Virus Information

Note: Right-click any of these options 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.
- Multipartite Viruses: Viruses that infect both program files and boot records.
- Windows Viruses: Viruses that infect Windows programs.
- Macro Viruses: Viruses that infect macros (for example, macros in Microsoft Word and Excel documents).
- Malicious programs: Viruses that infect agent programs (such as those that download software from the Internet, for example, Java and Active X).

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

Note: 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 quarantine the file that contains the virus and submit it to SARC (Symantec AntiVirus Research Center) for further analysis or delete the file and replace it with an uninfected copy.

{button ,AL("RespondBasics",0,`',`')} **More Info…** Click for more information.

Norton AntiVirus Main Window For System Status

The Norton AntiVirus main window with System Status selected lets you get information about virus protection on your system:

The status of Auto-Protect is displayed. It is recommended that Auto-Protect always be enabled so that it can check for viruses while running in the background. Click the Disable/Enable button to turn off or on the Auto-Protect feature.

The list box contains several lines of status information. Each line contains a brief statement. You can select a line and click Details to get more information.

The Norton AntiVirus main window organizes the principle AntiVirus features into four groups. In addition to System Status you can:

- Click Scan for Viruses to run predefined scans or define new scans for later use. Predefined scans are listed in the text box.
- Click Reports to view Norton AntiVirus activity logs or use the Quarantine function to isolate infected or suspicious files for submission to Symantec AntiVirus Research (SARC).
- Click Scheduling to set up a scheduled scan to run when it is convenient for you.

You can also click any of the top buttons to help you better take advantage of Norton AntiVirus features:

- Click LiveUpdate to automatically update virus definitions and program updates.
- Click LiveAdvisor to connect to Symantec for messages about product information, upgrades, updates, and technical tips for the Symantec products you register.
- Click Rescue to create either a Zip Rescue disk or a set of rescue floppy disks.
- Click Options to customize Norton AntiVirus features.
- Click Help to get more information about the window you are viewing.

To get Help for many options in the Norton AntiVirus main window, position the cursor over the option, right-click, and choose What's This?

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

{button ,AL("Introduction")} **More Info…**… Click for more information.

Scan Results

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

Here is some additional information about the scan results:

- Scanned: Indicates whether files, master boot record, and/or boot records were scanned.
- Infected: Indicates which and/or how many of the above items, if any, were infected.
- Repaired, Quarantined or Deleted: Indicates how many items, if any, were repaired, quarantined or deleted.

{button ,AL("Scan")} **More Info…** Click for more information.

Details of Scan

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

- If you see that a file is still infected, you should try to repair it.
- If you attempted to repair it and it could not be repaired, you should quarantine the file or 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, quarantining, 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 selected virus.

{button ,AL("Scan")} **More Info…** Click for more information.

Problems Found

Note: Right-click any of these options 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 boot records

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

What to do if a virus was found:

1 If a file is infected, click Repair to have Norton AntiVirus attempt to restore it.

2 If an infected file or a file cannot be repaired, do one of the following:

- Click Quarantine to isolate the file (prevent it from being accessed or run). Quarantined files can be submitted to Symantec AntiVirus Research Center (SARC) for further analysis.
- 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.

{button ,AL("Respond")} **More Info...** Click 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 important to update your virus definitions regularly because new viruses are discovered all the time. If you have a modem or an Internet connection, 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 virus definitions.

{button ,AL("VirusProcs;VirusBasics")} **More Info…** Click for more information.

Virus Information

Note: Right-click any of these options 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, quarantine, 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.
- Windows Viruses: Viruses that infect Windows programs.
- Macro Viruses: Viruses that infect macros (for example, macros in Microsoft Word and Excel documents).
- Malicious programs: Viruses that infect agent programs (such as those that download software from the Internet, for example JAVA and Active X).
- Comments: Further description of the selected virus's characteristics.

{button ,AL("VirusProcs")} **More Info…** Click for more information.

System Integrity

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

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

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

Note: You should choose this option with caution since repairing after upgrading an operating system (for example, from Windows 95 to Windows 98) can cause system problems.

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

Note: You should choose Inoculation when you have upgraded an operating system (for example from Windows 95 to Windows 98).

- Continue: Continues the scan without responding to the change.
- Stop: Stops the scan and returns you to the Norton AntiVirus main window.

You must reinoculate if you've upgraded your operating system or converted from a 16 bit to 32 bit environment. If you choose Repair, you will lose the system changes and create problems.

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. Click Delete All to have Norton AntiVirus delete all the infected files found during the scan.

Note: 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 Macro Viruses.

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

Activity Log

Note: Right-click any of these options 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: 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.

{button ,AL("Respond",0,`',`')} More Info… Click 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 Virus Detections. Specify the types of events to display by selecting the appropriate check boxes.

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

{button ,AL("Respond")} **More Info…** Click for more information.

Exclude file

From the Exclude File dialog box you can exclude a 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:

1 From the Norton AntiVirus main window, click Options.

2 Click Exclusions and then 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.

{button ,AL("Exclusions")} **More Info…** Click for more information.

Inoculation changed

When Norton AntiVirus alerts you that a boot record's inoculation data has changed, do one of the following:

- If you are certain that the change is for legitimate reasons, click Inoculate to generate new inoculation information.

Note: Boot records change legitimately in very few situations. Upgrading operating systems (for example, from Windows 95 to Windows 98) is one of the few legitimate causes.

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

{button ,AL("Respond")} **More Info…** Click for more information.

Manual Scans Settings

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

The Manual Scans options let you choose settings that determine:

- What to scan in addition to files
- How Norton AntiVirus should respond when a virus is detected (If you select Custom Virus 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 types of files to scan

For maximum protection you should leave the preset options as they are.

{button ,AL("Scan",0,`',`')} More Info… Click 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.

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 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. Norton AntiVirus can then scan and protect them against infection.
- Other options are:
  - Click Remove to delete a selected file extension. Be careful, however. Removing extensions from the list reduces your protection against viruses.
  - Click Defaults to return the file extensions list to the preset options.

Auto-Protect Advanced Settings

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

The Auto-Protect Advanced options let you select which virus-like activities to allow or disallow.

- For maximum protection, you should also change all of these options to Ask Me What To Do. This option lets you decide which activities are legitimately performed by each file.
- You should also keep the preset options in the Floppy Disk Scans group box. (The first two options should be selected.)

{button ,AL("AutoProtect")} **More Info…** Click for more information.

Auto-Protect Settings

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

The Auto-Protect options allow 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 Select both options in the Scan Files When They Are group. (Note that the Run OrOpened option includes when a file is copied or moved.)

2 Click All Files if it is not already selected.

3 Always make sure that Start Auto-Protect When Windows Starts Up is selected.

4 Click Bloodhound under Auto-Protect and enable Bloodhound, which can dramatically increase your protection against new and unknown viruses.

{button ,AL("AutoProtect")} **More Info…** Click for more information.

Email Protection Settings

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

The Email Protection settings allow you to turn on email protection and select your email client program. You also select the response you want from Norton AntiVirus when an infected attachment is found in an email message.

Norton AntiVirus can automatically configure several popular email clients to allow virus checking. If your email client is not listed, check Manually Configured Email Client and then configure it manually.

{button ,AL("email")} **More Info…** Click for more information.

Email Protection Advanced Settings

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

The Email Protection Advanced settings allow you to display the email scanning icon in the notification area of the task bar, and to briefly display the Norton AntiVirus logo screen when email scanning starts.

You may select the option of temporarily disabling email protection. This disables email scanning without reconfiguring your email client.

You can turn off protection against timeouts when scanning email. This option, enabled by default, keeps your email client from displaying timeout errors while Norton AntiVirus is scanning large attachments.

{button ,AL("email")} **More Info…** Click for more information.

Startup Scan Settings

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

The Startup Scan options allow 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, select all the options in the Items To Scan group.
- You can also change the key you can use to bypass startup scans. This bypass feature is available whenever you start up the computer if you have selected a key.


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

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

The Inoculation tab lets you customize inoculation options. If you use the preset options you are well-protected.

Note: You may be notified of an inoculation change to a boot record whenever you upgrade software. This could result in many inoculation alerts. For this reason, the default is to enable Inoculate Boot Records.

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.

{button ,AL("Inoculation;ScanBasics")} **More Info...** Click for more information.

Activity Log Settings

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

The Activity Log options allow you to customize which Norton AntiVirus activities are stored in the log. 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, quarantined, 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.

You should use the preset options.

{button ,AL("Respond")} **More Info…** Click for more information.

Exclusions Settings

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

The Exclusions options allow you to exclude a file from being checked for viruses.

- 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.

{button ,AL("Exclusions")} **More Info…** Click for more information.

New/Edit Exclusion

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

Be careful! If you set an exclusion, you have reduced the level of protection against viruses.

{button ,AL("Exclusions")} **More Info...** Click for more information.

General Settings

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

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

You can select Back Up File In Quarantine Before Attempting A Repair to have Norton AntiVirus make a copy of the infected file before repairing it. The backed up file will be in the Quarantine folder as a backup item. The file cannot be accessed or run.

You can select Display The Logo Screen When Starting Norton AntiVirus to display the Norton AntiVirus logo whenever the program starts.

{button ,AL("Options")} **More Info…** Click 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).

Overwrite/Append

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

- 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

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).

There are three fields on this window.

- 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.

Verify Password

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

Virus Found in Download

Note: Right-mouse click any option (button, check box, 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.

Note: If 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.

Note: 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.

{button ,AL("Respond")} **More Info…** Click for more information.

Alerts Settings

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

The Alerts page lets you define how Norton AntiVirus informs you that it has detected a virus or possible virus. These options apply to all scans that Norton AntiVirus performs (scans you initiate, scheduled scans, and scans performed automatically by Auto-Protect or the Windows scanner).

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.

Bloodhound options

Norton AntiVirus includes a technology called Bloodhound, which dramatically increases your virus protection against new and unknown viruses. You can enable or disable Bloodhound by selecting or unselecting the check box. You can also drag the pointer to increase Bloodhound's sensitivity to possible viruses.

Bloodhound isolates and locates the various logical regions of a file and then analyzes the program logic for virus-like behavior. Bloodhound detects a high percentage of unknown viruses. In addition, Norton AntiVirus detects unknown viruses by monitoring activity on your computer for behaviors that viruses typically perform. When a suspicious activity is detected, Norton AntiVirus prevents the action from continuing.

Quarantine

Sometimes Norton AntiVirus detects an unknown virus that can't be eliminated with the current set of virus definitions. Or, you have file you think is infected that is not being detected. From the Norton AntiVirus Quarantine, a file can be sent over the Internet directly to the Symantec AntiVirus Research Center (SARC) for analysis. SARC determines if your file is infected, and then reports the results to you. If a new virus is discovered in your submission, SARC will create and send you updated virus definitions to detect and eliminate the new virus on your computer.

You must have an Internet connection and an email address to submit a sample and receive a reply. You are notified by email with the results of the analysis within seven days.

In addition to Quarantined files, the Quarantine stores two other groups of items:

- Backup Items: For data safety, Norton AntiVirus is preset to make a backup copy of a file before attempting a repair. These backups are also stored in the Quarantine. If the file is unrepairable, Quarantine automatically deletes it. If the files can be repaired, you may delete the infected item from the Quarantine once the repair is verified.
- Items Submitted To SARC: Files sent to SARC for analysis are isolated. After receiving the results of the analysis, you can determine what to do with the item.

Norton AntiVirus Main Window for Scans

The Norton AntiVirus main window with Scan for Viruses selected lets you manage the virus scans on your system:

The list box displays the names of predefined scan tasks. There are some built-in tasks and you can add new ones. You may run an existing task or define a new one. You can edit any tasks you create, except the built-in ones.

- To run a scan, select it from the list and click Run Scan Now.
- To create a new scan task, click Create New Scan. The Scan Task wizard will appear. Click Next go to the second wizard page. Add any folders and/or files you want scanned by this task. When you have selected all the folders and files, click Next and type in a descriptive name for this task. This is the name that will show up in the list box. Click Finish when you are done.
- Click More Actions to edit, delete, or rename a scan task. From this drop-down menu you can also select categories of scan tasks to view and look at the properties of a selected task.

