Norton AntiVirus main window

 Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

From the Norton AntiVirus main window you can do the following to detect viruses:

- Click Scan Now to scan selected drives immediately. (You don't have to close help. Simply click in the NAV main window, then click Scan Now.)
- Choose the Scan menu and select File or Folders to scan specific files or folders.

You can also click any of the buttons to access more NAV features:

- Click Options to display settings tabs where you can customize Norton AntiVirus features.
- Click Virus List to displays the Virus List where you can view information about the viruses you are protected against.
- Click Scheduler to display the Norton Program Scheduler where you can schedule scans or other events.
- Click Activity Log to display a history of Norton AntiVirus activities (for example, it lists each incident of a known virus detection or LiveUpdate).
- Click LiveUpdate to automatically update virus definitions.

To get Help, do one of the following:

- Click Help on the menu bar to display the Contents (Help Topics).
- Click the Help button to display to get context-sensitive help.
- Position the cursor over any option in the NAV main window, click the right mouse button, and choose one of the following:

What's This? Gives a brief description of the option.
Contents: Gives you access to Norton AntiVirus help topics and a Glossary of terms.

 Note that you can keep help open on your desktop by minimizing the help window or by simply clicking back and forth between help and the product. When you have read the information you need, simply click in the open NAV window. Then, if you need help again, simply reopen help by clicking on it in the taskbar below or by clicking in the help window itself.

Click here
{button ,AL("NAVDSK_I0000;NAVDSK_V0020;NAVDSK_V0055;NAVDSK_V0015;NAVDSK_V0045;NAVDSK_V0050;NAVDSK_V0010;NAVDSK_V0075")} for more information.

Virus Information

 Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The Virus Information dialog box contains information about the selected virus. If you are in the process of eliminating a virus, return to the Repair Wizard or other dialog box and repair or delete the virus. Below 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

 Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

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 and reports inoculation changes. Click Close to conclude this scan.

Here is some additional information about the scan results:

Scanned: Indicates whether memory, 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

 Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

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 (in Windows or DOS) 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

Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

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

- infected or uninoculated files or boot records
- files or boot records whose inoculation data has changed

The Status indicates whether or not an infected file was repaired or deleted, or if it remains infected. It also records inoculation data.

What to do if a virus was found

1. If a file is infected, or its inoculation data has not changed for legitimate reasons (such as an upgrade of the software), click Repair to have NAV attempt to restore it.
2. If an infected file or a file cannot be repaired, click Delete to remove the file.

What to do if an uninoculated file was found

1. If a file has not been inoculated, click Inoculate or Exclude.

   Inoculating the file gives you added protection. Excluding the file from future checks for inoculation data is more risky. You are reducing the level of protection.

What to do if an inoculation change was found

1. If a file's inoculation data has not changed for legitimate reasons (such as an upgrade of the software), click Repair to have NAV attempt to restore it.
2. If a file's inoculation data cannot be repaired, click Delete to remove the file.

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.

What to do next

1. 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 (resolved), and what was left unresolved.

2. Exit Norton AntiVirus 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).

In the rare cases that Norton AntiVirus cannot repair or delete the file, exit Norton AntiVirus and delete the file manually. Then replace the file with an uninfected copy.

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

Virus List

The Virus List displays a list of viruses that Norton AntiVirus can detect and, in most cases, eliminate.

 It is most important to update your Virus List once monthly because new viruses are discovered all the time. If you have a modem or an Internet connection, simply click LiveUpdate in the Norton AntiVirus main window. If you do not have a modem, see the User's Guide for directions on how to obtain new virus definitions from Symantec and how to update the Virus List.

To find a virus on the list:

- Use the scroll bar or type a few letters of the virus name to initiate the smart search feature to find the virus you're looking for.

 To reduce the number of viruses you have to search through, choose a type of virus from the Display drop-down list box. For example, you may want to filter the Virus List to display only boot viruses or macro viruses.

 If a virus is not found on the list, the virus. One other possibility is that the virus name may be different from what you expected. For example, the virus commonly known as Michelangelo is actually called Stoned. Michelangelo.D.

Click here
{button ,AL("NAVDSK_I0005;NAVDSK_V0255;NAVDSK_V0250;NAVDSK_V0260;NAVDSK_V0265;NAVDSK_V0270;NAVDSK_I0040")} for more information.

Virus Information

 Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The Virus Information dialog box contains information about the characteristics of the virus. If you are in the process of eliminating a virus, return to the Repair Wizard or other dialog box and repair or delete the virus.

Virus characteristics are explained below.

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.

System Integrity

 Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The System Integrity dialog box notifies you about changes in system files that may indicate the presence of a virus. Your options are:

Repair: Repairs a file or boot record and returns the file to its original state.

Inoculate: Reinoculates the item. (Choose this option only if you expected the reported change. Reinoculating means you are recording the "fingerprint" of the file as it is now.)

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

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

Virus Found

 This Virus Found alert appears when a known virus has been detected during a manual or scheduled scan.

What to do next

1 If a file is infected, click Repair to have Norton AntiVirus try to remove the virus and return the file to its original state.

2 If a file cannot be repaired, click Delete and, then, replace it with a clean (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.

 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 is not configured to allow that option or it may not be possible.

Repair: Click to have Norton AntiVirus 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 will 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 to notify you immediately when it detects a virus or possible virus on your system during a manual or scheduled scan. If you would like NAV to perform the entire scan and then summarize the problems, click Advanced on the Scanner tab in the Options dialog box and uncheck the Immediate Notification option. This allows you to use the Repair Wizard to eliminate the viruses for you.

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 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 cannot be recovered. After you have deleted the file, you can replace it with an uninfected copy. If you do not have a clean original or backup copy of the file, you may need to get one from the software manufacturer. Choose Delete All to have Norton AntiVirus delete all the infected files found during the scan.

 Note that Norton AntiVirus also scans Microsoft Word and Excel documents when scanning program files. Although these are not program files, they do contain code and can be infected by a new class of viruses called Macro Viruses.

You should not leave an infected file on your computer. NAV can repair most infected files. However, in case a file cannot be repaired, you must delete it from your disk. Be sure to get into the habit of keeping original disks in a safe place and making backup copies of your files.

Activity Log

 Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

Use the Activity Log to view a history of Norton AntiVirus 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, the Activity Log 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 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 main window.

Filter Activity Log

You can filter the Activity Log to display only specific categories of entries, such as Known Virus Detections. Specify the types of events to display by checking the appropriate check boxes.

For more help, position the cursor over any option on the tab, click the right mouse button, and choose What's This? to see a description of the option.

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 certain activities. You may want to exclude a program file that changes frequently for legitimate reasons.

To exclude files prior to scanning:

From the Norton AntiVirus main window, click Options. Then use the Exclusions tab to specify which files and virus-like activities to routinely exclude from scans. Be careful when you do this. You are reducing your level of protection.

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

Inoculation

When you inoculate a program file or boot record, Norton AntiVirus records critical information about it (similar to taking a "fingerprint"). On subsequent scans, NAV checks the file or boot record against the fingerprint and notifies you if there are any changes that could indicate the presence of an unknown virus.

- To ensure maximum protection, be sure that you have checked Inoculate Program Files on the Inoculation tab.
- You are alerted to any change in the inoculation data. You may want to uninoculate a file if changes in program configuration are written so frequently that you are always being alerted to the inoculation change and have to respond to requests to reinoculate.

To inoculate or uninoculate a file or files:

1 Click Inoculate item or Uninoculate item.

2 Use one of the following methods to select a file or files:

- Click the browse button to display a dialog box where you can locate a specific file or files.
- Type the pathname for the file, group of files, folder, or drive in the Item text box. Just enter the folder name to inoculate or uninoculate all files in the folder. Or, use a wildcard to specify a group of files.

3 Click OK to save settings and exit the dialog box.

Click here {button ,AL("NAVDSK_I0075")} for more information.

System inoculation

When you inoculate a program file or boot record, Norton AntiVirus records critical information about it (similar to taking a "fingerprint"). On subsequent scans, NAV checks the file or boot record against the "fingerprint" and notifies you if there are any changes that could indicate the presence of an unknown virus.
Only boot records on your startup disk and program files can be inoculated. Norton AntiVirus uses the Program File Extensions list to determine if a file can be inoculated.
You are alerted to any change in the inoculation data. You may want to uninoculate a file if changes in program configuration are written so frequently that you are always being alerted to the inoculation change and have to respond to requests to reinoculate.

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

Inoculate file

When you inoculate a program file or boot record, Norton AntiVirus records critical information about it (similar to taking a "fingerprint"). On subsequent scans, NAV checks the file or boot record against the "fingerprint" and notifies you if there are any changes that could indicate the presence of an unknown virus.

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

Inoculation changed

- If you are certain that the file or boot record has changed for legitimate reasons, click Inoculate to generate new inoculation information. Otherwise, use one of the following options to resolve the inoculation change:

- Note that boot records and system files change legitimately in very few situations.
- If you suspect a virus, click Repair to return the file or boot record to the way it was when you last inoculated it.
- If you suspect a virus in a program file and have an uninfected backup copy of the file, click Delete; then replace it with the uninfected copy.

Note that the Delete button is dimmed if the item is a boot record.

- If you do not want to inoculate the file and you do not want future notifications about inoculating this file, click Exclude.
  Be careful! Excluding files means you are reducing your level of protection.

If the file cannot be repaired or deleted:

1. Click Stop.
2. Exit Norton AntiVirus.
3. Restart your computer from your NAV Rescue Disk, labeled Norton AntiVirus Emergency Boot Disk, and scan again.
4. If you get the same results, delete the file from your disk manually (from the Windows Explorer) and replace it with a clean copy.
5. Inoculate the file.

Click here {button ,AL("NAVDSK_I0075;NAVDSK_V0230")} for more information.

Scanner Settings

- Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The Scanner tab allows you to choose settings that determine:

- What to scan
- How Norton AntiVirus should respond when a virus is detected (If you select Custom response, you can then click Customize to choose how Norton AntiVirus should respond to particular types of virus infections: file, boot record, and macro viruses.
- What buttons to display when NAV prompts you about a problem found during a manual scan

We recommend that you leave the preset options as they are (all options for What To Scan are checked and Program files is selected). However, for maximum protection, click All Files instead of Program Files.

Your other options on this screen are the buttons:

- Click to display the Heuristic Scanning options dialog box to enable Bloodhound technology, which can dramatically increase your protection against new and unknown viruses.
- Click Advanced to display a dialog box where you can make choices about network scans and what to scan at startup.

Click here
{button ,AL("NAVDSK_I0065;NAVDSK_V0080;NAVDSK_V0085;NAVDSK_V0092;NAVDSK_V0095;NAVDSK_V0065;NAVDSK_V0055;NAVDSK_V0075;NAVDSK_V0020")} for more information.

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.
- The file extensions list contains the majority of extensions used for program files. Norton AntiVirus only scans files with extensions on this list.
- Note that Norton AntiVirus also scans Microsoft Word and Excel documents when scanning program files. Although these are not program files, they do contain code and 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 box where you can add them to the list. Then NAV can scan them and protect them against infection.
- Other options are:

  - Click Remove to delete a highlighted file extension.
Be careful, however. Removing extensions from the list reduces your protection against viruses.
  - Click Default to return the file extensions list to the preset options.

Scanner Advanced Settings

- Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

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

- Whether you want to Allow Network Scanning. This option has to be checked for network drives to appear in the Norton AntiVirus main window Drives list box.
- Whether you want to Allow Scanning to be Stopped while the scan is in progress.
- Whether you want Immediate Notification of a virus found during a manual or scheduled scan. This forces you to take action on each alert as it occurs. When this option is not checked, the Repair Wizard appears after it has completed a scan and summarized all of the problems found.
- Whether to always scan floppy disks instead of having to specify this option every time you perform a manual scan. Check this for maximum protection.

Click here {button ,AL("NAVDSK_V0055;NAVDSK_V0075")} for more information.

Auto-Protect Advanced Settings

- Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The Auto-Protect Advanced Settings dialog box lets you select which virus-like activities to allow or disallow.

- For maximum protection, you should also change all of these options to Prompt. This option allows you to decide which activities are legitimately performed by each file.
- You should also keep the preset options in the Check Floppies group box. (The first two options should be checked.)

Click here {button ,AL("NAVDSK_I0045;NAVDSK_V0140")} for more information.

Auto-Protect Settings

Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The Auto-Protect tab allows you to customize the automatic protection feature of Norton AntiVirus. This feature provides your first line of defense against virus infection.

If you performed a complete setup of Norton AntiVirus, leave the preset options as they are. However, for maximum protection:

1. Check all options in the Scan A File When group box. (Note that the Opened option includes when a file is copied or moved.)
2. Click All Files instead of Program Files.
3. Always make sure that Load Auto-Protect At Startup is checked.

