

## Virus Information

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

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

Memory Resident: Stays in DOS memory after it activates.

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

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

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

Encrypting: Encrypts its code to make detection more difficult.

Polymorphic: Appears differently in each infected file.

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.

---

Click here {button ,AL("NAVDISK\_V0190;NAVDISK\_V0175;NAVDISK\_V5000")} for more information.



## Norton AntiVirus main window

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

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

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

### You can also click any of the buttons to access more Norton AntiVirus features:

- Click Options to display settings tabs where you can customize Norton AntiVirus features.
- Click Virus List to displays the Virus List where you can view information about the viruses you are protected against.
- Click Scheduler to display the Norton Program Scheduler where you can schedule scans or other events. (Windows 95 only)
- Click Activity Log to display a history of Norton AntiVirus activities (for example, it lists each incident of a known virus detection or LiveUpdate).
- Click LiveUpdate to automatically update virus definitions.
- Click Quarantine to isolate infected or suspicious files for submission to Symantec AntiVirus Research (SARC).
- Click Disable/Enable Auto-Protect to turn off or on Norton AntiVirus automatic protection features.
- Click Info to get information on quarantined items or virus definitions.

### To get Help, position the cursor over any option in the Norton AntiVirus main window, click the right mouse button, and choose one of the following:

- What's This? Gives a brief description of the option.
- Contents: Gives you access to Norton AntiVirus help topics and Product Support online, including links to the Technical Support web site.

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

Click here

---

{button ,AL("NAVDSK\_I0000;NAVDSK\_V0020;NAVDSK\_V0055;NAVDSK\_V0015;NAVDSK\_V0045;NAVDSK\_V0050;NAVDSK\_V0010;NAVDSK\_V0075")}



## 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 memory, master boot record, boot records, and/or files were scanned.

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

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

---

Click here {button ,AL("NAVDSK\_V0175;NAVDSK\_V0180;NAVDSK\_V0200")} for more information.



## Details of Scan

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

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

---

Click here {button ,AL("NAVDISK\_V0175;NAVDISK\_V5000")} for more information.





## Problems Found

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

The Problems Found dialog box shows you the name of the infected or uninoculated 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.

---

Click here

{button ,AL("NAVDSK\_V0180;NAVDSK\_V0175;NAVDSK\_V0185;NAVDSK\_V5000;NAVDSK\_V0190")}  
for more information.



## Virus List

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



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

### To find a virus on the list:

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

**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.

---

Click here

{button ,AL("NAVDSK\_I0005;NAVDSK\_V0255;NAVDSK\_V0250;NAVDSK\_V0260;NAVDSK\_V0265;NAVDSK\_V0270;NAVDSK\_I0040")} for more information.



## **Virus Information**

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

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

---

Click here {button ,AL("NAVDSK\_V0250;NAVDSK\_V0255;NAVDSK\_V0260;NAVDSK\_I0005")} for more information.



## System Integrity

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

The System Integrity dialog box notifies you about changes in 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. Choose 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-mouse click any option (button, checkbox, etc.) and choose What's This? to display an explanation of what it does.

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

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

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

---

Click here {button ,AL("NAVDSK\_V0295;NAVDSK\_V0220;NAVDSK\_V0225;")} for more information.



**Clear Activity Log**

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





## Filter Activity Log

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

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

---

Click here {button ,AL("NAVDSK\_V0225;NAVDSK\_V0020;NAVDSK\_V0295")} for more information.



## **Exclude file**

From the Exclude File dialog box you can exclude this file from triggering alerts for certain activities. You may want to exclude a program file that changes frequently for legitimate reasons.

### **To exclude files prior to scanning:**

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

---

Click here {button ,AL("NAVDSK\_V0145;NAVDSK\_V0150;NAVDSK\_I0095")} for more information.



## Inoculation 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.

---

Click here {button ,AL("NAVDSK\_I0075;NAVDSK\_V0230")} for more information.



## Scanner Settings

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

**The Scanner tab allows you to choose settings that determine:**

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

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

**Your other options on this screen are the buttons:**

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

---

Click here

{button ,AL("NAVDSK\_I0065;NAVDSK\_V0080;NAVDSK\_V0085;NAVDSK\_V0092;NAVDSK\_V0095;NAVDSK\_V0065;NAVDSK\_V0055;NAVDSK\_V0075;NAVDSK\_V0020")} for more information.





**New file extensions**

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



## File Extensions

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

- The file extensions list contains the majority of extensions used for program files. Norton AntiVirus only scans files with extensions on this list.



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

- If you are using custom applications with unique file extensions, click New to display a dialog box where you can add them to the list. Then Norton AntiVirus can scan them and protect them against infection.
- Other options are:
  - Click Remove to delete a highlighted file extension. Be careful, however. Removing extensions from the list reduces your protection against viruses.
  - Click Default to return the file extensions list to the preset options.



## Scanner Advanced Settings

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

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

- Whether you want to Allow Network Scanning. This option has to be checked for network drives to appear in the Norton AntiVirus main window Drives list box.
- Whether you want to Allow Scanning to be Stopped while the scan is in progress.
- Whether to scan all removable media, hard drives, and/or network drives every time you scan instead of having to specify this option every time you perform a manual scan. Check this for maximum protection.

---

Click here {button ,AL("NAVDSK\_V0055;NAVDSK\_V0075")} for more information.



## Auto-Protect Advanced Settings

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

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

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

---

Click here {button ,AL("NAVDSK\_I0045;NAVDSK\_V0140")} for more information.





## Auto-Protect Settings

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

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

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

- 1 Check all options in the Scan A File When group box. (Note that the Opened option includes when a file is copied or moved.)
- 2 Click All Files instead of Program Files.
- 3 Always make sure that Load Auto-Protect At Startup is checked.
- 4 Click Heuristics to display the Heuristic Scanning options dialog box to enable Bloodhound technology, which can dramatically increase your protection against new and unknown viruses.

