From this main window you can do the following:

- Select the Scan Now button to scan selected drives immediately.
- Select a menu command to scan specific files or folders.
- Click a button to change options, schedule scans, or view information.

Click Scan Now to initiate a scan of the drive or drives that are checked in the Drives list box in this window.

Click one or more drives to include in the scan you are about to initiate. Or, click any highlighted drive to exclude it from the scan. These selections return to the preset options when you exit Norton AntiVirus Scanner.

Check one or more drive types you want to scan now. Or, uncheck to exclude these items from the scan. These selections return to the preset options when you exit Norton AntiVirus Scanner.

 The All Network Drives option is dimmed unless you have specifically set that option in the Options -- Scanner Advanced Settings dialog box.

Click Close to exit the Virus Information dialog box.

File Name: The name of the infected file and its path.
Status: Whether it is infected, repaired, or deleted.
Virus Name and Aliases: The most common names by which the virus is known.
Infects: What files or boot records the virus attacks.
Likelihood: Options are: Common or Rare.
Length: Length, in bytes, of the virus code.

Memory Resident: Stays in DOS memory after it activates.

Size Stealth: Tries to conceal itself from detection by disguising its size.

Full Stealth: Tries to conceal itself from detection by disguising its size and attributes.

Triggered Event: Performs some action based on certain criteria (for example a date on the computer's system clock).

Encrypting: Encrypts its code to make detection more difficult.

Polymorphic: Appears differently in each infected file.

Click Print to display the Print dialog box where you can print to a printer or to a file.

Click Close to exit the dialog box and complete the scan.

Click Print to display the Print dialog box where you can print to a printer or to a file.

Click Details to display the Details of Scan dialog box where you can see more information. This button is dimmed if no problems were found.

Click Close to close the Details of Scan dialog box and return to the Scan Results dialog box.

Click Info to display the Virus Found Information dialog box where you can find descriptive information about the virus.

Click Repair to display the Repair File dialog box where you can repair this file or boot record or all infected files or boot records.

Click Delete to display the Delete File dialog box where you can delete this file or all infected files.

Click Exclude to display the Exclude File dialog box where you can choose to keep this file from being checked for known viruses.

Click Done to exit the Problems Found dialog box. You see the Scan Results dialog box that summarizes this scan, including what was scanned, what was cleaned (repaired or deleted), and what was left unresolved. From the Scan Results dialog box, you can click Close to conclude this scan.

Click Info to display the Virus Information dialog box which shows more information about the virus. This button is dimmed if no infected files were found.

Click Print to display the Print dialog box where you can print to a printer or to a file.

Click Filter to display a dialog box where you can choose to display one or more specific types of Norton AntiVirus Scanner events.

Click Clear to display a dialog box where you can delete all entries in the Activity Log.

Click Close to exit the Activity Log.

Select Yes to erase everything in the Activity Log. Otherwise, the log expands indefinitely or until it reaches the maximum size.

 To change the maximum size of the Activity Log, click Options in the Norton AntiVirus Scanner main window. Then make your change on the Activity Log tab.

Click the Display combo box to display a list of virus types. Click one of the choices to filter the Virus List so that you can view either: all viruses, common viruses, program viruses, boot viruses, stealth viruses, polymorphic viruses, or multipartite viruses.

The Virus List includes the names of all the viruses for which Norton AntiVirus Scanner has a virus definition. NAV Scanner uses virus definitions to detect viruses. Since new viruses are being created all the time, you need to update the Virus List regularly. Click Help for more information on updating the Virus List.

To search for a virus by name, type the first letter to invoke the Smart Search text box where you can continue typing the virus name.

Click Info to display the Virus Information dialog box where you can view detailed information about the selected virus.

Click Print to display the Print dialog box where you can print to a printer or to a file.

Click Delete to display the Delete Virus Definition dialog box where you can delete the selected virus from the Virus List.

Comments describes what the virus does to your files.

Click Exclude to exclude the file from further scans.

Click Repair to have Norton AntiVirus Scanner remove the virus from the infected file or boot record.

Click Continue to continue without taking any action.

Click Delete to permanently remove this file from your disk. After you have deleted the file, you should replace it.

Files deleted by Norton AntiVirus Scanner cannot be recovered. If you do not have a clean copy of the file, you need to acquire one from the manufacturer.

Click Stop to stop the scan without taking any further action.

Click Include Subfolders to include all subfolders in the selected folder.

From this Repair File dialog box you can remove a virus from an infected file or boot record. Click Repair or Repair All to have Norton AntiVirus Scanner repair one or all of the files identified during the scan.

Click Repair to have Norton AntiVirus Scanner restore the file or boot record to an uninfected state.

Click Repair All to have Norton AntiVirus Scanner repair all the infected files found during the scan.

From this Delete File dialog box, click Delete or Delete All to have Norton AntiVirus Scanner delete one or all of the infected files found during the scan. After you have deleted a file, you need to replace it with an uninfected copy.

ℹ️ Files deleted by Norton AntiVirus Scanner cannot be recovered. If you do not have a clean copy of a deleted file, you need to acquire one from the manufacturer.

Click Delete to have Norton AntiVirus Scanner delete this file. Files deleted by Norton AntiVirus Scanner cannot be recovered. After you have deleted a file, you need to replace it with an uninfected copy.

Click Delete All to have Norton AntiVirus Scanner delete all the infected files found during the scan. After you have deleted the files, you need to replace them with clean copies.

Click any of the following to specify which events you want to be displayed in the Activity Log.

Displays events occurring on a specific date or occurring before, after, or between specified dates. Click an option in the Dated drop-down list box, then enter the date or dates to define the range.

Click an option in the Dated drop-down list box, then enter the date or dates to define the range.

Click an option in the Dated drop-down list box, then enter the date or dates to define the range.

From this Exclude File dialog box you can exclude this file from future checks for known viruses.

Click Exclude to exclude this item from future checks for known viruses.

🛈   The item is added to the list of excluded files displayed in the Exclusions List.

Repair: Removes a virus from a file or boot record.

Continue: Continues the scan without responding to the change in your file.

Stop: Stops the scan and returns you to the Norton AntiVirus Scanner main window.

The Comments describe what the virus does to your files.

Summary: Reports if infected files or infected boot records were found.
Items Scanned: Lists the drives, folders, or files that were scanned.
File Type: Lists the types of files that were scanned.
Other Settings: Reports on other settings, such as whether compressed files were included in the scan.
Scan Time: Reports the duration of the scan.

Scanned: Lists whether the master boot record, boot records, or files were scanned.
Infected: Lists what items, if any, were infected.
Cleaned: Lists whether infected items were cleaned; that is, whether the infected file was deleted or repaired.

The Details of Scan dialog box summarizes the current scan. The Status column indicates whether or not an infected file was repaired, deleted, or if it remains infected.

The Problems Found dialog box summarizes the current scan. The Status column indicates whether or not an infected file was repaired, deleted, or if it remains infected.

- If the file remains infected, you should try to repair it.
- If it cannot be repaired, you should delete the file and replace it with a clean copy.
- If you do not have a copy of the file, you should acquire one. Leaving the file on your system without repairing or deleting it may cause other files to become infected.

Records detections of known viruses.

Returns the file to its original, uninfected state.

Aborts the download. You will not be able to save the file to your local hard drive. You will need to download the file from a different site.

Continues the download and notifies you each time a new virus is found. You can select Info to find out about the virus.

⚠️   Use this option cautiously. If you save this file to your hard drive, you will be saving an infected file that you must repair before you can execute or distribute it.

Continues the download but also continues scanning the compressed file.

The safest option would be to Abort the download. However, this option will continue to notify you each time another virus is identified. Therefore, you know whether the compressed file contains one or many infected files. Also, each time a virus is detected, you can select Info and read about the characteristics of the virus. With all of this information, you can choose to continue to Ignore the warning or to Abort the download at any time during the scan.

Continues the download but discontinues the scan.

⚠   Use this option cautiously. You will have no information about how many or what types of viruses may be found in other files inside this compressed file. You should not execute or distribute this compressed file until you have cleaned up all the infected files it contains.

Select what to scan when you initiate a scan using the menu commands on the Scan menu or the Scan Now button. (For maximum protection, check Master Boot Record and Boot Records.)

Checks for viruses resident in your computer's memory before any files are scanned. If a virus is in memory while you are scanning, every file scanned can become infected.

Checks for boot viruses in the master boot record of your hard disk.

Checks for boot viruses in the boot records on your hard disk and on any floppy disks that you scan.

Scans all files on your disk. This includes files that are less likely to contain viruses. Check this option for maximum protection.

Scans files with the extensions contained in the Program File Extensions list. These are the files most likely to become infected.

Click to display the Program File Extensions list where you can view, add, or delete program file extensions.

Scans files compressed using any one of several popular compression utilities. Scanning time may increase if you have many compressed files. Note that compressed files within compressed files are not scanned.

Select an option to choose how to respond when a virus is found. Select Prompt to have the most control over what happens to an infected file.

Informs you when a virus is found. When you select Prompt, you should also specify which buttons to display when prompted.

Notify Only informs you when a virus is found but does not allow you to repair or delete the infected file.

Repair Automatically repairs an infected file or boot record as soon as a virus is detected. You are informed of the results at the end of the scan.

Delete Automatically deletes an infected file as soon as a virus is detected. You are informed of the deletion at the end of the scan. Use caution when selecting this option. Be sure that you have an uninfected copy of the file available (for example, on a disk, from a BBS or other source). Files deleted by Norton AntiVirus Scanner cannot be restored.

If you selected Prompt from the drop-down list box above, you can choose which options should be displayed when NAV Scanner detects a virus.

Allows you to repair the file or boot record.

Allows you to delete the infected file.

Allows you to continue scanning without resolving the problem. (This button only appears if you use the Immediate Notification option found in the Scanner Advanced Settings dialog box which you can access by clicking the Advanced button at the bottom right of this Scanner tab.)

Allows you to exclude the file from being checked for known viruses. (Be careful! You are reducing your protection.)

Click Advanced to display the Scanner Advanced Settings dialog box which contains more options, including network scanning, immediate notification when a virus is found, and drive preselection.

Check the options you want to enable:

Allow Network Scanning: Allows Norton AntiVirus Scanner to scan network drives. (This can be very time-consuming.)

Allow Scanning to be Stopped: Enables the Stop button in the Scan Progress dialog box, allowing you to stop a scan in progress.