The Norton AntiVirus main window organizes the principle AntiVirus features into four groups. In addition to Scan For Viruses you can:

- Click System Status to display information important to the virus protection of your computer. The text box provides summary text for which you can get more detail by clicking Details.
- Click Reports to view Norton AntiVirus activity logs or use the Quarantine function to isolate infected or suspicious files for submission to Symantec AntiVirus Research (SARC).
- Click Scheduling to set up a scheduled scan to run when it is convenient for you.

You can also click any of the top buttons to help you better take advantage of Norton AntiVirus features:

- Click LiveUpdate to automatically update virus definitions and program updates.
- Click LiveAdvisor to connect to Symantec for messages about product information, upgrades, updates, and technical tips for the Symantec products you register.
- Click Rescue to create either a Zip Rescue disk or a set of rescue floppy disks.
- Click Options to customize Norton AntiVirus features.
- Click Help to get more information about the window you are viewing.

To get Help for many options in the Norton AntiVirus main window, position the cursor over the option, right-click, and choose What's This?

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

{button ,AL("Introduction")} **More Info...** Click for more information.

Norton AntiVirus Main Window For Reports

The Norton AntiVirus main window with Reports selected lets you activate the Quarantine feature or view predefined Norton AntiVirus reports:

- Select View And Manage The Items In Quarantine and click Open to start the Quarantine feature. Quarantine lets you isolate infected or suspicious files for submission to Symantec AntiVirus Research (SARC).
- Select View The Log Of Norton AntiVirus Activities and click Open to view a history of Norton AntiVirus activities.
- Select the third list item and click Open to view the list of viruses that Norton AntiVirus is protecting you against.

The Norton AntiVirus main window organizes the principle AntiVirus features into four groups. In addition to Reports you can:

- Click System Status to display information important to the virus protection of your computer. The text box provides summary text for which you can get more detail by clicking Details.
- Click Scan for Viruses to run predefined scans or define new scans for later use. Predefined scans are listed in the text box.
- Click Scheduling to set up a scheduled scan to run when it is convenient for you.

You can also click any of the top buttons to help you better take advantage of Norton AntiVirus features:

- Click LiveUpdate to automatically update virus definitions and program updates.
- Click LiveAdvisor to connect to Symantec for messages about product information, upgrades, updates, and technical tips for the Symantec products you register.
- Click Rescue to create either a Zip Rescue disk or a set of rescue floppy disks.
- Click Options to customize Norton AntiVirus features.
- Click Help to get more information about the window you are viewing.

To get Help for many options in the Norton AntiVirus main window, position the cursor over the option, right-click, and choose What's This?

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

{button ,AL("Introduction")} **More Info...** Click for more information.

Norton AntiVirus Main Window For Scheduling

The Norton AntiVirus main window with Scheduling selected lets you manage the virus scans on your system:

The list box displays the names of scheduled events. You can modify, view the properties of, or delete any existing event. You can also create a new scheduled event.

- To create a new scheduled event, click New Event. The Scheduling wizard will appear. Click Next go to the second wizard page. Select the type of event you want to create, then click Next. Follow the rest of the Scheduling wizard supplying the information requested for the type of event you selected.
- Click More Actions to delete an event or change the schedule of an event. From this drop-down menu you can also select categories of scan tasks to view and look at the properties of a selected task.
- Click Event Properties to view the properties of an event.

The Norton AntiVirus main window organizes the principle AntiVirus features into four groups. In addition to Quarantine and Reports you can:

- Click System Status to display information important to the virus protection of your computer. The text box provides summary text for which you can get more detail by clicking Details.
- Click Scan for Viruses to run predefined scans or define new scans for later use. Predefined scans are listed in the text box.
- Click Reports to view Norton AntiVirus activity logs or use the Quarantine function to isolate infected or suspicious files for submission to Symantec AntiVirus Research (SARC).

You can also click any of the top buttons to help you better take advantage of Norton AntiVirus features:

- Click LiveUpdate to automatically update virus definitions and program updates.
- Click LiveAdvisor to connect to Symantec for messages about product information, upgrades, updates, and technical tips for the Symantec products you register.
- Click Rescue to create either a Zip Rescue disk or a set of rescue floppy disks.
- Click Options to customize Norton AntiVirus features.
- Click Help to get more information about the window you are viewing.

To get Help for many options in the Norton AntiVirus main window, position the cursor over the option, right-click, and choose What's This?

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

{button ,AL("Introduction")} **More Info…** Click for more information.

Scheduling

Note: Right-click any of these options and choose What's This? to display an explanation of what it does.

The Scheduling page lets you define how the scheduler functions.

As soon as you install Norton AntiVirus, you are already protected against viruses.

From the main window you can do the following:

- Click Scan For Viruses to run a predefined scan or define a new scan.
- Click System Status to view detailed information about virus protection on your computer.
- Click Reports to run Quarantine or view activity logs and the virus list.
- Click Scheduling to set up or edit events that run automatically.
- Click LiveUpdate to automatically update virus definitions and program files.
- Click LiveAdvisor to connect to Symantec for messages about product information, upgrades, updates, and technical tips for the Symantec products you register.
- Click Rescue to create either a Zip Rescue disk or a set of rescue floppy disks.
- Click Option to customizes Norton AntiVirus features.

Click to disable (or enable) automatic protection. Disabling automatic protection is not recommended unless you have been requested to do so in order to install new software. Disabling automatic protection seriously reduces your protection against virus infection.

Click to see the status of your quarantined files and/or the status of virus definition updates.

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 Virus Information dialog box.

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 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 Quarantine to display the Quarantine dialog box where you can isolate the infected file (prevent it from being accessed or run). From the Quarantine dialog box, you can also submit the file for further analysis by SARC (Symantec AntiVirus Research Center).

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 the Activity Log Filter dialog box, where you can choose to display one or more specific types of Norton AntiVirus events.

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

Click Close to exit the Activity Log.

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 malicious programs. 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. Norton AntiVirus uses virus definitions (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 regularly. 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.

Note: 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 the 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 the 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.

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

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

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

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.

- If the file remains infected, you should try to repair it.
- If it cannot be repaired, you should do one of the following:
- delete the file and replace it with a clean copy.
- quarantine the file to prevent it from being accessed or run.
- 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.

Click Close to exit the Virus List without saving any changes to the settings.

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 Norton AntiVirus 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.

Click to quarantine the selected file.

Click to quarantine all files.

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

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

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.

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.

Click Inoculate to inoculate the item.

Click Inoculate to inoculate the item.

Click Continue to continue without taking any action.

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

Click Inoculate to inoculate the selected item only.

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

The System Integrity dialog box notifies you about changes in system files and boot records. Your options are:

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

  Note: You should choose this option with caution since repairing after upgrading an operating system (for example, from Windows 95 to Windows 98) can cause system problems.

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

  Note: You should choose Inoculation when you have upgraded an operating system (for example from Windows 95 to Windows 98).

- Continue: Continues the scan without responding to the change.
- 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 Info to display information about the virus.

Click Repair to restore the boot record to match its "fingerprint" taken when you first inoculated the item.

Click Inoculate to reinoculate the boot record.

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

Specifies what item is to be inoculated or uninoculated.

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.

Allows you to continue the current operation. No change is made to the inoculation data.

Sometimes Norton AntiVirus detects an unknown virus that can't be eliminated with the current set of virus definitions. Or, you have file you think is infected that is not being detected. From the Norton AntiVirus Quarantine, a file can be sent over the Internet directly to the Symantec AntiVirus Research Center (SARC) for analysis. You must have an Internet connection to submit a sample and an email address to receive a reply. You are notified by email with the results of the analysis within seven days.

Scanned: Lists whether memory, master boot record, boot records, or files were scanned.

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

Repaired, Quarantined or Deleted: Indicates how many items, if any, were repaired, quarantined or deleted.

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

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

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

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

Excludes the item from monitoring of 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 so that the master boot record and boot records on your hard disk receive inoculation protection.

Lists all the predefined and user defined scans. Double-click one to run it.

Click to run the scan selected in the Scans list box above.

Click to run the Scan Wizard to define a scan with particular parameters.

Drop-down list of commands to edit, delete, remove predefined scans and to change what is displayed in the Scans list box.

Lists information about the status of virus protection on your computer. Select an item and click Details to get more information.

Click to display more information about the item selected in the Status list box.

Lists reporting features. Double-click an item to open..

Click to open the report selected in the Reports list.

List of scans scheduled to run automatically.

Click to run the Scheduling Wizard and define a new event which will run automatically.

Drop-down list of commands to edit or delete scheduled events.

Click to display more information about the event selected in the Scheduled Events list box.

Click Close to exit the Virus List.

Click Find to enter the name of a virus you want to locate.

Click Find Next to find the next virus that matches the name entered in the Find a virus dialog.

Introducing Norton AntiVirus

When you install Norton AntiVirus and accept the preset options, your computer is safe. As part of the installation, your computer is scanned for viruses.

Norton AntiVirus automatically checks boot records for viruses at system startup, checks programs for viruses at the time you use them, scans all local hard drives for viruses once per week, and monitors your computer for any activity that might indicate the work of a virus in action. It also scans files you download from the Internet and checks floppy disks for boot viruses when you use them.

With Norton AntiVirus, you can scan files, folders, or entire drives for viruses, and quarantine infected files for submission to the Symantec AntiVirus Research Center (SARC). Files submitted to SARC are analyzed and the results are reported automatically within seven days.

To use Norton AntiVirus, click Norton AntiVirus on the left side of the screen.

{button ,JI(`>maintwo',`IDH_NAV_Key_tasks')} **How to…** Click here to see important tasks you can perform with Norton AntiVirus.

You may also select one of these features available from the top bar of the Norton AntiVirus main window.

- LiveUpdate automatically updates virus definitions and program updates.
- LiveAdvisor connects to Symantec for messages about product information, upgrades, updates, and technical tips for the Symantec products you register.
- Rescue creates either a Zip Rescue disk or a set of rescue floppy disks.
- Options customizes Norton AntiVirus features.
- Help presents more information about the window you are viewing.

{button ,AL("Introduction;MainWindow",0,`',`')} **More Info...** Click for more information.

How Norton AntiVirus works

The scanner, which examines program files for the signatures of known viruses, is the heart of Norton AntiVirus protection. It searches for virus signatures when you initiate manual scans, when you schedule scans to run at specific times, during startup scans that run automatically every time you start your computer, and by the Auto-Protect feature every time a file is used. The scanner also verifies that boot records protected by inoculation have not been altered.

Manual scans

Use the Scan Now button in the Norton AntiVirus main window to initiate manual scans. These scans detect known viruses in specific files, folders, or drives on your computer.

Scheduled Scans

Scheduled scans are manual scans that run automatically at predetermined times. These scans supplement other automatic protection features to ensure that your computer is virus-free. As part of the Norton AntiVirus installation, a scan of your computer is scheduled to run automatically once per week.

Startup Scans

The first wave of defense against virus attacks are special scans that occur automatically each time your computer starts up. These scans catch viruses that infect the files and boot records your computer uses to ready itself for work. Startup scans are a vital part of virus protection because they make sure that your computer is virus-free each time you start it up. The startup scan is turned on during installation, unless you specifically turn it off.

Auto-Protect

Auto-Protect, the Norton AntiVirus automatic protection feature, scans program files, documents, and document template files for viruses whenever they are used. Auto-Protect, in addition to checking files for known viruses, uses Bloodhound technology and virus-like activity monitors (such as an attempted format of a hard disk) to make sure that unknown viruses are neither infecting your computer nor damaging data during the course of normal operation. Auto-Protect is already turned on after installation, unless you specifically turn it off.

Inoculation

Once your disks are scanned to verify that they are free of viruses, Norton AntiVirus inoculates boot records to makes sure they stay virus-free. When a boot record is inoculated, Norton AntiVirus records critical information about it (similar to taking a fingerprint) in a special file designed specifically to store this inoculation data. On subsequent scans, Norton AntiVirus compares the current fingerprint to its stored fingerprint. You are alerted if there are any changes that could indicate the presence of a virus. Boot records are inoculated automatically as part of your Norton AntiVirus installation.