---

Click here {button ,AL("NAVDSK\_V0135;NAVDSK\_V0140;NAVDSK\_I0010")} for more information.



## Startup Settings

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

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

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



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



## Inoculation Settings

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

The Inoculation tab allows you to customize inoculation options. If you 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 Inoculate Automatically.

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

---

Click here {button ,AL("NAVDSK\_I0075;NAVDSK\_V0050")} for more information.



## Activity Log Settings

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

The Activity Log tab allows you to customize how to display the history of Norton AntiVirus activities. If you performed a complete setup of Norton AntiVirus, the preset options record detections of known viruses, completion of scans, and what action was taken on infected files (whether they were repaired, 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.

We recommend that you use the preset options.

---

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





## Exclusions Settings

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

The Exclusions tab allows you to exclude a file for 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.

---

Click here {button ,AL("NAVDSK\_I0095;NAVDSK\_V0135;NAVDSK\_V0020")} for more information.



## New/Edit Exclusion

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



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

---

Click here [{button ,AL\("NAVDSK\\_I0095;NAVDSK\\_V0135"\)}](#) for more information.



## General Settings

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

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

---

Click here {button ,AL("NAVDISK\_V0010;NAVDISK\_V0020")} for more information.



**Deny Access**

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





## **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).

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.



## **Password Settings**

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

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

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

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

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





## Virus Found in Download

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

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

Repair: Removes the virus from the file.

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

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

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

**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.

---

Click here {button ,AL("NAVDSK\_V0900")} for more information.



## **Virus Found in Download (Compressed file)**

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

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

### **In this case, the safest option is:**

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

### **A less safe option is:**

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

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

### **The least safe option is:**

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

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

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



## Network Browser

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

- You can select Microsoft domains, workgroups, servers, or local workstations as network alert targets. When a domain or workgroup is targeted, every member machine receives the alert.



When typing a domain name, add an asterisk (for example, Duluth\*); when typing a server name, precede it with two backward slashes (for example, \\Rm315).

- You can add NetWare servers alert targets. When a virus is detected on the workstation, a notification is sent to the NetWare server. When Norton AntiVirus for NetWare (Norton AntiVirus for NetWare) is running, it takes action based on how it has been configured to respond to a workstation virus alert.
- You can relay alerts to one or more remote workstations. By relaying all alerts to a single remote machine, you can effectively establish a dedicated alert server that centrally processes all alerts, as well as centralize the alert log. (All packets received from the machines originally configured to receive the alerts are automatically added to the remote machine's Windows NT event log.)
- You can forward quarantined files to a specific Quarantine server.

---

Click here [{button ,AL\("NAVDSK\\_F0198;NAVDSK\\_F0185;NAVDSK\\_F0186"\)}](#) for more information.



## Alerts Settings

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

The Alerts tab allows you to:

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





## **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.



### **Heuristic scanning options**

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

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.



## **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. SARC reports the results to you. If a new virus is discovered in your submission, SARC will create and send you special 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.

As soon as you install Norton AntiVirus...

**YOU ARE ALREADY PROTECTED AGAINST VIRUSES**

From this main window you can do the following:

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



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

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

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

**Note:** If the All Network Drives option is dimmed, you may need to enable Allow Network Scanning in the Options -- Scanner Advanced Settings dialog box.

Click to disable automatic protection. This 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 display an information box that tells you 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, 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 a dialog box, where you can choose to display one or more specific types of Norton AntiVirus events.

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

Click Close to exit the Activity Log.



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 (special programs used to identify viruses) to find and get rid of viruses. Since new viruses are being created all the time, you need to update the Virus List by adding new virus definitions provided by Symantec regularly easily. 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 this Repair File dialog box you can remove a virus from an infected file and/or return the identified file to its original state. Click Repair or Repair All to have Norton AntiVirus repair one or all of the files identified during the scan.

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

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

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

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

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

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

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



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

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

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

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

## 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.

### Here's what Norton AntiVirus does 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.
- Monitors your computer for any activity that might indicate the work of a virus in action.
- Scan files you download from the Internet.
- Checks floppy disks for boot viruses when you use them.
- Updates your virus protection regularly.

### Here's what you can do with Norton AntiVirus:

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

### Click here to view a guided tour:

 [Norton AntiVirus Guided Tour](#)

---

Click here

{button ,AL("NAVDSK\_I0010;NAVDSK\_I0060;NAVDSK\_I0020;NAVDSK\_I0065;NAVDSK\_I0075;NAVDSK\_V0250;NAVDSK\_I0025;NAVDSK\_V0010")}

 for more information.



## Product Support Online

For Internet access , click here:

[Norton AntiVirus Technical Support](http://service.symantec.com/nav.html) via the Internet at <http://service.symantec.com/nav.html>

[Symantec AntiVirus Research Center](http://www.symantec.com/avcenter) via the Internet at <http://www.symantec.com/avcenter>


[Symantec AntiVirus Research Center Virus Encyclopedia](http://www.symantec.com/avcenter/vinfodb.html) via the Internet at <http://www.symantec.com/avcenter/vinfodb.html>

To consult the online manuals,

First click here:

 [Install Adobe Acrobat Reader](#)

Then click here to select a manual:


 [Norton AntiVirus 5.0 Reference Guide for Windows 95/98](#)

 [Norton AntiVirus 5.0 User's Guide for Windows 95/98](#)

 [Norton AntiVirus 5.0 Reference Guide for Windows NT](#)

 [Norton AntiVirus 5.0 User's Guide for Windows NT](#)

To view a short video or interactive tutorial, click:

 [About Viruses](#)

 [About SARC \(Symantec AntiVirus Research Center\)](#)

 [Norton AntiVirus Guided Tour](#)

 [What to do When Norton AntiVirus Reports a Problem](#)





## How Norton AntiVirus works

### 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 with the Scan Now button in the main window or scheduled to run automatically--it is searching for these telltale signatures. If a file is found that has been infected by one of these viruses, Norton AntiVirus has the tools to eliminate the virus automatically.