Immediate Notification: Click to display an alert box whenever a problem is detected while scanning. This allows you to respond immediately, without waiting until the scan is completed.

Allows Norton AntiVirus Scanner to scan network drives. (This can be very time-consuming.)

Enables the Stop button in the Scan Progress dialog box, allowing you to stop a scan in progress.

Check to display an alert box whenever a problem is detected while scanning. This allows you to respond immediately, without waiting until the scan is completed.

Specifies the drives that you want selected automatically in the Drives group box in the Norton AntiVirus Scanner main window.

All floppy drives are automatically selected to be scanned when you initiate a scan.

All hard drives are automatically selected to be scanned when you initiate a scan.

All network drives are automatically selected to be scanned when you initiate a scan.

You must have checked Allow Network Scanning in the Advanced settings group box before you can scan network drives. Your network access privileges affect the drives on which you may scan, repair, or delete files.

Click Default to reset the extensions to the original list installed with Norton AntiVirus Scanner.

Click New to display a dialog where you can add a new extension (you'll be prompted to type the extension's letters).

Click Remove to delete the selected extension.

Check to add a message with instructions or special warnings to all alerts that Norton AntiVirus Scanner displays.

Check to add a message with instructions or special warnings to all alerts that Norton AntiVirus Scanner displays.

Check if you want Norton AntiVirus Scanner to sound a tone when it alerts you of a virus.

Check to specify how long notification dialog boxes stay on your screen. Then enter a number of seconds (between 1 and 99) in the Seconds combo box.

Select the number of seconds (between 1 and 99) the alert should stay on the screen.

Check each type of event that you want Norton AntiVirus Scanner to record in the Activity Log.

Records the date and ending time of scans that you initiate and scheduled scans.

Records changes to the Virus List.

Check to limit the size of the Activity Log file, then enter the desired size in the kilobytes combo box. When the specified file size is reached, each new entry added to the Activity Log causes the oldest entry or entries to be deleted.

You can set a limit for the log file size. When the specified file size is reached, each new entry added to the Activity Log causes the oldest entry or entries to be deleted.

Select the maximum size for the Activity Log file.

Enter the pathname for the Activity Log file or use the browse control to choose an Activity Log filename from a list of files on your computer.

Norton AntiVirus Scanner uses the entries in the Exclusion List in all scans it performs.

Click New to display a dialog where you can add a new exclusion.

Click Edit to display a dialog where you can edit an exclusion.

Click Remove to delete an exclusion.

Type the pathname for a file or group of files to exclude from checks for known viruses, or use the browse control to select a single file from a list.

Check to exclude the activity for the specified file or group of files (for example, *.COM).

Excludes the item from checks for known viruses.

Check to make a copy of the infected file before repairing it (".VIR" is the preset backup file extension). You can change this extension in the Backup extension text box.

Enter the extension you want to use to indicate backup copies of infected files. ".VIR" is the preset backup file extension.

Check to scan the High Memory Area when scanning memory. Some (but not many) viruses can be active in this area of memory. Note that scanning time is slightly slower when this option is checked.

This dialog indicates that you have no disk in the drive you are attempting to scan.

Click Retry to retry the scan after inserting a floppy disk into the drive. Or, if you are attempting to scan a hard drive, make sure you have administrator access level privileges to this drive.

Click Continue to continue the scan.

Click Skip to skip this drive.

The Virus List includes the names of all viruses for which Norton AntiVirus Scanner has a virus definition. NAV Scanner uses virus definitions to detect infected files. To ensure maximum protection, you need to update the Virus List monthly. Click Help for more information on updating virus definitions.

Click Close to exit the Virus List.

WARNING: Do not delete a virus definition unless you are sure you don't need it. Once a virus definition is deleted, files and boot records are no longer protected from that virus.

The Virus Information dialog box gives detailed information about the virus you selected in the Virus List box. Use the arrow buttons to page forward or back to the next or previous virus in the list box.

No help is provided for this unspecified portion of the dialog box. Move the cursor over a specific control and click right mouse button again.

The Scan Results dialog box summarizes information about the scan just performed.

The Virus Information dialog box contains information about the characteristics of the virus found and a description of what it does to your system.

Select what to scan, how Norton AntiVirus Scanner should respond when a virus is detected, and what buttons to display when NAV Scanner prompts you about a problem found during a manual scan.

Use these settings to further customize the way Norton AntiVirus Scanner scans for viruses when you initiate scans.

The alert settings define how Norton AntiVirus Scanner informs you that it has detected a virus. These options apply to all scans that Norton AntiVirus Scanner performs.

The Activity Log contains a history of Norton AntiVirus Scanner activity. For example, Norton AntiVirus Scanner is preset to record detections of known viruses and what action was taken on infected files (whether they were repaired, deleted, added to the Exclusions List, or left untouched.)

You can add exclusions to Norton AntiVirus Scanner manually. Be careful! Excluding files reduces protection against viruses.

The settings in this dialog apply to all scans.

Type a new extension in the Extension to Add text box (up to three characters). You may use wildcards in the extension, but not to represent all three characters. This new extension is added to the Program File extensions list. Norton AntiVirus Scanner scans any files with this extension as program files when it scans for viruses.

Click to confirm that you want to delete all files.

Click to confirm that you want to delete all files.

Click to confirm that you want to delete all files.

The Program File extensions list contains the majority of extensions used for program files. If you are using custom applications that use unique file extensions, add them to the list.

Use the Activity Log to view a record of Norton AntiVirus Scanner activities. You can specify which types of activities to view at this time by clicking Filter. If you want to permanently change the kinds of events that NAV Scanner records, go to the Activity Log tab in the Options dialog box.

To find help:
1. Click InfoDesk on the Help Menu and then select Norton AntiVirus Scanner from the InfoDesk Contents.
   Or,
   Click Help in any dialog box for information about what you can do from that dialog box.
   Or,
   Click the ? from the title bar in dialog boxes over an option and click the left mouse button once.
   Or,
   Position the pointer over an option and press **F1**.
2. Position the pointer over any option, click the right mouse button, and choose one of the following:

   What's This?   Gives a brief description of the option.
   How to   Displays a menu of procedures that you can initiate from within the dialog box.
   InfoDesk   Displays the Norton InfoDesk which gives you access to Norton AntiVirus Scanner help topics and a Glossary of terms.

Click here {button ,AL("NAVDSK_V0325")} for more information.

To change how Norton AntiVirus Scanner works:
1. Click Options in the Norton AntiVirus Scanner main window.
   The Options dialog box appears.
2. Click one of the following tabs:

   Scanner: Controls what is scanned and how Norton AntiVirus Scanner responds when you initiate a scan from the main window.
   Scanner: Controls what is scanned and how Norton AntiVirus responds when you scan.
   Alerts: Tells Norton AntiVirus what to display when a virus is found.
   Activity Log: Determines which events are recorded by NAV.
   Exclusions: Specifies which files are not monitored for known viruses.
   General: Applies to all scans you initiate.

3. Use the right mouse button to click on any of the controls to see what it does.
4. Change any settings you want.
5. Click OK to close and exit the screen. (If you don't click OK, you lose your changes.)
   These settings now take precedence over the preset options.

To use Norton AntiVirus Scanner:
1. Initiate manual scans of selected files, folders, or drives using the menu commands or the Scan Now button in the Norton AntiVirus Scanner main window. See <u>Initiate scans</u>.
2. Update virus definitions monthly. See <u>About updating virus definitions</u>.

To change scan options:
1. Click Options in the Norton AntiVirus Scanner main window.
   The Options dialog box appears.
2. Click the Scanner tab if it is not already on top.
3. Click the right mouse button over any option and click What's This? to find out what the option does.
4. Make your changes.
5. Click OK to save your changes and exit.

Click here {button ,AL("NAVDSK_V0065;NAVDSK_V0090;NAVDSK_V0055")} for more information.

To exclude files from being scanned for known viruses:
1. Click Options in the Norton AntiVirus Scanner main window.
    The Options dialog box appears.
2. Click the Exclusions tab to bring it to the front.
3. Click New.
    The New Exclusion dialog box appears.
4. Use the browse control to display a file selection dialog from which you can choose a file to display in the Item text box.
    Or,
    Type a filename in the Item text box. You can use wildcards such as c:\ archive*.ZIP. You should check Include Subfolders if you want to ensure all the descending subfolders are searched for files with that extension.
5. Click OK to save settings and exit the dialog box.

Click here {button ,AL("NAVDSK_V0050;NAVDSK_I0095")} for more information.

To find viruses on your computer:
1. Initiate virus scans at any time by choosing which drives to scan and clicking Scan Now in the NAV Scanner main window.
   Or,
   Use the Scan menu in the NAV Scanner main window to choose specific files or folders to scan.

   We advise you to always scan disks before you use them or when downloading files from bulletin boards.
2. Update your <u>virus definitions</u> monthly.

Click here {button ,AL("NAVDSK_V0250;NAVDSK_V0050;NAVDSK_I0095")} for more information.

To ensure maximum protection:

- Perform regular scans of your hard drive (at least once weekly.)
- Scan all floppy disks before using them.
- Order regular updates for your virus definitions files.
- See <u>Customize Scanner settings for maximum protection</u>

To initiate scans:
1. Open the Norton AntiVirus Scanner main window if it is not already displayed.
2. Check a drive or drives in the Drives list box or check a category of drives in the Drive Types group box and click Scan Now.

     The All Network Drives option is dimmed if you are not connected to a network or if Norton AntiVirus Scanner is configured not to allow network drive scanning. (See the Scanner Advanced Settings dialog box to reconfigure this option.)
     Or,
Click Folders from the Scan menu, select the folder, and click Scan.
Or,
Click File from the Scan menu, select the file or type in a filename, and click OK.
The Scan dialog box reports on the progress of the scan.

Click here {button ,AL("NAVDSK_V0065")} for more information.

To respond to virus-found alerts:
1. Don't panic! If a virus is found, it can be removed from your computer.
2. Read the message in the alert box to understand the type of problem that was found.
3. When downloading files, click the appropriate button (some buttons are relevant to individual files while others are relevant to compressed files):

   Repair: Eliminates the virus and returns the infected file or boot record to its original state (individual files only).

   ⓘ In the rare case the file cannot be repaired, you can Abort the download or Ignore this alert and attempt to remove the virus later. You should not, however, execute or distribute this virus-infected file until the virus has been removed.