Click here {button ,AL("NAVDSK_V0135;NAVDSK_V0140;NAVDSK_I0010")} for more information.

Auto-Protect Virus Sensor Settings

- Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The Auto-Protect Virus Sensor Settings dialog box allows you to monitor for unknown viruses which are viruses for which Norton AntiVirus does not yet have a definition.

- For maximum protection:

  - Make sure that Use Virus Sensor Technology is checked.

  - Do not check Exclude.

- You can also protect against unknown viruses by inoculating files.

Click here {button ,AL("NAVDSK_V0050;NAVDSK_I0075;NAVDSK_V0135")} for more information.

Startup Settings

- Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The Startup tab allows you to define what is scanned automatically when you start up your computer.

- If you performed a complete setup of Norton AntiVirus, use the preset options.
- For maximum protection, check all the options in the What To Scan group box.
- You can also change the keys you can use to bypass startup scans. This bypass feature is available whenever you start up the computer if you have selected keys.

    - We don't recommend that you bypass the startup scan. It is one of your best first lines of defense against virus infection.

Inoculation Settings

- Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The Inoculation tab allows you to customize inoculation options. If you performed a complete setup of Norton AntiVirus, use the preset options. (Inoculate Boot Records And System Files is checked.) However, for maximum protection, you can:

1. Check Inoculate Program Files and Inoculate Files On Floppies.

   - If you choose to inoculate program files, you are notified whenever you upgrade the software. This could result in many inoculation alerts. You may want to change the When An Inoculated Item Has Changed option from Prompt to Inoculate Automatically.

2. You can also type in a new path for the inoculation data. (The preset path is \NCDTREE.) Just specify the folder; the drive is already determined for you because each drive contains its own inoculation data.

Click here {button ,AL("NAVDSK_I0075;NAVDSK_V0050")} for more information.

Alerts Settings

- Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The Alerts tab allows you to:

- define how Norton AntiVirus informs you that it has detected a virus or possible virus.
- alert Norton AntiVirus NLM I (if present)
- forward alerts to Norton AntiVirus NT alert services

These options apply to all scans that Norton AntiVirus performs (scans you initiate, scheduled scans, and scans performed automatically by Auto-Protect).

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

Activity Log Settings

Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The Activity Log tab allows you to customize how to display the history of Norton AntiVirus activities. If you performed a complete setup of Norton AntiVirus, the preset options record detections of known viruses, completion of scans, 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 entries are deleted and overwritten with new ones.

We recommend that you use the preset options.

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

Exclusions Settings

- Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The Exclusions tab allows you to exclude a condition or virus-like activity that would normally be detected except that you have told Norton AntiVirus not to check for this activity in a particular file. Setting exclusions doesn't mean "don't find viruses;" it means that you let some activity proceed because you know a virus did not cause it. Exclusions are for files that are known to change often for perfectly good reasons. Because these files change often, Norton AntiVirus warns you each time, but excluding them allows the changes to occur without the constant warnings.

- You assign exclusions to items: drives, folders, groups of files, or single files. Each item can have more than one exclusion.
- When you click Remove, the exclusion is immediately removed from the list. There is no confirmation request.
- Be careful! Assigning exclusions reduces your level of protection.

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, you have reduced the level of protection against viruses.

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

General Settings

- Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

The General tab settings apply to all scans: scans you initiate, scheduled scans, and scans performed by Auto-Protect.

- Check Back Up File Before Attempting A Repair to have NAV 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.

    - All files with the backup extension are added automatically to the Exclusions List so they are not reported again during a scan. The file type appears as "Virus Infected File" when you list files using the Windows Explorer.

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

Deny Access

If you are attempting to access a floppy disk drive and are denied access, there is no disk in the drive. If you are attempting to access a hard disk drive, you need to resolve the problem that is causing you to be denied access (for example, on a network you may not have access rights).

You are about to overwrite an existing file with the file you're printing to disk.

- You can do one of the following:
- 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.

Set/Change Password

Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

Before setting or changing your password, make sure you've selected the items you want protected.

Passwords can be from 1 to 16 characters in length and are not case-sensitive (a is the same as A).

Old Password: If this is the first time you've created a password, this text box is dimmed. If you're changing a password, enter the old one here.

New Password: Enter the new password in the text box. As you enter the new password, Norton AntiVirus replaces the characters in your password with asterisks (*) on the screen for security.

Confirm New Password: Enter the new password again in the text box.

Inoculation

When you inoculate a program file or boot record, Norton AntiVirus records critical information about it (similar to taking a "fingerprint"). On subsequent scans, NAV checks the file or boot record against the "fingerprint" and notifies you if there are any changes that could indicate the presence of an unknown virus.

- You are alerted to any change in the inoculation data. You may want to uninoculate a file if changes in program configuration are written so frequently that you are always being alerted to the inoculation change and have to respond to requests to reinoculate.

To inoculate or uninoculate a file or files:

1 Click Inoculate Item or Uninoculate Item.

2 To select the file or files, do one of the following:

- Click the browse button to display a dialog box where you can locate a specific file or files.
- Type the pathname for the file, group of files, folder, or drive in the Item text box, enter the folder name to inoculate all files in the folder, use a wildcard to specify a group of files.

3 Click OK to save settings and exit the dialog box.

Click here {button ,AL("NAVDSK_I0075")} for more information.

Password Settings Reference

Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

Use these settings to define what features you want password-protected, and to set or change the password.

Password Protect: Activates the Set Password button so you can open the Set Password dialog box and set a password. Turning this button off removes all password protection.

Maximum Password Protection: Sets password protection for all Norton AntiVirus features listed. You are not able to access any of these features without the password.

Custom Password Protection: Sets password protection for the items you select in the list box. You are not able to access any of these features without the password.

Virus Found in Download

- Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

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 that 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 is not 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)

- Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

If the Virus Found in Download dialog box is displayed and the file has been determined to be a "compressed" file (for example, 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 cannot repair viruses within a compressed file until you uncompress it.

In this case, the safest option is:

Abort: Aborts the download. The file is not 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 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 at 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.

Verify Password

You must enter your password before you can change any protected Norton AntiVirus options settings.

Network Browser

- Right-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.
- You can select Microsoft domains, workgroups, servers, or local workstations as network alert targets. When a domain or workgroup is targeted, every member machine receives the alert.
    - When typing a domain name, add an asterisk (for example, Duluth*); when typing a server name, precede it with two backward slashes (for example, \\Rm315).
- You can add NetWare servers alert targets. When a virus is detected on the workstation, a notification is sent to the NetWare server. When Norton AntiVirus for NetWare (NAV for NetWare) is running, it takes action based on how it has been configured to respond to a workstation virus alert.
- You can relay alerts to one or more remote workstations. By relaying all alerts to a single remote machine, you can effectively establish a dedicated alert server that centrally processes all alerts, as well as centralize the alert log. (All packets received from the machines originally configured to receive the alerts are automatically added to the remote machine's Windows NT event log.)

Click here {button ,AL("NAVDSK_F0198;NAVDSK_F0185;NAVDSK_F0186")} for more information.

Heuristic scanning options

Norton AntiVirus includes a new technology called Bloodhound to dramatically increase your virus protection against new and unknown viruses. You can drag the pointer to increase Bloodhound's sensitivity to possible viruses.

Custom Response settings

Custom Response lets you specify different actions for file, macro, and boot virus detections.

Delete All files

Click Delete to confirm that you want to delete all files.

As soon as you install Norton AntiVirus...

YOU ARE ALREADY PROTECTED AGAINST VIRUSES

From this main window you can do the following:

- Choose the Scan Now button to scan selected drives immediately.
- Choose a menu command to scan specific files or folders.
- Click a button to change options, schedule scans, or view information.
- Click LiveUpdate to automatically update virus definitions and program files.

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

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

Click one or more drive types that you want to scan now. Or, click any checked option to exclude it from the scan. These selections return to the preset options when you exit Norton AntiVirus.

- If the All Network Drives option is dimmed, you may need to enable Allow Network Scanning 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 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 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 files or boot records.

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

Click Inoculate to display the Inoculate File dialog box, where you can inoculate this file or all files or boot records. This button is dimmed if there were no inoculation changes.

Click Exclude to display the Exclude File dialog box, where you can choose to keep this file from being checked during future scans.

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 (resolved), 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 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.

Choose Yes to erase everything in the Activity Log. Otherwise, the log expands indefinitely or until it reaches the maximum size (50K by default).

- To change the maximum size of the Activity Log, click Options in the Norton AntiVirus 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 one of the following categories of viruses: all, common, program, boot, stealth, polymorphic, multipartite, Windows, macro, and agent . For a definition of each of these virus types, click Help and click Types of Viruses.

The Virus List includes the names of all the viruses that Norton AntiVirus can detect and, in most cases, eliminate. NAV uses virus definitions (special programs used to identify viruses) to find and get rid of viruses. Since new viruses are being created all the time, you need to update the Virus List by adding new virus definitions provided by Symantec monthly at no charge. Click LiveUpdate from the Norton AntiVirus main window to automatically acquire new virus definitions and update the Virus List.

- To search for a virus by name, click inside the Virus List and begin by entering the first letter to display the Smart Search text box, where you can continue entering the virus name. The text box appears at the bottom of the Virus List.

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.

Comments describes what the virus does to your files or boot records.

Click Exclude to exclude the file from further checks. Be careful! Excluding a file reduces your level of protection.

Click Repair to have Norton AntiVirus restore the file to its original state.

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 with a clean (uninfected) copy.

- Files deleted by Norton AntiVirus cannot be recovered. If you do not have an original or backup copy of the file, you need to acquire one from the software 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 and/or return the identified file to its original state. Click Repair or Repair All to have Norton AntiVirus repair one or all of the files identified during the scan.

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

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

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

- Files deleted by Norton AntiVirus cannot be recovered. If you do not have an uninfected original or backup copy of a deleted file, you need to acquire one from the software manufacturer.

Click Delete to have Norton AntiVirus delete this file. Files deleted by Norton AntiVirus 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 delete all the infected files found during the scan. After you have deleted the files, you need to replace them with clean (uninfected) copies. If you do not have uninfected original or backup copies of the files, you need to acquire them from the software manufacturer.

Click any of the items listed 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 in between specified dates. Click an option in the Dated drop-down list box, then enter the date or dates to define the scope.

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

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

From this Exclude File dialog box you can exclude this file from future checks for known viruses. You can choose to do this for files that can change frequently due to configuration.

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

- The item is added to the list of excluded files displayed on the Exclusions tab.

The Inoculate File dialog box allows you to inoculate files during a scan.

- When you inoculate a program file or boot record, Norton AntiVirus records critical information about it (similar to taking a "fingerprint"). On subsequent scans, NAV checks the file or boot record against the fingerprint and notifies you if there are any changes that could indicate the presence of an unknown virus.

Click Inoculate to inoculate the selected file only.

Click Inoculate All to inoculate all uninoculated files found during this scan.

The System Integrity dialog box notifies you about changes in system files. Your options are:
Repair: Returns a file or boot record to its original state.
Inoculate: Reinoculates the item. (Choose this option only if you expected the reported change. Reinoculating means you are recording the "fingerprint" of the file as it is now.)
Continue: Continues the scan without responding to the change in your system file.
Stop: Stops the scan and returns you to the Norton AntiVirus main window.

Click Continue to continue the scan without responding to the alert.

Click Inoculate to inoculate the file or files.

Click Inoculate to inoculate the file or files.

Click Exclude to exclude the file from being checked for inoculation data.

Click Delete to delete the file.

Click Continue to continue without taking any action.

Click Info to display information about the virus.

Click Repair to restore the file to match its "fingerprint" taken when you first inoculated the file.

Click Delete to delete the file.

Click Inoculate to reinoculate the file.

Click Exclude to exclude the file from further checks for inoculation changes.

Click Stop to stop the operation without taking any action.

Click Continue to continue without taking any action.

Click Stop to stop the operation without taking any action.

The Comments describe what the virus does to your files or boot records.

Summary: Reports if infected files, infected boot records, or inoculation issues were found.
Items Scanned: Lists the drives, directories, or files that were scanned.
File Type: Lists the types of files that were scanned.
Inoculation: Reports whether inoculation was active or disabled.
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 memory, master boot record, boot records, or files were scanned.

Infected: Lists what items, if any, were infected.

Cleaned: Lists whether infected items were cleaned.

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. Also, inoculation status is reported. For example, the status can indicate whether a boot record or program file is uninoculated or if its inoculation data has changed. Use this dialog box to review what was found (for example, infected item or inoculation issue) and how Norton AntiVirus responded.

The Problems Found dialog box summarizes the current scan. The Status column indicates whether or not an infected file was repaired, deleted, or remains infected. Also, inoculation status is reported. For example, the status can indicate whether a boot record or program file is uninoculated or if its inoculation data has changed.