Each time a new virus is discovered, its virus signature must be added to the virus definitions file by the Symantec engineers. For this reason, you need to update your virus definitions file regularly. Symantec has made this extremely 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.

---

Click here

{button ,AL("NAVDSK\_I0015;NAVDSK\_V0055;NAVDSK\_I0075;NAVDSK\_V0015;NAVDSK\_I0025;NAVDSK\_I0065;NAVDSK\_V0055")} for more information.



## About Norton AntiVirus Auto-Protect

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

- Detecting viruses that may already exist and remove 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:

**Note:** Norton AntiVirus is preset to load automatic protection 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.

---

Click here {button ,AL("NAVDSK\_V0010;NAVDSK\_I0075;NAVDSK\_I0025;NAVDSK\_I0035")} for more information.



## The importance of a Norton AntiVirus Rescue Disk Set



When you set up Norton AntiVirus, you were advised to create a Norton AntiVirus Rescue disk set. 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 Norton AntiVirus and pointing to Rescue Disk. If you did create the Norton AntiVirus rescue disk set, be sure you have stored the disks in a safe place.

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

---

Click here [{button ,AL\("NAVDSK\\_V0360;NAVDSK\\_V0385"\)}](#) for more information.



## **What is a computer virus?**

Computer viruses are, simply, 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 which 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.

---

Click here {button ,AL("NAVDISK\_I0030;NAVDISK\_I0035;NAVDISK\_V0055;NAVDISK\_I0040")} 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 designed to do any serious damage; 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 e-mail 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, in fact, merely affected the programs that control the display or keyboard. Not even your disks themselves are physically damaged, just what's stored on them. Viruses can only infect files and corrupt data.
- Infect write-protected disks or text-based e-mail 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.

---

Click here {button ,AL("NAVDSK\_I0030;NAVDSK\_I0035;NAVDSK\_V0055;NAVDSK\_I0040")} for more information.



## **Types of viruses**

Known viruses are categorized in the [Virus List](#) by how often you find them, what they infect, and how they behave.

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

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

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

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

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

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

**Windows Viruses:** Viruses that infect Windows programs.

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

---

Click here [{button ,AL\("NAVDISK\\_I0025;NAVDISK\\_V0055;NAVDISK\\_I0035"\)}](#) for more information.



## **Virus-like activities**

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

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

---

Click here {button ,AL("NAVDSK\_I0025;NAVDSK\_I0035;NAVDSK\_I0095")} 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 (called Auto-Protect), you can also initiate scans at any time and schedule scans to occur at predetermined times.

### To initiate scans:

- 1 Open the Norton AntiVirus main window if it is not already displayed.
- 2 Choose one of the following options:
  - Check a drive or drives in the Drives list box or check a category of drives in the Drive Types group box and click Scan Now.  
**Note:** The All Network Drives option is dimmed if you are not connected to a network or if Norton AntiVirus is configured not to allow network drive scanning. (See the Scanner Advanced Settings dialog box to reconfigure this option.)
  - Click File, Folders, or Path from the Scan menu and select what to scan.

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

---

Click here {button ,AL("NAVDSK\_V0055;NAVDSK\_V0075;NAVDSK\_V0065;NAVDSK\_V0020;")} 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:** that Norton AntiVirus also scans Microsoft Word and Excel documents when scanning program files. Although these are not program files, they do contain code and can be infected by Macro Viruses. Therefore, some of your data files are now at risk. You need to make backup copies regularly.

---

Click here {button ,AL("NAVDSK\_10010;NAVDSK\_V0055;NAVDSK\_V0340;NAVDSK\_V0335")} for more information.



## 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 Then 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
  - Work with compressed files
  - 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.

---

Click here {button ,AL("NAVDSK\_I0010;NAVDSK\_V0055;NAVDSK\_V0340;NAVDSK\_V0335")} for more information.



## About Inoculation

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

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.

---

Click here [{button ,AL\("NAVDSK\\_I0010"\)}](#) for more information.



## **About the Virus List**

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

To prevent newly discovered viruses from invading your computer, you should update your virus definition files regularly. Norton AntiVirus uses the information in virus definitions files to detect viruses during scans. Updated virus definitions files are available 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.

---

Click here {button ,AL("NAVDSK\_I0070;NAVDSK\_I0260")} for more information.





## About the Activity Log

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

From the Activity Log dialog box you can:

- Click Print to print the Activity Log to a printer or a file.
- Click Filter to display specific events, such as all virus detections.

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

---

Click here {button ,AL("NAVDSK\_V0215;NAVDSK\_V0220;NAVDSK\_V0225")} for more information.



### **About 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.

**Note:** Norton AntiVirus for Windows 98 and Windows 95 use different schedulers. The Windows 98 version uses the new built-in Windows scheduler, while the Windows 95 version uses the Norton Program Scheduler.

---

Click here {button ,AL("NAVDSK\_V0075;NAVDSK\_V0900")} 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 checked and the file is moved without renaming.

---

Click here [{button ,AL\("NAVDSK\\_V0040"\)}](#) for more information.



## About the Repair Wizard

Norton AntiVirus now has a Repair Wizard that walks you through the steps of eliminating any viruses found on your computer during a scan that you initiate or schedule. When a virus is found, the Repair Wizard offers you the choice of:

- Repairing all the viruses at once.
- 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 re-scan 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.

---

Click here {button ,AL("NAVDSK\_V0010;NAVDSK\_I0075;NAVDSK\_I0025;NAVDSK\_I0035")} 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. 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 special 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.