Virus definitions files

Virus definitions files contain information that Norton AntiVirus uses during scans to detect known viruses. Norton AntiVirus depends on up-to-date information. Each time a new virus is discovered, its virus signature must be added to a virus definitions file. You should update your virus definitions files at least once per month so that Norton AntiVirus has the information it needs to find all known viruses. New virus definitions files are available from Symantec regularly. If you have a modem or an Internet connection, Norton AntiVirus can update your virus definitions files for you automatically.

All computer viruses fall into two groups:

- **Known viruses:** A known virus has been identified. 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 from the Scan For Viruses page of 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 need to update your virus definitions file regularly. Symantec has made this easy with the automatically scheduled Live Update feature.

- **Unknown viruses:** An unknown virus is one that does not yet have a virus definition. Norton AntiVirus includes an advanced heuristic technology called Bloodhound to detect unknown program and macro viruses. Bloodhound isolates and locates the various logical regions of a file and then analyzes the program logic for virus-like behavior. Bloodhound detects a very high percentage of unknown viruses. In addition, Norton AntiVirus detects unknown viruses by monitoring activity on your computer for behaviors that viruses typically perform. When a suspicious activity is detected, Norton AntiVirus prevents the action from continuing.

{button ,AL("Introduction",0,`',`')} **More Info...** Click for more information.

About Norton AntiVirus Auto-Protect

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

- Detecting viruses that may already exist and removing them.
- Preventing viruses from infecting your computer.
- Monitoring for activity that may indicate an unknown virus.

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.

To enable Auto-Protect:

1 Right-click the Norton AntiVirus icon in the lower right corner of the taskbar on your Windows desktop.

2 Click Enable Auto-Protect.

The button changes to Disable Auto-Protect and the icon changes.

Note: Norton AntiVirus is preset to enable Auto-Protect whenever you start your computer.

To disable Auto-Protect temporarily:

1 Right-click the Norton AntiVirus icon in the lower right corner of the taskbar on your Windows desktop.

2 Click Disable Auto-Protect.

The button changes to Enable Auto-Protect and the icon changes.

{button ,AL("AutoProtect;IntroCommon",0,`',`')} More Info. . . Click for more information.

The importance of Rescue Disks

- When you set up Norton AntiVirus, you were advised to create Rescue Disks. If you did not do so then, you should create the disks now. The Rescue Disk option can be found by opening the Windows Start menu, pointing to Programs and pointing to Rescue Disk. If you did create Rescue Disks, 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 restart your computer with the Rescue Disks. These disks contain a backup copy of all information necessary to restore your computer to an uninfected state. If you do not have Rescue Disks, 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.

{button ,AL("Rescue",0,`',`')} **More Info...** Click for more information.

What is a computer virus?

Computer viruses are executable computer programs. Like biological viruses, they find and attach themselves to a host. Just as a cold virus finds and attaches itself to a human host, a computer virus attaches itself to an item, such as a computer startup area (boot record) or an executable file.

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.

Viruses are categorized by their infection targets:

Program viruses infect program files, which commonly have extensions such as .COM, .EXE, .SYS, .DLL, .OVL, or .SCR. The most common programs targeted by viruses are standard DOS programs that use the .COM and .EXE file extensions. Program files are attractive targets for virus writers because they are widely used and have relatively simple formats to which viruses can attach.

Boot viruses infect the non-file (system) areas of hard and floppy disks. These areas offer an efficient way for a virus to spread from one computer to another. Boot viruses have achieved a higher degree of success than program viruses in infecting their targets and spreading.

Macro viruses infect data files with macro capabilities and are the newest threat to the computing public. For example, Microsoft Word document and template files are susceptible to macro virus attacks. They spread rapidly as infected documents are shared on networks or downloaded from Internet sites.

{button ,AL("VirusBasics",0,`',`')} **More Info...** Click for more information.

What viruses do and don't do

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 damaging; they simply replicate or display messages.

Viruses do the following:

- Infect executable program files, such as word processing, spreadsheet, or operating system programs.
- 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.
- Infect a file before it is attached to an email message, data disks and disks used to transfer programs.

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 merely affected the programs that control the display or keyboard. Not even your disks are physically damaged, just what's stored on them. Viruses can only infect files and corrupt data.
- Infect write-protected disks or text-based email messages.

Note: 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 Macro Viruses.

{button ,AL("VirusBasics",0,`',`')} **More Info...** Click for more information.

Types of viruses

Viruses are categorized by their infection targets:

- Program viruses infect program files, which commonly have extensions such as .COM, .EXE, .SYS, .DLL, .OVL, or .SCR. The most common programs targeted by viruses are standard DOS programs that use the .COM and .EXE file extensions. Program files are attractive targets for virus writers because they are widely used and have relatively simple formats to which viruses can attach.
- Boot viruses infect the non-file (system) areas of hard and floppy disks. These areas offer an efficient way for a virus to spread from one computer to another. Boot viruses have achieved a higher degree of success than program viruses in infecting their targets and spreading.
- Macro viruses infect data files with macro capabilities and are the newest threat to the computing public. For example, Microsoft Word document and template files are susceptible to macro virus attacks. They spread very rapidly as infected documents are shared on networks or downloaded from Internet sites.

Program Viruses: Like normal programs, program viruses must be written for a specific operating system. The vast majority of viruses are written for DOS but some have been written for Windows 3.x, Windows 95/98, and even UNIX. All versions of Windows are compatible with DOS and can host DOS viruses with varying degrees of success.

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

Unlike program viruses, almost any boot virus can infect DOS, Windows 3.x, Windows 95/98, Windows NT, and even Novell Netware systems. This is because they exploit inherent features of the computer (rather than the operating system) to spread and activate.

Many boot viruses assume the hard disk is using a normal DOS file system. Such an assumption is not always correct if you are using an operating system other than DOS or Windows 3.x. On Windows NT, for example, you can choose to use the NTFS file system instead of the DOS-compatible FAT file system. If a virus encounters a system using NTFS, it still successfully infects the computer but it may accidentally damage some of your files or boot records (disk system areas) in the process. When this happens, NT won't be able to start and you may need to reinstall Windows.

Another interesting aspect of Windows NT is that it will disable any boot viruses when it starts, assuming it can still start. This means that boot viruses can infect a machine running Windows NT but they can't spread to other systems while Windows NT is running. Don't, however, assume that the virus is benign. Every time you boot your system, the virus activates and has a chance to activate its trigger and deliver its payload. For example, on March 6th, the Stoned.Michelangelo virus writes random bytes to every cylinder on the hard drive, corrupting the original data. In a fraction of a second, key non-file areas used on computer start-up are the first to be wiped out in the process. It is virtually impossible to prevent the virus from destroying all data on the hard disk once the destructive trigger routine has activated.

Macro viruses: Many older applications had simple macro systems that allowed you to record a sequence of operations within the application and associate them with a specific keystroke. Later, you could perform the same sequence of operations by merely hitting the specified key.

Newer applications provide much more complex macro systems. You can write entire macro-programs that run within the word processor or spreadsheet environment and are attached directly onto word processing and spreadsheet files. The ability to tote one or more macros around with a data file is a very powerful feature. Unfortunately, this ability also makes it possible to create macro viruses.

A typical chronology for macro virus infection begins when an infected document or spreadsheet is loaded. The application also loads any accompanying macros that are attached to the file. If one or

more of the macros meet certain criteria, the application will also immediately execute these macros. Macro viruses rely upon this auto-execution capability to gain control of the application's macro system.

Once the macro virus has been loaded and executed, it waits for you to edit a new document, then kicks into action again. It attaches its virus macro programs onto the new document, then allows the application to save the document normally. In this fashion, the virus spreads to another file and does so in a completely discrete fashion. You have no idea of the infection. If this new file is later opened on another computer, the virus will once again load, be launched by the application, and find other unsuspecting files to infect.

Finally, as far as a macro virus is concerned, the application serves as the operating system. A single macro virus can spread to any of the platforms on which the application is installed and running. For example, a single macro virus that uses Microsoft Word could conceivably spread to Windows 3.x, Windows 95/98, Window NT, and the Macintosh.

Stealth Viruses: Stealth viruses actively seek to conceal themselves from attempts to detect or remove them. They use techniques such as intercepting disk reads to provide an uninfected copy of the original item in place of the infected copy (read-stealthing viruses), altering disk directory or folder data for infected program files (size-stealthing), or both. For example, the Whale virus is a size-stealthing virus. It infects .EXE program files and alters the folder entries of infected files when other programs attempt to read them. The Whale virus adds 9216 bytes to an infected file. Because changes in file size are an indication that a virus might be present, the virus then subtracts the same number of bytes (9216) from the file size given in the directory/folder entry to trick the user into believing that the file's size has not changed.

Polymorphic Viruses: Most simple viruses attach identical copies of themselves to the files they infect. An anti-virus program can detect the virus's code (or signature) because it is always the same and quickly ferret out the virus. To avoid such easy detection, polymorphic viruses operate somewhat differently. Unlike the simple virus, when a polymorphic virus infects a program, it scrambles its virus code in the program body. This scrambling means that no two infections look the same, making detection more difficult.

Multipartite Viruses: Multipartite viruses are both program and boot viruses. For example, if you run a word processing program infected with the Tequila virus, the virus activates and infects your hard disk boot record. Then, the next time you boot your computer, the Tequila virus activates again and starts infecting every program you use, whether it is on a hard or floppy disk. Windows Viruses: Viruses that infect Windows programs.

Companion Viruses: A companion virus is the exception to the rule that a virus must attach itself to a file. The companion virus instead creates a new file and relies on a behavior of DOS to execute it instead of the program file that is normally executed. Companion viruses use a variety of strategies. Some companion viruses create a .COM file with a name identical to an existing .EXE file. For example, the companion virus might create a file named CHKDSK.COM and place it in the same directory as CHKDSK.EXE. Whenever DOS must choose between executing two files of the same name where one has an .EXE extension and the other a .COM extension, it executes the .COM file.

Malicious programs: Viruses that infect agent programs (such as those that download software from the Internet; for example, JAVA and ActiveX).

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. (This is not an option for NEC PC98xx machines.)

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.

{button ,AL("VirusBasics",0,`',`')} **More Info...** Click for more information.

Scanning for viruses on your computer

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, 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 and select Scan For Virus if it is not already selected.

2 Choose one of the following options:

- Select one of the predefined scans from the list and click Run Scan Now.
- Click Create New Scan to define a new scan and then run your new scan.

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

{button ,AL("Scan",0,`',`')} **More Info...** Click for more information.

Removing viruses from your computer

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 also have the option of quarantining the file for further investigation. When a file is quarantined, you cannot access the file or run it. You can submit quarantined files to the Symantec AntiVirus Research Center for further investigation.

- 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: 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 Macro Viruses. Therefore, some of your data files are now at risk. You need to make backup copies regularly.

{button ,AL("RespondBasics",0,`',`')} **More Info...** Click for more information.

What to do when Norton AntiVirus alerts you

Norton AntiVirus alerts you when:

- A known virus or unknown virus is found.
- A virus-like activity is detected (an operation that viruses often perform when spreading or damaging files).
- The inoculation data for a boot record has changed.

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 Follow the instructions for one of the following conditions:

- Repair an infected file or boot record
- Quarantine an infected or suspicious item
- Delete an infected file
- Respond to a virus-like activity alert
- Respond to an inoculation change alert


You should not leave an infected file on your computer. Norton AntiVirus can repair most infected files. However, in the case that a file cannot be repaired, you must delete it from your disk or quarantine the file so it cannot be accessed or run outside of Quarantine.


Files deleted by Norton AntiVirus cannot be recovered. 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.

{button ,AL("RespondBasics",0,`',`')} **More Info...** Click 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 definitions files regularly. Norton AntiVirus uses the information in virus definitions files to detect viruses during scans. Updated virus definitions files are available regularly via LiveUpdate. You can schedule automatic updates to occur when you want them to. Once the updated virus definitions files are installed, you see the new virus names in the Virus List.

{button ,AL("VirusBasics",0,`',`')} **More Info...** Click 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.

