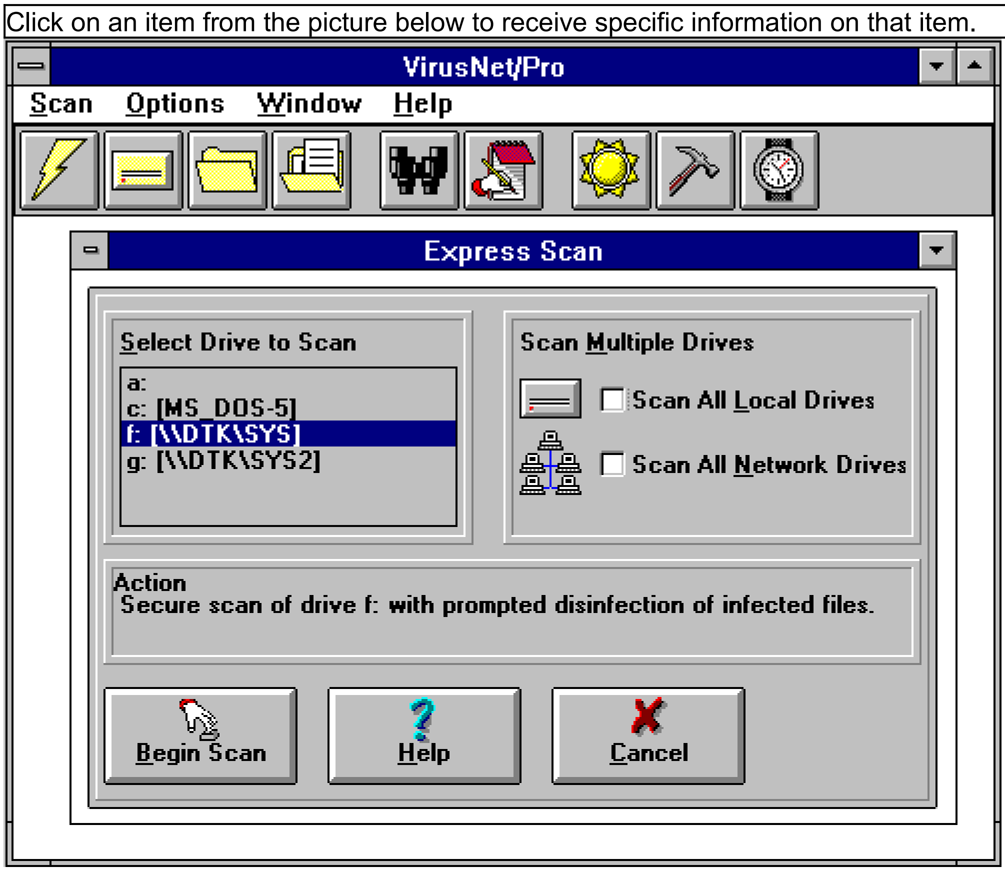
Click on an item from the picture below to receive specific information on that item.



Action
Secure scan of drive f: with prompted disinfection of infected files.

Steps to Cure A Virus Infection
Steps to Implement Virus Monitoring

VirusNet Task Scheduler

The Task Scheduler is part of the LAN Scheduler & Distrubution (LANSD) program. The Task Scheduler runs events at specific times or intervals. Events can include programs, batch files and messages. Tasks can be run from Windows, during network login, or during workstation bootup. If LANSD is installed, a scheduler icon will be displayed on the icon bar, and a Scheduler menu choice will appear on the Options menu.

There are three LANSD programs which have Scheduling abilities:

SCHEDWIN.EXE - Windows-based scheduler which manages private workstation schedules and performs scheduled DOS and Windows events. It is run in the background during Windows startup or from an icon in the Program Manager. SCHEDWIN is also used to manage Network Schedules from the LANSD Windows Network Console.

LANAGENT.EXE - LANAGENT will run scheduled events from a batch file or network login script. Its other duties include managing software distribution and the workstation virus monitor.

SCHEDDOS.EXE - DOS-based scheduler which manages private workstation schedules and performs scheduled events, either in a batch file such as AUTOEXEC.BAT or through its full screen interface. When run in a batch file to perform events, the /RUN command-line switch must be used (SCHEDDOS /RUN). SCHEDDOS is also used to manage Network Schedules from the LANSD DOS Network Console.

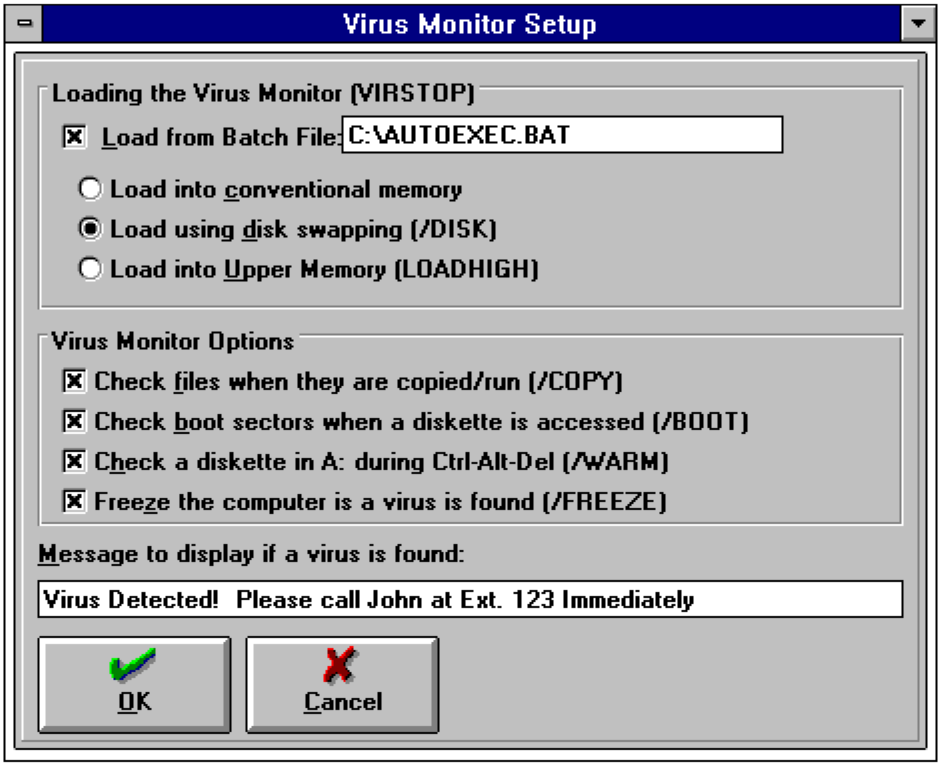
More detailed help for the Windows Task Scheduler is located in a separate help file.