   Abort: Aborts the download. The file will not be saved to your local drive. You will need to download the file from a different site.
   Ignore: Continues the download. Use this option cautiously. You are downloading a virus-infected file onto your disk.

   ⓘ Continues the download and continues scanning the compressed file. You are notified each time a new virus is found. (You may have one or many infected files within the compressed file.) Each time a new virus is identified you can choose Info and find out about the virus. This may influence your decision as to whether or not to Abort the download.

   Ignore all: Norton AntiVirus Scanner stops scanning the file (compressed files only) and the download continues uninterrupted by further alerts. In other words, you will know that one file within the compressed file is infected with least one virus (the one that caused the alert box to appear) but you won't know if there are other infected files.
   Info: Displays detailed information about the virus that was found.

Or,
4. When scanning from the Norton AntiVirus Scanner main window:

   Repair: Eliminates the virus and returns the infected file or boot record to its original state.
   Delete: Eliminates the virus by deleting the infected file. Deleted files cannot be recovered. After you delete the file, you should replace it with an uninfected copy.
   Exclude: Continues the operation and excludes the file from virus detections in the future. Be sure to use this button only when you are sure it is not a real problem.
   Info: Displays detailed information about the virus that was found.
   Stop: If a scan is in progress, the scan stops. Clicking Stop does not solve the problem that was reported to you.
   Continue: If a scan is in progress, the scan continues.

Click here {button ,AL("NAVDSK_V0065;NAVDSK_V5000;NAVDSK_V0175;NAVDSK_V0335;NAVDSK_V0325")} for more information.

To always scan floppies:
1. Click Options in the Norton AntiVirus Scanner main window.
    The Options dialog box appears.
2. Click the Scanner tab if it is not already on top.
3. Click Advanced at the bottom of the tab.
    The Scanner Advanced Settings dialog box appears.
4. Check All Floppy Drives in the Preselect at Start group box and click OK to save settings and exit the dialog box.
    The Scanner tab reappears.
5. Click OK to save settings and exit the dialog box.

Click here {button ,AL("NAVDSK_V0055")} for more information.

To keep up with new viruses:
To ensure that your computer is protected from new viruses, update the Virus List each month. Click here
{button ,AL("NAVDSK_I0070")} and select "About updating virus definitions."

Click here {button ,AL("NAVDSK_V0250;NAVDSK_V0050;NAVDSK_V0055")} for more information.

To select which files to scan when you initiate a scan:

1. Click Options in the Norton AntiVirus Scanner main window.
   The Options dialog box appears.
2. Click the Scanner tab to bring it to the front.
3. From the Scanner tab, check the areas your computer should scan before program files are scanned.

   ⓘ   By default Master boot record, Boot records and Within compressed files are already checked.

   ⓘ   Scanning time may increase if you have many compressed files.

5. Click Program Files to scan only files which are susceptible to virus infection. However, if you work in an environment where you may encounter program files that do not have standard file extensions, click All Files.

   ⓘ   Microsoft Word documents are included in the program files group. Although these are not program files, they do contain code and can be infected by a new class of viruses called "Macro viruses."

6. Click Select to display the Program File Extensions dialog box which lists the file extensions that NAV Scanner scans.

Click here {button ,AL("NAVDSK_V0055")} for more information.

To choose which program files to scan when you initiate a scan:
1. From the Scanner tab, click the type of files to scan: All Files or Program files.
   - In most cases, scanning program files only is sufficient. For maximum protection, click All Files.
2. If you have selected Program Files, click Select to display the Program File Extensions dialog box.
3. Click New to display the New Program File Extension dialog box.
4. Type in any non-standard file extensions that you use to name executable files.
   - Microsoft Word documents are included in the program files group. Although these are not program files, they can do contain code and can be infected by a new class of viruses called "Macro viruses."
5. Click OK to save settings and exit the New Program File Extensions dialog box.
   The Program File Extensions dialog box reappears.
6. Click OK to save settings and exit the Program File Extensions dialog box.
   The Scanner tab reappears.
7. Click OK to save settings and exit the Options dialog box.

Click here {button ,AL("NAVDSK_V0055")} for more information.

To choose how NAV Scanner should respond when a virus is found during a scan:
1. Click Options from the Norton AntiVirus Scanner main window.
   The Options dialog box appears.
2. From the Scanner tab, click any of the options in the How to Respond drop-down list box.
3. Click the right mouse button on the selected option to display a help menu. Click What's This? to see a description of the option.
         We recommend you choose Prompt for the most control.
4.   If you select Prompt, specify in the Buttons to display if prompted group box which options you want Norton AntiVirus Scanner to make available when a virus is found.
5. Click OK to save settings and exit the dialog box.
   Note that the choices you make on this options screen only apply to scans you initiate from the Norton AntiVirus Scanner main window. When downloading files, options are preset.

Click here {button ,AL("NAVDSK_V0055")} for more information.

To set general scanning options:

1. Click Options in the Norton AntiVirus Scanner main window.
    The Options dialog box appears.
2. Click the General tab to bring it to the front.
3. Check Back Up File Before Attempting a Repair to have NAV Scanner make a copy of the infected file before repairing it.
    The default extension for virus-infected, backed-up files is VIR. You can, however, enter a different extension for the file in the Backup Extension text box.
4. Under Windows 95, if you want to set maximum protection, check Scan high memory when scanning memory. However, this is not recommended unless you are in a high-risk environment. Very few viruses are active in high memory and scanning time is slower.
5. Click OK to save settings and exit the dialog box.

Click here {button ,AL("NAVDSK_V0055")} for more information.

To scan drives:
1. Open the Norton AntiVirus Scanner main window if it is not already displayed.
2. Check specific drives to scan in the Drives list box or select multiple drives at once by checking one or more options in the Drive Types group box and click Scan Now.
   The All Network Drives option is dimmed if you are not connected to a network or if Norton AntiVirus Scanner is configured not to allow network drive scanning.

To scan a folder:
1. Double-click Folders from the Scan menu.
2. Select the folder you want to scan.
3. Click Scan.

To scan an individual file:

1. Click File from the Scan menu.
2. Select the file you want to scan.
3. Click Open.
   Or,
   Under Windows NT, click OK.

To edit exclusions:
1. Click Options in the Norton AntiVirus Scanner main window.
   The Options dialog box appears.
2. Click the Exclusions tab to bring it to the front.
3. Select an item from the Items list box**.**
4. Click Edit
5. Make the desired changes.
6. Click OK to save settings and exit the dialog box.

To delete an exclusion:
1. Click Options in the Norton AntiVirus Scanner main window.
    The Options dialog box appears.
2. Click the Exclusions tab to bring it to the front.
3. Select an item from the Items list box**.**
4. Click Remove.
    The file is removed from the exclusions list.
5. Click OK to save settings and exit the dialog box.

To decide what to scan when you initiate a scan:

If you performed a complete setup of Norton AntiVirus Scanner, the preset options protect you adequately in most environments. To set up maximum protection, make the following changes from the Scanner tab:

▶ Click All Files instead of Program Files in the What to Scan group box.

🛈 Note that the choices you make on this options screen only apply to scans you initiate from the Norton AntiVirus Scanner main window. When downloading files, options are preset.

To customize how to respond to problems found during a scan:
1. Click Options in the Norton AntiVirus Scanner main window.
    The Options dialog box appears.
2. Click the Scanner tab to bring it to the front.
    If you performed a complete setup of NAV Scanner, the preset options in the Buttons to Display if Prompted group box are:
    Repair: Repairing a file or boot record removes the virus.
    Delete: Deleting the file removes it from your disk. Files deleted by Norton AntiVirus Scanner cannot be recovered. After you have deleted the file, you can replace it with an uninfected copy.
    Continue: Ignores the issue.
3. Check to add options or uncheck to delete options.
    🛈   Although you may want to enable the Exclude option to prevent certain files from being checked for known viruses, be aware that selecting this option puts you at greater risk of infection.
🛈   If an option is not checked, the button is dimmed when it appears in the Problems Found dialog. Note that the Repair and Delete buttons may also be dimmed if NAV Scanner is unable to repair or delete the selected file.
🛈 Note that the choices you make on this options screen only apply to scans you initiate from the Norton AntiVirus Scanner main window. When downloading files, options are preset.

To respond to alerts:
1. Don't panic! If a virus is found, it can be removed from your computer.
2. Read the message in the alert box to understand the type of problem that was found.
3. When downloading files, click the appropriate button (some buttons are relevant to individual files while others are relevant to compressed files):

   Repair: Eliminates the virus and returns the infected file or boot record to its original state (individual files only).

   ⓘ In the rare case the file cannot be repaired, you can Abort the download or Ignore this alert and attempt to remove the virus later. You should not, however, execute or distribute this virus-infected file until the virus has been removed.

   Abort: Aborts the download. The file will not be saved to your local drive. You will need to download the file from a different site.
   Ignore: Continues the download. Use this option cautiously. You are downloading a virus-infected file onto your disk.

   ⓘ Continues the download and continues scanning the compressed file. You are notified each time a new virus is found. (You may have one or many infected files within the compressed file.) Each time a new virus is identified you can choose Info and find out about the virus. This may influence your decision as to whether or not to Abort the download.

   Ignore all: Norton AntiVirus Scanner stops scanning the file (compressed files only) and the download continues uninterrupted by further alerts. In other words, you will know that one file within the compressed file is infected with least one virus (the one that caused the alert box to appear) but you won't know if there are other infected files.
   Info: Displays detailed information about the virus that was found.

Or,
4. When scanning from the Norton AntiVirus Scanner main window:
   Repair: Eliminates the virus and returns the infected file or boot record to its original state.
   Delete: Eliminates the virus by deleting the infected file. Deleted files cannot be recovered. After you delete the file, you should replace it with an uninfected copy.
   Exclude: Continues the operation and excludes the file from virus detections in the future. Be sure to use this button only when you are sure it is not a real problem.
   Info: Displays detailed information about the virus that was found.
   Stop: If a scan is in progress, the scan stops. Clicking Stop does not solve the problem that was reported to you.
   Continue: If a scan is in progress, the scan continues.

To work with scan results:

Click Print to print the scan results to a printer or a file.

Click Details to view details about the scan, such as which files had problems and how each problem was resolved. If no problems were found, the Details button is dimmed.

The Scan Results dialog box appears at the end of a scan, after you have responded to any problems. It summarizes what happened during the scan.