Note: 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 page 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.

{button ,AL("IntroCommon;Report",0,`',`')} **More Info...** Click for more information.

About Scheduling Scans and LiveUpdates

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.

{button ,AL("Schedule",0,`',`')} **More Info...** Click 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.

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

{button ,AL("IntroCommon;Exclusions",0,`',`')} **More Info…** Click for more information.

About the Repair Wizard

Norton AntiVirus 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 during any scan, the Repair Wizard appears offering you the choice of:

 Repairing all the viruses at once.

 Seeing what viruses have infected your computer and asking you to repair or delete each one, one at a time.

 Quarantining infected files for submission to the Symantec AntiVirus Research Center (SARC) for further analysis.

Once the Wizard has done its work, it is always a good idea to rescan your computer just to ensure that all the viruses have been eliminated.

Note: If you have chosen to delete files that could not be repaired and 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.

{button ,AL("IntroCommon;Repair",0,`',`')} **More Info…** Click for more information.

About Norton AntiVirus Quarantine

Sometimes Norton AntiVirus detects an unknown virus that can't be eliminated with the current set of virus definitions. Or, you have a file you think is infected that is not being detected. You can store files in a special area called the Quarantine. Files in the Quarantine cannot interact with the rest of your system, so if they are infected, the virus will not spread. From the Norton AntiVirus Quarantine, a file can be sent over the Internet directly to the Symantec AntiVirus Research Center (SARC) for analysis. SARC determines if your file is infected. If the file is not infected, SARC reports the results to you. If a new virus is discovered in your submission, SARC will create and send you updated virus definitions to detect and eliminate the new virus on your computer.

You must have an Internet connection to submit a sample and an email address to receive a reply. You are notified by email with the results of the analysis within seven days.

In addition to Quarantined files, the Quarantine stores two other groups of items:


Backup Items: For data safety, Norton AntiVirus is preset to make a backup copy of a file before attempting a repair. These backups are also stored in the Quarantine. After the repaired file is verified, you can delete the infected item from the Quarantine.


Items Submitted To SARC: Files sent to SARC for analysis are isolated. After receiving the results of the analysis, you can determine what to do with the item.

{button ,AL("IntroCommon;Quarantine",0,`',`')} **More Info…** Click for more information.

About updating virus definitions with LiveUpdate

To prevent new viruses from infecting your computer, you must update your virus definitions files frequently. 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 regularly. You can also schedule LiveUpdates to occur more frequently or at any time you choose.

Note: You can also find updated virus definitions files on several different online systems (click More Info below and select Sources For Updating Virus Definitions.) or request them by mail or email.

{button ,AL("Update",0,`',`')} **More Info...** Click for more information.

Sources for updating virus definitions

If you have a modem and you accepted the preset options when you installed Norton AntiVirus, LiveUpdate automatically updates your virus definitions regularly.

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

Internet

To use the FTP site:

- Access **ftp.symantec.com** (from your Internet browser, type ftp://ftp.symantec.com)

The definitions are found at: public/english_international/antivirus_definitions/norton_antivirus

To use the Web site:

1. Access www.symantec.com and select country.
2. Click AntiVirus Research Center.
3. Click Download Updates.
4. Select the Norton AntiVirus product running on your computer and follow the on-screen directions.

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

Microsoft Network

1. Choose Go To from the View menu.
2. Choose Other Location.
3. Type **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.

Email

Whenever a major virus threat is discovered that requires an update to your virus protection, Symantec can notify you by email so you can run LiveUpdate immediately. The email includes an attachment that can start a LiveUpdate session for you.

To receive LiveUpdate Email:

1 From your web browser, go to

   http://www.symantec.com/avcenter/newsletter.html

2 Fill out the registration form.

3 Click Subscribe Me.

Symantec will notify you by email whenever protection updates are available.

To start a LiveUpdate session from the LiveUpdate Email:

1 When you receive a LiveUpdate Email, launch or run the email attachment called LIVEUPDT.NLU from your mail program. You must launch or run the attachment. Simply reading or viewing it will not work.

   When the attachment runs, it automatically starts a LiveUpdate session on your computer. You don't have to do anything else.

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 Norton AntiVirus definitions and follow the on-screen directions to download the files.

Type /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.

{button ,AL("Update",0,``,`')} **More Info...** Click for more information.

Command line switches

NAVW32.EXE is the Windows interface and scanner. It can be run with command-line switches, typically from the Start menu Run command, to override configuration settings.

NAVW32 [[pathname] options]

pathname	Any drive, folder, file, or combination of these is scanned. If you want to scan a combination of items, use a space to separate the items. You can use wildcards when specifying pathnames for a group of files (for example, NAVW32 A:C:\MYDIR*.EXE).
/A	All drives, except drives A: and B:, are scanned. Network drives are scanned if the Allow Network Scanning option is selected in the Scanner Advanced Settings dialog box.
/L	All local drives, except drives A: and B:, are scanned.
/S	All subfolders specified in the pathname are also scanned.
/M[+|-]	Enables (+) or disables (-) scanning of memory (for example, NAVW32 C:/M or NAVW32 D:/M-).
/MEM	Only memory is scanned.
/B[+|-]	Enables (+) or disables (-) scanning of boot records (for example, NAVW32 A: /B+ or NAVW32 B: /B-).
/BOOT	Only the boot records of the specified drives are scanned.
/NORESULTS	No scan results are reported on screen.
/DEFAULT	Returns settings to how they were when you received Norton AntiVirus.
/HEUR:[0|1|2|3]	Set Bloodhound(tm) sensitivity (0 disables).

{button ,AL("commandline",0,`',`')} **More Info...** Click for more information.

Check to ensure that your CD is in the drive and the drive can be read.

About Inoculation

Inoculation is another way to detect *unknown* viruses, or those viruses for which Norton AntiVirus does not yet have a definition.

Norton AntiVirus automatically inoculates, or records, critical information about the boot records your computer uses at start up. This is similar to taking a fingerprint. On subsequent scans, Norton AntiVirus checks the record 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 for legitimate purposes. For example, you may have installed a new version of the software and that software made modifications to your boot records.

 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.

{button ,AL("NAVDSK_I0010",0,`',`')} **More Info...** Click for more information.

The Virus Infection Cycle

There are three stages in the life of computer viruses: infection, detection, and recovery. In the infection stage, a virus infects a file in your computer. In the detection stage, the virus is identified and isolated. In the recovery stage, the virus is eliminated. Unless the virus is eliminated or quarantined, it continues to infect other files and possibly damage data on your disks. These stages are detailed below.

Infection	**Source**	
	Reused floppy disks from unknown sources	
	Disks from home or school	
	Disks borrowed from friends	
	Programs downloaded from BBSs or the Internet	
	Software bargains (from non-reputable dealers)	
	Re-shrink-wrapped or opened software	
	Pirated software	
	Preformatted floppy disks	
	Infection	
	Boot from infected disk	
	Reboot with infected floppy disk left in drive	
	Run infected program	
	Open infected document or spreadsheet	
	Spread	
	Share disk or infected program	
	Log on to network	
Detection	**Observation**	
	Strange system behavior	
	Files missing or programs not working	
	Utility	
	Virus detected by anti-virus software	
Recovery	**Cleanup**	
	Reinstall programs from master disks	
	Repair files with anti-virus software	
	Restore from uninfected backup	
	Followup	
	Rescan all files to find source of infection	
	Scan all floppy disks to find source of infection	
	Discard backups that may be infected	
	Increase virus protection for a while	

{button ,AL("VirusBasics",0,`',`')} **More Info...** Click for more information.

Tips to avoid viruses

Follow these tips to minimize your virus risk:

 Make sure automatic protection is turned on at all times. Automatic protection is already set up for you when you install Norton AntiVirus using the preset options.

 Perform a manual scan (or schedule a scan to occur automatically) of your hard disks weekly. These scans supplement automatic protection and confirm that your computer is virus-free. A scan is already scheduled to run automatically once per week when you install Norton AntiVirus using the preset options.

 Scan all floppy disks before first use.

 Update your virus definitions files regularly.

 Create and maintain a Norton AntiVirus rescue disk set to facilitate recovery from certain boot viruses.

 Make periodic backups of your hard disk.

 Buy legal copies of all software you use and make write-protected backups.

{button ,AL("VirusBasics",0,`',`')} **More Info...** Click for more information.

Virus Technologies

Program and boot viruses can be categorized by the technology they use to replicate and attempt to avoid detection. Each is described in the following sections.

Stealth Viruses: Stealth viruses actively seek to conceal themselves from attempts to detect or remove them. They use techniques such as intercepting disk reads to provide an uninfected copy of the original item in place of the infected copy (read-stealthing viruses), altering disk directory or folder data for infected program files (size-stealthing), or both. For example, the Whale virus is a size-stealthing virus. It infects .EXE program files and alters the folder entries of infected files when other programs attempt to read them. The Whale virus adds 9216 bytes to an infected file. Because changes in file size are an indication that a virus might be present, the virus then subtracts the same number of bytes (9216) from the file size given in the directory/folder entry to trick the user into believing that the file's size has not changed.

Polymorphic Viruses: Most simple viruses attach identical copies of themselves to the files they infect. An anti-virus program can detect the virus's code (or signature) because it is always the same and quickly ferret out the virus. To avoid such easy detection, polymorphic viruses operate somewhat differently. Unlike the simple virus, when a polymorphic virus infects a program, it scrambles its virus code in the program body. This scrambling means that no two infections look the same, making detection more difficult.

Multipartite Viruses: Multipartite viruses are both program and boot viruses. For example, if you run a word processing program infected with the Tequila virus, the virus activates and infects your hard disk boot record. Then, the next time you boot your computer, the Tequila virus activates again and starts infecting every program you use, whether it is on a hard or floppy disk. Windows Viruses: Viruses that infect Windows programs.

Companion Viruses: A companion virus is the exception to the rule that a virus must attach itself to a file. The companion virus instead creates a new file and relies on a behavior of DOS to execute it instead of the program file that is normally executed. Companion viruses use a variety of strategies. Some companion viruses create a .COM file with a name identical to an existing .EXE file. For example, the companion virus might create a file named CHKDSK.COM and place it in the same directory as CHKDSK.EXE. Whenever DOS must choose between executing two files of the same name where one has an .EXE extension and the other a .COM extension, it executes the .COM file.

Malicious programs: Viruses that infect agent programs (such as those that download software from the Internet; for example, JAVA and ActiveX).

{button ,AL("VirusBasics",0,`',`')} **More Info...** Click for more information.

About Timeout Protection

When you check Timeout Protection, Norton AntiVirus sends periodic messages to your email client while it is scanning large attachments so that the email client doesn't display a message saying that it is taking too long to receive the email.

Because Norton AntiVirus receives and scans the entire email attachment before passing it on to the email client, large attachments can cause your email client to time out.

Note: Timeout protection places hidden text at the top of your email messages. Your email client should remove this text. If you see the text "NAV Timeout Protection" in your email messages you can safely ignore it.

To find help:

- Do one of the following:


Choose Norton AntiVirus from the Help menu.


From any Norton AntiVirus dialog box:


Click the help button.


Right-click any options in a Norton AntiVirus screen and choose What's This? for a brief definition of the option.


Choose Technical Support Website from the Help menu.


Choose Visit The Symantec Website from the Help menu.


You can keep help open on your desktop by minimizing the help window or by clicking back and forth between help and the product.

{button ,AL("Help",0,`',`')} **More Info...** Click for more information.

Help Menus

The following menus are available from within help topic main windows:

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, and 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 use Norton AntiVirus:

1. Double-click the Norton AntiVirus icon on the Windows taskbar in the lower right corner of the desktop to open Norton AntiVirus.
2. From the Norton AntiVirus main window you can view the current status of your system; initiate manual scans of selected files, folders, or drives; run the Norton AntiVirus Quarantine program; and schedule regular virus scans.

{button ,AL("ScanBasics;Startup",0,`',`')} **More Info...** Click for more information.

To disable and enable Auto-Protect

Note: Norton AntiVirus is preset to enable Auto-Protect whenever you start your computer.