VirusNet Virus Monitor Setup

See Also:

Steps to Implement Workstation Virus Monitoring

The **Virus Monitor** button is displayed on the Scan Options window. This option provides workstation configuration of the virus monitor. When the VirusNet program is exited, and the Save Changes box is checked, the settings in this window will be implemented.



Virus Monitor Setup

Loading the Virus Monitor (VIRSTOP)

☒ Load from Batch File: C:\AUTOEXEC.BAT

○ Load into conventional memory

● Load using disk swapping (/DISK)

○ Load into Upper Memory (LOADHIGH)

Virus Monitor Options

☒ Check files when they are copied/run (/COPY)

☒ Check boot sectors when a diskette is accessed (/BOOT)

☒ Check a diskette in A: during Ctrl-Alt-Del (/WARM)

☒ Freeze the computer is a virus is found (/FREEZE)

Message to display if a virus is found:

Virus Detected! Please call John at Ext. 123 Immediately

Load from Batch File - Place an X in this box if you want VirusNet to automatically maintain the batch file where the workstation virus monitor will be run.

If the above choice is selected, the following options will be available.

After the Load from Batch File prompt, a text field is displayed. Type in the full path of the batch file where the Virus Monitor command will be inserted. For example, **C:\AUTOEXEC.BAT** will insert the Virus Monitor command into the workstations AUTOEXEC file. This will automatically run the Virus Monitor when the workstation is booted. If the batch file does not exist, it will be created automatically.

Load into conventional memory - Loads the Virus Monitor into low DOS memory.

Load using disk swapping - Loads the Virus Monitor using its /DISK option. This requires no upper memory, but will reduce conventional memory overhead significantly.

Load into upper memory - On DOS 5.0 and higher systems, the LH command is used to load the Virus Monitor into upper memory. For systems with older versions of DOS, the Virus Monitor will be loaded into conventional memory.

Virus Monitor Options

The Virus Monitor is configured by placing an X in front the appropriate options. These options are passed to the Virus Monitor as command-line parameters. They are automatically implemented when the Virus Monitor is loaded by the workstation from the batch file defined above. The following options are available:

Check files when they are copied/run - The /COPY command-line switch is implemented. As program files are run or copied, they will be checked on-the-fly for viruses. If this feature is not selected, program files will still be checked for viruses before they are run. They will not be checked, however, when they are copied.

Check boot sectors when a diskette is accessed - The /BOOT command-line switch is implemented. When a diskette is first accessed, it will be automatically scanned for boot track viruses.

Check a diskette in A: during Ctrl-Alt-Del - The /WARM command-line switch is implemented. This protects against getting a boot track virus from a diskette left in the A: drive during a warm reboot.

Freeze the computer if a virus is found - The /FREEZE command-line switch is implemented. If a virus is detected by one of the above checks, the computer will immediately be locked, preventing further harm to the system.

Message to display if a virus is found - This message will be displayed to the user if a virus is detected. It can contain a Virus Help Desk contact. For example, **Virus Detected! Please Call John at Ext. 324.**

VirusNet Steps to Implement Virus Monitoring

To implement workstation virus monitoring, follow these steps:

1. Select the **VirusNet / Monitor** button.

2. Define the desired options on the Virus Monitor Setup window.

3. Select the **OK** button.

4. When you exit the VirusNet program, select the Save Changes check box. The VIRSTOP command will be placed in the batch file defined in the Virus Monitor setup window.

Express Scan is the fastest way to scan for viruses. Just select the Begin Scan button and the scanner will begin scanning the drive highlighted in the Select Drive to Scan window.

To remove the Express Scan window, click on the Cancel button.

If a Secure or Heuristic scan is performed, the Scan Results window will be displayed in the Scanner Summary window..

Once you have selected where you wish to scan, press the Begin Scan button to start the scanning process. VirusNet will use the options set in the Options|Set Options window. If an item is not selected, the Begin Scan button will not be available.

Select this button to receive help on the options available in the Express Scan window. If you are not on the Express Scan window, you can receive help from anywhere in the program by pressing the F1 key.

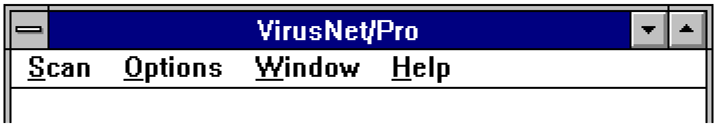
To scan all Local and/or All Network Drives, select the appropriate choice in the Scan Multiple Drives window. A description of the action the scanner will take is displayed in the Action window. The scanner will use any options which have been set under the Options|Set Options menu choice.

Select one or more drives to scan. To select a drive, click on it with the mouse or press ***<Alt>*S** and then highlight it with the arrow keys. To select more than one drive, hold the ***<Ctrl>*** key down and click on the drive letter. To select several consecutive drives, hold the ***<Shift>*** key and use the mouse or arrow keys to highlight the desired drives.

Select this button to remove the Express Scan window from the screen. Alternately, you can click with the mouse on the menus at the top of the screen.

The Action Window shows the type of scan (Heuristic, Secure, or Checksum) and drives that will be scanned.

VirusNet Menu Bar



Click on an item from the picture above to receive specific information on that item.

The Menu Bar allows you to gain more control over the scanner through various pull-down menu choices. The Scan Menu allows you to select the file, directory or drive you wish to scan, as well as access the Express Scan menu.   The Options Menu allows you to customize scanner options, view the Virus Information database and access the Notepad Editor.

For help with the menu choices, select one of the previous topics by highlighting it with the Tab key or clicking on it with the mouse.

VirusNet Notepad Editor

The Notepad Editor allows you to view, edit, save, append and print log reports and virus information. It is also used to build the CRC Exclude files list. Once the scanner has completed a Secure or Heuristic scan, choose the Details button from the Scanner Results window. The Notepad will display the full results of the scan.

The Notepad can also edit small text files less than 32K in size such as AUTOEXEC.BAT and CONFIG.SYS. Select the Options Menu and then select Notepad Editor from the menu.

Since the Notepad operates almost identically to the notepad provided with Windows, please refer to the Windows Notepad Help for further information on using its basic features.

