that application is launched. The virus replicates by copying itself into other programs and system resources.

virus definition

The information The Norton AntiVirus uses to detect and eliminate viruses and their strains from infected files.

Repair Actions for a Hard Disk Partition Table Virus

A virus of this type is repairable by The Norton AntiVirus only if the original partition table information was copied by the virus to a known location. For all other cases, the partition table must be repaired manually.
A partition table virus can be removed manually in one of three ways:

1. With a Rescue Disk
   Note: a Rescue Disk must have been created previously.
   a. Turn off the computer.
   b. Insert an uninfected, write protected DOS floppy disk in drive A and turn on the computer.
   Important: the DOS version on the floppy must be EXACTLY the same version as on the hard disk.
   c. Insert a write protected copy of the program disk for the **DOS version** of The Norton AntiVirus.
   Note: You won't be able to run Windows temporarily while you continue this procedure.
   d. Type RESCUE and press Enter.
   e. Choose RESTORE RESCUE DISKETTE from the list that appears.
   f. Insert your rescue disk in the appropriate floppy drive. Follow the prompts and instructions to restore the partition table from your rescue disk.

2. With Norton Utilities (4.5 Advanced or later),
CAUTION: This procedure requires a high degree of familiarity with the Norton Utilities. Call the Technical Support Department for help if there is any doubt about attempting this procedure. Incorrect operation may result in loss of data!
   a. Turn off the computer.
   b. Insert an uninfected, write protected DOS floppy disk in drive A and turn on the computer.
   Important: the DOS version on the floppy must be EXACTLY the same version as on the hard disk.
   c. Using the disk editor, check through track 0 to see if a valid partition table was copied to another location. If so, copy that sector back to Cylinder 0, Side 0, Sector 1. If no copy of the original partition table is found, fill the entire partition table sector with zeros, escape to DOS, and run "NDD C: /REBUILD" to recreate the Master Boot Program and partition table.

3. Without Norton Utilities,
   a. Turn off the computer.
   b. Insert an uninfected, write protected DOS floppy disk in drive A and turn on the computer.
   Important: the DOS version on the floppy must be EXACTLY the same version as on the hard disk.
   c. Backup all data and then destructively low-level format the disk.
   (**Note:** in some cases this may be done only by the manufacturer).
   d. Partition the drive using the DOS FDISK command.
   e. Format the drive using the DOS FORMAT command.
   f. Restore the backed up data.

Repair Actions for a Hard Disk Boot Sector Virus

To repair a hard disk boot sector virus:

1. With a Rescue Disk

Note: a Rescue Disk must have been created previously.

a. Turn off the computer.

b. Insert an uninfected, write protected DOS floppy disk in drive A and turn on the computer.
Important: the DOS version on the floppy must be EXACTLY the same version as on the hard disk.

c. Insert a write protected copy of the program disk for the **DOS version** of The Norton AntiVirus.
Note: You won't be able to run Windows temporarily while you continue this procedure.

d. Type RESCUE and press Enter.

e. Choose RESTORE RESCUE DISKETTE from the list that appears.

f. Insert your rescue disk in the appropriate floppy drive. Follow the prompts and instructions to restore the hard disk boot sector information from your rescue disk.

2. Without a Rescue Disk

a. Turn off the computer.

b. Insert an uninfected, write protected DOS floppy disk in drive A and turn on the computer.
Important: the DOS version on the floppy must be EXACTLY the same version as on the hard disk.

c. Use the DOS SYS command to rebuild the boot sector.
At the A:> prompt, type:

```
C:[path]SYS C:
```

where [path] is the directory path to where the DOS files are stored on the hard disk.

Repair Actions for a Floppy Disk Boot Sector Virus

To repair a floppy disk boot sector virus:

1. Ensure that your computer is uninfected.
2. Copy the files on the infected floppy disk to another disk or to the hard drive.
   Important: Do *not* use the DOS DISKCOPY command.
3. Reformat the floppy disk. Use the /s option if the disk is to be bootable.
4. Copy the files back onto the reformatted disk.

Removing a Virus from Memory

To remove a virus from memory:

1. Turn off the computer.
2. Insert an uninfected, write protected DOS floppy disk in drive A and turn on the computer.
   Important: the DOS version on the floppy must be *exactly* the same version as on the hard disk.
3. Insert a write protected copy of the program disk for the **DOS version** of The Norton AntiVirus.
   Note: You won't be able to run Windows temporarily while you continue this procedure.
4. Scan the hard disk using the DOS version of The Norton AntiVirus on the floppy drive to find any files that may have been infected by the virus. If any infected files are found, either repair or delete them. Once you're sure your system is clean, reboot the system in the usual way.

Repairing versus Deleting Infected Files

An infected file may be repaired only if a virus has not permanently overwritten any information in that file. If a file is repairable, in most cases it can be repaired without damage to the original contents of the file. If a repaired file does not operate properly, reload the file from a known good master file.
Note: any "repaired" file should be rescanned prior to use.

If a file cannot be repaired, it should be deleted and a new copy loaded from a known good master file.