- 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 can cause other files to become infected.

Choose 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 all of the items.

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, including 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, including .doc, .dot and .xls files that can contain macro viruses.

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 can increase slightly if you have many compressed files. Note that compressed files within compressed files are not scanned. This option is preset for maximum protection.

Choose an option to specify how to respond when a virus is found. Choose 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 also need to specify which buttons to display when an alert appears.

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 or from a BBS or other source). Files deleted by Norton AntiVirus cannot be restored.

Shutdown Computer shuts down your computer when a virus is detected. You must then restart your computer. To remove a virus, you must use your NAV Rescue Disk, labeled Norton AntiVirus Emergency Boot Disk, to both reboot your computer and scan again to find and remove the virus.

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

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 appears only 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. Use sparingly because 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 this option to Allow Network Scanning. This allows you to highlight and choose a specific network drive or All Network Drives from the main window. If this option is not checked, you can't perform network scans.

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 option allows you to respond immediately, without waiting until the scan is completed.

Specifies the drives that you want automatically selected in the Drives list box when you start Norton AntiVirus.

All floppy disk drives and other removable media are automatically selected to be scanned when you initiate a scan.

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

Check this option to automatically select all network drives when you start Norton AntiVirus. This option is dimmed unless you have checked Allow network scanning, above.

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

Click New to display a dialog box, where you can add a new extension (you'll be asked to enter the extension's letters).

Click Remove to delete the selected extension.

Choose one of these options to tell Norton AntiVirus when to scan files automatically:
Run: Scans a program file each time you run it.
Opened: Scans files whenever they are opened, such as when you copy a file.
Created: Scans files when they are created on your drive by an installation program or by some other means.

Scans a program file each time you run it.

Scans files whenever they are opened, such as when you copy a file. Also scans files when they are moved.

Scans files when they are created on your drive by an installation program or by some other means (such as downloading a file).

Choose an option to specify which files to scan automatically.

Scans all files that you access. This includes files 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 be infected, including .doc, .dot, and .xls files that may contain macro viruses.

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

Choose what to do when a virus is found.

Choose what to do when a virus is found.

Prompt informs you when a known virus is found and allows you to choose how to respond. If you choose Prompt, you need to select which buttons to display if alerted from the choices below.

Deny Access prevents you from using a file when a known virus is detected.

Repair Automatically restores an infected file or boot record without notifying you. The outcome of the repair is recorded in the Activity Log.

Delete Automatically deletes an infected file as soon as a virus is detected.

- Use caution when selecting this option because files deleted by Norton AntiVirus cannot be restored. You need to replace the file with an uninfected copy.

Shutdown Computer shuts down your computer when a known virus is detected. To remove a virus, you must use your NAV Rescue Disk, labeled Norton AntiVirus Emergency Boot Disk, to both reboot your computer and scan again to find and remove the virus.

If you selected Prompt from the When A Virus Is Found list box, you can select the buttons to display.

Allows you to repair the file or boot record.

Allows you to delete the file.

Allows you to continue accessing the file. If you select the Continue button when a virus is found, you can activate the virus.

Check to allow the Norton AntiVirus Auto-Protect icon to be shown on the task bar.

Check to allow the Norton AntiVirus Auto-Protect feature to be disabled.

Allows you to stop accessing the file. The virus is not activated, but the file is still infected.

Allows you to exclude the file from being checked for known viruses. (Use sparingly because this reduces your protection against viruses!)

Click to display the Auto-Protect Advanced Settings dialog box.

Click to display the Auto-Protect Virus Sensor Settings dialog box.

Use these settings to have Norton AntiVirus check for virus-like activities and scan floppy disks for boot viruses before using them.

Use these settings to determine what Norton AntiVirus does when it detects each virus-like activity.

Prompt informs you when a program tries to perform the activity and allows you to decide whether the activity should continue, stop, or be excluded from future checks. This choice provides you with the best combination of flexibility and protection.

Allows the activity to continue every time without informing you. Chooseing Allow offers you no protection against an unknown virus performing that activity.

Don't Allow prevents the activity from occurring every time it is detected. This selection provides the greatest protection, but can impede your work.

All information on the disk is erased and cannot be recovered. This type of format is generally performed by the software manufacturer. If this activity is detected, it almost certainly indicates an unknown virus at work.

Very few programs write to hard disk boot records. Unless you are specifically using a program that writes to the hard disk boot records, such as FORMAT, this activity probably indicates a virus.

Only a few programs (such as the operating system FORMAT or SYS commands) write to floppy disk boot records.

Some programs save configuration information within themselves. Although this activity often happens legitimately, it could indicate an unknown virus at work.

Many DOS programs change a file's read-only attribute. Although this activity often happens legitimately, it could indicate an unknown virus at work.

Because boot viruses are most likely to spread through floppy disks, it is important to check every floppy disk you use. For maximum protection, ensure that both the first two options are checked.

Checks for boot viruses on each floppy disk you access (such as, when you list the folder, copy a file, write to a file, or run a file).

Checks a floppy disk in drive A: for boot viruses when you shut down your computer.

Also checks a floppy disk in drive B: for boot viruses when you shut down your computer. Check this option if you have a system that can boot from a disk in the B: drive.

Check to have Norton AntiVirus monitor computer activity for the signs of an unknown virus (one for which Norton AntiVirus does not yet have a definition) trying to replicate.

Choose one of the following choices from the list box:
Prompt: Informs you when an unknown virus is found and allows you to choose how to respond. Choose this option to have the most control over what happens to an infected file.
Repair Automatically: Repairs an infected file without asking you. The outcome of the repair is recorded in the Activity Log.
Delete Automatically: Deletes an infected file without asking you.
Be careful if selecting this option. Files deleted by Norton AntiVirus cannot be restored.
Shutdown Computer: Shuts down your computer when an unknown virus is detected.

Informs you when an unknown virus is found and allows you to choose how to respond. Choose this option to have the most control over what happens to an infected file.

Repairs an infected file without asking you. The outcome of the repair is recorded in the Activity Log.

Deletes an infected file without asking you.

- Be careful if selecting this option. Files deleted by Norton AntiVirus cannot be restored.

Shuts down your computer when an unknown virus is detected.

If you selected Prompt in the When An Unknown Virus Is Found list box, you can select the buttons to display.

Allows you to remove the virus and restore the file to its original state.

Allows you to delete the file.

Allows you to continue working without taking action on the file. The file remains infected with the unknown virus.

Allows you to exclude the file from future checks for unknown viruses. Using this option can reduce your protection against unknown viruses.

Use these settings to determine what to scan during system startup. We recommend that you check Memory, Master Boot Record, Boot Records and System Files as an important step in preventing viruses from activating or spreading.

- If a system file is infected, the virus activates when you start up your computer and can infect other programs as you run them.

Scans for any viruses resident in your computer's memory. Viruses in memory can spread to other files that you access.

Scans for boot viruses in the master boot record.

Scans for boot viruses in the boot records on your hard disk.

Scans the operating files that your computer uses to start up and run Windows.

Specify the keystroke combination you want to use to prevent automatic protection from loading when your computer starts up. The options are: None, Both Shift Keys, Both Alt Keys, Both Ctrl Keys.
Choose None if you don't want a bypass key combination.

Choose if you don’t want a bypass key combination.

Choose if you want to press both Shift keys to bypass a scan at startup.

Choose if you want to press both Alt keys to bypass a scan at startup.

Choose if you want to press both control Ctrl keys to bypass a scan at startup.

Loads Auto-Protect at startup. We highly recommend checking this so that Auto-Protect loads as soon as your computer starts up, which helps ensure maximum protection.

Check so that the master boot record, boot records, and system files on your hard disk receive inoculation protection.

Check so that program files are checked for inoculation on all hard disks and network drives.

Check to inoculate all program files on floppy disks.

Choose an option to choose how to respond to an inoculation issue. Choose Prompt to have the most control over what happens to the file.

Choose an option for how to respond When An Item Has Not Been Inoculated. The preset option is Inoculate Automatically. For more control, Prompt informs you when it finds an uninoculated program file or boot record and allows you to choose how to respond.

Inoculate Automatically inoculates each uninoculated file or boot record as soon as it is detected. The item is scanned for known viruses before it is inoculated to ensure it is virus-free.

Notify Only- Don't Inoculate merely informs you that a file or boot record is uninoculated. It does not inoculate the item.

Deny Access informs you that a program file has not been inoculated and does not allow you to use that program. (This option does not apply to boot records.)

Choose an option for how to respond When An Inoculated Item Has Changed. The preset option is Prompt (which informs you when it finds a program file or boot record that has changed and lets you choose what to do).

Notify Only- Don't Reinoculate merely informs you that a file or boot record has changed. It does not reinoculate the item.

Deny Access informs you that a program file has changed and prevents you from using that file. (This option does not apply to boot records.)

Choose the buttons to display if alerted.

Allows you to repair a file or boot record with an inoculation change, returning the item to its state when it was last inoculated.

Allows you to delete a file with an inoculation change. For boot records and system files, this button won't be displayed in the Inoculation alert box.

Allows you to inoculate or reinoculate a changed file or boot record.

Allows you to continue the current operation (scanning or accessing a file). No change is made to the inoculation data.

Allows you to stop the current operation (scanning or accessing a file). No change is made to the inoculation data.

Allows you to exclude the file from future checks for inoculation and inoculation changes.

Enter a folder path for the inoculation files. The path must begin with a backslash. The preset path is \NCDTREE.

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

Enter a message with instructions or special warnings to appear in all alerts that Norton AntiVirus displays.

Check if you want Norton AntiVirus 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.

Choose 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 to record in the Activity Log.

Records known virus detections (viruses identified in the Virus List).

Records unknown virus detections (viruses not yet identified in the Virus List).

Records detections of files that have not been inoculated or have changed since inoculation.

Records virus-like activity detections (activities that many viruses perform when spreading or damaging data, such as an attempt to format your hard disk).

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

Records each update of the Virus List. The updates occur when you update the virus definitions files that Norton AntiVirus uses to detect viruses. You can update the files by clicking LiveUpdate in the Norton AntiVirus main window. LiveUpdate also performs scheduled updates automatically.

Click 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 deletion of the oldest entry or entries.

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 deletion of the oldest entry or entries.

Choose the maximum size for the Activity Log file.

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

Norton AntiVirus uses the entries in the Exclusion List in all scans it performs. An exclusion is a condition or virus-like activity that would normally be detected, but you have told Norton AntiVirus not to check for it in a particular file. Excluding files doesn't mean "don't find viruses" (unless you specifically select that option); rather, it means let some activity proceed because you know a virus did not cause it.

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

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

Click Remove to delete an exclusion.

Enter the pathname for a file or group of files to exclude, or use the browse button to select a single file from a list.

Click the activities that you wish to exclude for the specified file or group of files (for example, *.COM).

Excludes the item from checks for known viruses.

Excludes the item from checks to see if it's been inoculated and checks for inoculation changes.

Excludes the item from checks for unknown viruses.

Excludes the item from checks for attempts to perform a low-level format of your hard disk, which obliterates all information on the disk.

Excludes the item from checks for attempts to write to the boot records on your hard disk. This action is performed legitimately by very few programs.

Excludes the item from checks for attempts to write to the boot record on a floppy disk. This action is performed legitimately by very few programs.

Excludes the item from checks for attempts to write to a program file. Some programs save configuration information within themselves rather than in a separate file.

Excludes the item from checks for attempts to change a read-only file so that it can be written to. This option applies specifically to operations executed by DOS applications.

Check to make a copy of the infected file before repairing it. Norton AntiVirus uses .VIR as the preset option for the 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. Norton AntiVirus uses VIR as the preset option for the backup file extension. The file type appears as “Virus Infected File” when you list files using the Windows Explorer.

Designates that the specified item is to be inoculated when you click OK.

Designates that the specified item is to be uninoculated when you click OK.

Specifies what item (drive, folder, group of files, or file) is to be inoculated or uninoculated. You can use a wildcard to specify a group of files. You can also use the browse button to select a single file.

This dialog box 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 disk drive, resolve the problem that is causing you to be denied access to the drive.

Click Continue to continue the scan.

Click Skip to skip this drive.

Check to turn on password protection.

Check to password-protect all listed features.

Check to password-protect only the items you select in the list box.

Type a password in the New Password text box; then type it again in the Confirm Password text box.

Type your existing password in the Old Password text box.

Type a password in the New Password text box; then type it again in the Confirm Password text box.

These are the features you can protect with a password.

Choose Set Password to display the Set Password dialog box.

You must type in your password before you can access this feature.

Click to confirm that you want to delete the file.

Click to confirm that you want to delete the file.

Click to confirm that you want to delete the file.

Click Delete to confirm that you want to delete all files.