---

Click here {button ,AL("NAVDSK\_V0010;NAVDSK\_I0075;NAVDSK\_I0025;NAVDSK\_I0035")} for more information.



### **About updating virus definitions with LiveUpdate**

To prevent the new viruses that have been discovered since you bought Norton AntiVirus, you **MUST** update your protection (virus definitions) frequently. Otherwise, Norton AntiVirus cannot do its job. If your computer is connected to a modem and you accepted the preset options when you installed Norton AntiVirus, LiveUpdate is already scheduled to update virus definitions files 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 or request them by mail.

---

Click here {button ,AL("NAVDSK\_I0071")} for more information.



## Sources for updating virus definitions

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

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

### 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 World Wide WEB site:

- 1 Access www.symantec.com and select country.
- 2 Click AntiVirus Research Center.
- 3 Click Download Updates.
- 4 Click to 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 Enter **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 Enter SYMANTEC.
- 4 Double-click Support Solutions
- 5 Double-click Norton AntiVirus 95 (the same files are used for Windows NT).

The virus definitions are located in the File library.

### Symantec BBS

---

Settings for the Symantec BBS are:


8 data bits, 1 stop bit; no parity

**To contact the Symantec BBS, use one of the following telephone numbers:**

- 300- to 28,800-baud modems (541) 484-6669 [24 hrs.]

**To access definitions from the initial menu of the Symantec BBS:**

- 1 Press **F** to get a file.
- 2 Press **N** to get the latest Norton AntiVirus definitions and follow the on-screen directions to download the files.

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

### **Virus Definitions Update Disks**

---

You can order virus definitions update disks from Symantec to arrive by mail. This service requires a fee:

- In the United States, call (800) 453-1149.
- Outside the United States, contact your local Symantec office or representative.

The file you receive is a compressed archive that contains several files.

---

Click here {button ,AL("NAVDSK\_V0550")} for information on installing new virus definition files.



## 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.
/NORERESULTS	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)





## **Credits**

### **Product Management**

Betsy Baker, Steve Cullen, Lily De Los Rios, Alex Haddox, Marian Merritt, John Moldenhauer, Robert Pettit, Sharon Ruckman, Jack Tang

### **Program Management**

Brian Foster, Francia Saplala, Gary Westerland

### **Software Development**

David Allee, Jim Brennan, David Buches, Tim Cashin, Michael Dunn, Scott Edwards, Barry Gerhardt, David Hertel, Michael Keating, John Millard, David Shannon, Radoslav Stanev, Jacob Taylor

### **Quality Assurance**

Kerry Boyte, Paul "FB" Davis, Rob Ficcaglia, Olga Komsitsky, Bob Kolosky, Marc Marcuse, Melissa Mendonca, Chris Nevarez, Greg Patterson, Garret Polk , Ellis Rahhal, Jim Waggoner

### **SWAT Team**

Jim Belden, Stanley Ballenger, Rekha Chintalacharuv, Chuck Eaton, Nigel Gallagher, Vance Gloster, Igor Goldshteyn, Rion Millen, Rajesh Pulinthanatu, Dan Sackinger, Mark Santhasouk, Francia Saplala, Scott Smith, P. Venkatraman, Mark Zaremba

### **Shared Tech**

Cameron Bigger, Don Carver, Leo Cohen, Alireza Faroush, Ben Hallert, Bruce Hellstrom, Roger Holman, Jim Lamb, Jim Lucan, Bryan Martin, Patrick Martin, Bruce McCorkendale, Eoghan O'Donnell, Heath Perryman, Sam Porterfield, Mark Spiegel, Peter Van Nuys, Oleg Volochtchouk

### **Documentation and Online Help**

Kurt Ament, Elizabeth Anders, Alfred Ghadimi, Karen Goldsmith, Robert Hoffman, Romey Keys, Robert Squires

### **Technical Support**

Beth Bryant, Earl Campbell, Brian Cochrane, Erich Dobroth, Christine Frazer, Rochelle Hamlett, Pamela Heine, Ty Hodson, Todd Kieser, Carrie Kelso, Danny Krautschek, Tyrone McDermott, Deborah Light, David Lucas, Russell Lusignan, Dan Pederson, LaVonne Perry, Leon Plueard, Carol Simmonds, Matthew Smith, Olga Stamatiou, Chris Steele, Joe Trozelle, Joe Waisman, Robert Walling, Jason Walsh, Gwen White, Ken Zug

### **Engineering Services Team**

Stephen Blackmoore, Emma Fielding, Sara Flood, Renal Fuller, Pat Hoed, Will Jobe, Helen Kim, Sebastian Lai, Dave Lewis, Scott Mynatt, Reiko Nozawa, Sheelagh O'Connor , Ed Thompson, Dwight Wilson

### **Symantec AntiVirus Research Center (SARC)**


David Banes, Diop Bankole, Frank Barajas, Sherralee Buzzell, Matt Candelaria, Darren Chi, Eric Chien, Steven Chu, Philip DeBats, Raul Elnitiarta, Chris FormulakYuji Hoshizawa, Henry Jalandoni, Tigran Khanpalyan, Darren Kessner, Maryl Magee, Carey Nachenberg, Cary Ng, Abid Oonwala, Peter Pak, Charles Renert, Ian Roessle, Steve Trilling, Rene Visser, Kurt Weber, John Wilber, Motoaki Yamamura

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

**To find help:**

▶ Do one of the following

- Choose Contents from the Help menu.
- From any Norton AntiVirus dialog:
  - Click the help button.
  - Right-click any option in a Norton AntiVirus screen and choose What's This? for a brief definition of the option.
- Choose Product Support Online from the Help menu.

 Note that you can keep help open on your desktop by minimizing the help window or by simply clicking back and forth between help and the product.