VirusNet Steps to Cure a Virus Infection

Step by Step

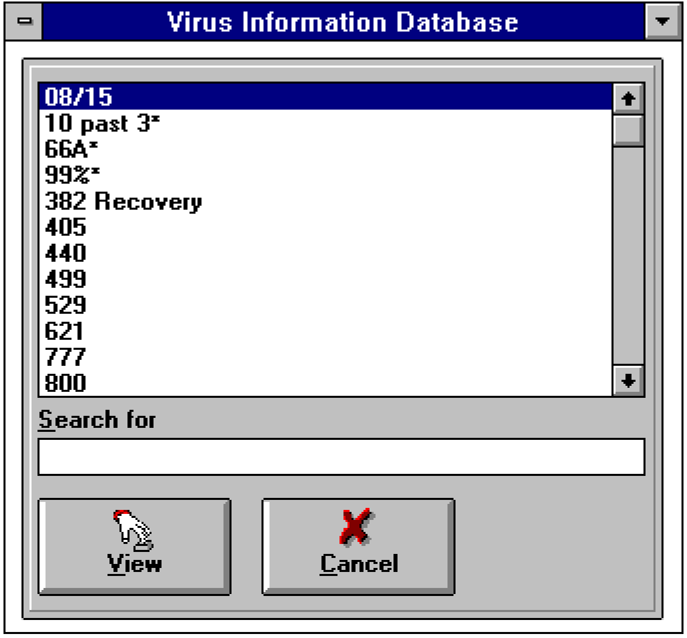
To cure a virus infection, follow these steps:

1. If you are currently working in a program, save your work, and exit the program.
2. Turn off the computer for at least 10 seconds.
3. Find your original bootable DOS disk and make sure it is write protected.

    Write-Protecting Disks
    5¼" disks : Put a write protect label over the notch on the right side of the disk.
    3½" disks : The notch on the right side of the disk must be open for the disk to be write protected.
4. Insert the write-protected DOS disk into the A: drive and turn the computer on.
5. After the computer has booted, insert a write-protected copy of VirusNet into drive A: (You may use drive B: if you wish, just substitute B: for A: in the examples below.)
6. To find and remove viruses, run VN /HARD /DISINF from the DOS prompt.
7. If VirusNet has been installed on the hard disk, you may run VNDOS.EXE to start the scanner. However, if a virus is already in memory, the scanner will become infected when it is run, possibly preventing it from running properly. For this reason, it is recommended to run the scanner from a write-protected floppy disk.
8. VirusNet will scan all programs on the hard drive for viruses and any viruses found will be automatically removed. Infected program files which cannot be recovered will be deleted. When scanning is complete, you can view the report of its virus scan findings.
9. If a virus is found when VirusNet does its memory check, your bootable DOS disk is also infected. Find another write-protected bootable DOS disk, insert it into drive A:, and reboot the computer. Follow from Step 4 above until no virus is found by the memory virus check.
10. Skip to Step 13 if you do not have any floppy disks which you suspect are infected by a virus. If you do have disks that may be infected, insert one of them into drive B: and select the letter of your floppy drive to scan.
11. After each disk is scanned, another disk may be inserted into the floppy drive and scanned.
12. When scanning is finished, remove all disks from the floppy drives and reboot your computer.
13. After the computer has booted from the hard disk, insert the write-protected VirusNet disk into the floppy drive and run VN /HARD from the floppy disk.
14. If you receive a message that memory is infected, repeat the virus removal procedure from Step 2. When the scanner does not report a virus in Step 13, your virus problem has been corrected and you may safely use your computer.

VirusNet Virus Information

Click on an item from the picture below to receive specific information on that item.



08/15
10 past 3*
66A*
99%*
382 Recovery
405
440
499
529
621
777
800

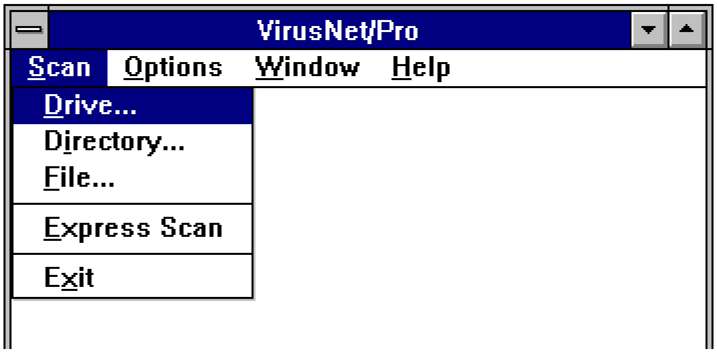
The Virus Information window is accessed from the Options | Virus Information menu. It contains information about many viruses, **but is not a complete list of all of the viruses that VirusNet can detect**. Use the arrow keys to scroll through the list, or type the first few letters of a virus name. By double clicking with the mouse on a virus name (or pressing *Enter* or typing the complete virus name or selecting the View button), a thorough description of the virus, its infection types, aliases, and whether VirusNet can remove the virus will be displayed.

This is a scrollable list of viruses that are described in the database. Names with an asterisk next to them are the original names for the virus. Other names in the list may be aliases or slight modifications of the original virus. To receive information about a virus, double click on its name, select the View button, or highlight the name and press the *Enter* key.

The Search For field allows you to type in the first few characters of the name of the virus you are looking for. The highlight bar will move through the list matching the letters that you typed. When the desired virus name is highlighted, press *Enter* to receive information about that virus. Letters will not be allowed that do not match the name of one of the viruses. If you type the entire name of a virus, its information will be displayed.

Selecting the View button displays information about the virus that is highlighted in the virus list.

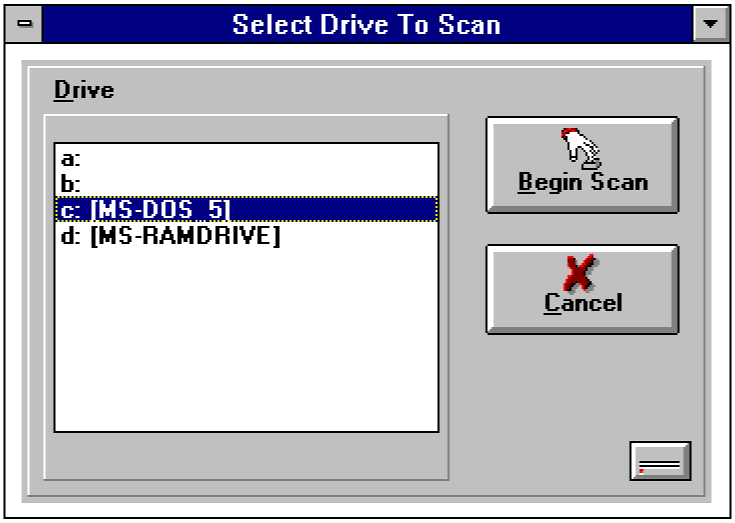
VirusNet Scan Menu



Click on an item from the picture above to receive specific information on that item.