Click to confirm that you do not want to delete all files.

Type a new extension in the Extension To Add text box (up to three characters). You can use wildcards in the extension, but not to represent all three characters. This new extension is added to the Program File Extensions List, and Norton AntiVirus treats any files with this extension as a program file when it scans for viruses and inoculates.

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

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

Inoculates each uninoculated program file and boot record as soon as it is detected.

The Activity Log contains a history of Norton AntiVirus activity. For example, Norton AntiVirus 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).

Click Inoculate to record a "fingerprint" of the file that helps Norton AntiVirus detect any future changes to the file that might indicate the presence of an unknown virus.

Use the Activity Log to view a record of Norton AntiVirus 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 records, go to the Activity Log tab in the Options dialog box.

Returns the file to its original, uninfected state.

Aborts the download. You are not able to save the file to your local hard disk drive. You 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 disk drive, you are 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 continues to notify you each time another virus is identified, telling you whether the compressed file contains one or many infected files. 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 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.

Check this box to send alerts to Norton AntiVirus for NetWare, if the Norton AntiVirus NLM (NetWare Loadable Module) is present on your network.

Specify which NetWare Server to alert, or select All NetWare Servers to send an alert to all servers listed.

Check this option to allow network scanning. This allows you to select a specific drive from the main window.

Choose a target from the browser or type a target name in the Target text box below.

Click to enable Bloodhound Heuristic technology, which dramatically increases your protection against new and unknown viruses.

Drag the pointer to increase Bloodhound's sensitivity in detecting new and unknown viruses.

These options let you specify different actions for file, macro, and boot virus detections.

Choose the action you want Norton AntiVirus to perform when a virus is found in a file.

Choose the action you want Norton AntiVirus to perform when a virus is found in a document or template file.

Choose the action you want Norton AntiVirus to perform when a virus is found in a boot record.

Click to display a dialog box where you can modify the settings used by Bloodhound Heuristics, which detect new and unknown viruses.

Check if you want the Norton AntiVirus NLM alerted. You can specify a particular server or notify all NetWare servers running the NLM.

Click to display the Customize Response dialog where you can differentiate between how Norton AntiVirus responds to file, boot record, and macro viruses.

About Norton AntiVirus

Norton AntiVirus is the most sophisticated and powerful product available to safeguard your computer from virus infection, no matter what the source. If you performed a complete (not custom) setup of Norton AntiVirus, you are protected from viruses that spread from hard or floppy disks, viruses that travel across networks, and even viruses that are transmitted across the Internet.

Here's what Norton AntiVirus does automatically:

- Checks system files and boot records for viruses at system startup.
- Checks programs for viruses at the time you use them.
- Scans your startup drive for viruses once per week.
- Monitors your computer for any activity that might indicate the work of a virus in action.
- Scan files you download from the Internet.
- Checks floppy disks for boot viruses when you use them.
- Updates your virus protection at least once monthly.

Here's what you can do with Norton AntiVirus:

- Scan specific files, folders, or entire drives for viruses.
- Schedule virus scans to run at predetermined times.
- Schedule or initiate LiveUpdates of new virus definitions files.

Click here
{button ,AL("NAVDSK_I0010;NAVDSK_I0060;NAVDSK_I0020;NAVDSK_I0065;NAVDSK_I0075;NAVDSK_V0250;NAVDSK_I0025;NAVDSK_V0010")} for more information.

How Norton AntiVirus works

Click here to view a short video about How Norton AntiVirus protects you.

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 scans your disk and files--initiated with the Scan Now button in the main window or scheduled to run automatically--it is searching for these telltale signatures. If a file is found that has been infected by one of these viruses, Norton AntiVirus 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 file by the Symantec engineers. For this reason, you should update your virus definitions file monthly. Symantec has made this extremely easy with the automatically scheduled Live Update feature.

Keeping viruses off of your computer requires Norton AntiVirus to:

- Detect viruses that may already exist and remove them (Auto-Protect).
- Prevent viruses from infecting your computer (Auto-Protect and Inoculation).
- Monitor for activity that may indicate an unknown virus (Auto-Protect and Sensor technology).
- The automatic features shown are turned on by preset options. Depending on your risk level, you may increase or decrease protection settings.

In addition to the scans that Auto-Protect performs in the background, you can also initiate scans at any time and schedule scans to occur at predetermined times.

Click here
{button ,AL("NAVDSK_I0015;NAVDSK_V0055;NAVDSK_I0075;NAVDSK_V0015;NAVDSK_I0025;NAVDSK_I0065;NAVDSK_V0055")} for more information.

About Norton AntiVirus Auto-Protect

Auto-Protect works in the background to protect you in several ways:

- Scans program files whenever they are used.
- Uses a sophisticated unknown virus detection feature called Virus Sensor Technology that monitors your computer for new viruses that have not yet been included in the Norton AntiVirus virus definitions files.
- Monitors your computer for virus-like activities (such as an attempt to format your hard disk) and warns you so you can prevent this behavior.

To enable Auto-Protect:

- Norton AntiVirus is preset to load automatic protection whenever you start your computer.

To disable Auto-Protect temporarily:

1 Double-click the Auto-Protect icon on the Windows taskbar.
2 Click Disable.
The button changes to Enable and the icon changes.
3 Click Minimize to close the Norton AntiVirus Auto-Protect dialog box.

Click here {button ,AL("NAVDSK_V0010;NAVDSK_I0075;NAVDSK_I0025;NAVDSK_I0035")} for more information.

The importance of a NAV Rescue Disk Set

- When you set up Norton AntiVirus, you were advised to create a NAV Rescue Disk Set. If you did not do so then, you should create the disks now. If you did create the NAV Rescue Disk Set, be sure you have stored the disks in a safe place.

If a virus damages boot records (files containing information necessary to start up your computer), you will be prompted to reboot your computer with the disk you made, labeled Norton AntiVirus Emergency Boot Disk. These disks contain a backup copy of all information necessary to restore your computer to an uninfected state. If you do not have a NAV Rescue Disk Set, you may not be able to restart your computer without risk of spreading a serious virus infection and causing damage to other files on your disk.

Click here {button ,AL("NAVDSK_V0360;NAVDSK_V0385")} for more information.

What is a computer virus?

Click here to view a short video About Viruses.
A computer virus is, simply, a program designed to attach itself to another computer program. Some computer viruses damage the data on your disks by corrupting programs, deleting files, or even reformatting your entire hard disk. Most viruses, however, are not designed to do any serious damage; they simply replicate or display messages. Most viruses stay active in memory until you turn off your computer. When you turn off the computer you remove the virus from memory, but not from the file, files, or disk it has infected. So the next time you use your computer, the virus program is activated again and attaches itself to more programs. A computer virus, like a biological virus, lives to replicate.

Click here {button ,AL("NAVDSK_I0030;NAVDSK_I0035;NAVDSK_V0055;NAVDSK_I0040")} for more information.

What viruses do and don't do

- Computer viruses infect executable program files, such as word processing, spreadsheet, 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 experience 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.
- Note that Norton AntiVirus also scans Microsoft Word and Excel documents when scanning program files. Although these are not program files, they do contain code and can be infected by a new class of viruses called Macro Viruses.

Click here {button ,AL("NAVDSK_I0030;NAVDSK_I0035;NAVDSK_V0055;NAVDSK_I0040")} for more information.

About unknown viruses

First, a *known* virus is one for which Norton AntiVirus has recorded information in the virus definitions file. If, during a scan, one of these viruses is found, NAV has the tools to eliminate the virus. An *unknown* virus, on the other hand, is one that does not yet have a virus definition.

Unfortunately, new viruses are being developed by ill-intentioned programmers every day. To keep up with these new viruses, Norton AntiVirus monitors your computer for virus-like activities and for programs that have been modified without your knowledge. When either condition is detected, NAV prevents the action from continuing and takes corrective action.

- Note that Norton AntiVirus also scans Microsoft Word and Excel documents when scanning program files. Although these are not program files, they do contain code and can be infected by a new class of viruses called Macro Viruses.

Click here {button ,AL("NAVDSK_I0025;NAVDSK_I0045")} for more information.

Types of viruses

There is a new class of viruses called Macro Viruses that infect your data files. They are typically found in Microsoft Word and Excel documents. Norton AntiVirus now scans .dot and .doc when scanning program files. Other known viruses are categorized in the Virus List by how often you find them, what they infect, and how they behave.

Common Viruses: Viruses that you are most likely to encounter.

Program Viruses: Viruses that can infect program files that you run.

Boot Viruses: Viruses that can infect boot records or master boot records on disks.

Stealth Viruses: Viruses that try to conceal themselves from attempts to detect or remove them.

Polymorphic Viruses: Viruses that appear differently in each infected file, making detection more difficult.

Multipartite Viruses: Viruses that infect both program files and boot records.

Windows Viruses: Viruses that infect Windows programs.

Agent Viruses: Viruses that infect agent programs (such as those that download software from the Internet).

Click here {button ,AL("NAVDSK_I0025;NAVDSK_V0055;NAVDSK_I0035")} for more information.

Virus-like activities

Virus-like activities are those activities that viruses usually perform when attempting to infect your files. Any of these activities may occasionally be legitimate in your work context. Therefore, you can exclude certain files from being checked for any of the activities listed below.

Low-Level Format Of Hard Disk: All information on the disk is erased and cannot be recovered. This type of format is generally performed at the factory only. If this activity is detected, it almost certainly indicates an unknown virus at work.

Write To Hard Disk Boot Records: Very few programs write to hard disk boot records. If this activity is detected, it could indicate an unknown virus at work.

Write To Floppy Disk Boot Records: Only a few programs (such as the operating system FORMAT command) write to floppy disk boot records. If this activity is detected, it could indicate an unknown virus at work.

Write To Program Files: Some programs save configuration information within themselves. Although this activity often happens legitimately, it could indicate an unknown virus at work.

DOS Read-Only Attribute Change: This option applies specifically to operations executed by DOS applications. Many DOS programs change a file's read-only attribute. Although this activity often happens legitimately, it could indicate an unknown virus at work.

Click here {button ,AL("NAVDSK_I0025;NAVDSK_I0035;NAVDSK_I0095")} for more information.

Finding viruses

Computer viruses can exist in two forms. They are either active in your computer's memory or lying dormant in files or boot records. It is important to scan these areas for viruses and remove any found.

In addition to the scans that occur automatically by the automatic protection feature (called Auto-Protect), you can also initiate scans at any time and schedule scans to occur at predetermined times.

To initiate scans:

1. Open the Norton AntiVirus main window if it is not already displayed.
2. Choose one of the following options:

   - 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 is configured not to allow network drive scanning. (See the Scanner Advanced Settings dialog box to reconfigure this option.)

   - Click Folders from the Scan menu, select the folder, and click Scan.
   - Click File from the Scan menu, select the file or type in a filename, and click Open.

   The Scan dialog box reports on the progress of the scan.

If you find a virus that cannot be repaired:

You should not leave an infected file on your computer. NAV can repair most infected files. However, in the case that a file cannot be repaired, you must delete it from your disk. Be sure to get into the habit of keeping original disks in a safe place and making backup copies of your files. If you do not have a clean copy of the file, you may be able to get one from the manufacturer.

Click here {button ,AL("NAVDSK_V0055;NAVDSK_V0075;NAVDSK_V0065;NAVDSK_V0020;")} for more information.

Removing viruses

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

- Repair the infected file, boot record, or master boot record.
- Delete the infected file from the disk and replace it with an uninfected copy.
- You should not leave an infected file on your computer. NAV can repair most infected files. However, in the case that a file cannot be repaired, you must delete it from your disk. You need to get into the habit of keeping original disks in a safe place and making backup copies of your files. If you do not have an uninfected backup copy of a file, the original program disk, or online access to the file, you need to get a new copy of the file from the software manufacturer.
- Note that Norton AntiVirus also scans Microsoft Word and Excel documents when scanning program files. Although these are not program files, they do contain code and can be infected by a new class of viruses called Macro Viruses. Therefore, some of your data files are now at risk. You need to make backup copies regularly.

Click here {button ,AL("NAVDSK_10010;NAVDSK_V0055;NAVDSK_V0340;NAVDSK_V0335")} for more information.

Responding to alerts

Norton AntiVirus alerts you when:

- A virus or unknown virus is found
- A virus-like activity is detected (an operation that viruses often perform when spreading or damaging files)
- An inoculation issue is detected (either a file has not been inoculated or a file has changed since it was inoculated)

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 file cannot be repaired	Delete an infected file
A compressed file is infected	Work with compressed files
A suspicious activity was detected	Respond to a virus-like activity alert
The file is not inoculated	Respond to an inoculation request
The inoculated file has changed	Respond to an inoculation change

- You should not leave an infected file on your computer. NAV can repair most infected files. However, in the case that a file cannot be repaired, you must delete it from your disk. You need to get into the habit of keeping original disks in a safe place and making backup copies of your files. If you do not have an uninfected backup copy of a file, the original program disk, or online access to the file, you need to get a new copy of the file from the software manufacturer.