---

Click here `{button ,AL("NAVDSK_V0325")}` 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, 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 task bar in the lower right corner of the desktop to open Norton AntiVirus.
- 2 From the Norton AntiVirus main window, initiate manual scans of selected files, folders, or drives using the menu commands or the Scan Now button in the Norton AntiVirus main window. See [Initiate scans](#).

---

Click here {button ,AL("NAVDSK\_V0050;NAVDSK\_V0030;NAVDSK\_V0035")} for more information.

**Note:** Norton AntiVirus is preset to load automatic protection whenever you start your computer.

**To disable Auto-Protect temporarily:**

- 1 Right-click the Norton AntiVirus icon on the Windows task bar in the lower right corner of the desktop to open Norton AntiVirus..
- 2 Click Disable Auto-Protect.

**To enable Auto-protect again:**

- ▶ Repeat the steps above. (Click Enable Auto-Protect in step 2.)

---

Click here [{button ,AL\("NAVDSK\\_I0015;NAVDSK\\_V0120"\)}](#) for more information.

**To bypass startup protection:**

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

**Note:** Bypassing startup protection reduces your level of protection.

---

Click here [{button ,AL\("NAVDSK\\_V0160"\)}](#) for more information.



**To always scan floppies (during scans you initiate):**

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

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

---

Click here {button ,AL("NAVDSK\_V0055")} for more information.

**To keep up with new viruses:**

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

- ▶ Do one of the following
  - If your computer is connected to a modem or to the Internet, simply click the LiveUpdate button in the Norton AntiVirus main window and follow the onscreen prompts to initiate a LiveUpdate at any time you choose.
  - If your computer is connected to a modem or to the Internet, schedule automatic LiveUpdates to occur more than once a month using the Norton Program Scheduler.
  - If you don't have a modem or an Internet connection, order virus definitions update disks from Symantec to arrive by mail. This service requires a fee:
    - In the United States, call (800) 441-7723.
    - Outside the United States, contact your local Symantec office or representative.
  - Follow the instructions on the update that you receive.

---

Click here {button ,AL("NAVDSK\_V0550")} for detailed instructions on installing new virus definitions files.

**To 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.

---

Click here [{button ,AL\("NAVDSK\\_V0250;NAVDSK\\_I0071"\)}](#) for more information.

### To update virus definitions using LiveUpdate:

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

**1** In the Norton AntiVirus main window, click LiveUpdate.

**2** In the How Do You Want To Connect drop-down list box, select one of the following:

Find Device Automatically: Norton AntiVirus determines if you have an Internet connection or must connect using your modem.

Internet: Norton AntiVirus connects to the Symantec FTP (File Transfer Protocol) site on the Internet.

Modem: Norton AntiVirus dials a preset number and connects to a Symantec server through your modem.

**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 on your next scan.

**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:

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

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

---

Click here {button ,AL("NAVDSK\_V0550")} for detailed instructions on installing new virus definitions files.

**To schedule virus scans for Windows 95:**

- 1 Click Scheduler in the Norton AntiVirus main window
- 2 Click Add. (If the button isn't visible, select Add from the Event menu.)
- 3 Select Scan For Viruses in the Type Of Event drop-down list box.
- 4 Check Enable This Event. If you uncheck this option, the scan won't run.
- 5 Enter a brief description in the Description text box.  
This text appears in the Events list box in the Scheduler main window.
- 6 Enter the drive letter or pathname for the drive, folder, or file you want scanned in the What To Scan text box.  
To scan more than one item, use a space between them. For example:  
C: D:\Applications  
If the path uses spaces, enclose the item in double quotes. For example:  
"C: \GP Was Here\Gone.exe"
- 7 Select how often you want the scan to occur in the Frequency drop-down list box.
- 8 Finish scheduling the scan by entering the correct time, day, and date information and click OK.



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

---

Click here {button ,AL("NAVDSK\_V0055")} for more information.

## Scanning for viruses on your computer

► **To find viruses on your computer do one of the following**

- Initiate virus scans at any time by opening the Norton AntiVirus main window, choosing which drives to scan, and clicking Scan Now.
- Use the Scan menu in the Norton AntiVirus main window to choose specific paths, files or folders to scan.

---

Click here

{button ,AL("NAVDSK\_I0015;NAVDSK\_V0055;NAVDSK\_V0250;NAVDSK\_V0075;NAVDSK\_V0050")}  
for more information.

**To initiate scans:**

- 1 Open the Norton AntiVirus main window if it is not already displayed.
- 2 Choose one of the following options:
  - Check a drive or drives in the Drives list box or check a category of drives in the Drive Types group box and click Scan Now.

**Note:** If the All Network Drives option is dimmed, open the Options /Scanner/ Advanced Settings dialog box to check All Network Drives and then reconfigure this option.

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

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

---

Click here {button ,AL("NAVDSK\_V0075;NAVDSK\_V0065")} for more information.

**To scan drives:**

- 1 Open the Norton AntiVirus main window if it is not already displayed.
- 2 Check specific drives to scan in the Drives list box or select multiple drives at once by checking one or more options in the Drive Types group box and click Scan Now.

The All Network Drives option is dimmed if you are not connected to a network or if Norton AntiVirus is configured not to allow network drive scanning.

---

Click here {button ,AL("NAVDSK\_V0075")} for more information.



**To scan a folder:**

- 1 Choose Folders from the Scan menu.
- 2 Click the checkboxes next to the folders you want to scan.
- 3 Click Scan.

---

Click here [{button ,AL\("NAVDSK\\_V0075"\)}](#) for more information.

**To scan a path:**

- 1 Choose Path from the Scan menu.
- 2 Enter a path to scan.
- 3 Check Scan Subfolders to scan all folders in the path.

---

Click here [{button ,AL\("NAVDSK\\_V0075"\)}](#) for more information.