The Scan Menu allows you to select a Drive, Directory, or File that you wish to scan.   This menu also has the Exit option, which allows you to end your VirusNet session.

VirusNet Scan Drive

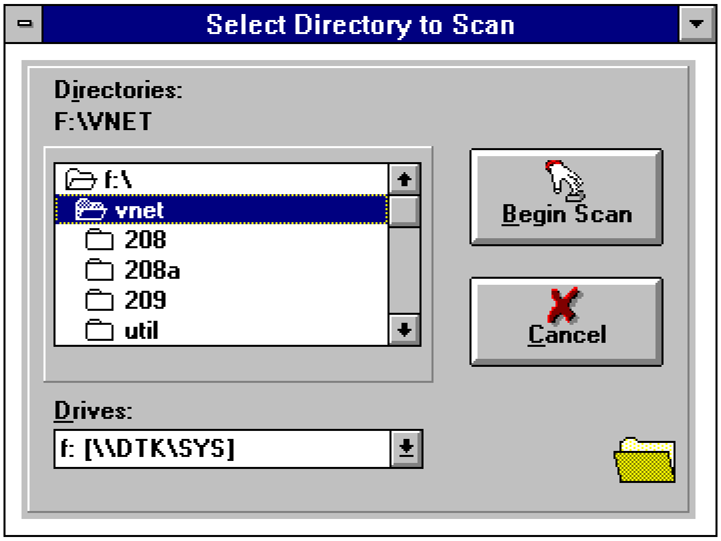


Click on an item from the picture above to receive specific information on that item.

The Drive Window allows you to select one or more drives to scan. The letter of the drive is displayed first. If the drive is a local, the volume of the drive will be displayed in square brackets. If the drive is on a network, the file server and volume name of the drive will be displayed.

Step by Step

Scan Directory



Directories:
F:\VNET

Drives:
f: [\\DTK\SYS]

Click on an item from the picture above to receive specific information on that item.

Select the drive you wish to work with by clicking on the ⬇ which is to the right of the drive box. Then select the appropriate drive. For keyboard users, press the ***<Alt>D*** to move the cursor to the drive box. Then press the letter of the drive you wish to access.

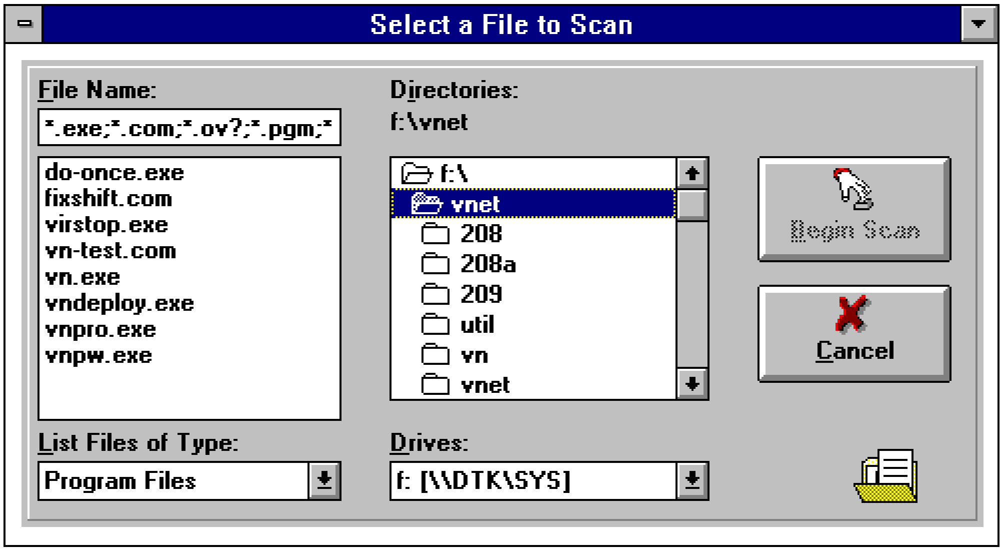
Select the directory on the indicated drive by using the mouse or arrow keys. To move among the directories, double click on the directory you wish to open, or highlight it with the arrow keys and press *Enter*.

The file type allows you to filter out the files in a directory by certain extensions. Select the type of file you wish to work with by clicking on the ▼ which is to the right of the type box. Then select the appropriate choice. For keyboard users, press the ***<Alt>L*** to move the cursor to the type box. Then use the up/down arrow keys to select the type that you wish.

Type in the name of a file you wish to select.   You may type in standard DOS wildcards to extend your search to certain patterns.

Select an appropriate file by double clicking on it with the mouse or highlighting it with the up/down arrow keys and pressing *Enter*.

VirusNet Scan File



File Name: *.exe;*.com;*.ov?;*.pgm;*

do-once.exe
fixshift.com
virstop.exe
vn-test.com
vn.exe
vndeploy.exe
vnpro.exe
vnpw.exe

Directories: f:\vnet

f:\
vnet
208
208a
209
util
vn
vnet

List Files of Type: Program Files

Drives: f: [\\DTK\SYS]

Click on an item from the picture above to receive specific information on that item.

VirusNet Exit Scanner

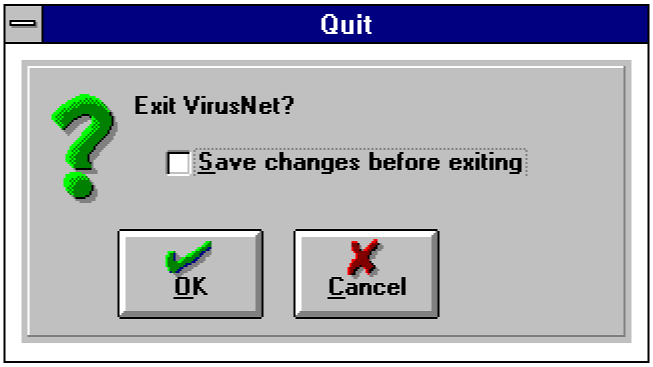
Select this choice to exit VirusNet.   You can also double click on the ⊟ button which is located at the top left corner of the VirusNet title bar.   If you have made any scanner options changes, the Quit window will be displayed, where you will have the option of saving those changes.