Click here {button ,AL("NAVDSK_I0010;NAVDSK_V0055;NAVDSK_V0340;NAVDSK_V0335")} for more information.

Determining your risk level

Norton AntiVirus provides several layers of virus protection. The options selected for you when you set up Norton AntiVirus provide excellent protection for most environments.

However, if your risk level is high, you may want to customize Norton AntiVirus to provide more protection. On the other hand, if your risk level is low, you may want to reduce or eliminate unnecessary protection.

Use the following to determine your risk level profile:

Very low risk profile

Single-user PC
No network connection
No modem
Format all floppies before first use
Don't receive files on floppies
Only use shrink-wrapped software from reputable dealers

- **Recommendation:** Make no changes. Use the preset options.

Low risk profile

No network connection
Modem (mostly email, few or no downloaded programs from commercial BBSs or on-line services)
Use just a few applications regularly

- **Recommendation:** Make no changes. Use the preset options.

Medium risk profile

Network connection
Use shared network programs
Use preformatted floppies
Use recycled floppies of unknown origin
Share files on floppy disks
Buy bargain or "swap meet" software

- **Recommendation:** Change the Options settings.

1 In the Norton AntiVirus Main Window, click the Options button.
2 Click on the tab as shown and check the options indicated:

- Activity Log tab: Inoculation Activities
- Inoculation tab: Inoculate Program Files

High risk profile

Network connection (LAN without a professional administrator)
No AntiVirus software running on a network
Internet connection
Modem (download programs from BBSs and online services)
Use preformatted floppies
Use recycled floppies of unknown origin
Share files on floppy disks
Collect software
Trade computer games
Other people frequently use your computer

- **Recommendation:** Change the Options settings.

1 In the Norton AntiVirus Main Window, click the Options button.
2 Click on the tab as shown and check the options indicated::

- Scanner tab/Advanced Settings dialog box: Allow Network Scanning
- Auto-Protect tab/Advanced Settings dialog box: Prompt for DOS Read-Only Attribute Change
- Activity Log tab: All Items
- Inoculation tab: Inoculate Program Files
  Inoculate Files On Floppies
  When An Item Has Not Been Inoculated: Prompt

About updating virus definitions

To prevent the new viruses that have been discovered since you bought Norton AntiVirus, you MUST update your protection (virus definitions) frequently. Otherwise, Norton AntiVirus cannot do its job. If your computer is connected to a modem and you accepted the preset options when you installed Norton AntiVirus, LiveUpdate is already scheduled to update virus definitions files once monthly. This is a no charge on-line service.
You can also schedule LiveUpdates using the Norton Program Scheduler.

- If your computer is not connected to a modem, you can find updated virus definitions files on several different bulletin board systems or request them by mail.

Click here {button ,AL("NAVDSK_I0071")} for more information.

About Inoculation

Inoculation is another way to detect *unknown* viruses, or those viruses for which Norton AntiVirus does not yet have a definition. System files and boot records are inoculated by preset options. For other files, you can choose to inoculate at any time.

Why Inoculate?

When you inoculate a file, Norton AntiVirus records critical information about it (similar to taking a "fingerprint"). On subsequent scans, Norton AntiVirus checks the file against the "fingerprint" and notifies you if there are any changes that could indicate the presence of an unknown virus.

What causes an inoculation change?

An inoculation change could occur for the following reasons:

- A change to the file for legitimate purposes. For example, you may have installed a new version of the software and forgotten to inoculate the new program file.
- An unknown virus that is not in the definitions file. Either Norton AntiVirus doesn't have a definition for it or you don't have the most recent definitions.

Why uninoculate?

If you are removing a program from your drive or no longer want to use inoculation, you should uninoculate files to remove the inoculation data and free up space on your disk. Inoculation data is stored in a NCDTREE folder.

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

About the Virus List

You can see which viruses Norton AntiVirus 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 uses the information in virus definitions files to detect viruses during scans. Updated virus definitions files are available monthly. Once installed, you see the new names in the Virus List.

Click here {button ,AL("NAVDSK_I0070;NAVDSK_I0260")} for more information.

About the Activity Log

The Activity Log file contains details about Norton AntiVirus activities, such as when problems were found and how they were resolved. You can use the Activity Log, after a scan, to find the names of files on your disk that are still infected and may need to be deleted and replaced with new copies.

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 have filtered 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 Norton Program Scheduler

You can schedule virus scans and LiveUpdates that run unattended on either specific dates and times or at periodic intervals. If you are using the computer when the scheduled event begins, it runs in the background so that you do not have to stop working.

- After adding or changing a scheduled scan, make sure you click Minimize so that the Scheduler remains active. The Scheduler must be active and minimized for scheduled events to run. And, of course, be sure that the computer is on. The event will not run when the computer is off.

Click here {button ,AL("NAVDSK_V0075")} for more information.

About Exclusions

Norton AntiVirus uses the entries in the Exclusions List in all scans it performs. An exclusion is a condition that would normally be detected, but you have told Norton AntiVirus not to check for a particular file.

- If you move or rename a file, you automatically invalidate its exclusions. One exception exists: Include subfolders is checked and the file is moved without renaming.

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

About the Repair Wizard

Norton AntiVirus now has a Repair Wizard that walks you through the steps of eliminating any viruses found on your computer during a scan that you initiate or schedule. When a virus is found, the Repair Wizard offers you the choice of repairing all the viruses at once or allowing you to see what viruses have infected your computer and asking you to repair or delete each one, one at a time. Once the Wizard has done its work, it is always a good idea to re-scan your computer just to ensure that all the viruses have been eliminated.

- Note that NAV can repair most infected files but, in the rare case a file cannot be repaired, you may have to delete the file to get rid of the virus. If you have to repair the virus, you are prompted each time you are asked to choose to make the deletion. You will have a chance to back out.
- Files deleted by Norton AntiVirus cannot be recovered. However, you should not leave an infected file on your computer. If the file cannot be repaired, you must delete it from your disk.

- If you don't have an uninfected copy of a program file, you can get a replacement copy from the manufacturer. If you don't have an uninfected copy of a Microsoft .doc, .dot. or .xls file (which may be infected with the new Macro Viruses), you still need to delete the file from your disk to keep from spreading the infection. You should get into the habit of keeping original disks in a safe place and making backup copies of your files.

Responding to alerts

Norton AntiVirus alerts you when a virus is found

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 file cannot be repaired — Delete an infected file
- A compressed file is infected — Work with compressed files
- You should not leave an infected file on your computer. NAV can repair most infected files. However, in the case that a file cannot be repaired, you must delete it from your disk. You need to get into the habit of keeping original disks in a safe place and making backup copies of your files. If you do not have an uninfected backup copy of a file, the original program disk, or online access to the file, you need to get a new copy of the file from the software manufacturer.

Click here {button ,AL("NAVDSK_I0010;NAVDSK_V0055;NAVDSK_V0340;NAVDSK_V0335")} for more information.

How Norton AntiVirus works

Click here to view a short video about How Norton AntiVirus protects you.

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 scans your disk and files--initiated with the Scan Now button in the main window or scheduled to run automatically--it is searching for these telltale signatures. If a file is found that has been infected by one of these viruses, Norton AntiVirus 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 file by the Symantec engineers. For this reason, you should update your virus definitions file monthly. Symantec has made this extremely easy with the automatically scheduled Live Update feature.

Keeping viruses off of your computer requires Norton AntiVirus to:

- Detect viruses that may already exist and remove them (Auto-Protect).
- Prevent viruses from infecting your computer (Auto-Protect and Inoculation).
- Monitor for activity that may indicate an unknown virus (Auto-Protect and Sensor technology).
- The automatic features shown are turned on by preset options. Depending on your risk level, you may increase or decrease protection settings.

In addition to the scans that Auto-Protect performs in the background, you can also initiate scans at any time and schedule scans to occur at predetermined times.

Click here {button ,AL("NAVDSK_I0015;NAVDSK_V0055;NAVDSK_I0075;NAVDSK_V0015;NAVDSK_I0025;NAVDSK_I0065;NAVDSK_V0055")} for more information.

Sources for updating virus definitions

If you have a modem and accepted the preset options when you installed Norton AntiVirus, LiveUpdate automatically updates your virus definitions once monthly. You can schedule more frequent automatic updates using the Norton Program Scheduler.

If you choose to update virus definitions on your own, the following sources are available to you.

CompuServe

To directly access the Symantec Forum:

- Enter 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. Enter **SYMANTEC**.
3. Click Virus Control Center.
4. Click Virus Definitions Library and follow the on-screen directions.

Internet

To use the FTP site:

- Access **ftp.symantec.com**

The files are located in the /public/win95_nt/nav/ directory.

To use the World Wide WEB site:

1. Access www.symantec.com
2. Click AntiVirus Research Center.
3. Click Download Updates.
4. Click NAV and follow the on-screen directions.

Microsoft Network

1. Choose Go To from the View menu.
2. Choose Other Location.
3. Enter SYMANTEC.
4. Double-click Support Solutions
5. Double-click Norton AntiVirus 95 (the same files are used for Windows NT).
   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 one of the following telephone numbers:

- 300- to 28,800-baud modems (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 and follow the on-screen directions to download the files.

- Enter /GO GETFILE at any prompt to return to this File menu.

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.

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_V0550")} for information on installing new virus definition files.

Credits

Product Management

Lily Duong, Alex Haddox, Neils Johnson, Marian Merritt, John Moldenhauer, Robert Pettit, Sharon Ruckman

Project Management

Gary Westerland, Francia Saplala

Software Development

David Allee, Jim Brennan, David Buches, Darren Chi, George Dzieciol, Scott Edwards, Barry Gerhardt, Tchavdar Ivanov, Michael Keating, John Millard, Carey Nachenberg, Dan Sackinger, Ken Sackinger, Thomas Smith, Radoslav Stanev, Jacob Taylor, Steve Trilling

Quality assurance

Dan Bjerke, Kerry Boyte, Chris Brown, Rob Ficcaglia, Kevin Ho, Debbie Ka, Sean Martin, Melissa Mendonca, Howard Mora, Tom Morrissey, Greg Patterson, Garret Polk, Sam Porterfield, Brent Ridley, Jeff Sulton, Kent Tang, Morry Teitelman, Dan Uyemura, and Michael "Sparky" Willison

SWAT Team

Jonathon Allee, Stanley Ballenger, Jim Belden, Tim Cashin, Paul Davis, Michael Dunn, Igor Goldshteyn, Bob Kolosky, Zoey Reyes, Scott Smith

Shared Tech

Cameron Bigger, Don Carver, Alireza Faroush, Roger Hollman Jim Lamb, Jim Lucan, Bruce McCorkendale, Bryan Martin, Patrick Martin, Heath Perryman, Mark Spiegel, Oleg Volochtchouk

Documentation and Online Help

Elizabeth Anders, Jennifer Brawer, Annette Brown, Alfred Ghadimi, Karen Goldsmith, Robert Hoffman, Romey Keys, and Sheelagh O'Connor

Technical Support Team

Valentine Ashman, Andrea Baughman, Michelle Bodrug, Earl Campbell, Don Crosgrey, Kyle Dodge, Thomas Dunsmoor, Don Faiman, Christine Frazer, Peter Fuzessery, Rochelle Hamlet, Mark Hammerschmith, Pam Heine, Don Hess, Todd Kieser, Danny Krautschek, Richard Lee, Michael Logue, David Lucas, Russell Lusignan, Patrick MacPherson, Larry McHenry, Patrick Merjo, Stephen Mickeler, Dimitri Mitskopoulos, Don Oldenburg, Dn Pederson, LaVonne Perry, Leon Plueard, Clive Rose, Chris Shapcott, Brian Sharman, Matthew Smith, Eric Stallings, Olga Stamatiou, Chris Steele, Robert Walling, Jason Walsh, Michael Williams, James Whitted

Engineering Services Team

Frank Arjasbi, Stephen Blackmoore, Erick Bryant, Peter Cagney, James Dietrich, Richard Espy, Renal Fuller, Alex Harrington, Will Jobe, Kim Johnston, Sebastian Somchai Lai, Mike Linsenmayer, Alena Montfort, and Dwight Wilson

Symantec AntiVirus Research Center (SARC)

Darren Lee Ang, David Banes, Diop Bankole, Frank Barajas, Sherra Buzzell, Matt Candelaria, Philip DeBats, Eric Chien, Raul Elnitiarta, Chris Formulak, Tigran Khanpapyan , Maryl Magee, Abid Oonwala, Charles Renert, René Visser, John Wilber, Motoaki Yamamura

Help could not start the video. To run the video from Help, your Norton AntiVirus CD must be in the drive and the drive must be able to be read. If your CD drive is not designated as the D: drive, you can run the videos by inserting the Norton AntiVirus CD and selecting View Videos.