**To scan an individual file:**

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

---

Click here [{button ,AL\("NAVDSK\\_V0075"\)}](#) for more information.

**To 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 (for example, VIRUS FOUND, INOCULATION CHANGED, etc.). In this case, choose the appropriate action: Repair, Quarantine, Delete, Exclude, Stop, Continue, Inoculate.

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

## Action buttons

- Repair:** Eliminates the virus and returns the infected file or boot record to its original state.
- Quarantine:** Isolates the file and prevents it from being accessed or run. Quarantined files can be submitted to SARC for further analysis.
- 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.
- Stop:** If a scan is in progress, the scan stops. Clicking Stop does not solve the problem that was reported to you.
- Continue:** If a scan is in progress, the scan continues. If you are accessing a file, access is granted. Clicking Continue does not solve the problem that was reported to you.
- Inoculate:** Generates inoculation data for a boot record. Norton AntiVirus notifies you if the file ever changes, which could indicate an unknown virus.

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

**To use the Repair Wizard:**

▶ Simply follow the instructions on the screen. 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.

**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.

**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

- Choose Inoculate if the boot record has changed for legitimate reasons since the last time you inoculated it. (For example, you may have installed a new version of a software product. Another example is if you have a dual boot system and boot from one system to another, the boot record changes. In this case, you do not want to make a Repair because you would create the wrong operating system boot records.)
- Choose 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. Installing products or repartitioning your hard disk, as well as changing between dual boot systems, can modify the boot records. Note that Norton AntiVirus does not check for inoculation changes on NEC PC98xx machines.

---

Click here {button ,AL("NAVDSK\_I0075")} 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 Next, use your Norton AntiVirus Rescue Disk, labeled Norton AntiVirus 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. You should come up to an A prompt. Either follow the prompts for running a scan or type NAVDX from the A prompt.
- 5 If you do not have a Rescue boot disk set 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 a Norton AntiVirus Rescue Disk Set:**

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

### **To delete an infected file:**

- 1** Click Delete in the Norton AntiVirus alert box, then follow the prompts on your screen.  
If the Delete command button is dimmed, either Norton AntiVirus is configured not to enable it or the item cannot be deleted.
- 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 WIN95/98 startup disk you made when you installed Win95/98.
- 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 diskette 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 Norton AntiVirus Rescue Disk, labeled Norton AntiVirus 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**

- Choose 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, select. (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.
- Choose 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.)
- Choose 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 remove viruses from downloaded compressed files:**

- ▶ Do one of the following
- Abort the download and try to obtain a clean copy of the file from a different source.
- Save the file to a temporary directory, uncompress it, scan again, and attempt to repair any infected files.

**To restart a shutdown computer:**

- 1 Restart your computer by placing the disk, labeled Norton AntiVirus Rescue Boot Disk in drive A: and turning on your computer.

If you did not create a Norton AntiVirus Rescue Boot Disk, use the Norton AntiVirus Emergency disk that came with your original box.

- 2 When prompted, remove your first rescue disk and insert the one labeled "Norton AntiVirus Program Disk."

- 3 Type Go at the DOS prompt and press Enter.

Norton AntiVirus scans the C: drive and informs you when a virus is found.

**Note:** By specifying your startup drive, C:, on the command line, you'll overcome certain viruses, such as the Stoned.Empire.Monk virus, which hides the C: drive from the operating system.

- 3 Once all viruses have been eliminated, remove any floppy disks and reboot your computer by switching the power off and then on to return to Windows.

- 4 Scan again.

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

### **To remove viruses from infected compressed files:**

Although Norton AntiVirus can detect an infected file in a compressed file, it cannot repair the file in its compressed state.

- 1** Right-click the Norton AntiVirus icon in the Windows taskbar and disable Auto-Protect temporarily.
- 2** In a temporary folder, uncompress the compressed file using a utility such as PKUNZIP.EXE
- 3** Scan the temporary folder and repair or delete any infected files.
- 4** Remove the whole compressed file from your disk.

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

- 5** Enable Auto-Protect.



You can leave the infected compressed file on your computer. As long as you never uncompress it and attempt to use the files, it does not spread the virus. However, if you continue to scan compressed files, you continue to receive the warning about infections.

**To change how Norton AntiVirus works:**

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click one of the tabs.  
A brief description of the tab appears at the top of the tab.
- 3 Use the right mouse button to click any control to see what it does.
- 4 Change any settings you want.
- 5 Click OK to close and exit the screen. (If you don't click OK, you lose your changes.)

These settings now take precedence over the preset options. You don't need to restart your computer.

---

Click here {button ,AL("NAVDSK\_V0050")} for more information.

**To change scan options for scans you initiate or schedule:**

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Scanner tab if it is not already on top.
- 3 Click the right mouse button over any option and click What's This? to find out what the option does.
- 4 Make your changes and click OK to save settings and exit.

---

Click here {button ,AL("NAVDSK\_V0050;NAVDSK\_V0065;NAVDSK\_V0055")} 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 the Scanner tab to bring it to the front.
- 3 From the Scanner tab, check the areas your computer should scan before program files are scanned.

**Note:** By default, all options are already checked 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 You can click Select to display the Program File Extensions dialog box, which lists the file extensions that Norton AntiVirus scans.

---

Click here {button ,AL("NAVDISK\_V0075;NAVDISK\_I0065;NAVDISK\_V0055")} for more information.

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

- 1 Click Options from the Norton AntiVirus main window.
- 2 From the Scanner tab, click any of the options in the How To Respond drop-down list box.
- 3 Click the right mouse button on the selected option to display a help menu. Click What's This? to see a description of the option.
- 4 Do one of the following
  - If you choose Prompt, specify in the Buttons To Display If Prompted group box which options you want Norton AntiVirus to make available when a virus is found.
  - If you select Custom Response, click the Customize button to display a dialog where you can specify which options you want Norton AntiVirus to make available for three types of infections: file viruses, boot record viruses, and macro viruses.
- 5 Click OK to save settings and exit the dialog box.