The Cancel Button stops the current action and in most cases, will remove the pop-up window from the screen.

On the CRC scanning screen, the Cancel Button will stop the current scan. The button will then display Exit. By pressing this button again, the CRC screen will be removed.

The icon in the bottom corner of several windows is a visual aid used to identify the action performed by the window. The icon will also be used to identify the window when it is miminized.

VirusNet Quit Window



Exit VirusNet?

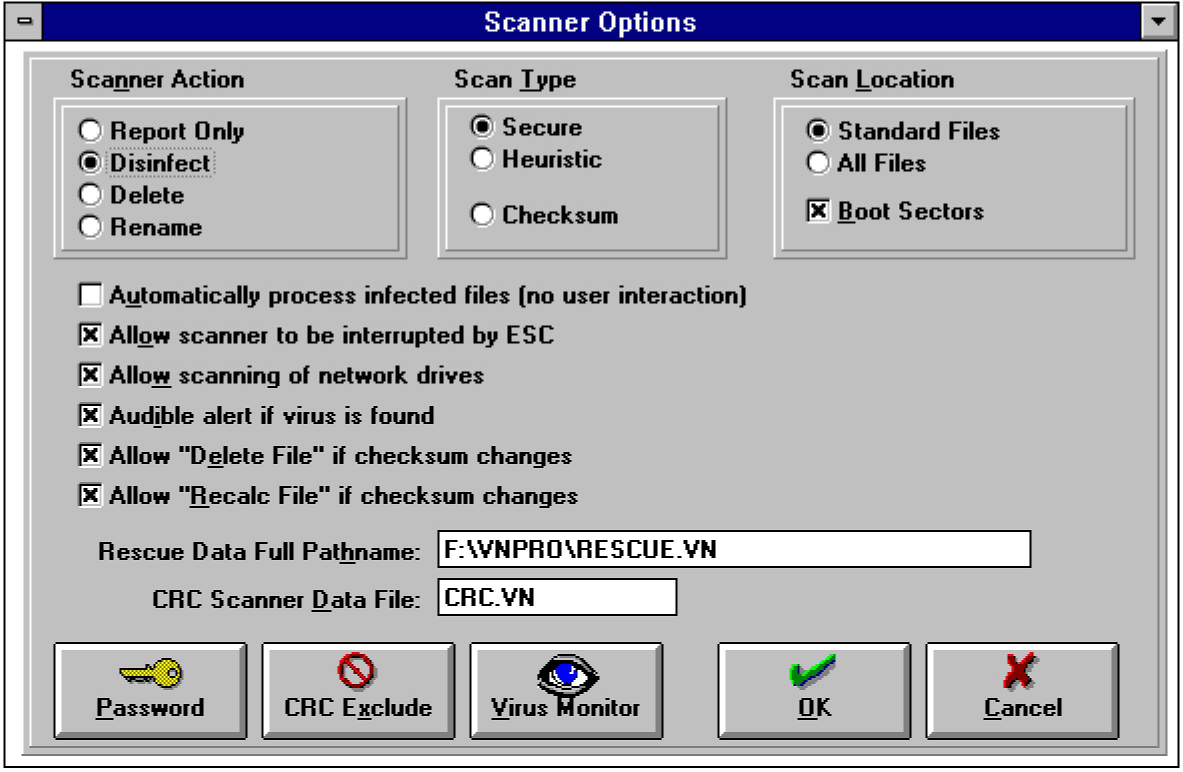
□ Save changes before exiting

Click on an item from the picture above to receive specific information on that item.

The Quit Window is displayed when you exit VirusNet without saving changes to the Scanner Options. Select the Save changes before exiting choice to save any scanner options changes. If this item is selected, an ✖ will be displayed in the square to the left of the save changes prompt. Click on the OK button to exit VirusNet, and optionally save any changes that were made.

If you do not wish to exit, click on the Cancel Button.

Click on an item from the picture below to receive specific information on that item.



Scanner Action

○ Report Only
● Disinfect
○ Delete
○ Rename

Scan Type

● Secure
○ Heuristic
○ Checksum

Scan Location

● Standard Files
○ All Files
☒ Boot Sectors

□ Automatically process infected files (no user interaction)
☒ Allow scanner to be interrupted by ESC
☒ Allow scanning of network drives
☒ Audible alert if virus is found
☒ Allow "Delete File" if checksum changes
☒ Allow "Recalc File" if checksum changes

Rescue Data Full Pathname: F:\VNPRO\RESCUE.VN

CRC Scanner Data File: CRC.VN

The Scanner Options window allows you to customize many aspects of VirusNet. From this menu, you can adjust the type of scan, action taken if a virus is found, and various user controls. This window can be password protected to prevent unauthorized modification of its contents.

The Scanner Action window allows you to adjust the actions of the Secure Scan. Each of the possible choices is described below.

Report Only - This instructs the scanner to only produce a report of the scanning results. If a virus infection is found, the infected file/boot track will be displayed in the report. However, no action will be taken on the infected file. This is the only option available during Heuristic and Checksum scanning.

Disinfect - If a virus infection is found, this options tells the Secure Scanner to try to remove the virus. The virus will be removed if possible. Some viruses cannot be removed since they destroy a part of the file. If the virus cannot be removed, the file will be overwritten and deleted. Boot track viruses usually can be removed by restoring the infected area.

Delete - Instructs the scanner to overwrite any infected files and then deletes them. This option does not affect boot track viruses. If you suspect that you have a boot track virus, select the Disinfect option described above.

Rename - The scanner will rename all infected EXE files to VXE and all infected COM files to VOM. As in the Delete option above, boot track viruses are not affected by this action. Choose the Disinfect option if you have a boot track virus.

The Scan Type window allows you to choose the way VirusNet looks for viruses.

Secure - Secure scan detects known viruses and many variants through a combination of signatures and algorithms. It is capable of detecting stealth and polymorphic viruses. If you have a virus infection, Secure scan is the only option which allows you to remove infected files. This is the option you should use most of the time. If you suspect that you have a virus that secure scan does not detect, try the Heuristic or Checksum options described below.