View Videos

Click here to view…

- About Viruses
- Norton AntiVirus: The Guided Tour
- What To Do When Norton AntiVirus Alerts You
- About SARC (Symantec AntiVirus Research Center)

To find help, choose one of the following options:

- Choose Contents from the Help menu.
- From any Norton AntiVirus dialog:
  - Click the ? on the title bar. Position it over an option in the dialog box and click the left mouse button once.
  - Position the cursor over an option and press F1.
  - Position the cursor over an option, click the right mouse button, and choose one of the following:

What's This? Gives a brief description of the option.

Contents : Gives you access to Norton AntiVirus help topics and a Glossary of terms.

- Note that you can keep help open on your desktop by minimizing the help window or by simply clicking back and forth between help and the product. When you have read the information you need, simply click in the open NAV window. Then, if you need help again, either reopen help by restoring the help window or by clicking in the help window itself.

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

To change how Norton AntiVirus works:

1. Click Options in the Norton AntiVirus main window.
2. Click one of the following tabs:
   Scanner: Controls what is scanned and how Norton AntiVirus responds when you initiate manual scans.
   Auto-Protect: Determines how virus protection works in the background.
   Startup: Determines what is scanned when you start your computer.
   Alerts: Tells Norton AntiVirus what to display when a virus, virus-like activity, or inoculation change is found and who to alert.
   Inoculation: Allows you to add protection against unknown viruses.
   Activity Log: Determines which events are recorded by NAV.
   Exclusions: Specifies which files are not monitored for some virus symptoms.
   General: Applies to all scans you initiate, Auto-Protect scans, and scheduled scans.
   Password: Allows you to password-protect some or all Norton AntiVirus features.
3. Use the right mouse button to click any control 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. You don't need to restart your computer.

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

To use Norton AntiVirus:

1. Determine whether you are sufficiently protected. See Determining your risk level.

   - If you chose a complete setup of Norton AntiVirus and accepted the recommended options, you are sufficiently protected in most cases.

2. Initiate manual scans of selected files, folders, or drives using the menu commands or the Scan Now button in the Norton AntiVirus main window. See Initiate scans.
3. Inoculate your files and customize your scan options to increase protection if your risk level is high (for example, you frequently exchange floppy disks with others or are connected to a network that is not protected by Norton AntiVirus). See Inoculate files.
4. Update virus definitions regularly. See Update virus definitions.

Click here {button ,AL("NAVDSK_V0050;NAVDSK_V0030;NAVDSK_V0035")} for more information.

To change scan options for scans you initiate or schedule:

1 Click Options in the Norton AntiVirus main window.
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_V0050;NAVDSK_V0065;NAVDSK_V0055")} for more information.

Norton AntiVirus is preset to load automatic protection whenever you start your computer. The Norton AntiVirus Auto-Protect icon is displayed in the Windows system tray (near the clock).

To disable Auto-Protect temporarily:

1. Double-click the Auto-Protect icon.
2. Click Disable.
   The button changes to Enable and the icon changes.
3. Click Minimize to close the Norton AntiVirus Auto-Protect dialog box.

To enable Auto-protect again:

Repeat the steps above. (Click the Enable button in step 2. The button changes to Disable.)

Click here {button ,AL("NAVDSK_I0015;NAVDSK_V0120")} for more information.

To bypass startup protection:

Press and hold both Alt keys during the entire boot process. This bypasses startup protection for this startup only. You can specify different bypass keys from the Options - Startup tab.

- Bypassing startup protection reduces your level of protection.

Click here {button ,AL("NAVDSK_V0160")} for more information.

To exclude files from being scanned for some virus symptoms:

1 Click Options in the Norton AntiVirus main window.
2 Click the Exclusions tab to bring it to the front.
3 Click New.
4 Do one of the following:

- Use the browse button to display a file selection dialog box from which you can choose a file that will be displayed in the Item text box.

- Enter a filename in the Item text box. You can use wildcards such as c:\ *.COM. You should check Include Subfolders if you want to ensure that all files with that extension are excluded.

5 Check any of the boxes in the Exclude From group box.

- Before making your choices, click the right mouse button over any option to display a help menu. Click What's This? to see a description of the option.

6 Click OK to save settings and exit the dialog box.

- You would choose to exclude a file only if you are certain that some of the virus-like activities Norton AntiVirus checks for are not indications of a virus, but are legitimate activities. Be careful! Excluding files reduces your level of protection.

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

To find viruses on your computer:

1. Determine whether you are sufficiently protected.
2. Check one of the following options:
   - Initiate virus scans at any time by choosing which drives to scan and clicking Scan Now in the NAV main window.
   - Use the Scan menu in the NAV 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.
3. Schedule scans regularly.
4. Leave Auto-Protect enabled and use the preset options that are loaded when you perform a complete setup of Norton AntiVirus**.**
5. Update your virus definitions regularly.

Click here {button ,AL("NAVDSK_I0015;NAVDSK_V0055;NAVDSK_V0250;NAVDSK_V0075;NAVDSK_V0050")} for more information.

To set up maximum protection:

When you install Norton AntiVirus with the preset options, your computer is automatically protected against known and unknown viruses and alerts you whenever a virus is found. However, you can increase your protection by doing the following:

Customize Scanner settings for maximum protection

Customize Auto-Protect settings for maximum protection

Inoculate files

{bmct symw4003.mrb If you have a modem and accepted the preset options when you installed, you will receive monthly updates of files that Norton AntiVirus needs to keep your virus protection up[to date.

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 Click the appropriate button:

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 notifications of this kind 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. If you are accessing a file, access is granted. Clicking Continue does not solve the problem that was reported to you.

Click here {button ,AL("NAVDSK_V0175;NAVDSK_V5000;NAVDSK_V0335;NAVDSK_V0340;NAVDSK_V0345")} for more information.

To always scan floppies (during scans you initiate):

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

If you performed a complete setup of Norton AntiVirus and accepted all recommended options, Auto-Protect scans floppy disks at startup and when they are accessed. What you are setting here simply means NAV will also always scan floppy drives when you initiate a scan.

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

To keep up with new viruses, choose one of the following options:

- You should update virus definitions once a month. To do this, you must either access an online service or request the updates by mail from Symantec. Without monthly updates, your computer is not fully protected.

- If your computer is connected to a modem or to the Internet, if you accepted the preset option when you installed Norton AntiVirus, you will automatically receive pre-scheduled LiveUpdates.
- If your computer is connected to a modem or to the Internet, simply click the LiveUpdate button in the Norton AntiVirus main window and follow the onscreen prompts to initiate a LiveUpdate at any time you choose.
- If your computer is connected to a modem or to the Internet, you can schedule automatic LiveUpdates to occur more than once a month using the Norton Program Scheduler.
- If you don't have a modem or an Internet connection, you can order virus definitions update disks from Symantec to arrive by mail. This service requires a fee:

  - In the United States, call (800) 203-4403.

  - Outside the United States, contact your local Symantec office or representative.
- Follow the instructions on the update that you receive.

Click here {button ,AL("NAVDSK_V0550")} for detailed instructions on installing new virus definitions files.

To schedule virus scans:

1. Click Scheduler in the Norton AntiVirus main window
2. Click Add. (If the button isn't visible, select Add from the Event menu.)
3. Select Scan For Viruses in the Type Of Event drop-down list box.
   - 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. Enter a brief description in the Description text box.
   This text will appear in the Events list box in the Scheduler main window.
7. Enter 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
   If the path uses spaces, enclose the item in double quotes. For example:
   "C: \GP Was Here\Gone.exe"
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 and click OK.

- 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.

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

To select which files to scan when you initiate a manual or scheduled scan:

1 Click Options in the Norton AntiVirus main window.

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, all options are already checked if you performed a complete setup of Norton AntiVirus.
  - Scanning time may increase slightly if you have many compressed files.

4 Click Program Files to scan only files that 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.

- Note that Norton AntiVirus also scans Microsoft Word and Excel documents when scanning program files. Although these are not program files, they do contain code and can be infected by a new class of viruses called Macro Viruses.

5 You can click Select to display the Program File Extensions dialog box, which lists the file extensions that NAV scans.

Click here {button ,AL("NAVDSK_V0075;NAVDSK_I0065;NAVDSK_V0055")} for more information.

To choose which program files to scan when you initiate a manual or scheduled scan:

1 From the Scanner tab, click the type of files to scan: All Files or Program Files.

- In most cases, scanning only program files 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 Enter any nonstandard file extensions that you use to name executable files.

5 Click OK to save settings and exit the New Program File Extension 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.

- Note that Norton AntiVirus also scans Microsoft Word and Excel documents when scanning program files. Although these are not program files, they do contain code and can be infected by a new class of viruses called Macro Viruses.

Click here {button ,AL("NAVDSK_I0065;NAVDSK_V0075;NAVDSK_V0055")} for more information.

To choose how to respond when a virus is found during a manual or scheduled scan:

1. Click Options from the Norton AntiVirus main window.
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.
4. Do one of the following:
   If you choose Prompt, specify in the Buttons To Display If Prompted group box which options you want Norton AntiVirus to make available when a virus is found.
   If you select Custom Response, click the Customize button to display a dialog where you can specify which options you want Norton AntiVirus to make available for three types of infections: file viruses, boot record viruses, and macro viruses.
5. Click OK to save settings and exit the dialog box.

Click here {button ,AL("NAVDSK_I0065;NAVDSK_V0075;NAVDSK_V0055")} for more information.

To set general scanning options:

1. Click Options in the Norton AntiVirus main window.
2. Click the General tab to bring it to the front.
3. Check Back Up File Before Attempting A Repair to have NAV 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.

   - All files with the specified backup extension are added automatically to the Exclusions List so they are not reported again during a scan. The file type appears as "Virus Infected File" when you list files using the Windows Explorer.

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 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 is configured not to allow network drive scanning.

Click here {button ,AL("NAVDSK_V0075")} for more information.

To scan a folder:

1 Choose Folders from the Scan menu.
2 Select the folder you want to scan.
3 Click Scan.

Click here {button ,AL("NAVDSK_V0075")} for more information.

To scan an individual file:

1 Click File from the Scan menu.
2 Select the file you want to scan.
3 Click OK or Open.

Click here {button ,AL("NAVDSK_V0075")} for more information.

To determine how protection works at startup:

1 Click Options in the Norton AntiVirus main window.

2 Click the Startup tab to bring it to the front.

3 Specify in the What To Scan group box the areas that you want Norton AntiVirus to scan each time you start your computer.

- We recommend that you leave the preset options as they are (Memory, Master Boot Record, Boot Records, and System Files are checked).

4 Choose your bypass keys (Both Alt keys is the preset option).

- If you work in a high risk environment, or if many other people use your computer, we recommend that you choose None.

Click here {button ,AL("NAVDSK_I0065")} for more information.

To select when files should be scanned by Auto-Protect:

1. Click Options in the Norton AntiVirus main window.
2. Click the Auto-Protect tab to bring it to the front.
3. Check when NAV should scan a file automatically.
   - Check all options to ensure maximum protection.
4. Click OK to save your settings and close the dialog box.

Click here {button ,AL("NAVDSK_I0065")} for more information.

To select how to respond when Auto-Protect finds problems:

1. Click Options in the Norton AntiVirus main window.
2. Click the Auto-Protect tab to bring it to the front.
3. Click to select any of the options, then click the right mouse button to display a help menu. Click What's This? to see a description of each option.
4. If you choose Prompt, specify in the Buttons To Display If Prompted group box which options you want Norton AntiVirus to make available when a virus is found. Remember to click any of the options with the right mouse button to display help that describes the option.
5. Click OK to save settings and exit the dialog box.

To monitor for virus-like activities:

1. Click Options in the Norton AntiVirus main window.
2. Click the Auto-Protect tab to bring it to the front.
3. Click Advanced at the bottom of the tab.
4. Click an option in each drop-down list box to specify what Norton AntiVirus should do when it detects the virus-like activity.
   The preset option for some activities is Allow. To set a higher level of protection, click Prompt. This option gives you the choice to Continue, Stop, or Exclude every time the activity occurs. In other words, you can evaluate whether or not you should allow the activity.
5. Click OK to close the dialog box.
6. Click OK to save your settings and close the Options dialog box.

Click here {button ,AL("NAVDSK_I0045")} for more information.