To disable Auto-Protect temporarily:

1. Right-click the Norton AntiVirus icon on the Windows taskbar in the lower right corner of the desktop.
2. Click Disable Auto-Protect from the pop-up menu.

To enable Auto-protect again:

- Repeat the steps above, clicking Enable Auto-Protect in step 2.

{button ,AL("Rescue;AutoProtect",0,`',`')} **More Info...** Click for more information.

To bypass startup protection:

Press and the Alt key during the entire boot process. This bypasses startup protection for this startup only. You can specify different bypass keys from the Options – Startup Scan page.

Note: Bypassing startup protection reduces your level of protection.

{button ,AL("Startup",0,`',`')} **More Info...** Click for more information.

To keep up with new viruses:

Note: Without regular updates, your computer is not fully protected. If your computer is connected to a modem or to the Internet, and if you accepted the preset option when you installed Norton AntiVirus, you will automatically receive pre-scheduled LiveUpdates.

Do one of the following:

- If your computer is connected to a modem or to the Internet, click the LiveUpdate button in the Norton AntiVirus main window and follow the on-screen prompts to initiate LiveUpdate at any time you choose.
- If your computer is connected to a modem or to the Internet, schedule automatic LiveUpdates to occur once every two weeks.
- If you don't have a modem or an Internet connection, order virus definitions update disks from Symantec to arrive by mail. This service requires a fee. Consult the Customer Support help page for applicable Symantec phone numbers.
- Follow the instructions on the update that you receive.

{button ,AL("ViruseProcs",0,`',`')} More Info... Click 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.
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.

{button ,AL("ViruseProcs",0,`',`')} More Info… Click for more information.

To update virus definitions using LiveUpdate:

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.

Note: 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 after you restart your computer.

Note: 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. Consult the Customer Service help page for applicable Symantec phone numbers

---

{button ,AL("VirusProcs",0,`',`')} **More Info...** Click for more information.

To schedule virus scans:

1. Click Scheduling in the Norton AntiVirus main window.
2. Click New Event.
3. On the first page of the Scheduling wizard, click Next.
4. Select Schedule A Virus Scan.
5. Click Next and select the desired scan task from the list. If you do not see the scan task you want to schedule, you will need to define a new task.
6. Click Next and enter a brief description in the Description text box.

   This text appears in the Events list box in the Scheduler main window.
7. Click Next and select how often you want the scan to occur.
8. Click Next and enter the time and date when you want this event to first run.
9. Click Next, then click Finish.

The Scheduler must be loaded in order to execute the scans you have scheduled.

{button ,AL("Schedule",0,`',`')} **More Info...** Click for more information.

Scanning for viruses on your computer

To find viruses on your computer do one of the following:


Initiate virus scans by opening the Norton AntiVirus main window, selecting Scan for Viruses, selecting a scan task from the list, and clicking Run Scan Now.


Create a new scan task by opening the Norton AntiVirus main window, selecting Scan for Viruses, and clicking Create New Scan. Then follow the instructions in the Scan Task wizard.

{button ,AL("ScanBasics",0,`',`')} **More Info...** Click for more information.

To initiate scans:

1. Open the Norton AntiVirus main window if it is not already open.
2. Select Scan for Viruses.
3. Select one of scan tasks from the list and click Run Scan Now. If you want a different scan, click Create New Scan and follow the instructions in the Scan Task wizard.

{button ,AL("Scan",0,`',`')} **More Info...** Click for more information.

To scan drives:

1. Open the Norton AntiVirus main window if it is not already open.
2. Select Scan for Viruses.
3. Select Scan All Hard Disks For Viruses from the list and click Run Scan Now. You may also define a new scan task to scan only selected hard drives by clicking Create New Scan and following the instructions in the Scan Task wizard.

{button ,AL("Scan",0,`',`')} **More Info...** Click for more information.

To scan a folder:

1. Open the Norton AntiVirus main window if it is not already open.
2. Select Scan for Viruses.
3. Select Scan One or More Folders For Viruses from the list and click Run Scan Now. Select the folder(s) you want scanned from the directory tree.
4. Click Scan.

{button ,AL("Scan",0,`',`')} **More Info...** Click for more information.

To scan a path:

1. Open the Norton AntiVirus main window if it is not already open.
2. Select Scan for Viruses.
3. Select Scan One or More Folders For Viruses from the list and click Run Scan Now. Select the highest level folder in the path you want scanned from the directory tree.
4. Click Scan.

{button ,AL("Scan",0,`',`')} **More Info...** Click for more information.

To scan an individual file:

1. Open the Norton AntiVirus main window if it is not already open.
2. Select Scan for Viruses.
3. Select Scan One or More Files For Viruses from the list and click Run Scan Now. Select the files you want scanned from the dialog box.
3. Click Open.

{button ,AL("Scan",0,`',`')} **More Info...** Click for more information.

To respond to a Norton AntiVirus alert:

1. Don't panic! If a virus has attacked your computer, the damage can be undone and the virus can be eliminated.
2. If the alert is the Repair Wizard, it is best to let the Wizard automatically repair all the infected files. You don't have to do anything except click Next.
3. If the alert is an Auto-Protect alert, you see a message detailing the type of alert. In this case, follow the on-screen instructions.

Action buttons

If you chose to eliminate viruses manually in the Repair Wizard, you will have the following options for each virus.

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.

Quarantine: Isolates the file and prevents it from being accessed or run. Quarantined files can be submitted to SARC for further analysis.

Done: Returns to the Scan Results dialog box. Click Done when you have finished eliminating the listed viruses. Clicking Done does not process any remaining viruses.

To use the Repair Wizard:

Follow the on-screen instructions. It is wisest to allow the Repair Wizard to automatically repair all damaged files. However, you have the option of manually repairing files and getting information about infected items.

To repair damaged files automatically:

1. On the first Repair Wizard window, select Automatic and click Next.

   The following screen displays a list of infected files.

2. Click Next.

   The Repair Wizard will automatically fix the files. On the last Repair Wizard window you may click More Info to see details of the scan and wizard actions.

3. Click Finish.

To repair damaged files manually and view information about infected files:

1. On the first Repair Wizard window, select Manual and click Next.
2. Select a file from the list of infected files.

   Information about the selected file and a recommendation on how to handle it is displayed at the bottom of the window. You may click Info to get more details about the infected file and the virus it contains.

3. Click one of the action buttons to repair, delete, exclude, or quarantine the file.
4. Click Done when you are finished.

Note: If some files cannot be repaired, the Repair Wizard will prompt you to either quarantine (isolate) the files and submit them to Symantec AntiVirus Research Center (SARC) for further analysis or to delete the infected files from your computer and replace them with uninfected copies.

{button ,AL("Respond",0,`',`')} **More Info...** Click for more information.

To respond if a file cannot be repaired:

1. If Norton AntiVirus cannot repair the infected file, you have two options:


Choose Quarantine from an alert box in Norton AntiVirus to isolate the file and prevent it from being accessed or run. Later, you can send the infected file to SARC for further analysis.


Choose Delete from an alert box in Norton AntiVirus or 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.

To respond to inoculation changes:

- Do one of the following:

Select Inoculate if the boot record has changed for legitimate reasons since the last time you inoculated it. Legitimate reason would be an upgrade to your operating system (to Windows 98, for example) or repartitioning your hard disk. If the inoculation alert appears after one of these actions, you should re-inoculate.

Select Repair if you are certain that the boot record did not change for legitimate reasons. Anything that modifies the boot record can make this dialog box display. Do not Repair if your virus definitions are not up-to-date. Update the definitions and run a scan first.

Note: Inoculation changes in boot records and system files are an indication but not a certainty of a viral infection due to an unknown virus. Boot records do change for legitimate reasons as well as viral reasons. Upgrading your operating system or repartitioning your hard disk can modify the boot records. Note that Norton AntiVirus does not check for inoculation changes on NEC PC98xx machines.

{button ,AL("NAVDSK_I0075",0,`',`')} **More Info...** Click for more information.

To remove a virus found in memory:

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.

1. Shut down your computer.
2. Turn off your computer using the power switch.
3. Use your Rescue Boot Disk created when you installed Norton AntiVirus or the Norton AntiVirus Emergency Boot Disk that came with the product.
4. Turn on the PC. An A prompt should appear. Either follow the prompts for running a scan or type NAVDX from the A prompt.
5. If you do not have Rescue Disks or the Emergency Boot Disk, you may use a write-protected Windows 95/98 Startup disk or a 7.1 or higher Dos system disk to boot your computer. If this is also not available, get someone to create a boot disk for you with Dos 7.1 or higher. Once you have restarted the computer, you will need to run Navdx.exe from the directory on the hard drive where you installed Norton AntiVirus.

Note: 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.

To create Rescue Disks:

1. Click Rescue at the top of the Norton AntiVirus main window..
2. Select Norton Zip Rescue to create a Norton Zip Rescue disk set, or Basic Rescue to create floppy disks.
3. Select the destination drive. Typically, this will be either your Zip drive, if you have one, or your floppy drive (drive A).
4. Click Create to create new Rescue Disks or Update to update existing Rescue Disks.

To delete an infected file:

1. Click Delete in the Norton AntiVirus alert box, then follow the on-screen prompts.

   If the Delete button is dimmed, either Norton AntiVirus is configured not to enable it or the item cannot be deleted.

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.

To respond if Norton AntiVirus cannot repair an infected file:

- Do one of the following:

Quarantine the infected file so that it cannot be accessed or run. Submit the file to SARC for further analysis.

Delete the infected file from your computer.

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.

To respond if Norton AntiVirus cannot successfully repair a system file:

1. Restart your computer using the Windows 95/98 startup disk you made when you installed Windows 95/98.
2. From the A prompt, type Sys C: and press Enter.

   This will rewrite the boot record on the C drive and the system files.
3. When the A prompt displays, take the disk out and reboot your PC with a Ctrl+Alt+Del or Shut it off and turn it back on.

Note: If it is Win.com that is infected, you may have to manually copy the file from the disk to the appropriate folder on the hard drive.

To respond if Norton AntiVirus cannot successfully repair the master boot record or a boot record on your hard disk:

- Use your write-protected Rescue Boot Disk to restore the boot records to an uninfected state.

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

- Copy any important files from the floppy disk to another disk. The floppy disk is still infected and you cannot boot from it.

To respond to a virus-like activity alert:

- Do one of the following:

Select Continue to allow the activity to proceed if the message in the alert box describes an activity that is valid in the context of the application you are running. (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 Stop to prevent the action from taking place if the activity detected is not related to what you are trying to do. (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.)

Select Exclude 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. (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.)

To remove viruses from downloaded files:

1. Scan the file from the Norton AntiVirus main window.
2. Either let the Repair Wizard automatically repair the files or select the file you want to repair in the Problems Found dialog box.
3. Click Repair.
4. Click 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.

To restart a shutdown computer:

1. Restart your computer by placing the Rescue Boot Disk in drive A: and turning on your computer.

   Note: If you did not create Rescue Disks, use the Norton AntiVirus Emergency disk that came with your original box.

2. Follow the on-screen directions.

   Note: If your Rescue Disks are not current you can still use them to remove viruses from your computer. When Norton Rescue starts from the Rescue Boot Disk, skip the Rescue Recovery task and go directly to the Norton AntiVirus task.

   You are prompted when it is time to insert other Rescue Disks.

3. When the process is complete, remove the Rescue Disk from the A: drive and restart your computer.

   Note: The first two tasks in Norton Rescue, Rescue Recovery and Norton AntiVirus, handle Virus emergencies. You should not need any additional tasks listed in Norton Rescue to solve virus emergencies.

4. Scan again.

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

To change how Norton AntiVirus works:

1. Click Options on the Norton AntiVirus main window.
2. Click an item in the Options outline at the left side of the Options dialog box.

   A brief description of the item appears at the top of the window.
3. Right-click any option and click What's This? for more information about that option.
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.

{button ,AL("Options",0,`',`')} **More Info...** Click for more information.

To change scan options for scans you initiate or schedule:

1. Click Options on the Norton AntiVirus main window.
2. Click Manual Scans if it is not already selected.
3. Right-click any option and click What's This? for more information about that option.
4. Make your changes and click OK to save settings and exit.