To use scan details:

Save or print the details about any of the files that were infected if you need to refer to the information later or show it to someone else.

To use the Activity Log:

1.　　　Click Activity Log in the Norton AntiVirus Scanner main window.
The Activity Log displays a history of Norton AntiVirus Scanner activities.

2.　　　Click Filter to display a dialog box where you can specify the types of events you want to look at in the Activity Log.

3.　　　Click Clear to display a dialog box where you can confirm that you want to clear the Activity Log of all entries. (If you don't clear it, it expands until it reaches the maximum size, and then the earliest entries are overwritten.)

　　　Note that filtering the Activity Log affects only what is displayed, not what is logged. You can modify what events are logged as well as the size of the Activity Log by clicking Options in the Norton AntiVirus Scanner main window and choosing the Activity Log tab.

4.　Click Close to exit the Activity Log.

To filter the Activity Log entries:
1. Click Filter in the Activity Log dialog box.
   The Activity Log Filter dialog box appears.
2. Specify the types of events to display by clicking the appropriate check boxes:
   Known Virus Detections: Displays detections of viruses for which NAV Scanner has a definition.
   Completion of Scans: Displays information about when scans occurred.
   Virus List Changes: Displays information about changes to the Virus List.
   Dated: Indicates the date or range of dates for displaying the selected events. Click an option in the Date drop-down list box, then enter the date or dates to define the scope.
3. Click OK to save settings and exit the dialog box.

To clear the Activity Log:
1. Click Clear in the Activity Log dialog box.
   The Clear Activity Log dialog box appears.
2. Click Yes to clear the Activity Log and continue.

To install new virus definitions files:
1. Use your modem and telecommunications software to download files containing the latest definitions.
   Click here {button ,AL("NAVDSK_I0070")} and choose "About updating virus definitions" to display the various sources available.
   Or,
   Order regular monthly updates to arrive by mail. In the United States, call (800) 453-1149. Outside the United States, contact your local Symantec office or representative.
2. Copy the compressed archive to your Norton AntiVirus folder. C:\Program Files\Norton AntiVirus is the default location.
3. From a system prompt, use the PKUNZIP utility to extract the files from the compressed archive. For example, type:
   PKUNZIP 01NAV96.ZIP
   When prompted to Overwrite, press "y" for yes. You're replacing your existing files with the new ones.
4. Type EXIT and press Enter to return to the Windows desktop.
5. Initiate a scan with Norton AntiVirus Scanner to activate the new virus definitions.
6. Read the text files (*.TXT) for late-breaking information about newly discovered viruses and any special precautions that you should take.

If you don't have copy of PKUNZIP, the utility that extracts the compressed files, it is available for download at both the Symantec Internet site and the Symantec BBS. The file, called "PKZ204G.EXE," is a self-extracting archive. Just run the downloaded file to get PKUNZIP. The PKUNZIP utility is also available from the other online services. You will need to perform a file search for PKZIP or PKUNZIP to locate the proper library.

To use the Virus List:

1. Click Virus List in the Norton AntiVirus Scanner main window.
   The Virus List appears. The list box displays the name of the virus and what it infects (program files, boot records, or both).
2. Select a category from the Display drop-down list box to view different categories of viruses.
   Or,
   Click Info to view details, such as symptoms and aliases, about a particular virus.
   Or
   Click Print to print the Virus List to a printer or a file.
   Or,
   Click Delete to delete the currently highlighted definition.

    Don't delete a virus definition unless you are sure you don't need it anymore. Once a virus definition is deleted, files and boot records are no longer protected from that virus until you update the virus definition files again.

To search the Virus List:
1. Activate the Virus List box by clicking inside the list box.
2. Start typing the name of the virus you want to find.
    The Smart Search text box appears at the bottom of the list.
3. Continue typing until the virus you're searching for is highlighted in the Virus List.

To display information about a virus:
1. Click Virus List in the Norton AntiVirus Scanner main window.
   The Virus List appears. The list box displays the name of the virus and what it infects (program files, boot records, or both).
2. Click in the Virus List itself. Start typing the first few letters of the virus you are searching for.
   The Smart Search text box appears at the bottom of the list.
3. Continue typing until the virus you're searching for is highlighted in the Virus List.
4. Click Info to view details, such as symptoms and aliases, about the highlighted virus.

To remove virus definitions:
1. Click Virus List in the Norton AntiVirus Scanner main window.
    The Virus List appears. The list box displays the name of the virus and what it infects (program files, boot records, or both).
2. Click in the Virus List itself. Start typing the first few letters of the virus you are searching for.
    The Smart Search text box appears at the bottom of the list.
3. Continue typing until the virus you're searching for is highlighted in the Virus List.
4. Click Delete to delete the currently highlighted definition.
    Don't delete a virus definition unless you are sure you don't need it anymore. Once a virus definition is deleted, files and boot records are no longer protected from that virus until you update the virus definitions files again.
5. Click OK to save your changes and exit the dialog box.

To print to a printer:
1. Click Print to display a print dialog box.
2. Click Print to printer.
3. Click OK to save your changes and exit the dialog box.

To print to a file:
1. Click Print to display a dialog box.
2. Click Print to file.
3. Type in the name of a file or click the browse button.
4. Click OK to save your changes and exit the dialog box.

To append a file:

If you have chosen a file that already exists, you have the choice to Overwrite or Append. Click Append if you want to add to the existing file rather than writing over the existing one.

To decide what to log:

The Activity Log contains a history of Norton AntiVirus Scanner activity. The preset options are detections of known viruses and what action was taken on infected files. You can customize the Activity Log to record other types of events (such as Virus List changes) as well.

1. Click Options in the Norton AntiVirus Scanner main window.

    The Options dialog box appears.
2. Click the Activity Log tab to bring it to the front.
3. In the Log Following Events group box, check each type of event that you want Norton AntiVirus Scanner to record.
4. Click OK to save changes and close the dialog box.

To scan network drives:
1. Click Options in the Norton AntiVirus Scanner main window.
   The Options dialog box appears.
2. Click the Scanner tab to bring it to the front.
3. Click Advanced at the bottom of the tab.
   The Advanced Scanner Settings dialog box appears.
4. Check Allow Network Scanning.
5. Click OK to close the dialog box.
6. Click OK to save your settings and close the Options dialog box.

   Note that your ability to scan networks also depends on your network privileges.

Click here {button ,AL("NAVDSK_V5005")} for more information.

To customize Scanner settings for maximum protection:
1. Click Options in the Norton AntiVirus Scanner main window.
   The Options dialog box appears.
2. Click the Scanner tab to bring it to the front.
3. Check all options in the What to Scan group box; click the All Files option.
4. Be sure that Prompt is selected in the When a Virus is Found drop-down list box.
5. Be sure that neither Continue nor Exclude is checked in the Buttons to Display if Prompted group box.
6. Click OK to save settings and exit the dialog box.

Help Menus

The following menus are available from within the help topic.

File

Click Open to choose from a list of any other available help files
Or,

Click Print Topic to display a print dialog box from which you can print the current topic

Or,

Click Exit to close the help dialog box.

Edit

Select help text to Copy to another file or Click Annotate to create your own help notation. To view this notation later, click on the paperclip icon that appears next to the text.

Bookmark

Click Define and name your bookmark so you can use it to find the topic again and Click OK to save settings and exit the dialog box.

To return to this topic later, click Bookmark and then click the topic name.

Options

Set a variety of options for how help should display including how the help menus appear. You have the option of seeing the standard button bar which shows the options such as Contents, Index, etc. Or you can customize a toolbar which allows you to display menu options and buttons as icons.

To repair an infected file or boot record:

1. Click Repair in the Norton AntiVirus Scanner alert box.
If the Repair command button is dimmed, either Norton AntiVirus Scanner is configured not to enable it or the item cannot be repaired.

2. After repairing infected files or boot records, scan your drives and floppy disks again to verify that there aren't any other files or boot records that contain viruses.
If Norton AntiVirus Scanner is not able to repair a file or boot record, you are notified that the repair was not successful.

If Norton AntiVirus Scanner could not repair the infected file (under Windows NT)

▶   If Norton AntiVirus Scanner cannot repair the infected file, the only way to remove the virus is to delete the file. After you delete the infected file, you can replace it with an uninfected copy.

If the infected file is a system file that is in use or otherwise required for operation, you must perform a manual repair. During Windows NT installation, you created an Emergency Repair Disk. Try using this disk to restore the damaged system file. If this too fails, you must reinstall Windows NT from your original installation disks. As a safety precaution, first back up your data files and uninfected program files.

If Norton AntiVirus could not repair the infected file (under Windows 95)

▶   The only way to remove the virus is to delete the file. After you delete the infected file, you can replace it with an uninfected copy. If the infected file is a system file (such as, COMMAND.COM, IO.SYS, or WIN.COM), you can restore these system files using the WIN95 startup disk you made when you installed WIN95.

ⓘ   If you didn't create a WIN95 startup disk, you can do so now by clicking Start on the WIN95 taskbar, then making the following choices: Settings; Control Panel; Add/Remove Programs; Startup Disk.

If Norton AntiVirus Scanner could not successfully repair a boot record (under Windows NT)

▶   You must have administrator-level privileges to access boot records. If you have the proper privileges and cannot effect a repair, Windows NT itself may be preventing the boot record modifications. In this case, use the Norton AntiVirus Scanner for DOS, a free program provided by Symantec that runs under MS-DOS rather than Windows NT, to repair boot records.

If you don't succeed with the DOS scanner, use the Emergency Repair Disk that you created during Windows NT installation to restore the boot records. If this too fails, you must reinstall Windows NT from your original installation disks. Do not boot from the infected system before attempting a repair.

If Norton AntiVirus could not successfully repair the master boot record or a boot record on your hard disk (under Windows 95)

▶   In this case, use the Norton AntiVirus Scanner for DOS, a free program provided by Symantec that runs under MS-DOS rather than Windows 95, to repair boot records.

If you don't succeed with the DOS scanner, use the disk that you created during Windows 95 installation to restore the boot records. If this too fails, you must reinstall Windows 95 from your original installation disks. Do not boot from the infected system before attempting a repair.

If Norton AntiVirus could not successfully repair a boot record on a floppy disk (under Windows 95)

▶   The virus is removed and the information on the disk is still accessible. However, the floppy disk is no longer bootable. You can use the DOS SYS command to make the disk bootable again. Refer to your DOS manual for instructions on how to use the SYS command.