Heuristic - Through powerful rules-based-algorithms, Heuristic scanning can detect known and unknown viruses based on characteristics. Heuristic scanning first checks for viruses with the Secure scan algorithm described above. If a file or boot track does not appear to be infected, a heuristic analysis is performed to see if there is anything virus-like or dangerous about the file/boot track.

Checksum - Checksum scanning looks for changes in programs. The first time a program is scanned, a CRC (cyclical redundancy check) signature is created of that file. On subsequent scans, if the file has changed, the checksum scanner will notify of the change. Checksum scanning is a powerful tool in detecting unknown viruses. However, a file that changes does not always indicate that there is a virus. Some files modify themselves with configuration information. If a checksum scan detects a changed file, it is recommended that you run the Heuristic or Secure scan to determine if the file is infected.

The Scan Location window allows you to select the type of files that the Secure or Heuristic scanner looks for. You can choose between Standard and All files.

Standard files are any files that contain code that the computer runs. Examples include files that have extensions of EXE, COM, OVL, SYS, CMD and BIN.

All files should only be selected if a virus infection has already been detected. With this option selected, all program and data files will be scanned. This option can lengthen the time of the scan considerably and is not recommended for normal use.

Boot Sectors allows you to determine if the scanner looks at the DOS and Master Boot Sectors as part of its scan. This option should normally be selected, since many of the most common viruses are boot sector viruses. If the scanner does not read your boot sectors properly, you can disable this option. Boot sectors may not be read properly if you are running a security software or DOS emulation under another operating system.

Automatically process infected files affects the Secure Scan option. If a virus is detected, this option determines whether the scanner prompts the user if the Scan Action should be performed. If this option is selected, the virus will automatically be dealt with as set in the Scan Action window. To be prompted before the scanner performs an action on a virus, leave this option blank.

Allow scanner to be interrupted by ESC should be selected if you want the option of pressing the *ESC* key to stop the scanner. This option has no effect on the Checksum Scanner, which can be stopped at any time.

Allow scanning of network drives determines whether any network drive letters are displayed in the drive boxes. To prevent a user from scanning network drives, leave this option blank.

Audible alert if virus is found will send an alert tone through your PC speaker if a virus has been detected by the Secure or Heuristic Scan.

Allow Delete File if checksum changes enables you to display or hide the Delete button in the checksum scanner. Since files that become modified do not positively identify a virus infection, the Delete feature should only be used by reasonably technical users who are very familiar with their programs.

Allow Recalc File if checksum changes enables you to display or hide the Recalc button in the checksum scanner. Recalculating a file tells the checksum scanner to recompute a new image of the file and store it for future reference. If the file were actually infected with a virus, the new checksum would include the virus in its calculation. The Recalc feature should only be used by experienced users who are familiar with their programs.

Rescue Data Full Pathname allows you to save information used to recover a PC on a floppy disk, network drive, or hard drive. Type in the location and file name you wish to use to store the Rescue Disk information. For example, type A:\RESCUE.VN to store rescue information to the root directory of a floppy drive. Or type G:\\VNPRO\RESCUE.VN to store the rescue information for all workstations centrally on the network.

Do not store the rescue file permanently on a hard disk, since the file will not be accessible if the hard drive becomes corrupted.

CRC Scanner Data File is the name of the file where Checksum Scanner information is stored. Each drive has a file of this name stored in its root directory. Since viruses have been known to delete checksum files that use a fixed name, you may wish to use a different name than the one that is supplied with VirusNet.

Click on the Password Button to assign, change or delete the administrators password. If you need to lock in certain scanner options, it is a good idea to password protect access to the Scanner Options screen.

Certain files may change frequently since configuration information is written to them.   To have the Checksum Scanner skip these files, select this button.   You will then be brought into the CRC Exclude Files Editor, where you can type a list of filenames that shoud be skipped from checksum scanning.

The Save Button saves any changes you have made.   Each time VirusNet is run, it will use the settings on the Scanner Options screen.

The Accept Button allows you to temporarily use the settings specified on the Scanner Options screen. When the program is exited, any changes will be lost. The Accept Button can be used by the Network Administrator to override any stored settings without modifying the configuration file shared by any other users.

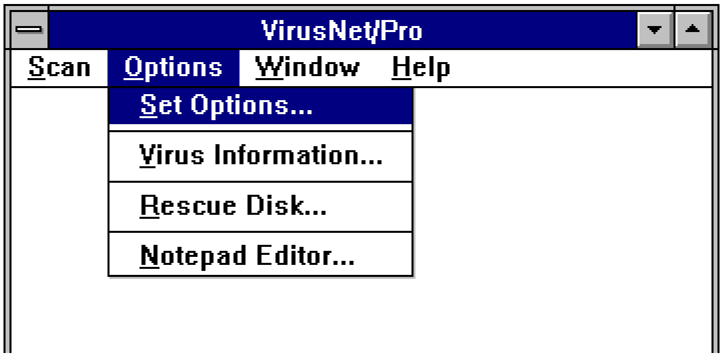
▼ should be clicked on if you wish to minimize a window. This symbol is located in the upper-right corner of many windows. To reactivate a window once it has been minimized, double click on its icon.

▲ should be selected if you wish to maximize the size of a window. Not all windows have this option available.

⊟ should be double clicked on to close a window. This is the same as selecting the Cancel Button.

There are many more features for manipulating windows besides these. Please refer to your Microsoft Windows documentation and on-line help for more information.

VirusNet Options Menu



Click on an item from the picture above to receive specific information on that item.

The Options Menu provides access to the Scanner Options window, Virus Information database, Rescue Disk and Notepad Editor.

The Window choice allows you to arrange your VirusNet desktop so that windows and icons are easy to see. The Tile command arranges the open windows side by side. The Cascade command layers open windows so that each title bar is visible.

