

User's Guide

McAfee Safe & Sound for Windows 95/98



2805 Bowers Avenue
Santa Clara, CA 95051

COPYRIGHT

Copyright © 1998 Network Associates, Inc. and its Affiliated Companies. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Network Associates, Inc.

TRADEMARK NOTICES

McAfee and McAfee Software are registered trademarks of Network Associates, Inc. McAfee Safe & Sound™, McAfee Nuts & Bolts™, Discover®, Discover Pro™, McAfee Image™, Bomb Shelter™, PC Checkup™, Retake™, Year 2000 Checker™, Virus Scanner™, Disk Minder™, Rescue Disk™ are trademarks of Network Associates, Inc. Microsoft® Windows® is a registered trademark of Microsoft Corporation. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

FEEDBACK

Network Associates appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. Please address your feedback to: Network Associates, Inc., Documentation, 2805 Bowers Avenue, Santa Clara, CA 95051-0963, send e-mail to documentation@nai.com, or send a fax to Network Associates Documentation at (408) 970-9727.

Table of Contents

Chapter 1. Welcome to Safe & Sound.....	7
Safe & Sound Overview.....	8
Before You Start.....	9
What This Package Contains.....	9
What You Need Before Starting.....	9
Getting Started.....	11
Safe & Sound Quick Install	11
Safe & Sound Quick Start.....	12
Getting Help.....	12
Chapter 2. PC Checkup.....	13
Performing a Standard Diagnosis and Repair	14
Chapter 3. Retake	17
Protected Volume Files (The Ultimate Backup Protection)	17
Why You Should Make Regular Backups With Retake	18
How Retake Creates Automatic Backups	19
Defining Your Backup Strategy	20
Where Will You Store the Backup Set?	20
What Files are Important to You?	21
How Often Should You or Retake Make Backups?	21
Creating a Backup Set.....	22
Restoring Files from a Backup Set	27
Modifying or Deleting Backup Sets.....	28
Modifying an Existing Backup Set.....	28
Deleting a Backup Set	28

Repairing and Rebuilding a Backup Set	29
---	----

Chapter 4. Virus Scanner31

What is a Virus?.....	31
How Are Viruses Transmitted?	32
What Types of Viruses Can I Encounter?	33
Boot Sector Viruses.....	33
File Viruses.....	33
Macro Viruses.....	33
Logic Bombs, Trojans, and Worms.....	34
How Can You Combat Viruses?	34
Recovering From a Virus Attack	35

Chapter 5. Tools.....37

Bomb Shelter	38
Starting Bomb Shelter.....	39
Recovering from an Application Error	40
Selecting Bomb Shelter Properties	42
Testing Bomb Shelter	43
Deactivating Bomb Shelter	44
Discover	46
The Discover Window	46
Working With Advanced Information.....	48
Rescue Disk.....	50
Using a Rescue Disk.....	50
Disk Minder in DOS	51
Image/Restore in DOS	52
SysRecover	53
Recover Backup	53
Unformat.....	53
Image	54
Creating an Image of Your Disks	54
Setting Image Properties	55
Restoring Drives From an Image File	55

Year 2000 Checker	58
What is the Year 2000 Problem?	58
Why is the Y2K Issue so Urgent?	58
Why Do We Have Y2K Problems With Our Computers?	59
What are the RTC, BIOS, DOS, and Windows Clocks?	60
How to Ensure Y2K Compliancy of Your PC's Clocks	61
What Dates Does Year 2000 Checker Test and Why?	61
What Other Y2K Problems Must You Resolve?	62

Welcome to Safe & Sound

Thank you for purchasing Safe & Sound, a collection of the finest utilities available for diagnosing, repairing and protecting your PC and its valuable data. With Safe & Sound, you can diagnose and repair your system and application software; create a recovery disk and image snapshots of critical sectors of your hard drives; locate and protect against computer viruses; avoid lost data during application crashes; automatically or interactively create backup sets; back up to a protected volume file which makes your data recoverable when it otherwise would not be; and ensure that your PC meets Year 2000 hardware compliancy. Safe & Sound also places a wealth of information about your PC system at your fingertips with Discover.

From the moment you install Safe & Sound, it begins protecting your PC. First, by guiding you to create a recovery disk that you can use later if problems arise. Second, by activating Bomb Shelter, which immediately protects you against losing unsaved information in the event that an application crashes. Next you'll want to use Retake to create a backup set of your drives' valuable data that you can restore in case any unrecoverable problems arise.

What you're about to learn:

- What utilities are included with Safe & Sound and what you can do with each one.
- What you need before starting.
- How to install Safe & Sound software and create a recovery disk (see Safe & Sound Quick Install).
- How to start the Safe & Sound utilities.