To work with compressed   files, choose one of the following actions:
▸   Remove the whole compressed file from your disk
In other words, if NAV Scanner finds that GOATS.COM is infected and GOATS.COM is part of ANIMALS.ZIP, you must delete the whole .ZIP file.
        Or,
        Uncompress the compressed file using a utility such as PKUNZIP.EXE. Delete the infected file and replace it with an uninfected copy.
🛈   You can leave the infected compressed file on your computer. As long as you never uncompress it and attempt to use the files, it does not spread the virus. However, if you continue to scan compressed files, you continue to receive the warning about infections.

To browse for files:

▶ Click the browse button to display a dialog box where you can locate a specific file or files.

Or,

Type the pathname for the file, group of files, folder, or drive in the Item text box. Just enter the folder name to act on all files in the folder. Or, use a wildcard to specify a group of files.

To set back up options:

If you performed a complete setup of Norton AntiVirus Scanner, the Back Up a File Before Attempting to Repair option is already checked. We recommend you leave this preset option as is.

However, note that if you do back up files, you have to delete the backups after the repair has been successfully made. ".VIR " files are added to the Exclusions List so they don't trigger virus alerts.

To make decisions about alerts:

1. Consider the following:

   The message you enter in the Display Alert Message text box appears on all of the alert screens displayed in Norton AntiVirus Scanner Windows dialog boxes and the Problems Found screen.

2. You can specify a time for when alerts should be removed from the screen in the Remove Dialog Alert after *n* seconds. However, be aware this only affects alerts if you have specified Notify only in the How to respond group box on the Scanner tab in the Options dialog box.

To use virus-found information:

When Norton AntiVirus Scanner finds a virus, you need to take action. You should attempt to repair the infected file or boot record.

If Norton AntiVirus Scanner could not repair the infected file (under Windows NT)

▶   If Norton AntiVirus Scanner cannot repair the infected file, the only way to remove the virus is to delete the file. After you delete the infected file, you can replace it with an uninfected copy.

If the infected file is a system file that is in use or otherwise required for operation, you must perform a manual repair. During Windows NT installation, you created an Emergency Repair Disk. Try using this disk to restore the damaged system file. If this too fails, you must reinstall Windows NT from your original installation disks. As a safety precaution, first back up your data files and uninfected program files.

If Norton AntiVirus could not repair the infected file (under Windows 95)

▶   The only way to remove the virus is to delete the file. After you delete the infected file, you can replace it with an uninfected copy. If the infected file is a system file (such as, COMMAND.COM, IO.SYS, or WIN.COM), you can restore these system files using the WIN95 startup disk you made when you installed WIN95.

🛈   If you didn't create a WIN95 startup disk, you can do so now by clicking **Start** on the WIN95 taskbar, then making the following choices: **Settings**; **Control Panel**; **Add/Remove Programs**; **Startup Disk**.

If Norton AntiVirus Scanner could not successfully repair a boot record (under Windows NT)

▶   You must have administrator-level privileges to access boot records. If you have the proper privileges and cannot effect a repair, Windows NT itself may be preventing the boot record modifications. In this case, use the Norton AntiVirus Scanner for DOS, a free program provided by Symantec that runs under MS-DOS rather than Windows NT, to repair boot records.

If you don't succeed with the DOS scanner, use the Emergency Repair Disk that you created during Windows NT installation to restore the boot records. If this too fails, you must reinstall Windows NT from your original installation disks. Do not boot from the infected system before attempting a repair.

If Norton AntiVirus could not successfully repair the master boot record or a boot record on your hard disk (under Windows 95)

▶   In this case, use the Norton AntiVirus Scanner for DOS, a free program provided by Symantec that runs under MS-DOS rather than Windows 95, to repair boot records.

If you don't succeed with the DOS scanner, use the disk that you created during Windows 95 installation to restore the boot records. If this too fails, you must reinstall Windows 95 from your original installation disks. Do not boot from the infected system before attempting a repair.

If Norton AntiVirus could not successfully repair a boot record on a floppy disk (under Windows 95)

🛈   The virus is removed and the information on the disk is still accessible. However, the floppy disk is no longer bootable. You can use the DOS SYS command to make the disk bootable again. Refer to your DOS manual for instructions on how to use the SYS command.

To exclude a file:

Click Exclude to skip this file in future scans.

To schedule virus scans:

NOTE: This feature is available under Windows 95 when you purchase the full Norton AntiVirus product or under Windows NT from the complete freeware product. However, if the Scheduler button has appeared in the Norton AntiVirus Scanner main window, follow the instructions below:

Under Windows NT, if the Scheduler appears in the Norton AntiVirus Scanner main window:

1. Click Scheduler.
   The Scheduled Scans dialog box appears.
2. Check Scan Automatically Every Week.
   Uncheck this option if you want to disable the automatic scans.
3. Specify the day of the week and the time for the scan.
4. Click OK to save settings and exit the dialog box.
   🛈   Note that you have to make sure the Scheduler service is running.

Under Windows 95, if the Scheduler appears in the Norton AntiVirus Scanner main window:

1. Click Scheduler in the Norton AntiVirus main window.
   The Norton Program Scheduler appears.
2. Click Add (If the button isn't visible, select Add... from the Event menu.)
   The Add Event dialog box appears so you can schedule any type of event.
3. Click Scan for Viruses in the Type of Event drop-down list box.
   The dialog box changes to accept information specific to a virus scan.
   🛈   You can schedule other types of events. Simply select a choice from the Type of Event drop-down list box. The dialog box changes so you can enter relevant instructions.
4. Check Enable This Event. If you uncheck this option, the scan won't run.
5. Check Audible Alarm to hear a sound when the scan starts.
6. **T**ype a brief description in the Description text box.
   This text will appear in the Events list box in the Scheduler main window.
7. Type the drive letter or pathname for the drive, folder, or file you want scanned in the What To Scan text box.
   To scan more than one item, use a space between them. For example:
   C: D:\ Applications
8. Select how often you want the scan to occur in the Frequency drop-down list box.
9. Finish scheduling the scan by entering the correct time, day, and date information.
10. Click OK to save settings and exit the dialog box.
   🛈   The Scheduler must be loaded in order to execute the scans you have scheduled.
   🛈   Click Minimize.

   The Scheduler remains active so that the scan can run at the time you specified.
   The scans you scheduled will run automatically. If your computer is turned off or the Scheduler is not loaded when a scan is scheduled, you are notified that the scan was canceled the next time the Scheduler loads.

To respond if a file cannot be repaired:

1. If Norton AntiVirus Scanner could not repair the infected file, the only way to remove the virus is to delete the file. You can delete the file in one of two ways:
   Click the Delete button from the alert box (if the button appears there)

ℹ️ If you are downloading a file, you do not have the option to delete the file at this time. If, however, you save the infected file to your local disk drive, you should scan again and delete the file. If you save an infected compressed file onto your local disk, you will need to uncompress the file in a temporary directory, scan again, and delete any infected file that cannot be repaired.
Or,
Delete the file manually from the hard disk or floppy disk.

2. Replace the file with an uninfected copy. For example, copy or reinstall the file from the original manufacturer's disks.

ℹ️ If an access denied dialog box is ever displayed, first make sure that you have the necessary permissions for the operation (scan, repair, or delete) you are trying to perform on that boot record, file, or folder.

To delete an infected file:
1. Click Delete in the Norton AntiVirus Scanner alert box, then follow the prompts on your screen.
   If the Delete command button is dimmed, either Norton AntiVirus Scanner is configured not to enable it or the item cannot be deleted. (For example, you cannot delete files in use by the system, boot records, or master boot records because they contain information your computer uses to start up).

ℹ️ If you are downloading a file, you do not have the option to delete the file at this time. If, however, you save the infected file to your local disk drive, you should scan again and delete the file. If you save an infected compressed file onto your local disk, you will need to uncompress the file in a temporary directory, scan again, and delete any infected file that cannot be repaired.
2. After deleting infected files, scan all of your drives and floppy disks with Norton AntiVirus Scanner to verify that there aren't any other files that contain viruses.
3. Once you are certain that your system is virus-free, replace the files you deleted with uninfected copies. (Make sure you scan the replacement files before copying them to your hard disk.)

ℹ️ If an access denied dialog box is ever displayed, first make sure that you have the necessary permissions for the operation (scan, repair, or delete) you are trying to perform on that boot record, file, or folder.

ℹ️ If you forget which file needs replacing, look at the Activity Log for the name of the file.

ℹ️ Note that Norton AntiVirus Scanner scans Microsoft Word documents also when scanning program files. Although these are not program files, they can be infected by a new class of viruses called "Macro viruses."

ℹ️ Files deleted by Norton AntiVirus Scanner cannot be recovered even with special file recovery utilities. Be sure you have an uninfected copy of a file before deleting it. However, even if you don't have a clean copy of the file, you still need to delete the infected one. It is not a good idea to leave a file containing a virus on your disk. You can usually obtain a new copy of a program file from the manufacturer.

To remove viruses from downloaded files:
1. Scan the file from the Norton AntiVirus Scanner main window.
2. Select the file you want to repair in the Problems Found dialog box.
3. Select Repair. The Repair File dialog box appears.
4. Select Repair in the Repair File dialog box.
   Or,
   Select Repair All to repair all the infected files listed in the Problems Found dialog box.
5. When all problems have been addressed, select Done in the Problems Found dialog box.
   After repairing infected files, scan your drives and floppy disks with Norton AntiVirus Scanner to make sure there aren't any other files that contain viruses.

Unable to Repair a File

If Norton AntiVirus Scanner could not repair an infected file, the only way to remove the virus is to delete the file. After you delete the infected file, you can replace it with an uninfected copy.

To delete an infected file:
1. Select the file you want to delete in the Problems Found dialog box.
2. Select Delete. The Delete File dialog box appears.
3. Select Delete in the Delete File dialog box.
   Or,
   Select Delete All to delete all the infected files listed in the Problems Found dialog box.
4. When all problems have been addressed, select Done in the Problems Found dialog box.
   After deleting infected files, scan your drives and floppy disks with Norton AntiVirus Scanner to make sure there aren't any other files that contain viruses. Then replace the files you deleted with uninfected copies. (Make sure you scan the replacement copies before copying them to your hard disk.)