{button ,AL("Scan",0,`',`')} **More Info...** Click for more information.

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

1. Click Options in the Norton AntiVirus main window.
2. Click Manual Scans if it is not already selected.
3. Select the areas your computer should scan before program files are scanned.

   Note: By default, all options are already selected if you performed a complete setup of Norton AntiVirus.
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.
5. Click Select Extensions to display the Program File Extensions dialog box, which lists the file extensions that Norton AntiVirus scans.

{button ,AL("Scan",0,`',`')} **More Info...** Click for more information.

To choose what Norton AntiVirus does when a virus is found during a manual or scheduled scan:

1. Click Options on the Norton AntiVirus main window.
2. Click Manual Scans if it is not already selected.
3. Select any of the options in the How To Respond drop-down list box.

If you select Custom Virus 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.

4. Right-click any option and click What's This? for more information about that option.
5. Click OK to save settings and exit the dialog box.

{button ,AL("Scan",0,`',`')} **More Info...** Click for more information.

To set additional scanning options:

1. Click the + (plus sign) next to either Manual Scans or Auto-Protect.
2. Click Bloodhound.
3. Make sure that Enable Bloodhound Heuristics is selected.

   You can drag the pointer to increase your virus protection against difficult to detect and unknown viruses. Scanning may take a bit longer.
4. Click OK to save settings and exit the dialog box.

To choose which file extensions Norton AntiVirus scans:

1. In the Manual Scans settings, click the type of files to scan: All Files or Program Files And Documents Only.
2. If you have selected Program Files And Documents Only, click Select Extensions to display the Program File Extensions dialog box.
3. Click New to display the Add 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 Options dialog box appears.
7. Click OK to save settings and exit the Options dialog box.

To remove a file extension from scanning:

1. In step 3 above, select an extension from the list and click Remove.
2. Continue with step 6 above.

To reset the list of file extension to the defaults:

1. In step 3 above, click Defaults.
2. Continue with step 6 above.

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 macro viruses.

{button ,AL("ScanBasics",0,`',`')} **More Info...** Click for more information.

To set general scanning options:

1. Click Options on the Norton AntiVirus main window.
2. Click General if it is not already selected.
3. Set the following options as appropriate:

 Select Back Up A File in Quarantine Before Attempting A Repair to have Norton AntiVirus make a copy of the infected file before repairing it.

 Select Enable Password protection to protect your option settings from unintentional change.

 Select Display The Logo Screen When Starting Norton AntiVirus to display the splash screen whenever you start Norton AntiVirus.

 Select Alert Me On Startup If My Virus Definitions Are Out Of Date to have Norton AntiVirus alert you if your virus definitions file is more than two weeks old.

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

{button ,AL("ScanBasics",0,`',`')} **More Info...** Click for more information.

To determine how protection works at startup:

1. Click Options on the Norton AntiVirus main window.
2. Click Startup Scan if it is not already selected.
3. Specify in the Items To Scan group box the areas that you want Norton AntiVirus to scan each time you start your computer.

You should leave the preset options as they are. (Everything is selected.)

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

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

5. Click OK to save settings and exit the Options dialog box.

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

1. Click Options on the Norton AntiVirus main window.
2. Select Auto-Protect if it is not already selected.
3. Select when Norton AntiVirus should scan a file automatically.

   Note: Check all options to ensure maximum protection.
4. Click OK to save your settings and close the Options dialog box.

{button ,AL("AutoProtect",0,`',`')} **More Info...** Click for more information.

To choose how Norton AntiVirus should respond when Auto-Protect finds problems:

1. Click Options on the Norton AntiVirus main window.
2. Click Auto-Protect if it is not already selected.
3. Click to select any of the options, then right-click to display a help menu. Click What's This? to see a description of each option.
4. Click OK to save settings and exit the Options dialog box.

To monitor for virus-like activities:

1. Click Options on the Norton AntiVirus main window.
2. Click the + (plus sign) next to Auto-Protect.
3. Click Advanced.
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 The Action. To set a higher level of protection, select Ask Me What To Do. 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 save your settings and close the Options dialog box.

{button ,AL("VirusProcs")} **More Info…** Click 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.

How to…

{button ,JI(`>TASK',`NAVW_PROC_CUSTOMIZE_SCANNER_SETTINGS_FOR_MAX_PROTECT')} Customize settings for maximum protection

{button ,JI(`>TASK',`NAVW_PROC_SCHEDULE_SCANS')} Schedule Scans

{button ,JI(`>TASK',`NAVW_HOWTO_SCHEDULE_LIVEUPDATES')} Schedule LiveUpdates

If you have a modem or other Internet connection and you accepted the preset options when you installed, you will receive regular updates of files that Norton AntiVirus needs to keep your virus protection up-to-date.

To customize settings for maximum protection:

1. Click Options on the Norton AntiVirus main window.
2. Click Manual Scans if it is not already selected.
3. Be sure that All Files is selected in the File Types To Scan group box.
4. Be sure that Ask Me What To Do is selected in the How To Respond When A Virus Is Found drop-down list box.
5. Click Auto-Protect.
6. Check all options under Scan Files When They Are (they are on by default).
7. Be sure that All Files is selected under File Types To Scan.
8. Be sure that Ask Me What To Do is selected in the How To Respond When A Virus Is Found drop-down list box.
9. Click the + (plus sign) next to Auto-Protect.
10. Click Advanced.
11. Click Ask Me What To Do in each of the Virus-Like Activity Monitors drop-down list boxes.
12. Check Scan Both Drives A: And B: in the Floppy Disk Scans group box.
13. Click Bloodhound, and then move the slider bar up to enable a higher level of detection for unknown viruses.
14. Click Email Protection.
15. Check Use Email Protection, and select your email client program from the list.

    If your email client is not listed, check Manually Configured Email Client and then configure it manually. Click More Info below and select To Configure Your Email Client for Protection.
16. Click OK to save settings and exit the Options dialog box.

{button ,AL("email;Scan",0,`',`')} **More Info...** Click for more information.

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.

Note: 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 the Activity Log:

1. Click Reports in the Norton AntiVirus main window.
2. Click View The Log Of Norton AntiVirus Activities, and then click Open.

   The Activity Log displays a history of Norton AntiVirus activities.

   Note: After a scan, use the Activity Log to look up files that may need to be deleted and replaced.
3. 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: 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 selecting the Activity Log tab.
4. 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.)
5. Click Close to exit the Activity Log.

To filter the Activity Log entries:

1. Click Reports in the Norton AntiVirus main window.
2. Click View The Log Of Norton AntiVirus Activities, and then click Open.
3. Click Filter. The Activity Log Filter dialog box opens.
3. Specify the types of events to display by clicking the appropriate check boxes.
4. Click OK to save settings and exit the dialog box.

To clear the Activity Log:

1. Click Reports in the Norton AntiVirus main window.
2. Click View The Log Of Norton AntiVirus Activities, and then click Open.
3. Click Clear in the Activity Log dialog box.
4. Click Yes to clear the Activity Log and continue.

To use the Virus List:

1. Click Reports in the Norton AntiVirus main window.
2. Click View The List Of Viruses That Norton AntiVirus Is Protecting You Against, and then click Open.

   The Virus List displays the name of the virus and what it infects (program files, boot records, or both).
3. 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. Click Reports in the Norton AntiVirus main window.
2. Click View The List Of Viruses That Norton AntiVirus Is Protecting You Against, and then click Open.
3. Click Find. The Find A Virus dialog box opens.
4. Start entering the name, or part of the name, of the virus you want to find, and then click OK.

   The first virus in the list matching your search criterion will be selected in the list.
5. Click Find Next to find the next item in the list matching your search criterion.

Note: 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 name may be different from what you expected. For example, the virus commonly known as Michelangelo is actually called Stoned. Michelangelo.D.

To display information about a virus:

1. Click Reports in the Norton AntiVirus main window.
2. Click View The List Of Viruses That Norton AntiVirus Is Protecting You Against, and then click Open.

   The Virus List displays the name of the virus and what it infects (program files, boot records, or both).
3. Select the virus you are interested in on the list, or use Find to find the virus.
4. Click Info to view details, such as symptoms and aliases, about the selected virus.

To print to a printer:

1. Click Print to display the Print dialog box.
2. Click Print To Printer.

To print to a file:

1. Click Print to display the Print 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 overwrite the existing one.

To browse for files, choose one of the following methods:


Click the browse button to display a dialog box where you can locate one or more 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 choose what to log:

Note: 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.

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, select any event that you want Norton AntiVirus to record.
4. Click OK to save changes and close the dialog box.

To customize alerts:

1. Enter a personalized alert message.

   Note: 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.

To password-protect features:

1. Click Options in the Norton AntiVirus main window.
2. Click General if it is not already selected.
3. Select Enable Password Protection to turn on the password protection feature.
4. 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.
5. Click OK to close the Set Password dialog box.
6. Click OK to close the Options window and save your settings.

Your option settings are now

To disable password protection:

1. Deselect Enable Password Protection, in step 3 above.
2. Click OK to close the Options window and save your settings.

To exclude files from being scanned for viruses:

1. Click Options on the Norton AntiVirus main window.
2. Click Exclusions tab if it is not already selected.
3. Click New.
4. Do one of the following:


Use the browse button to display the Select File To Exclude dialog box from which you can choose a file to 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 select Include Subfolders if you want to ensure that all files with that extension are excluded.


Be careful! Excluding files reduces your level of protection.

To edit exclusions:

1. Click Options on the Norton AntiVirus main window.
2. Click Exclusions if it is not already selected.
3. Select an item from the Items list box**.**
4. Click Edit and make the desired changes**.**
5. Click OK to save your changes.

To delete an exclusion:

1. Click Options in the Norton AntiVirus main window.
2. Click Exclusions if it is not already selected.
3. Select an item from the Items list box**.**
4. Click Remove.

   The file is removed from the exclusions list.

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.

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

2. Click OK.

To quarantine an infected or suspicious item:

You can quarantine files in one of the following three ways:

 Select Quarantine after receiving a Norton AntiVirus alert.

 Configure Norton AntiVirus to quarantine items rather than repair them or quarantine them if they cannot be repaired.

 Manually add a suspicious file to Quarantine.

To manually add an item to the Quarantine:

1. In the Norton AntiVirus main window, click Reports.
2. From the list of reports, click View And Manage The Items In Quarantine, and then click Open.
3. Click Add Item.
4. In the Add To Quarantine dialog box, locate the file you want to add.

   If the Remove File From Original Location option is checked, the potentially infected file can't be run accidentally.
5. Click Add.

To get information about a quarantined item:

1. In the Norton AntiVirus main window, click Reports.
2. From the list of options, select View And Manage The Items In Quarantine, and then click Open.
3. In the left panel of the Quarantine, click Quarantined items.
4. Do one of the following:

Select an item in the right panel and click Properties.

Double-click an item in the right panel.

To submit a quarantined file to SARC:

The Quarantine includes the Scan and Deliver Wizard to simplify sending an item to SARC for analysis. When you click Submit Item, the Wizard analyzes the file and may recommend an action instead of delivering it to SARC. For example, the virus may be one that can already be eliminated with your current set of virus definitions. You can, however, override the recommendation and submit it.

1. In the Norton AntiVirus main window, click Reports.
2. From the list of options, select View And Manage The Items In Quarantine, and then click Open.
3. In the left panel of the Quarantine, click Quarantined items.
4. Select a file in the list of Quarantined items and click Submit Item.
5. Follow the directions in the Scan and Deliver Wizard to collect information and submit the file to SARC for analysis.

To schedule LiveUpdates:

1. Click Scheduling in the Norton AntiVirus main window
2. Click New Event.
3. On the first page of the Scheduling wizard, click Next.
4. Select Schedule LiveUpdate To Update Your Virus Protection.
5. Click Next and enter a brief description in the Description text box.

   This text appears in the Events list box in the Scheduler main window.
6. Click Next and select how often you want the scan to occur.
7. Click Next and enter the time and date when you want this event to first run.
8. Click Next, then click Finish.

The Scheduler must be running in order to execute the scans you have scheduled.