Safe & Sound Overview

Safe & Sound contains these utility programs:

- **PC Checkup** thoroughly analyzes the state of your PC's hardware and software. It can repair many software and configuration problems for you. When PC Checkup finishes its diagnosis, it produces a full report of any problems. You can let PC Checkup fix them, or perform repairs yourself.
- **Retake** lets you create automatic or interactive backups of selected drives, directories, files or file types. You can back up to a protected volume file (a separate area on the drive). A protected volume file contains information about each file in every sector to ensure that files can be recovered even if the hard drive's directories and data are severely damaged or lost. You can also create mirror backups that instantly back up data as you save it, make backups after a time delay when the PC is idle, or create manual backups.
- **Virus Scanner** lets you scan your computer's memory, boot sector and drives for computer viruses at any time.
- **Bomb Shelter** protects various critical parts of your Windows system from being overwritten by other programs. It also acts as a safety net, allowing you to recover from application crashes (and save your work) rather than being forced to restart your computer and lose any unsaved data.
- **Discover** shows a wealth of hardware and software information about your PC. You can run benchmark tests to see how your PC's performance measures up against a comparable computer.
- **Instant Update** connects to the Internet and checks the Network Associates website to see if your copy of Safe & Sound needs updating.
- **Year 2000 Checker** lets you test your system hardware for Year 2000 compliancy. If it is not, Year 2000 Checker installs Y2Kfixer.com to make your PC compliant so it handles dates accurately starting on 01-01-2000.
- **McAfee Image** saves an "image" copy of critical disk information in a file, and restores the image later if your disk is corrupted.
- **Rescue Disk** creates a recovery disk that you can use to boot up the PC and begin recovery if you can't start your PC from the system hard drive.

Before You Start

This section describes what your McAfee Safe & Sound package should contain and prerequisites for using this software.

What This Package Contains

Your Safe & Sound software package should include:

- One Safe & Sound CD-ROM disc

If your PC does not have a CD-ROM drive, you can obtain a set of 3.5-inch disks from our Customer Service department.

- This *McAfee Safe & Sound User's Guide*
- A Registration card


Please fill out and return your Registration card to receive technical support. Also, by returning the Registration card, you'll ensure that you receive new product and product upgrade information.

What You Need Before Starting

To use Safe & Sound, you need:

- Safe & Sound software (on CD-ROM disc)
- A PC with a 386 or above CPU (central processing unit)
- Microsoft Windows 95 or Windows 98
- 8 MB (megabytes) of RAM (random access memory); 16 MB is recommended
- One 3.5-inch disk drive
- 18 MB of available hard drive space

- A CD-ROM drive
- A 16-color VGA monitor that supports 640 x 480 pixels (or better)

 *This guide assumes you know the basics of using Microsoft Windows. You should know how to point, click, double-click and drag. You should also know how to choose commands from menus, select options in dialog boxes, and enter, select and edit text. See your Microsoft Windows User's Guide or online Help for details.*

Getting Started

This section offers Quick Install and Quick Start procedures to help you install and start Safe & Sound. You'll also find information about getting online Help.

Safe & Sound Quick Install

To install Safe & Sound:

1. Insert the Safe & Sound CD into the CD-ROM drive.

The Safe & Sound Installer should autoplay (go to step 3), but if it doesn't go to step 2.

2. Double-click the My Computer icon, the Safsound icon and the Setup.exe or Setup icon.



3. Follow the on-screen instructions to supply the requested information.

Setup requires you to enter information for registering the software.

4. Insert a blank 3.5-inch disk in the drive to use as a recovery disk when the Rescue Disk wizard appears. Then click Next >.
5. Click Finish to restart your computer so Safe & Sound's Bomb Shelter can begin protecting your system.