---

Click here [{button ,AL\("NAVDSK\\_I0065;NAVDSK\\_V0075;NAVDSK\\_V0055"\)}](#) for more information.

**To choose what you can do when Norton AntiVirus finds a virus during a manual or scheduled scan:**

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Scanner tab to bring it to the front.

The preset options in the Buttons To Display If Prompted group box are:

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

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

Continue: Ignores the issue.

Quarantine: Isolates the virus-infected file so that it cannot spread, but does not attempt a repair. From the Quarantine you can submit the file to SARC (Symantec AntiVirus Research Center).

- 3 Click to add or delete Buttons To Display If Prompted options.

**Note:** If an option is not checked, the button is dimmed when it appears in a dialog box. Note also that the Repair and Delete buttons may be dimmed if Norton AntiVirus is unable to repair or delete the selected file.



**To set additional scanning options:**

**1** Click the Heuristics button in the Scanner tab.

**2** Make sure that Enable Bloodhound Virus Detection Technology is checked.

You can drag the pointer to increase your virus protection against difficult to detect and unknown viruses. Scanning may take a bit longer.

**3** Click OK to close the Heuristic Scanning Options dialog box.

**4** Click the Advanced button on the Scanner tab.

**5** Check the Advanced Settings options you want to enable.

**To choose which file extensions Norton AntiVirus scans:**

- 1 From the Scanner tab, click the type of files to scan: All Files or Program Files.  
**Note:** In most cases, scanning only program files is sufficient. For maximum protection, click All Files.
- 2 If you have selected Program Files, click Select to display the Program File Extensions dialog box.
- 3 Click New to display the New Program File Extension dialog box.
- 4 Enter any nonstandard file extensions that you use to name executable files.
- 5 Click OK to save settings and exit the New Program File Extension dialog box.  
The Program File Extensions dialog box reappears.
- 6 Click OK to save settings and exit the Program File Extensions dialog box.  
The Scanner tab reappears.
- 7 Click OK to save settings and exit the Options dialog box.



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

---

Click here {button ,AL("NAVDSK\_I0065;NAVDSK\_V0075;NAVDSK\_V0055")} for more information.



**To set general scanning options:**

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the General tab to bring it to the front.
- 3 Check Backup File in Quarantine Before Attempting A Repair to have Norton AntiVirus make a copy of the infected file before repairing it.
- 4 Click OK to save settings and exit the dialog box.

---

Click here {button ,AL("NAVDSK\_V0055")} for more information.

**To determine how protection works at startup:**

- 1 Click Options in the Norton AntiVirus main window.
  - 2 Click the Startup tab to bring it to the front.
  - 3 Specify in the What To Scan group box the areas that you want Norton AntiVirus to scan each time you start your computer.
-  We recommend that you leave the preset options as they are. (Everything is selected.)
- 4 Choose your bypass keys (Both Alt keys is the preset option).
-  If you work in a high risk environment, or if many other people use your computer, we recommend that you choose None.

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

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Auto-Protect tab to bring it to the front.
- 3 Check when 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 dialog box.

---

Click here {button ,AL("NAVDSK\_10065")} for more information.

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

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

**To monitor for virus-like activities:**

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Auto-Protect tab to bring it to the front.
- 3 Click Advanced at the bottom of the tab.
- 4 Click an option in each drop-down list box to specify what Norton AntiVirus should do when it detects the virus-like activity.

The preset option for some activities is Allow. To set a higher level of protection, click Prompt. This option gives you the choice to Continue, Stop, or Exclude every time the activity occurs. In other words, you can evaluate whether or not you should allow the activity.

- 5 Click OK to close the dialog box.
- 6 Click OK to save your settings and close the Options dialog box.

---

Click here {button ,AL("NAVDSK\_I0045")} for more information.

**To set up maximum protection:**

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


[Customize Scanner settings for maximum protection.](#)

[Customize Auto-Protect settings for maximum protection.](#)

[Schedule Scans in Windows 95](#)

[Schedule LiveUpdates in Windows 95](#)

[Schedule Scans in Windows 98](#)

 If you have a modem and 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 Scanner settings for maximum protection:**

- 1** Click Options in the Norton AntiVirus main window.
- 2** Click the Scanner tab to bring it to the front.
- 3** Check all options in the What To Scan group box; choose the All Files option.
- 4** Be sure that Prompt is selected in the When A Virus Is Found drop-down list box.
- 5** Be sure that neither Continue nor Exclude is checked in the Buttons To Display If Prompted group box.
- 6** Click Advanced at the bottom of the tab.
- 7** Check All Floppy Drives in the Preselect At Start group box, then click OK to save settings and exit the Scanner Advanced Settings dialog box.
- 8** Click Heuristics at the bottom of the tab to display the Heuristics scanning options dialog where you can enable a higher level of detection for rare virus infections.
- 9** Click OK to save settings and exit the dialog box.

---

Click here {button ,AL("NAVDSK\_V0135;NAVDSK\_V0235;NAVDSK\_V0075")} for more information.

**To customize Auto-Protect settings for maximum protection:**

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

---

Click here {button ,AL("NAVDSK\_V0130;NAVDSK\_V0235;NAVDSK\_V0075")} 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 Log in the Norton AntiVirus main window.

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.

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

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

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

**To filter the Activity Log entries:**

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

**To clear the Activity Log:**

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

**To use the Virus List:**

- 1 Click Virus List in the Norton AntiVirus main window.

The Virus List displays the name of the virus and what it infects (program files, boot records, or both).