Auto-Protect Actions

When Auto-Protect displays a virus alert, you will be given the following action options:

 Repair The Infected File: Removes the problem from the file. A backup of the file will be made before the repair, so you will not lose any data.

 Quarantine The Infected File: Isolates the file in the Quarantine folder. This prevents the problem from spreading.

 Delete The Infected File: Removes the infected file from your computer.

 Ignore The Problem And Continue With The Infected File: Uses the file in spite of the problem. You might spread the problem to other files or other computers if you choose this action.

 Do Not Open The File, But Leave The Problem Alone: Safely avoids using the infected file. While this does not cure the problem, it will not spread it.

 Ignore The Problem And Do Not Scan This File In The Future: Select only if you are sure that the file is safe. Norton AntiVirus will not scan this file for viruses in the future. You might spread the problem to other files or other computers if you choose this action.

To configure your email client for protection:

If your email client program is not listed in the Email Protection options list you may manually configure your client to work with Norton AntiVirus.

1. Click Options on the Norton AntiVirus main window.
2. Click Email Protection if it is not already selected.
3. Select Use Email Protection.
4. Select Manually Configure Email Client in the list.
5. Click OK to save settings and exit the Options dialog box.
6. Configure your email client to use the new settings shown below.

Setting Name	**Current Settings** (Example)	**New Settings** (Based on Example)
Incoming POP3 Server	mail.ispname.com	127.0.0.1
User name	userid	userid/ mail.ispname.com
Outgoing SMTP Server	mail.ispname.com	mail.ispname.com

See your email client's documentation for instructions on changing these settings.

To start Norton AntiVirus using its command-line switches:

1. Open a DOS window by clicking Start > Programs > MS-DOS Prompt.
2. At the prompt, type NAVW32 [[pathname] options]

   where [pathname] is an optional path to a drive, folder, or file you want to scan, and [options] is a string of command-line options.

{button ,AL("commandline",0,`',`')} **More Info...** Click for more information.

To configure a manually configured email client for protection

Now that you have selected a manually configured email client you must change some settings in your email program manually. Refer to your email program's help documentation to find out how to make these changes.

Note the existing settings since you will need them for the new settings.

The example uses the sample mail server name "mail.ispname.com" and user name "userid". You should use the mail server names and user name currently in your email settings.

Setting Name	**Current Settings** (Example)	**New Settings** (Based on Example)
Incoming POP3 Server	mail.ispname.com	127.0.0.1
User name	userid	userid/ mail.ispname.com
Outgoing SMTP Server	mail.ispname.com	mail.ispname.com

To unconfigure a manually configured email client

Now that you have deselected your email client from protection, you must reconfigure it to its correct settings so it will work properly. Refer to your email program's help documentation to find out how to make these changes.

The example uses the sample mail server name "mail.ispname.com" and user name "userid". You should use the mail server names and user name currently in your email settings.

Setting Name	Settings with Protection	Settings without Protection
Incoming POP3 Server	127.0.0.1	mail.ispname.com
User name	userid/ mail.ispname.com	userid
Outgoing SMTP Server	mail.ispname.com	mail.ispname.com

Tasks you can perform with Norton AntiVirus

The list below shows the most important tasks Norton AntiVirus helps you perform. Click a task to get more details.

{button ,JI(`>maintwo',`NAVW_PROC_FIND_VIRUSES_ON_YOUR_COMPUTER')} Scan for viruses on your computer.

{button ,JI(`>maintwo',`NAVW_INFO_REMOVING_VIRUSES')} Remove viruses from your computer.

{button ,JI(`>task',`NAVW_PROC_UPDATE_THE_VIRUS_LIST')} Update your virus protection with LiveUpdate.

{button ,JI(`>task',`NAVW_PROC_QUARANTINE_AN_ITEM')} Quarantine an infected file.

To receive LiveUpdate by email

Whenever a major virus threat is discovered that requires an update to your virus protection, Symantec can notify you by email so you can run LiveUpdate immediately. The email includes an attachment that can start a LiveUpdate session for you.

To receive LiveUpdate Email:

1. From your web browser, go to

   http://www.symantec.com/avcenter/newsletter.html
2. Fill out the registration form.
3. Click Subscribe Me.

Symantec will notify you by email whenever protection updates are available.

To start a LiveUpdate session from the LiveUpdate Email:

1. When you receive a LiveUpdate Email, launch or run the email attachment called LIVEUPDT.NLU from your mail program. You must launch or run the attachment. Simply reading or viewing it will not work.

   When the attachment runs, it automatically starts a LiveUpdate session on your computer. You don't have to do anything else.

Notes on Scanning Network Drives

Because you do not always have the same access privileges to a network drive as you have to a local drive, there are some restrictions when scanning network drives with Norton AntiVirus. Scanning network drives is more time consuming than scanning local drives. Other users may be creating, deleting, or moving files on a drive while Norton AntiVirus is scanning.

Drive access privileges	Operations you can perform
None	None
Read-Only	Scan, but not repair or delete infected files, or inoculate
Read-Write	Scan, repair, delete, and inoculate

Scanning network drives is more time consuming than scanning local drives. Other users may be creating, deleting, or moving files on a drive while Norton AntiVirus is scanning.

To auto-protect floppies

1. Click Options on the Norton AntiVirus main window.
2. Click the + (plus sign) next to Auto-Protect.
3. Click Advanced.
4. Click both options under Floppy Disk Scans.

   These options are set by default.
5. Click OK to save your settings and close the Options dialog box.

{button ,AL("AutoProtect;VirusProcs",0,`',`')} **More Info...** Click for more information.

To enable inoculation protection

1. Click Options on the Norton AntiVirus main window.
2. Click Inoculation.
3. Select Inoculate Boot Records.
4. Select an action from How To Respond When An Inoculated Boot Record Changes.
5. Click OK to save your settings and close the Options dialog box.

{button ,AL("Inoculation",0,`',`')} **More Info…** Click for more information.

To re-scan a quarantined item

1. In the Norton AntiVirus main window, click Reports.
2. From the list of options, select View And Manage The Items In Quarantine, and then click Open.
3. Click LiveUpdate in the Quarantine window. Follow the LiveUpdate wizard.

   Your installed set of virus definitions files is updated with the latest definitions automatically.
4. Select the file in the Quarantine and click Repair Item.

The file is scanned again with the new definitions.

To specify allowable Quarantine actions

1. In the Norton AntiVirus main window, click Reports.
2. From the list of options, select View And Manage The Items In Quarantine, and then click Open.
3. Select Options from the View menu
4. Click the Quarantine Files, Submitted Files, or Backup Files tabs and check which actions you want to permit for each file type.

If you do not want users to be able to change Quarantine options, you can set a password to prevent unwanted changes to Quarantine options from the General tab.

Specify a Quarantine options password

To password-protect access to Quarantine settings:

1. In the Norton AntiVirus main window, click Reports.
2. From the list of options, select View And Manage The Items In Quarantine, and then click Open.
3. Select Options from the View menu.
4. Click the General tab
5. Check Enable Password and click Set Password.

Enter a password of 1 to 16 characters in length. Passwords are not case-sensitive.

6. Re-enter the password in the Confirm New Password box.
7. Click OK to close the Change Password box.

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

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 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.

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

Allows you to repair the file or boot record.

Allows you to delete the infected file.

Allows you to exclude the file from being checked for known viruses. Use sparingly because you are reducing your protection!

Allows you to quarantine a file, which means the file cannot be accessed or run. Also, you can submit the file to the SARC (Symantec AntiVirus Research Center) for further analysis.

Click Advanced to display the Scanner Advanced Settings dialog box, which contains more options, including network scanning and drive preselection.

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

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.

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.

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).

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 an option to specify how to respond when a virus is found. Choose Ask Me What To Do to have the most control over what happens to an infected file.

Choose an option to specify how to respond when a virus is found. Choose Ask Me What To Do to have the most control over what happens to an infected file.

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.

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!)

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.

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

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.

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.

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.

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.

Choose None if you don’t want a bypass key combination.

Choose if you want to press the Shift key to bypass a scan at startup.

Choose if you want to press the Alt key to bypass a scan at startup.

Choose if you want to press the control Ctrl key 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 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, and 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.

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

Records detections of boot records that have changed or been inoculated.

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.

Records quarantined items.

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.

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.

Excludes the item from checks for known viruses.

Check to backup the file in Quarantine before attempting to repair. Quarantined files cannot be run or accessed while in Quarantine.

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.

Displays the Set Password dialog box.

You can choose to password protect all Norton AntiVirus features or to customize which feature are password protected. You must type in your password before you can access either feature.

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.

Select this check 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.

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

Check to have boot records automatically inoculated.

Choose how to respond when your are notified that a boot record's inoculation data has changed. Ask Me What To Do gives you the most control.

Choose an option to choose how to respond to an inoculation issue. Choose Ask Me What To Do to have the most control over what happens to the boot record.

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

Allows you to inoculate or reinoculate a changed boot record.

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

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

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

Click the activities that you wish to exclude for the specified item.

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.

Records/displays time and dates of denied access events.

Displays the list of Option pages in an outline format. Click an entry to display its options. Click the + (plus sign) to expand an entry.

Drop-down command list allows you to reset options to their defaults for the displayed page of options or for all options.

Check to have system files scanned when your computer starts up or is rebooted.

Click to have the Norton AntiVirus logo displayed whenever you start the Norton AntiVirus application.

Click to have Norton AntiVirus notify you when your virus definitions are more than two weeks old.

Check to turn on background checking of email attachments. After checking this option, select your email client from the list below.

Displays a list of supported email client applications. If your email application is not listed, check Manually Configured Email Client and then configure your email client manually.

Choose an option to specify how to respond when a virus is found in an email attachment. Choose Ask Me What To Do to have the most control over what happens to an infected attachment.

Check to temporarily disable email protection. When you uncheck this option to re-enable email protection your settings will be restored.

Check to run the scheduler when your computer starts up. The scheduler must be running for scheduled events to occur.

Check to display a scheduler an icon in the notification area at the far end of the Windows task bar.

Check to automatically run missed events the next time your computer starts.

Check to display a confirmation dialog when you exit the scheduler. This helps to prevent shutting down the scheduler accidentally.

Check to have the Norton AntiVirus logo displayed to remind you that email scanning is active.

Check to enable timeout protection so Norton AntiVius can scan large email attachments without causing your email client to time out.

Check to display the Norton AntiVirus Email Protection icon when email protection is active. It will appear in the notification area at the far end of the task bar.

Check to enable the Microsoft Office 2000 virus protection plugin. This protects you from macro viruses in Microsoft Office 2000 documents.

Check to scan the files contained in compressed files. Norton AntiVirus scans and repairs infections inside of many types of compressed files.

BBS (bulletin board system)

Any online service that allows messaging, electronic mail, and file transfer between computer users who usually connect to the system via modem.

boot record

The first physical sector on a floppy disk or the first logical sector of a hard disk partition. It identifies the disk's architecture. For bootable disks, it also contains the boot record program that loads the operating system. Also referred to as boot sector.

boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size,and so on). For bootable disks, it also contains a program that loads the operating system.

bootable disk

Any disk that contains the system files necessary to start your computer. While today's computers include a bootable hard disk that is normally used to start the machine, "bootable disk" usually refers to a floppy disk that can be used to start the machine in an emergency.

COMMAND.COM

The default command interpreter program for MS-DOS. It accepts commands typed from the keyboard and performs tasks such as loading other programs and directing the flow of information between programs and the CPU.

compression

Processing a file's or disk's data using a mathematical algorithm, such that the resulting data occupies less physical space on the disk. Individual files or entire disks may be compressed by various types of utility software.

CONFIG.SYS

A file containing commands that configure a system's hardware and load device drivers. It is automatically executed by MS-DOS when your system starts up.

email

Abbreviation for "electronic mail." Sending correspondence and information (including files) to another person who shares or has access to a common computer network.

file server

A central disk storage device (or devices) connected to a network that provides network users access to shared applications and data files.

floppy disk

One of several types of magnetic media used for storing data. Because the magnetic media is bonded to thin, flat disks of Mylar, floppy disks are flexible. This is in contrast to hard disks, which consist of a rigid material with a magnetic coating. The most popular floppy disk formats in use today are 3½ and 5¼-inch in diameter. Floppy disks are also known as "flexible disks" or "diskettes."

folder

A logical container for files and programs, usually represented in graphical interfaces by icon graphics resembling file folders. In addition to files and programs, folders may also contain other folders, allowing for a hierarchical organization of data on a disk. Folders are also known as "directories."

long filename (LFN)

A file system feature that allows you to name a file using up to 255 alphanumeric characters. Long filenames may contain both upper and lowercase letters, spaces, commas, semicolons, left and right square brackets, and plus and equals signs.