To monitor for unknown viruses:

1. Click Options in the Norton AntiVirus main window.
2. Click the Auto-Protect tab to bring it to the front.
3. Click Sensor at the bottom of the tab.
4. Check Use Virus Sensor Technology to detect when your programs become infected by an unknown virus.
5. Choose an option in the When An Unknown Virus Is Found drop-down list box.
   The preset option is Prompt, which is recommended because it allows you the most control.
6. If you selected Prompt, specify in the Buttons To Display If Prompted group box which options to make available when an unknown virus is found.
   - If you performed a complete setup of NAV, the first three options are checked. You may also check Exclude, but you should be very careful with this button. When you exclude files from being checked for unknown viruses, you reduce your protection level.
7. Click OK to save your setting and close the dialog box.

To edit exclusions:

1. Click Options in the Norton AntiVirus main window.
2. Click the Exclusions tab to bring it to the front.
3. Click Edit**.**
4. Make the desired changes.
5. Click OK to save settings and exit the dialog box.

To delete an exclusion:

1. Click Options in the Norton AntiVirus main window.
2. Click the Exclusions tab to bring it to the front.
3. Click Remove.
   The file is removed from the exclusions list.
4. Click OK to save settings and exit the dialog box.

To decide what to scan when you initiate a manual or scheduled scan:

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

1 Click All Files instead of Program Files in the What To Scan group box.
2 Click Advanced at the bottom of the tab.
3 Check All Floppy Drives in the Preselect At Start group box.

To decide what to scan at startup:

- If you performed a complete setup of Norton AntiVirus, the preset options on the Startup tab in the Options dialog box protect you adequately in most environments so they should not be altered. To ensure maximum protection:

1 Make sure that Load Auto-Protect At Startup is checked on the Auto-Protect tab.
2 Click None for bypass keys so that bypassing the scan at startup is not possible.
3 Check all options in the What To Scan group box.

Click here {button ,AL("NAVDSK_I0065")} for more information.

To select which files to inoculate:

When you set up Norton AntiVirus using the preset options, inoculation protection is set up for boot records and system files. You don't have to do anything further. However, in a high-risk environment, you may choose to check Inoculate Program Files and Inoculate Files on Floppies for maximum protection.

Click here {button ,AL("NAVDSK_I0065;NAVDSK_VI0075")} for more information.

To select how to respond to an inoculation request:

We recommend that you leave the preset options in the Buttons to Display If Prompted group box. However, if you choose to make changes, the options are:

Repair: Repairing a file or boot record returns the file to its original state.

Inoculate: Files are inoculated or reinoculated depending on the issue.

Stop: Stops the scan.

Delete: Deleting the file removes it from your disk**.** Files deleted by Norton AntiVirus cannot be recovered. After you have deleted the file, you can replace it with an uninfected copy.

Continue: Ignores the inoculation issue.

Exclude: Excludes the file from further checks for inoculation. Note that this option decreases your protection level.

Click here {button ,AL("NAVDSK_I0075")} for more information.

To respond if a file cannot be repaired:

1 If Norton AntiVirus cannot 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 Delete from an alert box in NAV.

- Delete the file manually from the hard disk or floppy disk from within Windows or DOS.

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

- Normally your data files are not affected. You are only replacing program or executable files. However, there is a new category of viruses called, "macro viruses," which can affect Microsoft Word and Excel files. If a .dot , .doc, or .xls file gets infected, NAV can usually repair it.

To respond to inoculation changes:

- Inoculation changes in a file occur for these reasons:
- The file has changed for legitimate reasons since the last time you inoculated it. For example, you may have installed a new version of the software and forgotten to reinoculate the program file.
- The file contains a virus that is not in the definitions file (perhaps because you don't have the most recent virus definitions or because it is a new virus for which Norton AntiVirus does not yet have a definition).
- If you are certain the file or boot record has changed for legitimate reasons, click Inoculate to generate new inoculation information. Otherwise, choose one of the following options to resolve the inoculation issue:
- If you suspect a virus, click Repair to return the file or boot record to the way it was when you last inoculated it.
- If you suspect a virus in a program file and have an uninfected backup copy of the file, click Delete to delete the file; then replace it with the uninfected copy.
- If you do not want to reinoculate the file and do not want future notifications about inoculating this file, click Exclude.

- Inoculation changes in boot records and system files are likely to indicate the presence of an unknown virus. Boot records and system files change legitimately in very few situations, such as when you install a new operating system or repartition your hard disk.

Click here {button ,AL("NAVDSK_I0075")} for more information.

To change how to respond to problems found during a scan:

1. Click Options in the Norton AntiVirus main window.
2. Click the Scanner tab to bring it to the front.
   If you performed a complete setup of NAV, the preset options in the Buttons To Display If Prompted group box are:
   Repair: Repairing a file or boot record returns the file to its original state.
   Delete: Deleting the file removes it from your disk. Files deleted by Norton AntiVirus cannot be recovered. After you have deleted the file, you can replace it with an uninfected copy.
   Continue: Ignores the issue.
3. Click to add or delete Buttons To Display If Prompted options.
   - Although you may want to enable the Exclude option to prevent certain files from being checked so you are not interrupted with messages, 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 a dialog box. Note that the Repair and Delete buttons may also be dimmed if NAV is unable to repair or delete the selected file.

To respond to a Norton AntiVirus alert:

1 Read the message in the alert box to understand the type of problem that was found.

2 Click the appropriate button:

- Click Repair to return the file or boot record to its original state.
- If a file cannot be repaired, click Delete to delete the file; then replace it with an uninfected copy.

  - Note that files deleted by Norton AntiVirus cannot be recovered and that NAV acts on program files (which can usually be replaced by re-installing files from the original disks).

    - Note that Norton AntiVirus also scans Microsoft Word documents (.doc and .dot) when scanning program files. Although these are not program files, they do contain code and can be infected by a class of viruses called Macro Viruses.

- Click Inoculate to generate inoculation data for a file or boot record.

NAV notifies you if the file ever changes, which could indicate an unknown virus.

- Click Exclude if you do not want to inoculate the file and do not want future notifications about inoculating this file.

Choosing this option puts you at some risk of infection by an unknown virus.

- Click Continue if you want to go ahead without taking any action.

This does not prevent Norton AntiVirus from notifying you in the future that this file has not been inoculated.

- Click Stop to halt the current operation.

For example, if you are trying to access a file, access will be denied.

- Click Info to display detailed information about the file.

 These buttons may not all be available either because Norton AntiVirus does not permit the operation, or because NAV is not configured to provide the option. To change how you respond to alerts, you can add or delete options from the Scanner, Auto-Protect, and Inoculation tabs that are available when you click Options in the Norton AntiVirus main window.

To work with scan results, do one of the following:

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 and summarizes what happened during the scan.

To use scan details:

Save or print the details about 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 main window.
The Activity Log displays a history of Norton AntiVirus activities.


After a scan, use the Activity Log to look up files that may need to be deleted and replaced.

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.


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

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, the Activity Log expands until it reaches the maximum size, and then the earliest entries are overwritten.)

4 Click Close to exit the Activity Log.

To filter the Activity Log entries:

1. Click Filter in the Activity Log dialog box.
2. Specify the types of events to display by clicking the appropriate check boxes.
3. Click OK to save settings and exit the dialog box.

To clear the Activity Log:

1. Click the Activity Log button in the Norton AntiVirus main window.
2. Click Clear in the Activity Log dialog box.
3. Click Yes to clear the Activity Log and continue.

To inoculate or uninoculate individual files or folders:

Make sure you have checked Inoculate Program Files on the Inoculation Settings tab.

1 Choose Inoculation from the Tools menu in the Norton AntiVirus main window.

2 Click Inoculate Item or Uninoculate Item.

3 Use one of the following options to select the file or files:

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

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

4 Click OK to save settings and exit the dialog box.

To set up Norton AntiVirus to inoculate during a scan:

 Make sure you have checked Inoculate Program Files on the Inoculation Settings tab.

1 From the Norton AntiVirus main window, click Options.

2 Click the Inoculation tab to bring the tab to the front and, then:

- make sure Inoculate Boot Records And System Files is checked.
- make sure that Inoculate Automatically appears in the When An Item Has Not Been Inoculated drop-down list box.

 If you performed a complete setup of Norton AntiVirus, these are the preset options.

 For maximum protection, also check Inoculate Program Files and Inoculate Files On Floppies.

3 Return to the Norton AntiVirus main window and scan the files, folders, or drives that you want to inoculate.

The files are automatically inoculated during the scan.

Click here {button ,AL("NAVDSK_I0075;NAVDSK_V0100")} for more information.

To reinoculate files or boot records that have changed:

1 From the Inoculation Changed alert, click Inoculate.

2 Click OK to exit the dialog box.

Click here {button ,AL("NAVDSK_I0075")} for more information.

To respond to an inoculation alert:

Choose one of the following:

Repair: Click if you want to replace the existing file with the information stored the first time you inoculated the file.

Inoculate: Click to inoculate the file and record a "fingerprint" of the file in an inoculation database. On future scans, Norton AntiVirus checks the file to ensure its fingerprint has not changed.

Exclude: Click to exclude the file from future checks for inoculation data.

Continue: Click to continue the scan without taking any action regarding inoculation.

Stop: Click to stop the scan.

Click here {button ,AL("NAVDSK_I0075")} for more information.

To install new virus definitions files:

 The update file you download is a special program that automatically installs the new virus definitions files on your computer.

1. Download the update program to any folder on your computer. The filename has the form *mm*NAV*yy*.EXE, where *mm* is the month and *yy* is the year.
2. From a My Computer or Windows Explorer window, double click the update program.
   The update program searches your computer for Norton AntiVirus.
3. Follow all prompts displayed by the update program.
4. The update program automatically installs the new virus definitions files in the proper folder.
   If prompted to overwrite, click Yes. Your old virus definitions files are being replaced with the new ones.
5. Initiate a scan with Norton AntiVirus to activate the new virus definitions.

Click here {button ,AL("NAVDSK_V0250;NAVDSK_I0071")} for more information.

To update virus definitions using LiveUpdate:

 After you click LiveUpdate once, it is preset to download new virus definitions files from Symantec once monthly. You can use the Norton Program Scheduler to schedule automatic LiveUpdates more frequently.

1 In the Norton AntiVirus main window, click LiveUpdate.
2 In the How Do You Want To Connect drop-down list box, select one of the following:
Find Device Automatically: Norton AntiVirus determines if you have an Internet connection or must connect using your modem.
Internet: Norton AntiVirus connects to the Symantec FTP (File Transfer Protocol) site on the Internet.
Modem: Norton AntiVirus dials a preset number and connects to a Symantec server through your modem.

 Be sure that you enter any dial-out code (for example, 9) if one is required. However, do not enter a 1 for long distance.

3 Click Next to start the automatic update.
The new virus definitions files are automatically installed and take effect on your next scan.

 If you don't have a modem or access to the Internet, you can order virus definitions update disks from Symantec to arrive by mail from Symantec. This service requires a fee:

 In the United States, call (800) 203-4403.

 Outside the United States, contact your local Symantec office or representative.

Click here {button ,AL("NAVDSK_V0550")} for detailed instructions on installing new virus definitions files.

To use the Virus List:

1. Click Virus List in the Norton AntiVirus main window.
   The Virus List displays the name of the virus and what it infects (program files, boot records, or both).
2. Use any of the following options to manage the Virus List:


Select a category from the Display drop-down list box to view different categories of viruses.


Click Info to view details, such as symptoms and aliases, about a particular virus.


Click Print to print the Virus List to a printer or to a file.

To search the Virus List:

1. Activate the Virus List box by clicking inside the list box.
2. Start entering 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 main window.
   The Virus List displays the name of the virus and what it infects (program files, boot records, or both).
2. Click in the Virus List itself. Start entering the first few letters of the virus name you are searching for.
   The Smart Search text box appears at the bottom of the list.
3. Continue entering the virus name 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 print to a printer:

1. Click Print to display a print dialog box.
2. Click Print To Printer.

To print to a file:

1. Click Print to display a dialog box.
2. Click Print To File.
3. Enter the name of a file.

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 write over the existing one.

To decide what to log:

 The Activity Log contains a history of Norton AntiVirus activity. The preset options instruct Norton AntiVirus to log detections of known viruses and record 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 main window.
2 Click the Activity Log tab to bring it to the front.
3 In the Log Following Events group box, check any event that you want Norton AntiVirus to record.
4 Click OK to save changes and close the dialog box.

To customize Scanner settings for maximum protection:

1 Click Options in the Norton AntiVirus main window.
2 Click the Scanner tab to bring it to the front.
3 Check all options in the What To Scan group box; choose 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 Advanced at the bottom of the tab.
7 Check All Floppy Drives in the Preselect At Start group box , then click OK to save settings and exit the Scanner Advanced Settings dialog box.
8 Click Heuristics at the bottom of the tab to display the Heuristics scanning options dialog where you can enable a higher level of detection for rare virus infections.
9 Click OK to save settings and exit the dialog box.