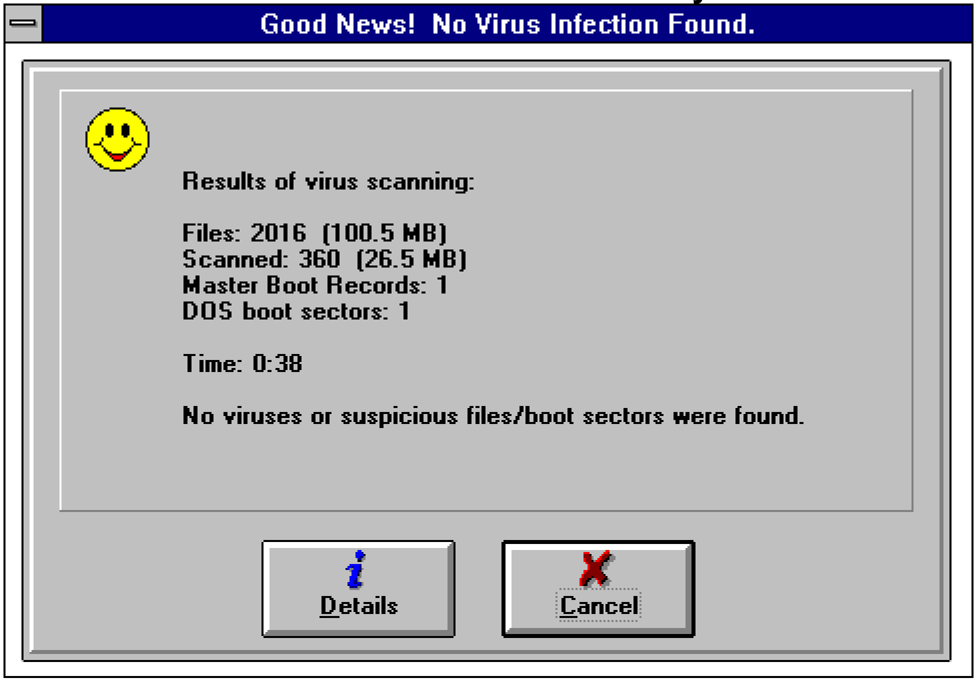
To arrange windows, from the Window menu, choose Cascade or Tile.

Use the Arrange command to evenly arrange any minimized windows which are represented as icons.

The Help Menu allows you to access the general Contents section of VirusNet help.   From there, you can navigate to more specific help information.   Also on this menu is the About selection, which contains information about this version of VirusNet, copyright information, and information about your software licence.

The OK button procedes with the action described in the window.

VirusNet Scan Results Summary



Good News! No Virus Infection Found.

Results of virus scanning:

Files: 2016 (100.5 MB)
Scanned: 360 (26.5 MB)
Master Boot Records: 1
DOS boot sectors: 1

Time: 0:38

No viruses or suspicious files/boot sectors were found.

Click on an item from the picture above to receive specific information on that item.

After a Secure or Heuristic scan is finished, the Scan Results Summary window will be displayed.   This window displays an an overview of the scanner results.

The results of the scan are displayed in this window. Included in the summary are the total number of files in the directories scanned, the actual number of files scanned, the number of Master and DOS boot records scanned, and the amount of time required for the scan. The last line tells you if a virus or suspicious code has been detected. If a virus is found, the summary window will also display the number of viruses detected, removed, deleted and renamed.

Select the Details button to view the complete virus report in the Notepad Editor.   In addition to the summary information, the full report will list any infected or suspicious files or boot tracks.

VirusNet Password Restricted Area

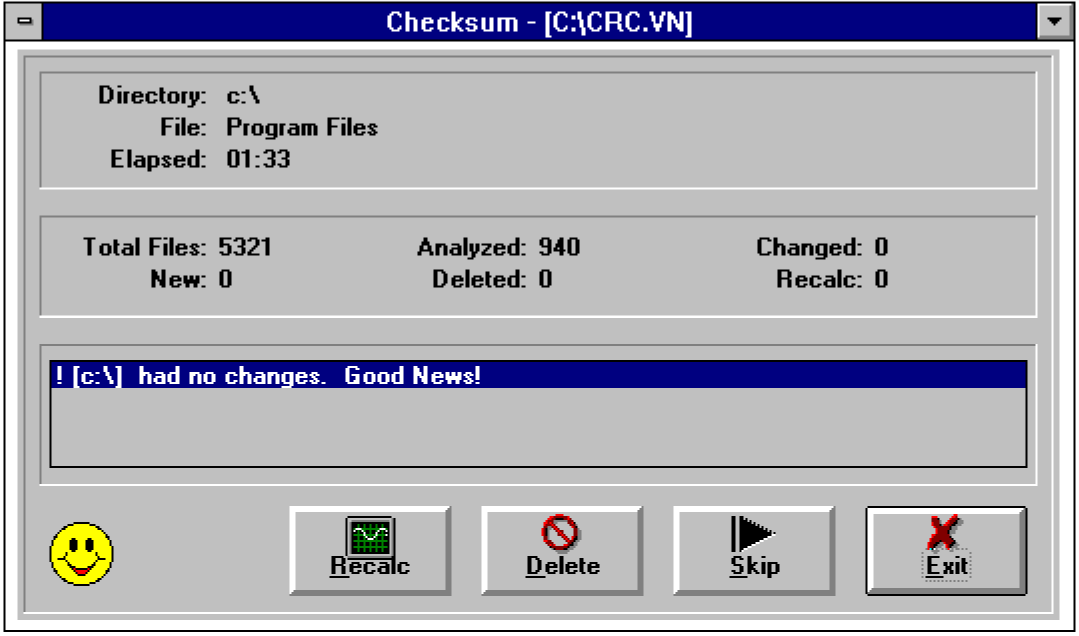
A password may be required to access certain features.   Type in the correct password and press *Enter*. If you do not know the password and need access to a certain area, contact your administrator.

VirusNet Password Protection

The Scanner Options screen can be protected by an administrator password. This will prevent unauthorized changes to certain scanner settings. Type in a password and press *Enter*. You will then be prompted to type it in a second time for verification. Press *Enter* or select the OK button when you have assigned the new password. To remove a password, click on the Delete button.

VirusNet Checksum Scanner

Click on an item from the picture below to receive specific information on that item.



Directory: c:\
File: Program Files
Elapsed: 01:33

Total Files: 5321
New: 0
Analyzed: 940
Deleted: 0
Changed: 0
Recalc: 0

! [c:\] had no changes. Good News!

The Checksum Scanner is a powerful tool for detecting unknown viruses. The first time a file is scanned, a digital signature of the file is is created. On subsequent scans, if the file has changed, the signature will be different and the scanner will notify you of the change. If a file has changed, it does not necessarily indicate that there is a virus. Some programs write configuration information to themselves, causing a change in their signature. However, if a file has been unchanged for some time, and then it changes, there may be reason for suspicion.

The Checksum Delete button will delete a file that has been modified since the last checksum scan. It should only be used if you are sure that the file has been infected. You may wish to scan using Secure or Heuristic options to positively identify that the file is infected. This option can be removed by changing the configuration in the Scanner Options window.