To remove viruses from downloaded files:

If Norton AntiVirus Scanner finds a virus in a downloaded compressed file, you should:

    Abort the download and try to obtain a clean copy of the file from a different source.

Or, if you choose not to abort the download,

    Save the file to a temporary directory, uncompress it, scan again, and attempt to repair any infected files.

To repair an infected file:
1. Uncompress the compressed file in a temporary directory.
2. Scan that directory from the Norton AntiVirus Scanner main window.
3. Select the file you want to repair in the Problems Found dialog box.
4. Select Repair. The Repair File dialog box appears.
5. Select Repair in the Repair File dialog box.
   Or,
   Select Repair All to repair all the infected files listed in the Problems Found dialog box.
6. When all problems have been addressed, select Done in the Problems Found dialog box.
   After repairing infected files, scan your drives and floppy disks with Norton AntiVirus Scanner to make sure there aren't any other files that contain viruses.

Unable to Repair a File

If Norton AntiVirus Scanner could not repair an infected file, the only way to remove the virus is to delete the file. After you delete the infected file, you can replace it with an uninfected copy.

To delete an infected file:
1. Select the file you want to delete in the Problems Found dialog box.
2. Select Delete. The Delete File dialog box appears.
3. Select Delete in the Delete File dialog box.
   Or,
   Select Delete All to delete all the infected files listed in the Problems Found dialog box.
4. When all problems have been addressed, select Done in the Problems Found dialog box.
   After deleting infected files, scan your drives and floppy disks with Norton AntiVirus Scanner to make sure there aren't any other files that contain viruses. Then replace the files you deleted with uninfected copies. (Make sure you scan the replacement copies before copying them to your hard disk.)

Norton AntiVirus Scanner main window

From this Norton AntiVirus Scanner main window you can do the following:

🛈   Click Scan Now to scan selected drives immediately.

🛈   Choose a menu command to scan specific files or folders.

🛈   Click one of these buttons:

Options: Displays the Options dialog box where you can customize Norton AntiVirus Scanner features.

Virus List: Displays the Virus List where you can view information about the viruses for which NAV Scanner has <u>definitions</u>.

Activity Log: Displays a history of Norton AntiVirus Scanner activities (for example, lists each incident of a known virus detection).

Click here {button ,AL("NAVDSK_I0000;NAVDSK_V0050;NAVDSK_V0010")} for more information.

Virus Information

The Virus Information dialog box contains information about the selected virus. Here is some additional information about virus types:

Memory Resident: Stays in DOS memory after it activates.

Size Stealth: Tries to conceal itself from detection by disguising its size.

Full Stealth: Tries to conceal itself from detection by disguising its size and attributes.

Triggered Event: Performs some action based on certain criteria (for example, a date on the computer's system clock).

Encrypting: Encrypts its code to make detection more difficult.

Polymorphic: Appears differently in each infected file.

Comments: Further description of the selected virus's characteristics.

          No matter what type of virus has been found, you need to eliminate it from your computer. If you tried to repair the virus and could not, you need to delete the file that contains the virus and replace that file with an uninfected copy of the file.

Click here {button ,AL("NAVDSK_V0190;NAVDSK_V0175;NAVDSK_V5000")} for more information.

Scan Results

The Scan Results dialog box summarizes information about everything that happened in the scan just performed. It shows how many viruses were found, repaired, or deleted. Click Close to conclude this scan.

Here is some additional information about the scan results:

Scanned: Indicates whether the master boot record, boot records, and/or files were scanned.

Infected: Indicates which and/or how many of the above items, if any, were infected.

Cleaned: Indicates whether infected items were cleaned; that is, how many items, if any, were deleted or repaired.

Click here {button ,AL("NAVDSK_V0175;NAVDSK_V0180;NAVDSK_V0200")} for more information.

Details of Scan

The Details of Scan dialog box summarizes what happened in the scan just performed.

- If you see that a file is still infected, you should try to repair it.
- If you attempted to repair it and it could not be repaired, you should delete the file manually and replace it with an uninfected copy.
- If you do not have a clean copy of the file, you should acquire one. Leaving the file on your system without repairing or deleting it may cause other files to become infected.
- Click Close to return to the Scan Results dialog box.
- Click Info to display the Virus Information dialog box where you can see detailed information about the highlighted virus.

Click here {button ,AL("NAVDSK_V0175;NAVDSK_V5000")} for more information.

Problems Found

The Problems Found dialog box shows you the Name of the:

ℹ️   infected file and boot records

The Status indicates whether or not an infected file was repaired or deleted, or if it remains infected.

What to do next:

1. If a file is infected, click Repair to have NAV Scanner attempt to restore it.
2. If an infected file cannot be repaired, click Delete to remove the file.

ℹ️   If you do not have a clean copy of the file, you need to acquire one. Leaving an infected file on your system without repairing or deleting it may cause other files to become infected.

3. After repairing or deleting any infected files, click Done to exit the Problems Found dialog box.
   You see the Scan Results dialog box which summarizes this scan, including what was scanned, what was cleaned (repaired or deleted), and what was left unresolved.
4. Exit Norton AntiVirus Scanner and replace the file with an uninfected or clean copy (for example, copy or reinstall the file from the disk that came from the software manufacturer onto your hard disk).

ℹ️   If an access denied dialog box displays, make sure that you have the necessary permissions for the operation (scan, repair, or delete) you are trying to perform on that boot record, file, or folder.

Click here {button ,AL("NAVDSK_V0180;NAVDSK_V5005;NAVDSK_V0175;NAVDSK_V0185;NAVDSK_V5000;NAVDSK_V0190")} for more information.

Virus List

It is most important to update your Virus List monthly because new viruses are discovered all the time. It is very simple to add new virus definitions to the list.

Click here {button ,AL("NAVDSK_I0070")}, select "About updating virus definitions," and choose a source from which to obtain the latest virus definitions files.

Or,

If you have obtained the latest virus definitions files, click here {button ,AL("NAVDSK_V0250")} , select "Install new virus definitions", and follow the procedure.

The Virus List shows the complete list of viruses that Norton AntiVirus Scanner protects against.

- Use the scroll bar or <u>smart search</u> feature to highlight a virus and select it. You see what kind of files (programs, boot records, or both) the virus infects.
- Use the Display drop-down list box to filter the list to display only certain types of viruses.
- If a virus is not found on the list, it may mean that it was never on the list, that it has been deleted from the list, that it is listed under a different name, or that you are not displaying all the names. If the name has been deleted, you are not protected against the virus.
- If the Virus List has been filtered to display only certain types of viruses, you do not see the complete list. Look at the Display drop-down list box to ensure that the All Viruses option appears.

Click here {button ,AL("NAVDSK_I0005;NAVDSK_V0255;NAVDSK_V0260;NAVDSK_V0265;NAVDSK_V0270;NAVDSK_I0040")} for more information.

Delete Virus Definition

Do not delete a virus definition unless you are sure you don't need it. Once a virus definition is deleted, files and boot records are no longer protected from that virus.

If you delete a selected virus definition, it is deleted in the Virus List box. The next time you access the Virus List, that virus name does not appear.

Click here {button ,AL("NAVDSK_I0005")} for more information.

Virus Information

The Virus Information dialog box contains information about the characteristics of the virus.

Virus Name and Aliases: The most common names by which the virus is known.

Infects: What file types or boot records the virus attacks.

Likelihood: Common or Rare.

Length: Length, in bytes, of the virus code.

Memory Resident: Stays in DOS memory after it activates.

Size Stealth: Tries to conceal itself from detection by disguising its size.

Full Stealth: Tries to conceal itself from detection by disguising its size and attributes.

Triggered Event: Performs some action based on certain criteria (for example, a date on the computer's system clock).

Encrypting: Encrypts its code to make detection more difficult.

Polymorphic: Appears differently in each infected file.

Comments: Further description of the selected virus's characteristics.

Click here {button ,AL("NAVDSK_V0250;NAVDSK_V0255;NAVDSK_V0260;NAVDSK_I0005")} for more information.

Virus Found

This Virus Found alert has appeared because a known virus has been detected during a scan.

What to do next
1. If a file is infected, click Repair to have Norton AntiVirus Scanner try to remove the virus.
2. If a file cannot be repaired, click Delete and, then, replace it with an uninfected copy.

If you do not have a clean copy of the file, you need to get one. Leaving an infected file on your system without repairing or deleting it may cause other files to become infected.

Or,

If the file is compressed, click here {button ,AL("NAVDSK_V5000")}, select "Work with compressed files," and follow the instructions.

Your options at this time may include any of the following buttons:

If a button is dimmed, Norton AntiVirus Scanner is not configured to allow that option or it may not be possible.

Repair: Click to have Norton AntiVirus Scanner repair a file or boot record by removing the virus and/or returning the file to its original state.

Delete: Click to delete a file if it cannot be repaired.

Exclude: Click to exclude the file from future checks for viruses. This can be a risky choice; a virus could creep in undetected.

Info: Click to display the Virus Information dialog box where you see details about the virus found.

Stop: Click to stop the scan.

Continue: Click to ignore the virus found. Note that you have to repair or delete the infected file at some time in the future or you may risk infecting other files.

This Virus Found alert appears when you have asked Norton AntiVirus Scanner to notify you immediately when it detects a virus on your system during a scan. If you would like NAV Scanner to perform the entire scan and summarize the problems, click Advanced on the Scanner tab in the Options dialog box and uncheck the Immediate Notification option.

Click here {button ,AL("NAVDSK_V0175;NAVDSK_V5000;NAVDSK_V0185")} for more information.

Repair file

Repairing a file or boot record removes the virus and returns the file to its original state. Click Repair All to have Norton AntiVirus Scanner repair all the infected files found during the scan. You are not prompted as each file is repaired.

Delete file

Files deleted by Norton AntiVirus Scanner cannot be recovered. After you have deleted the file, you can replace it with an uninfected copy. Choose Delete All to have Norton AntiVirus Scanner delete all the infected files found during the scan. Only infected program, or executable, files are deleted.

Note that Norton AntiVirus Scanner scans Microsoft Word documents (saved as .doc and .dot) also when scanning program files. Although these are not program files, they can be infected by a new class of viruses called "Macro viruses."

Activity Log

Use the Activity Log to view a history of Norton AntiVirus Scanner activities.

🛈 Click Filter to display a dialog box where you can specify the types of events you want to look at in the Activity Log.