- 2 Use any of the following options to manage the Virus List:
  - Select a category from the Display drop-down list box to view different categories of viruses.
  - Click Info to view details, such as symptoms and aliases, about a particular virus.
  - Click Print to print the Virus List to a printer or to a file.

**To search the Virus List:**

**1** Activate the Virus List box by clicking inside the list box.

**2** Start entering the name of the virus you want to find.

The Smart Search text box appears at the bottom of the list.

**3** Continue typing until the virus you're searching for is highlighted in the Virus List.



**To display information about a virus:**

- 1 Click Virus List in the Norton AntiVirus main window.

The Virus List displays the name of the virus and what it infects (program files, boot records, or both).

- 2 Click in the Virus List itself. Start entering the first few letters of the virus name you are searching for.

The Smart Search text box appears at the bottom of the list.

- 3 Continue entering the virus name until the virus you're searching for is highlighted in the Virus List.
- 4 Click Info to view details, such as symptoms and aliases, about the highlighted virus.

**To print to a printer:**

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

**To print to a file:**

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

**To append a file:**

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

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

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

**To 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 (such as Virus List changes) as well.

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Activity Log tab to bring it to the front.
- 3 In the Log Following Events group box, check any event that you want Norton AntiVirus to record.
- 4 Click OK to save changes and close the dialog box.

**To customize 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.
- 3 Specify whether or not Norton AntiVirus should alert Norton AntiVirus NLM (if present).
- 4 Specify whether or not to forward an alert to a Norton AntiVirus alert service and choose which service from a browser.

**To password-protect features:**

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Password tab.
- 3 Check Password Protect to turn on the password protection feature.
- 4 Do one of the following

To protect all of the features shown in the list box, select Maximum Password Protection.

To protect only certain features, select Custom Password Protection; then click the features you would like to protect in the list box.

- 5 Click Set Password and enter the password you want to use in the Set Password dialog box. The same password applies to all selected features.

Passwords can be from 1 to 16 characters in length and are not case-sensitive (a is the same as A). As you type, Norton AntiVirus replaces the characters on the screen with asterisks (\*) for security.

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



**To exclude files from being scanned for viruses:**

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Exclusions tab to bring it to the front.
- 3 Click New.
- 4 Do one of the following
  - Use the browse button to display a file selection dialog box from which you can choose a file that will be displayed in the Item text box.
  - Enter a filename in the Item text box. You can use wildcards such as c:\\*.COM. You should check Include Subfolders if you want to ensure that all files with that extension are excluded.



Be careful! Excluding files reduces your level of protection.

**To edit exclusions:**

- 1 Click Options in the Norton AntiVirus main window.
- 2 Click the Exclusions tab to bring it to the front.
- 3 Select an item from the Items list box.
- 4 Click Edit and make the desired changes.

**To delete an exclusion:**

- 1** Click Options in the Norton AntiVirus main window.
- 2** Click the Exclusions tab to bring it to the front.
- 3** 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 scan networks:**

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

**To quarantine an infected or suspicious item:**

- ▶ Do one of the following
  - 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 get information about a quarantined item:**

- 1 In the Norton AntiVirus main window, click Quarantine.
- 2 In the left panel of the Quarantine, click Quarantined items.
- 3 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 Quarantine.
- 2** Select a file in the list of Quarantined items and click Submit Item.
- 3** Follow the directions in the Scan and Deliver Wizard to collect information and submit the file to SARC for analysis.



**To schedule a scan or LiveUpdate for Windows 98:**

- 1** Click Start on the Windows taskbar, point to Programs, point to Norton AntiVirus, and click Schedule A Scan Or LiveUpdate.
- 2** In the Scheduled Tasks window, click Add Scheduled Task.
- 3** Follow the directions in the Scheduled Task Wizard.
- 4** Choose Norton AntiVirus as the application to run.
- 5** Set the scan schedule.
- 6** Close the Scheduled Tasks window.

**To schedule LiveUpdates for Windows 95:**

- 1 Click Scheduler in the Norton AntiVirus main window.
- 2 Click Add. (If the button isn't visible, select Add from the Event menu.)
- 3 Select Schedule LiveUpdate in the Type of Event drop-down listbox.
- 4 Check Enable This Event. If you uncheck this option, the LiveUpdate won't run.
- 5 Check Audible Alarm to hear a sound when the LiveUpdate starts.
- 6 Type a brief description in the Description text box.  
This text will appear in the Events listbox in the Scheduler main window.
- 7 Select how often you want the LiveUpdate to occur in the Frequency drop-down listbox.
- 8 Finish scheduling the LiveUpdate by entering the correct time, day, and date information and click OK to save settings and exit the dialog box.



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

- ▶ Click the Minimize button.

The Scheduler remains active so that the LiveUpdate can run at the time you specified.

The LiveUpdates you scheduled will run automatically. If your computer is turned off or the Scheduler is not loaded when a LiveUpdate is scheduled, you are notified that the LiveUpdate was canceled the next time the Scheduler loads.

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.



Scans files compressed using any one of several popular compression utilities. Scanning time can increase slightly if you have many compressed files. Note that compressed files within compressed files are not scanned. This option is preset for maximum protection.

Click to display the Customize Response dialog 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.

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



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

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

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

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

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

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

Click Remove to delete the selected extension.

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 Prompt 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 Prompt 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.

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

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 both Shift keys to bypass a scan at startup.

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

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

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



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

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

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

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

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

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.

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

Check if you want the alert forwarded to a Norton AntiVirus NT alert service. Then enter or browse for the location of the service.

Click to display the network browser where you can select a message relay target.



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

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

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 you are notified that a boot record's inoculation data has changed. Prompt gives you the most control.

Choose an option to choose how to respond to an inoculation issue. Choose Prompt 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.

**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, etc.). 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, 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 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 which 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 on-line 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, .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. **See also** [virus definition](#). It is important to update this list regularly.