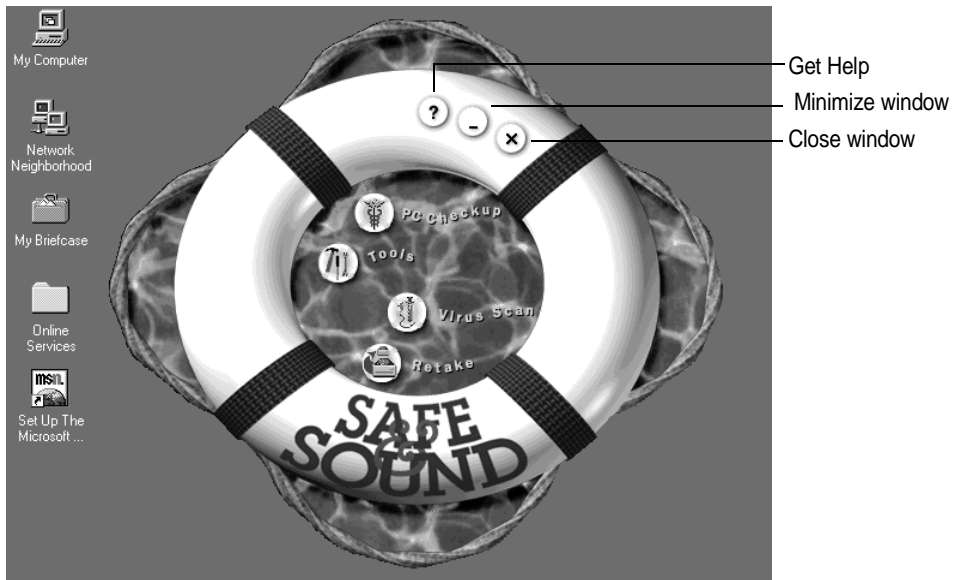
Safe & Sound Quick Start

You can start any Safe & Sound utility from Safe & Sound Central.

To start Safe & Sound:



1. Click the Start button on the taskbar.
2. Choose the Safe & Sound command directly from the Start menu, or from the Start > Programs > Safe & Sound menu.



Getting Help

Safe & Sound provides online Help to give you procedures and detailed information about the windows, dialog boxes and options available in the Safe & Sound utilities. There are two ways to access Safe & Sound's online Help:

- Click the ? button in Safe & Sound Central.
- In PC Checkup, Virus Scanner, Retake, Bomb Shelter, Discover, McAfee Image, Year 2000 Checker, and Rescue Disk, click the Help button.

Over time as you use your computer, the information stored on the hard drives changes. This happens when you save, modify or move documents as well as when you install, update or uninstall application programs. As the information changes, there is a slim chance that critical information, such as the master boot record used to start your PC, can accidentally become damaged.

In a perfect world, all application programs would coexist peacefully, store their data exactly where they should, and always play by the rules. In the real world, this doesn't always happen. The result can be missing files; orphaned shortcuts, fonts or registry entries; inefficient Windows settings; or even corrupted data that can prevent you from starting Windows, or worse yet, from starting your PC at all.

In a perfect world, the electric power coming into your computer would always flow like a clear, placid, spring-fed stream, with no power spikes or surges to inadvertently change the state of a critical bit of data, or worse. In computing, as in the real world, there may be perfect moments or a perfect day at a stream, but a perfect lifetime is exceedingly rare.

If you've encountered a problem with your computer, we understand your frustration. While you're trying to get good work done quickly—who these days has the luxury of doing work at a leisurely pace?—your PC stops in its tracks. Such problems force you to focus on the tool rather than on the work itself.

Our advice? First, remain calm. Second, take a deep breath. Third, read this chapter, which describes Safe & Sound's PC Checkup that can help you diagnose, repair and recover information on your system.

What you're about to learn:

- How to perform a standard or advanced diagnosis
- How to perform automatic or manual repairs

Performing a Standard Diagnosis and Repair


You should start with a standard diagnosis and repair. Then you can perform an advanced diagnosis and repair if necessary. PC Checkup lets you know which repairs you make can be undone later.

To use PC Checkup to diagnose and repair PC problems:

1. Click the Start button and do one of the following:
 - Choose the Safe & Sound command from the Start menu and click the Checkup button.
 - Choose the Programs > Safe & Sound > PC Checkup command.

The PC Checkup Wizard appears.

2. Click Next > to perform a standard diagnosis first.

 *Clicking Advanced lets you perform advanced diagnostics. This option lets you run a more detailed analysis of your PC. You should use this option after performing a standard diagnosis as described in this procedure. Clicking Undo lets you undo repairs made using PC Checkup. For more details about performing an advanced diagnosis and repair, see the Safe & Sound online Help.*

3. Select the items you want analyzed (by default all the options are selected).

When you select some of these options, the Properties button becomes active, indicating that there are options you can select to fine tune the diagnosis of this part of your system. The items you can diagnose are described in the Safe & Sound online Help.