🛈 Click Clear to display a dialog box where you can confirm that you want to clear the Activity Log of all entries. (If you don't clear it, it expands until it reaches the maximum size. Then the earliest entries are overwritten.)

🛈 Note that filtering the Activity Log affects only what is displayed, not what is logged. You can modify what events are logged as well as the size of the Activity Log by clicking Options in the Norton AntiVirus Scanner main window and choosing the Activity Log tab.

Click here {button ,AL("NAVDSK_V0295;NAVDSK_V0220;NAVDSK_V0225;")} for more information.

Clear Activity Log

Click Yes to erase everything in the Activity Log. Otherwise, the log expands indefinitely or until it reaches the maximum size you've set on the Activity Log tab in the Options dialog box available from the Norton AntiVirus Scanner main window.

Filter Activity Log

You can filter the Activity Log to display specific categories of entries, such as known virus detections only. Specify the types of events to display by checking the appropriate check boxes:

Known Virus Detections: Displays information on files infected with known viruses.

Completion of Scans: Displays information about when scans occurred.

Virus List Changes: Displays information about changes to the Virus List.

Dated: Indicates the date or range of dates for displaying the selected events. Click an option in the Date drop-down list box, then enter the date or dates to define the scope.

Click here {button ,AL("NAVDSK_V0225;NAVDSK_V0020;NAVDSK_V0295")} for more information.

Exclude file

From the Exclude file dialog box you can exclude this file from triggering alerts for virus detections.

ⓘTo exclude files prior to scanning:

From the Norton AntiVirus Scanner main window, click Options. Then use the Exclusions tab to specify which files to routinely exclude from scans.

Click here {button ,AL("NAVDSK_V0145;NAVDSK_V0150;NAVDSK_I0095")} for more information.

Scanner Settings

The Scanner tab allows you to choose settings that determine:

- What to scan
- How Norton AntiVirus Scanner should respond when a virus is detected
- What buttons to display when NAV Scanner prompts you about a problem found during a manual scan

Master boot record, Boot records, and Within compressed files are checked; Program files is selected. However, for maximum protection, click All Files instead of Program Files.

- Under Windows 95, Memory should also be selected.
- Windows NT, because of its flexibility, presents special problems for virus control. Under the NT file system (NTFS), you can set different access permissions to the file, folder, or object (such as the boot records) level for each user or group. Not all users will be able to scan all items.

Click here
{button ,AL("NAVDSK_V0080;NAVDSK_V0085;NAVDSK_V5005;NAVDSK_V0095;NAVDSK_V0065;NAVDSK_V0055;NAVDSK_V0020")} for more information.

Scheduled Scans

NOTE: This feature is available under Windows 95 when you purchase the full Norton AntiVirus product or under Windows NT from the complete freeware product. However, if the Scheduler button has appeared in the Norton AntiVirus Scanner main window, follow the instructions below:

Under Windows NT, if the Scheduler appears in the Norton AntiVirus Scanner main window:
1. Click Scheduler.
   The Scheduled Scans dialog box appears.
2. Check Scan Automatically Every Week.
   Uncheck this option if you want to disable the automatic scans.
3. Specify the day of the week and the time for the scan.
4. Click OK to save settings and exit the dialog box.

   Note that you have to make sure the Scheduler service is running.

New File Extensions

1. Type the extension to add.
2. Click OK to save your data and return to the Program File Extensions dialog box.

File Extensions

Use the Program File Extensions dialog box to add new extensions, delete extensions, and reset the extensions to the original list installed with Norton AntiVirus Scanner.

The file extensions list contains the majority of extensions used for program files. Norton AntiVirus Scanner only scans files with extensions on this list when Program files only is checked.

Note that Norton AntiVirus Scanner scans Microsoft Word documents (.DOT and .DOC) also when scanning program files. Although these are not program files, they can be infected by a new class of viruses called "Macro viruses."

If you are using custom applications with unique file extensions, click New to display a dialog where you can add them to the list. Then NAV Scanner can scan them and protect them against infection.

Other options are:

Click Remove to delete a highlighted file extension.

Or,

Click Default to return the file extensions list to the preset options.

Scanner Advanced Settings

The Scanner Advanced Settings dialog box allows you to further customize the way Norton AntiVirus Scanner scans for viruses when you initiate scans. Some options you may want to change are:

- Whether you want Immediate Notification of a virus found during a manual scan.
  - If you check this option, you receive a Virus Found alert as soon as a virus is detected. If you do not check this option, you see the Problems Found dialog box at the end of a complete scan.
- Whether to preset the option that Always scans floppy disks instead of having to specify this option every time you perform a scan.

Click here {button ,AL("NAVDSK_V0055")} for more information.

Alerts Settings

The Alerts tab allows you to define how Norton AntiVirus Scanner informs you that it has detected a virus.

Click here {button ,AL("NAVDSK_I0060")} for more information.

Activity Log Settings

The Activity Log tab allows you to customize how to display the history of Norton AntiVirus Scanner activity such as detections of known viruses and what action was taken on infected files (whether they were repaired, deleted, added to the Exclusions List, or left untouched.)

The log file size is also preset. You probably want to keep this limit so that it does not take up too much space on your disk. When the file reaches the maximum size, the earliest entry is deleted.

We recommend you use the preset options. If you choose to change the settings, the options are:

Known Virus Detections: Logs information on known virus detections.
Completion of Scans: Logs information about when scans occurred.
Virus List Changes: Logs information about changes to the Virus List.

Click here {button ,AL("NAVDSK_I0085;NAVDSK_V0050;NAVDSK_V0020")} for more information.

Exclusions Settings

The Exclusions tab allows you to exclude files, folders, or drives from virus detections.

- You assign exclusions to items: drives, folders, groups of files, or single files.
- When you click Remove, the exclusion is immediately removed from the list. There is no confirmation request.

Click here {button ,AL("NAVDSK_I0095;NAVDSK_V0135;NAVDSK_V0020")} for more information.

New/Edit Exclusion

You assign exclusions to items: drives, folders, groups of files, or single files.

Be careful, however, if you set an exclusion, a virus can creep in.

Click here {button ,AL("NAVDSK_I0095;NAVDSK_V0135")} for more information.

General Settings

The General tab settings apply to all scans.

🛈　　Check Back Up File Before Attempting a Repair to have NAV Scanner make a copy of the infected file before repairing it. The default extension for virus-infected, backed-up files is VIR. You can, however, enter a different extension for the file in the Backup extension text box.

🛈　　Under Windows 95, if you want to set maximum protection, check Scan high memory when scanning memory. However, this is not recommended unless you are in a high-risk environment. Very few viruses are active in high memory and scanning time is slower.

Click here {button ,AL("NAVDSK_V0010;NAVDSK_V0020")} for more information.

If you are attempting to access a floppy drive, there is no disk in the drive. If you are attempting to access a hard drive, you need to resolve the problem that is causing you to be denied access.

🛈　　　If an access denied dialog box displays, make sure that you have the necessary permissions for the operation (scan, repair, or delete) you are trying to perform on that boot record, file, or folder.

You are about to overwrite an existing file with the file you're printing to disk.
Click Overwrite to replace the old file.
Click Append to add information to the existing file.
Click Cancel to go back and change the filename.

Virus Found in Download

If the Virus Found in Download dialog box is displayed, you have the following options. You should always choose Repair as your first option.:

Repair: Removes the virus from the file.

In the rare case the file cannot be repaired, you can Abort the download or Ignore this alert and attempt to remove the virus later. You should not, however, execute or distribute this virus-infected file until the virus has been removed.

Abort: Aborts the download. The file will not be saved to your local drive. You will need to download the file from a different site.

Ignore: Continues the download. Use this option cautiously. You are downloading a virus-infected file onto your disk.

You should not execute or distribute this virus-infected file until it has been repaired. If it cannot be repaired, you should delete the file and replace it with an uninfected copy.

Info: The Virus Information dialog box shows more details about the virus.

Click here {button ,AL("NAVDSK_V0900")} for more information.

Virus Found in Download (.ZIP file)

If the Virus Found in Download dialog box is displayed and the file has been determined to be a "compressed" file (e.g. filename.zip), your options are different than if you had attempted to download a single, virus-infected file. A compressed file may contain many files that have been bundled together and given a single filename to save time and space as they are transferred from one computer to another. Norton AntiVirus Scanner cannot repair viruses within a compressed file until you uncompress it.

In this case, the safest option is:

Abort:	Aborts the download. The file will not be saved to your local drive. You will need to download the file from a different site.

A less safe option is:

Ignore:	Continues the download and continues scanning the compressed file. You are notified each time a new virus is found. (You may have one or many infected files within the compressed file.) Each time a new virus is identified you can choose Info and find out about the virus. This may influence your decision as to whether or not to Abort the download.

	You are downloading one or more virus-infected files onto your disk. You should not execute or distribute any virus-infected file until it has been repaired. You will need to save this compressed file to a temporary folder, uncompress it, and attempt to repair each individual virus-infected file. If a file cannot be repaired, you will have to delete the file and replace it with an uninfected copy.

The least safe option is:

Ignore all:	Norton AntiVirus Scanner stops scanning the compressed file and the download continues uninterrupted by further alerts. In other words, you will know that one file within the compressed file is infected with least one virus (the one that caused the alert box to appear) but you won't know if there are other infected files.

	You are downloading one or more virus-infected files onto your disk. You should not execute or distribute any virus-infected file until it has been repaired. You will need to save this compressed file to a temporary folder, uncompress it, and attempt to repair each individual virus-infected file. If a file cannot be repaired, you will have to delete the file and replace it with an uninfected copy.

Info:	The Virus Information dialog box shows more details about the virus.

About Norton AntiVirus Scanner

Norton AntiVirus Scanner is a comprehensive virus prevention, detection, and elimination software available for your computer. Use Norton AntiVirus Scanner to scan an entire disk (or disks), a particular folder and all of its files, or a specific file for virus infection.
🛈 　　　If you work in a high-risk environment where you frequently exchange floppy disks with other users or regularly download files from bulletin boards, you should scan floppy disks and new files before first use and scan your hard disks weekly.

Click here {button ,AL("NAVDSK_I0010;NAVDSK_I0060;NAVDSK_V0010")} for more information.