Click here {button ,AL("NAVDSK_V0135;NAVDSK_V0235;NAVDSK_V0075")} for more information.

To customize Auto-Protect settings for maximum protection:

1 Click Options in the Norton AntiVirus main window.
2 Click the Auto-Protect tab to bring it to the front.
3 Check all options in the Scan A File When group box (they are on by default).
4 Choose the All Files option in the What To Scan group box.
5 Be sure that Prompt is selected in the When A Virus Is Found drop-down list box.
6 Be sure that neither Continue nor Exclude is checked in the Buttons To Display If Prompted group box.
7 Click Advanced at the bottom of the tab.
8 Click Prompt in each of the Virus-Like Activity Monitors drop-down list boxes, then click OK to save settings and exit the dialog box.
9 Click Sensor at the bottom of the tab.
10 Check Use Virus Sensor Technology.
11 Click OK to save settings and exit the dialog box.

Click here {button ,AL("NAVDSK_V0130;NAVDSK_V0235;NAVDSK_V0075")} for more information.

To inoculate files:

Make sure you have checked Inoculate Program Files on the Inoculation Settings tab.

1 Choose Inoculation from the Tools menu.

2 Click Inoculate Item or Uninoculate.

3 Use one of the following options to select a file or files:

Click the browse button to choose a single file from a list, then click Open.

If the item is a folder, check Include subfolders to inoculate files in all descending folders.

Type the pathname for the file, group of files, folder, or drive in the Item text box.

4 Click OK to exit the dialog box.

Click here {button ,AL("NAVDSK_I0075;NAVDSK_V0050")} for more information.

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.

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

 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 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, then 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, and so on.

To remove a virus found in memory:

1 Shut down your computer using one of the following methods:

Choose the Shut Down command from the Windows Start menu.

A virus in memory means the virus has been activated, is spreading to other files, and in the worst cases, is damaging files on your disk.

Press Ctrl+Alt+Del and then click Shut Down.

2 Turn off your computer using the power switch.

Once your computer is turned off, the virus is removed from memory and is no longer spreading.

3 Next, use your NAV Rescue Disk, labeled Norton AntiVirus Emergency Boot Disk, to boot your computer and find and remove the virus.
If you don't have a NAV Rescue Disk Set, you can use your write-protected Windows 95 Emergency disk or a DOS 3.3 or higher system disk to boot your computer.

4 If you don't have a boot disk to use, create a bootable floppy disk on an uninfected computer that uses DOS 3.3 or higher.

Don't create a bootable disk on the infected computer at this time because the virus could infect it. Refer to your operating system manual for instructions on how to create a bootable floppy disk. If you don't have access to an uninfected computer, many software vendors will create a bootable disk for you if you supply a blank floppy disk.

If you don't use your Norton AntiVirus Emergency Boot Disk or an uninfected bootable floppy disk to restart your computer, you run the risk of activating the virus again.

To delete an infected file:

1. Click Delete in the Norton AntiVirus alert box, then follow the prompts on your screen.
   If the Delete command button is dimmed, either Norton AntiVirus is configured not to enable it or the item cannot be deleted. (For example, you cannot delete infected boot records or master boot records because they contain information your computer uses to start up.)
2. After deleting infected files, scan all of your drives and floppy disks with Norton AntiVirus 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.)

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

Files deleted by Norton AntiVirus cannot be recovered even with special file recovery utilities, such as the Norton Utilities. Be sure you have an uninfected copy of a file before deleting it. However, even if you don't have a clean (uninfected) 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 the file from the manufacturer.

Note that Norton AntiVirus also scans Microsoft Word and Excel documents (.doc, .dot, and .xls) when scanning program files. Although these are not program files, they do contain code and can be infected by a new class of viruses called Macro Viruses.

To repair an infected file or boot record:

1. Click Repair in the Norton AntiVirus alert box.
   If the Repair command button is dimmed, either Norton AntiVirus 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.
   In the rare instance when Norton AntiVirus is not able to repair a file or boot record, you are notified that the repair was not successful.

 Norton AntiVirus is preset to make backup copies of files before they are repaired. The backup files usually have a .VIR extension and appear in a folder showing "Virus Infected File" as the file type. Be sure to delete the backup files once you know the repair was successful.

If Norton AntiVirus 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 (such as, COMMAND.COM, IO.SYS, or WIN.COM), you can it 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 in this order: Settings, Control Panel. Add/Remove Programs, Startup Disk.

If Norton AntiVirus cannot successfully repair the master boot record or a boot record on your hard disk

 You can use your write-protected NAV Rescue Disk, labeled Norton AntiVirus Emergency Boot Disk, to restore the boot records to an uninfected state.

If Norton AntiVirus cannot successfully repair a boot record on a floppy disk

 The virus is removed and the information on the disk is still accessible. However, the floppy disk is no longer bootable.

To respond to a virus-like activity alert:

 If the message in the alert box describes an activity that is valid in the context of the application you are running, select Continue to allow the activity to proceed. (For example, if you are updating a software program and the alert warns you that there is an attempt to write to a program file, select Continue.) Otherwise, select one of the other response options:

 If the activity detected is not related to what you are trying to do, select Stop to prevent the action from taking place. (For example, if you are playing a game and receive an alert stating that there is an attempt to write to the boot records of your hard disk, select Stop to prevent your disk from being written to.)

 If the activity is valid in the context of the application you are running and you don't want Norton AntiVirus to alert you of this activity (performed by this application) in the future, select Exclude. (For example, if you are using a disk format utility to create a bootable floppy disk, you may want to select Exclude to prevent Norton AntiVirus from warning you every time you use the program to write to the boot records of a floppy disk.)

 A virus-like activity alert appears when Norton AntiVirus detects an activity that viruses often perform when spreading or doing damage to your files. A virus-like activity alert does not necessarily mean your computer has a virus; it is simply a warning. It's up to you to decide whether the operation is valid in the context in which it occurred.

To inoculate during a scan:

Choose any one of the following options that are available to you:

Inoculate: Select to inoculate the file and record a "fingerprint" of the file in an inoculation database. On future scans, Norton AntiVirus checks the file to ensure its fingerprint has not changed.

Exclude: Select to exclude the file from future checks for inoculation data.

Continue: Select to continue the scan without taking any action regarding inoculation.

Stop: Select to stop the scan.

Click here {button ,AL("NAVDSK_I0075")} for more information.

To resolve an inoculation change:

 If you are certain the file or boot record has changed for legitimate reasons, click Inoculate to generate new inoculation information. Otherwise, select an appropriate response option:

 Boot records and system files change legitimately in very few situations, such as when you install a new operating system or repartition your hard disk. Inoculation changes in boot records and system files are likely to indicate the presence of an unknown virus.

 If you suspect a virus, click Repair to return the file or boot record to the way it was when you last inoculated it.

 If you suspect a virus in a program file and have an uninfected backup copy of the file, click Delete to delete the file; then replace it with the uninfected copy. Note that files deleted by Norton AntiVirus cannot be recovered.

 If you do not want to reinoculate the file and do not want future notifications about inoculating this file, click Exclude.

 Inoculation changes in a file occur for these reasons:

 The file has changed for legitimate reasons since the last time you inoculated it. For example, you may have installed a new version of the software and forgotten to reinoculate the program file.

 The file contains a virus that is not in the definitions file (perhaps because you don't have the most recent virus definitions or because it is a new virus for which Norton AntiVirus does not yet have a definition).

Click here {button ,AL("NAVDSK_I0075")} for more information.

To restart a shutdown computer:

1. Restart your computer by placing the disk, labeled Norton AntiVirus Emergency Boot Disk in drive A:, turning on your computer.
2. When prompted, remove your first rescue disk and insert the one labeled "Norton AntiVirus Program Disk."
3. Type Go at the DOS prompt and press Enter.

   By specifying your startup drive, C:, on the command line, you'll overcome certain viruses, such as the Stoned.Empire.Monk virus, which hides the C: drive from the operating system.
   Norton AntiVirus scans the C: drive and informs you when a virus is found.
3. Once all viruses have been eliminated, remove any floppy disks and reboot your computer by switching the power off and then on to return to Windows.
4. Scan again.

Your computer shuts down when Norton AntiVirus detects a virus in memory if you select the option, Shutdown Computer, on the Auto-Protect tab in the Options dialog box.

To work with compressed files, choose one of the actions below:

WHY? Norton AntiVirus finds individual infected files that have been saved in one compressed file. However, you have to uncompress the file in order for Norton AntiVirus to repair or delete the individual infected file.

 Uncompress the compressed file using a utility such as PKUNZIP.EXE. Delete the infected file and replace it with an uninfected copy.

 Remove the whole compressed file from your disk.

In other words, if NAV finds that GOATS.COM is infected and GOATS.COM is part of ANIMALS.ZIP, you must delete the whole .ZIP file.

 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, choose one of the following methods:

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

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

To decide whether to back up:

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

 If you do back up files, you have to delete the backups after the repair has been successfully made. Norton AntiVirus adds .VIR files to the Exclusions List so they don't trigger virus alerts.

To customize alerts:

1. Enter a personalized alert message,.
   Remember that the message you enter in the Display alert message text box appears on all of the alert screens displayed in Norton AntiVirus Windows dialog boxes and the Problems Found screen.
2. Specify whether or not an audible alarm should be sounded when the alert is triggered.
3. Specify whether or not Norton AntiVirus should alert Norton AntiVirus NLM (if present).
4. Specify whether or not to forward an alert to a Norton AntiVirus alert service and choose which service from a browser.

To use virus-found information:

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

If Norton AntiVirus 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 (such as COMMAND.COM, IO.SYS, or WIN.COM), you can it using the startup disk you made when you installed Windows.

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

If Norton AntiVirus cannot successfully repair the master boot record or a boot record on your hard disk

 You can use your write-protected Norton AntiVirus Rescue Disk Set to restore the boot records to an uninfected state.

If Norton AntiVirus cannot successfully repair a boot record on a floppy disk

 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 create a NAV Rescue Disk Set:

1. Click Start on the Windows taskbar, click Programs, click the Norton AntiVirus group, and click Rescue Disk.
2. Follow the directions on the screen.

To inoculate files, choose one of the following options:

 Click Inoculate to record the "fingerprint" of the highlighted file.

 Click Inoculate All to inoculate all uninoculated files.

To exclude a file:

 Click Exclude to prevent this file from future checks.

 Use this option only if you know the file has changed for legitimate reasons. Excluding a file can allow a virus to creep in undetected.

To password-protect features:

1. Click Options in the Norton AntiVirus main window.
2. Click the Password tab.
3. Check Password Protect to turn on the password protection feature.
4. Do one of the following:
   To protect all of the features shown in the list box, select Maximum Password Protection.
   To protect only certain features, select Custom Password Protection; then click the features you would like to protect in the list box.
5. Click Set Password and enter the password you want to use in the Set Password dialog box. The same password applies to all selected features.
   Passwords can be from 1 to 16 characters in length and are not case-sensitive (a is the same as A). As you type, Norton AntiVirus replaces the characters on the screen with asterisks (*) for security.
6. Click OK in the Set Password dialog box.
7. Click OK.

Norton AntiVirus also asks for the password before allowing changes to the password protection options.

To remove viruses from downloaded files:

1. Scan the file from the Norton AntiVirus 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 to make sure there aren't any other files that contain viruses.

Unable to Repair a File

If Norton AntiVirus cannot 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 to delete the highlighted file (or 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 compressed files:

If Norton AntiVirus 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 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 to make sure there aren't any other files that contain viruses.

Unable to Repair a File

If Norton AntiVirus cannot 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 (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 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 initiate scans:

1. Open the Norton AntiVirus main window if it is not already displayed.
2. Choose one of the following options:

    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.

    If the All Network Drives option is dimmed, see the Scanner Advanced Settings dialog box to check All Network Drives and then reconfigure this option.

    Choose Folders from the Scan menu, select the folder, and click Scan.

    Click File from the Scan menu, select the file or type in a filename, and click Open.

   The Scan dialog box reports on the progress of the scan.

Click here {button ,AL("NAVDSK_V0075;NAVDSK_V0065")} for more information.

To scan networks:

1. Click Options in the Norton AntiVirus main window.
2. Click the Scanner tab to bring it to the front.
3. Click Advanced at the bottom of the tab.
4. Check Allow Network Scanning. (This is not a preset option when you perform a complete setup of NAV.)
5. Click OK to close the dialog box.
6. Click OK to save your settings and close the Options dialog box.

To use the Network Browser:

1 Select an item from the browser or type the name of the item to add in the Target text box.

When typing a server name, in the Target text box, precede it with two backward slashes; for example, \\server19.

2 Click OK.