MS-DOS imposed an "eight-dot-three" limit on filenames, allowing at most an eight-letter filename and three-letter extension separated by a period. Some older MS-DOS based applications do not support long filenames.

MSDOS.SYS

A system file that contains the kernel of the MS-DOS operating system.

network

A group of computers and associated hardware that are connected together by communication lines or other means for the purpose of sharing information and hardware between users.

network server

A computer that allows other computers on a network to access its files, and that can provide them with centralized and shared services, including programs, storage, and communications.

registry key

Category of information stored in the Windows registry. Registry keys are the means used to index and organize the data stored in the registry. Because registry keys can hold other keys ("subkeys") as well as data, the registry forms a hierarchical structure.

right-click

To click the right mouse button. By default, right-clicking while the mouse cursor is over an interface object displays a menu containing options specific to that object. The mouse key assignments can be switched for left-handed computer users such that clicking the left mouse button displays the context menu.

SYSTEM.INI

A Windows startup file that contains system-specific drivers and configuration information. Most of the information that was stored in SYSTEM.INI for Windows 3.1 has been relocated to the Windows registry. SYSTEM.INI still exists, however, for compatibility with older applications.

TSR (terminate-and-stay-resident)

A type of program that loads itself into memory the first time it is run and remains there until explicitly removed or until the computer is restarted. TSRs are also known as a "memory-resident programs."

WIN.INI

A Windows startup file that contains system settings and application preferences. Most of the information that was stored in WIN.INI for Windows 3.1 has been relocated to the Windows registry. WIN.INI still exists, however, for compatibility with older applications.

inoculation

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. System files and boot records are inoculated by preset options.

unknown virus

A virus for which Norton AntiVirus does not contain a virus definition. **See also** virus definition.

virus-like activities

These are activities that may be performed legitimately by some programs. However, in other cases, they may indicate a virus at work. For a complete description, look up "virus-like activities" in the help index.

boot virus

A virus that infects the boot record program on both hard and floppy disks and/or the master boot record program on hard disks. A boot virus loads into memory before DOS, taking control of your computer and infecting any floppy disks that you access. A boot virus may prevent your computer from starting up at all from an infected disk.

compressed file

Usually refers to a file or disk that has been processed by a compression (utility) program so that it takes less disk space than when it is in its normal (uncompressed) state.

high-risk environment

A high-risk environment is one that meets most of the following characteristics:

 You have a network connection (LAN without a professional administrator).

 No AntiVirus software is running on the network.

 You use shared network programs.

 You use a modem to download programs form BBSs and online services.

 You are connected to the Internet.

 You use preformatted floppies or recycled floppies of unknown origin.

 You share files on floppy disks, collect software, use pirated software, and/or trade computer games.

 Other people frequently use your computer.

infected file

A file that contains a virus.

known virus

Any virus that Symantec has analyzed and defined and that Norton AntiVirus can detect and identify by name.

multipartite virus

Viruses that affect both programs and boot files, and can spread from one type of file to another.

polymorphic virus

A type of virus that changes its telltale code segments so that it "looks" different from one infected file to another, thus making detection more difficult.

program virus

A virus that infects executable program files, which often have one of these file extensions: .COM, .EXE, .OVL, .DRV, .SYS, and .BIN. Program viruses can stay in memory even after a program is executed, until you turn off your computer.

smart search

A feature that allows you to begin typing the first few letters of a name to move quickly through the list.

stealth virus

A virus that actively seeks to conceal itself from discovery or defends itself against attempts to analyze or remove it.

Trojan horse

A program that promises to be something useful or interesting (like a game), but covertly may damage or erase files on your computer while you are running it. Trojan horses are not viruses.

virus definition

Virus information that allows Norton AntiVirus to recognize and alert you to the presence of a specific virus.

Virus List

The Virus List shows all viruses for which Norton AntiVirus has a virus definition. It is important to update this list regularly. **See also** virus definition.

System Messages

This topic contains an alphabetical list of the error messages you may see while using Norton AntiVirus. Whenever an item such as <FILENAME>, <DRIVE>, or <VIRUS NAME> appears, it is replaced by an actual filename, drive, or virus name in the message on your screen.

Boot record has changed since inoculation. Inoculation changes in a boot record are likely to indicate the presence of an unknown virus. However, there are a few situations where this kind of change is legitimate.

The configuration file NAVOPTS.DAT not found. Norton AntiVirus could not find the file that contains the configuration settings. Norton AntiVirus loaded with the default settings.

Error on drive <DRIVE>. Drive or device not ready. Norton AntiVirus could not access the specified drive because the drive door is open or there is a problem with the drive.

The <VIRUS NAME> boot virus was found on drive <DRIVE>. A virus was found in the boot record on the specified drive. To remove the virus, select the Repair command button.

The <VIRUS NAME> virus was found in memory. A virus was found in your computer's memory, which means it is active and possibly spreading to other files.

The boot record of drive <DRIVE> has changed since inoculation. Inoculation changes in a boot record are likely to indicate the presence of an unknown virus. However, there are a few situations where this kind of change is legitimate.

The boot record of drive <DRIVE> is infected with the <VIRUS NAME> virus. A virus was found in the boot record on the specified drive. To remove the virus, select the Repair command button.

The boot record on drive <DRIVE> is infected with the <VIRUS NAME> virus. Unable to inoculate boot records and system files. A virus was found in the boot record on the specified drive. Scan the drive to find and remove the virus, then inoculate the boot records and system files.

The file <FILENAME> in the compressed file <FILENAME> is infected with the <VIRUS NAME> virus. A virus was found in a file contained within the compressed file. Uncompress the file, then scan the files to find and remove the virus.

The file <FILENAME> is attempting to change the read-only attribute of file <FILENAME>. Norton AntiVirus is configured to notify you of this operation because it is an action that viruses sometimes perform.

The file <FILENAME> is attempting to format the hard disk. Norton AntiVirus is configured to notifying you because this is an activity that viruses sometimes perform.

The file <FILENAME> is attempting to write to <FILENAME>. Norton AntiVirus is configured to notify you of this operation because it is an action that viruses sometimes perform.

The file <FILENAME> is attempting to write to the boot record of drive <DRIVE>. Norton AntiVirus is configured to notify you of this operation because it is an action that viruses sometimes perform.

The file <FILENAME> is attempting to write to the master boot record of the hard disk. Norton AntiVirus is configured to notify you of this operation because it is an action that viruses sometimes perform.

The file <FILENAME> is infected with the <VIRUS NAME> virus. A virus was found in the specified file. To remove the virus you can delete the file or repair the file.

The file <FILENAME> was not allowed to change the read-only attribute of the file <FILENAME>. Norton AntiVirus is configured to not allow the read-only attribute changes to files because it is an action that viruses sometimes perform.

If you suspect a virus, scan your disks to find and eliminate the virus.

The file <FILENAME> was not allowed to format the hard disk. Norton AntiVirus did not allow the specified file to format your hard disk because it is an action that viruses sometimes perform.

If you suspect a virus, scan your disks to find and eliminate the virus.

The file <FILENAME> was not allowed to write to the boot record of drive <DRIVE>. Norton AntiVirus did not allow the specified file to write to the boot record of the specified disk because it is an action that viruses sometimes perform.

If you suspect a virus, scan your disks to find and eliminate the virus.

The file <FILENAME> was not allowed to write to the file <FILENAME>. Norton AntiVirus is configured to not allow changes to program files because it is an action that viruses sometimes perform.

If you suspect a virus, scan your disks to find and eliminate the virus.

The file <FILENAME> was not allowed to write to the master boot record of drive <DRIVE>. Norton AntiVirus is configured to not allow changes to the master boot record because it is an action that viruses sometimes perform.

If you suspect a virus, scan your disks to find and eliminate the virus.

The master boot record of drive <DRIVE> has changed since inoculation. Inoculation changes in the master boot record are likely to indicate the presence of an unknown virus. However, there are a few situations where this kind of change is legitimate.

The master boot record of drive <DRIVE> is infected with the <VIRUS NAME> virus. A virus was found in the master boot record on the specified drive. To remove the virus, select the Repair command button.

The master boot record on drive <DRIVE> is infected with the <VIRUS NAME> virus. Unable to inoculate boot records and system files. A virus was found in the master boot record on the specified drive. Scan the drive to find and remove the virus, then inoculate the boot records and system files.

Not enough memory for desired operation. Your computer does not have enough conventional memory to load Norton AntiVirus because there are terminate-and-stay-resident programs taking up space in conventional memory.

Unable to access drive: <DRIVE>. Norton AntiVirus could not access the specified drive because the drive door is open or there is a problem with the drive.

Unable to complete scan. Norton AntiVirus found more problems (infected files or inoculation changes) than it can report at one time. Correct the problems reported, then scan again. Norton AntiVirus will report any additional problems it finds.

Unable to delete write-protected file <FILENAME>. The file Norton AntiVirus is trying to delete is on a write-protected disk or in a folder for which you don't have write access.

Unable to find the virus definitions files. The files that Norton AntiVirus uses to detect known viruses cannot be found. You should reinstall Norton AntiVirus or get updated copies of the virus definitions files.

Unable to inoculate boot records on drive <DRIVE>. Norton AntiVirus cannot inoculate the boot records and system files because of a disk error. Your disk may have cross-linked files or a hardware problem.

Unable to open system messages file. The system messages files are not in the Norton AntiVirus

folder. Reinstall Norton AntiVirus.

Unable to print the requested information. The data cannot be printed because the printer is not connected or not online.

Unable to read the boot record. Norton AntiVirus was not able to access the boot record to check it for inoculation. This message can occur if you are using a program that locks the boot record in some way, preventing Norton AntiVirus from accessing it.

Unable to read the master boot record. Norton AntiVirus was not able to access the master boot record to check it for inoculation. This message probably indicates a hardware problem. This message also occurs if you are using a program that locks the boot record in some way, preventing Norton AntiVirus from accessing it.

Unable to reinoculate boot records on drive <DRIVE>. The boot records and system files cannot be reinoculated because you don't have read-write access to the inoculation file.

Unable to repair <FILENAME>. The file is still infected with the <VIRUS NAME> virus. Norton AntiVirus was not able to remove the virus from the specified file. You can eliminate the virus by deleting the file.

Unable to repair boot record of drive <DRIVE>. Norton AntiVirus was not able to repair a boot record on the specified drive.

Unable to repair master boot record of drive <DRIVE>. Norton AntiVirus was not able to repair the master boot record on the specified drive.

Unable to repair system files. The system files on your startup drive could not be repaired. To remove the virus, use the DOS SYS command from a write-protected bootable disk to restore the system files to an uninfected state. The SYS command is placed on your Norton Rescue Boot Disk.

Unable to repair the boot record of drive <DRIVE> with inoculation data. Norton AntiVirus was not able to restore the boot record to its previous state.

Unable to repair the file <FILENAME>. Norton AntiVirus was not able to repair the file. It is still infected with an unknown virus. You can eliminate the unknown virus by deleting the file.

Unable to repair the master boot record with inoculation data. Norton AntiVirus was not able to restore the master boot record to its previous state.

Unable to repair write-protected boot record of drive <DRIVE>. The boot record you are trying to repair is on a write-protected floppy disk. Remove write-protection, then repair the boot record.

Unable to update activity log file. The Activity Log could not be updated because you don't have read-write access to it.

Unable to update exclude file. The Exclusions List file could not be updated because you don't have read-write access to it.

Unable to update inoculation file. The inoculation file could not be updated because you don't have read-write access to it.

Unable to update the inoculation file in write-protected folder. You don't have write access to the folder where the inoculation file resides.