How Norton AntiVirus Scanner works

Symantec engineers work around the clock tracking reported outbreaks of computer viruses to identify new viruses. Once identified, information about the virus (a virus signature) is stored in a virus definitions file. When Norton AntiVirus Scanner scans your disk and files--initiated with the Scan Now button in the main window --it is searching for these telltale signatures. If a file is found that has been infected by one of these viruses, Norton AntiVirus Scanner has the tools to eliminate the virus automatically.
Each time a new virus is discovered, its virus signature must be added to the virus definitions files by the Symantec engineers. For this reason, you should update your virus definitions files regularly (a new file is available monthly from Symantec).

Click here {button ,AL("NAVDSK_I0070;NAVDSK_I0025")} for more information.

What is a computer virus?

A computer virus is, simply, a program designed to attach itself to another computer program. Thereafter, whenever the infected program is run, the attached virus program is activated and attaches itself to yet other programs. For example, a computer virus, which your computer may get by running an infected program from a borrowed floppy disk, infects other programs on your disk. A computer virus, like a biological virus, lives to replicate.

Some computer viruses, in addition to replicating, are programmed specifically to damage data by corrupting programs, deleting files, or even reformatting your entire hard disk. Most viruses, however, are not designed to do serious damage; they simply replicate or display messages.

Click here {button ,AL("NAVDSK_I0030;NAVDSK_I0040")} for more information.

What viruses do and don't do

🛈 Computer viruses infect executable files, such as word processing programs, spreadsheet programs, computer games, or operating system programs.

🛈 Viruses can also "infect disks" by attaching themselves to special programs in areas of your disks called boot records and master boot records. These are the programs your computer uses to start up.

🛈 Computer viruses do not damage hardware, such as keyboards or monitors. Though you may suffer strange behaviors such as screen distortion or characters not appearing when typed, a virus has, in fact, merely affected the programs that control the display or keyboard. Not even your disks themselves are physically damaged, just what's stored on them. Viruses can only infect files and corrupt data.

Click here {button ,AL("NAVDSK_I0025;NAVDSK_I0040")} for more information.

Virus risk under Windows NT

There are two main types of viruses:

🛈 Program viruses, which infect application, operating system and other executable files. Windows NT has inherited all MS-DOS program viruses, which do infect Windows NT executables. However, there are not yet any Windows NT specific viruses. Under Windows NT, DOS programs are run in DOS memory space. While in a DOS session, they continue to infect other programs and can interfere with DOS operations. Generally, program viruses remain active in your computer's memory after an infected program is executed until you end the DOS session.

🛈 Note that Norton AntiVirus Scanner scans Microsoft Word documents also when scanning program files. Although these are not program files, they can be infected by a new class of viruses called "Macro viruses."

🛈 Boot viruses are a particular risk under Windows NT. A boot virus activates at system startup, before the Windows NT operating system is loaded. If NT can load despite a boot virus infection, the virus is disabled in memory. Your computer is still infected, but the virus does not show its usual symptoms or spread while Windows NT is running. Many times, however, you won't be able to start up at all. If you boot into MS-DOS on a multi-boot system, the virus is not disabled.

🛈 All hard and floppy disks have boot records, whether or not they also contain operating system files. A disk does not have to be bootable to be infected by a boot virus; data disks can contain boot viruses too. A typical way a computer gets a boot infection is to restart with an infected floppy disk in the drive. Even if the floppy is not a boot disk, the virus activates and spreads.

🛈 Some viruses (called multipartite viruses) fall into both categories.   In addition, particular viruses in these categories may be categorized as stealth or polymorphic. Known viruses are categorized in the Virus List by how often you find them, what they infect and how they behave.

Click here {button ,AL("NAVDSK_I0025")} for more information.

Removing viruses

There are two ways to remove a virus from your computer:

- Repair the infected file, <u>boot record</u>, or master boot record.
- Delete the infected file from the disk and replace it with an uninfected copy. (If you do not have an uninfected backup copy of the file, the original program disk, or online access to the file, you need to get a new copy of the file.)

Click here {button ,AL("NAVDSK_I0010;NAVDSK_V0340;NAVDSK_V0335")} for more information.

Responding to alerts

Norton AntiVirus Scanner alerts you when a virus is found during a scan.

If an alert box appears on your screen:
1. Read the message in the alert box to understand the type of problem that was found.
2. Then follow the instructions for one of the following conditions:

- A file or boot record is infected Repair an infected file or boot record
- A downloaded file is infected   Remove viruses from downloaded files
- A file cannot be repaired   Delete an infected file
- A compressed file is infected   Work with compressed files
- A compressed downloaded file is infected   Remove viruses from downloaded compressed files

About updating virus definitions

Updated virus definitions files are available monthly on several different bulletin board systems or they can be mailed to you. The file you receive is a compressed archive that contains several files. Its name, which changes from month to month, uses the following form: *mm*NAV*yy*.ZIP where *mm* is the month and *yy* is the year.

Click here {button ,AL("NAVDSK_V0250")} and choose "Install new virus definitions files".

CompuServe

To directly access the Symantec Forum:
- Type the following at any ! prompt: **GO SYMNEW**

The files are located in the Norton AntiVirus library.

America Online

To access the Symantec bulletin board:
1. Choose **Keyword** from the GoTo menu.
2. Type **SYMANTEC**.
3. Click Virus Control Central.
4. Click Virus Definitions Library and follow the on-screen directions.

Internet

The current virus definitions files are located in the Symantec File Transfer Protocol (FTP) Internet site.

To use the FTP site:
- Access **ftp:// ftp.symantec.com**.

The files are located in the **/public/win95_nt/nav/** folder.

To use the FTP site through the World Wide WEB:
1. Access **http:// www.symantec.com**
2. Click AntiVirus Research Center.
3. Click Download Updates.
4. Click Norton AntiVirus and follow the on-screen directions.

Microsoft Network

To access the Symantec service:
1. Choose Go To from the View menu.
2. Type **SYMANTEC**.
3. Double-click Support Solutions.
4. Double-click Norton AntiVirus 95 (the same files are used for Windows NT.).
5. The virus definitions are located in the File Library.

Symantec BBS

Settings for the Symantec BBS are:
8 data bits, 1 stop bit; no parity

To contact the Symantec BBS, use the following telephone number:
- (541) 484-6669 [24 hrs.]

To access definitions from the initial menu of the Symantec BBS:
1. Press **F** to get a file.
2. Press **N** to get the latest NAV definitions.
3. Follow the on-screen directions to download the file.

To go directly to the file library:
1. As soon as you log in, type: /GO NAVNT
2. Follow the on-screen directions to download the file.

Virus Definitions Update Disks

You can order virus definitions update disks from Symantec to arrive by mail. This service requires a fee:
- In the United States, call (800) 453-1149.
- Outside the United States, contact your local Symantec office or representative.

Click here {button ,AL("NAVDSK_V0250")} for more information.

About the Virus List

You can see which viruses Norton AntiVirus Scanner detects by viewing the list of virus names. You can also view descriptions of particular viruses, including their symptoms and aliases.

To prevent newly discovered viruses from invading your computer, you should update your virus definition files regularly. Norton AntiVirus Scanner uses the information in these virus definition files to detect viruses during scans. Updated virus definition files are available monthly. Once installed, you see the new names in the Virus List.

Click here {button ,AL("NAVDSK_I0070")} for more information.

About the Activity Log

The Activity Log file contains details about Norton AntiVirus Scanner activities, such as when problems were found and how they were resolved. From the Activity Log dialog box you can:

- Click Print to print the Activity Log to a printer or a file.
- Click Filter to display specific events, such as all virus detections.
- Only the entries currently displayed in the list box are printed. If you filter the Activity Log, only the filtered entries are printed.
- Click Clear to delete all of the entries in the Activity Log.

From the Activity Log tab in the Options dialog box, you can limit or increase the size of the Activity Log. When the log reaches its maximum size, it begins to overwrite the earliest entries.

Click here {button ,AL("NAVDSK_V0215;NAVDSK_V0220;NAVDSK_V0225")} for more information.

About the Scheduler

NOTE: This feature is available when you purchase the full Norton AntiVirus for Windows 95 or under the complete Windows NT freeware product.

About Exclusions

Norton AntiVirus Scanner uses the entries in the exclusions list in all scans it performs. You assign exclusions to items: drives, folders, groups of files, or single files.

ℹ️   If you move or rename a file, you automatically invalidate its exclusions.

Click here {button ,AL("NAVDSK_V0040")} for more information.

About Security under Windows NT

Windows NT, because of its flexibility, presents special problems for virus control. Under the NT file system (NTFS), you can set different access permissions to the file, folder, or object (such as the boot records) level for each user or group. Not all users will be able to scan all items.

If an access denied dialog box is ever displayed, first make sure that you have the necessary permissions for the operation (scan, repair, or delete) you are trying to perform on that boot record, file, or folder.

Note that you may find the following rights and privileges apply to boot records:

In order to scan boot records, administrator-level rights are required (even on stand-alone computers).

For shared computers, file access is often limited to one's own files. Only one user must be designated as administrator with rights to scan the system files and boot records.

For servers, an administrator must initiate comprehensive scans but you can scan files on any drive to which you are connected.

Credits

Product Management

Lily Duong, Jeff Leeds, Sharon Ruckman, Germaine Ward

Development Team

David Allee, Darren Chi, Alexander Freylicher, Barry Gerhardt, Carey Nachenberg, Yoko Vang, Gary Westerland

Quality Assurance Team

Bob Kolosky, John M. Moldenhauer, Sam Porterfield, Ken Sackinger, Ray Waldin

Documentation and Online Help

Elizabeth Anders, Kurt Ament, Annette Brown, Alfred Ghadimi, Karen Goldsmith, Robert Hoffman, Romey Keys, Sheelagh O'Connor, Vickie Von Bergen, Laura Weatherford

Technical Support Team

Caroline Cento, Michael Fischer, Christine Frazer, Brett Johnson, Todd Kieser, Michael Logue

Engineering Services Team

Ardeshir Babak, Will Jobe, Jo Anne Johnson, James Reardon,

Virus Definitions

Jonathon Allee, Gioconda Becerra, Chris Brown, Matt Candelaria, Shane Coursen, Philip DeBats, Don Duperault, Chris Formulak, Kevin Marcus, Charles Renert, David Shannon, Jeffrey Sulton, John Wilber

External Test

Alena Cespivova, Jo Anne Johnson, Robert Stones

SWAT Team

Eric Gustafson, Ron Hayes, Neils Johnson, Howard Mora, Dan Sackinger, Scott Smith