The Checksum Skip button allows you to continue the scanning process and take no action on the currently modified file.   Use this option if you are not sure if the file modification is the result of a virus infection.   You can then run the scanner using the Secure or Heuristic options to determine if the modified file is actually infected.

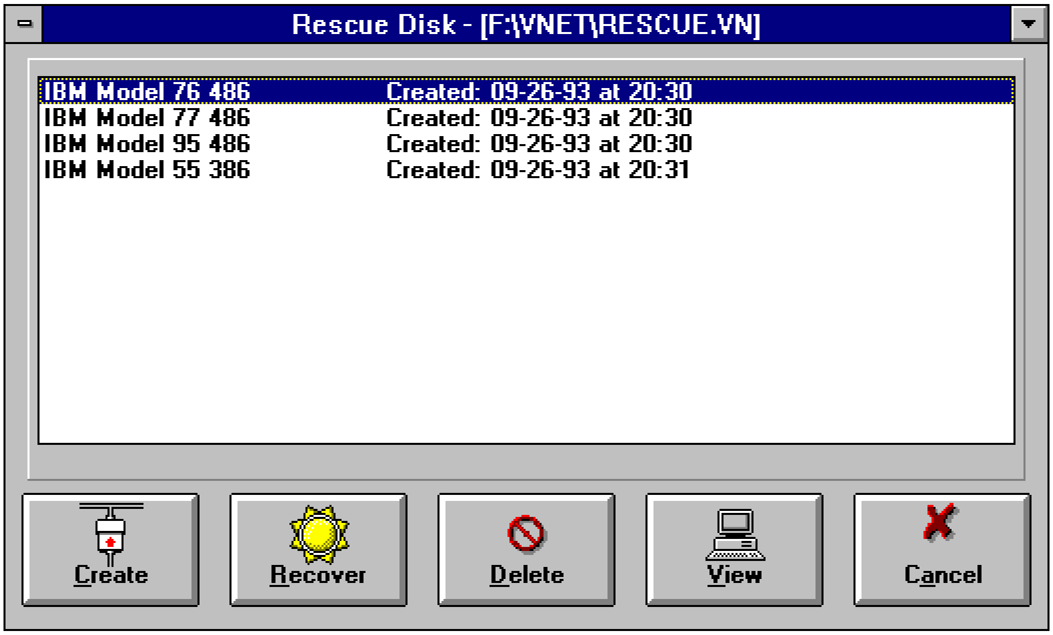
The Checksum Statistics window displays statistics generated by the checksum scanner. Included among the statistics are total files, total files scanned, and number of changed, deleted, and recalculated files. The elapsed time of the scan is also displayed.

The Checksum Status window displays the findings of the Checksum Scanner. If the list of messages is larger than the window size, you can scroll through the messages with the arrow keys or mouse. When a file that has changed is highlighted, option buttons will be displayed allowing you to recalculate a new signature for the file, delete the file, or skip the file and continue scanning. Depending on the settings of the Scanner Options, some of these options may not be available to you.

The Checksum Recalc button recalculates the digital signature or fingerprint of a file and stores the new signature in its database. A file should be recalculated when you know the change to a file is not the result of a virus infection. Situations where this could apply include files that write configuration information to themselves and updated versions of program files. If a file has changed and there is no apparent reason for the change, you should run the scanner in Secure or Heuristic mode to see if there is an actual virus infection. This option can be removed by changing the configuration in the Scanner Options window.

The Scanner Results icon gives you a quick visual indication of the results of your scan. A smiling icon indicates that no viruses or file changes have been detected. A blue face with a straight mouth indicates that a suspicious file or file change has been detected. This does not mean that there is a virus, but that the situation should be more closely examined. A red face with a round mouth indicates that a virus infection was found. Please review the scanner results carefully since important information about the status of your system will be presented.

VirusNet Rescue Disk



Rescue Disk - [F:\VNET\RESCUE.VN]

```
IBM Model 76 486          Created: 09-26-93 at 20:30
IBM Model 77 486          Created: 09-26-93 at 20:30
IBM Model 95 486          Created: 09-26-93 at 20:30
IBM Model 55 386          Created: 09-26-93 at 20:31
```

Click on an item from the picture above to receive specific information on that item.

The Rescue Disk stores vital parts of a PCs hard disk and CMOS.   This information can be used to regain access to a PC that fails to bootup properly.   Reasons that a PC mail fail to boot include a virus, dead CMOS battery and corrupted boot track and partition table.

The Rescue Disk file can store information for many PCs in a central database, making it ideal for storing critical information for all PCs in a department.   Once the file has been created, it should be kept in a safe place, preferably on a write-protected diskette.   The rescue file can also be stored to a network drive.   If it is stored on a LAN and a workstation fails to boot, the rescue file will have to be copied to a floppy disk and accessed from that PCs floppy drive, or the PC must be logged into the network by loading the necessary files from diskette.   The location and name of the Rescue Disk file can be set in the Scanner Options section described earlier in this chapter.

Select the Create Button to create and save rescue information for a PC. You will then be asked to provide a description of up to 30 characters to uniquely identify the PC. After you provide a unique identifier for the PC, the Master Boot Track, DOS Boot Track and CMOS will be saved. To help in identification of the computer for future recovery, the PC CPU type and BIOS date, along with current date and time, will also be saved.

Select this feature to restore the highlighted PCs rescue information to the PC you are working on. This option should only be used if the PC cannot be booted or accessed because of a disk or CMOS battery failure. Before selecting Recover, make sure that the correct PC is highlighted from the list. When Recover is selected, the saved information for the currently highlighted PC will be used. To add a margin of safety to the recovery process, the CPU type and BIOS date of the original PC is compared to that of the current PC. If they do not match, you will receive strong warning messages indicating that the recovery information selected may not be for this computer.

The only time you should ignore this warning message is if you have upgraded the CPU or BIOS since the recovery information was first saved. Do not proceed if you are not certain that the saved information is from this computer. Disastrous results can occur if the recovery information is from a different computer.

It is quite interesting to view a PC's CMOS information and boot records. Highlight a PC and select this button, or simply press <Enter> when the cursor is on a highlighted PC.

The list of PCs covered by Rescue Disk protection is displayed in this window. Highlight a row in the list and then select the desired option button. Double-click on an item in the list to view the rescue information for that item.

Select this choice to remove the rescue information for a particular PC.   If this PC fails to boot in the future, you will not be able to use the rescue feature until a new rescue record is created.