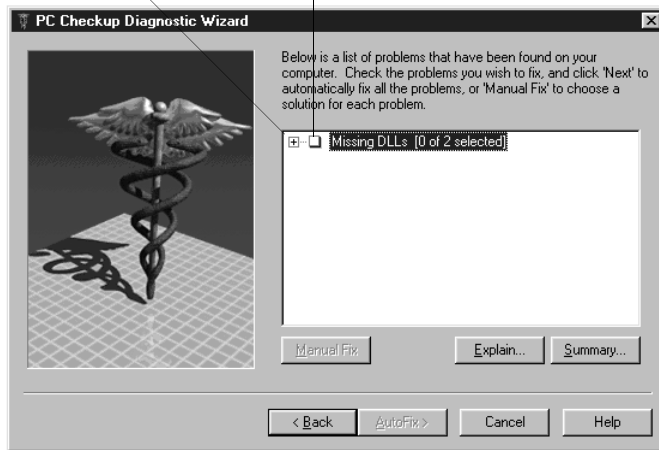
4. Click Next >.

PC Checkup begins diagnosing your PC. You can click Skip to skip any item, or click Stop to halt the diagnosis. Depending on the number of items selected and the speed of your PC, the time it takes to diagnose your PC varies.

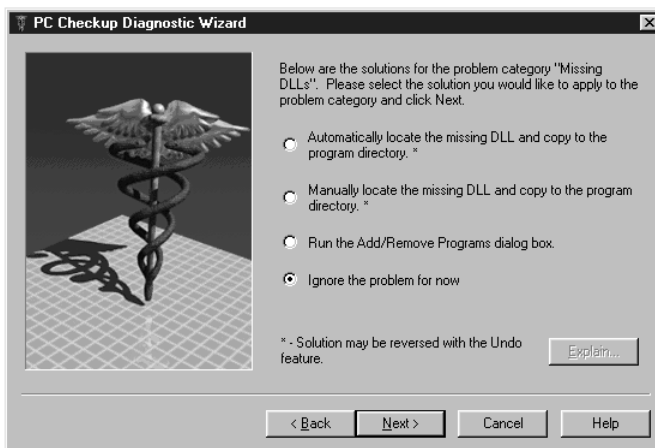
When the diagnosis is complete, PC Checkup makes a Summary list available along with options for repairing any problems it encountered during testing.

Click the + button to view individual problems

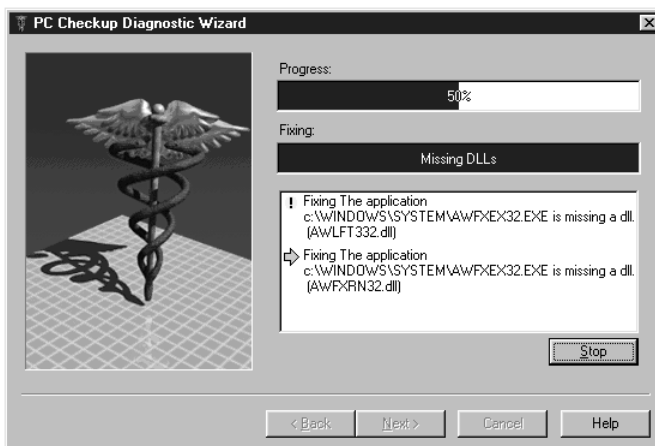
Place a check mark beside items or problems to fix



5. Do any of the following:
- Click the Plus (+) button to view individual problems.
 - Click a check box to select a problem or all problems for an item that you want to fix.
 - Select an item or problem in the list and click Explain to get information about it.
 - Click the Summary button to view or print a list of the problems found on your PC.
 - Click the AutoFix > button to let PC Checkup fix all the problems that it can for you.
 - Click the Manual Fix button to select from a list of solutions for each item. It steps you through each item, giving you an opportunity to automatically fix the problems, manually fix them yourself, ignore them for now, and other solutions appropriate for those problems.



When you do a manual repair, PC Checkup lets you select a solution for each item with problems. After you select one of the solutions, the Explain button becomes active so you can view an explanation of what that solution will do. Once you finish reading the explanation, simply click elsewhere to dismiss the pop-up help message. Also, each solution that can be undone later is marked with an asterisk.



PC Checkup lets you know how the repair is progressing and describes the problem being fixed

You can fix any problems not solved with AutoFix manually. Press < Back, select the problems to fix, and click the Manual Fix button.

The most important asset on your computer is the information, or *data*, you create and store there. Over time, this data grows in size and value. The storage devices where you keep this information, although typically quite reliable, are still vulnerable to a wide range of environmental and human factors that can damage or destroy all or part of the data stored there.

Valuable and vulnerable disk organizational structure information is also stored in various places on a hard drive. This includes the boot sector, partition tables, directories, the FAT (file allocation table), and other structural components. These structural components are used by Windows to find data on the drive, organize it, and so on. If any one of these components is damaged or destroyed, you will not be able to access the data you've stored on the drive.

Let's take a closer look at one of these structural components, the file allocation table. The FAT, your drive's roadmap, points to the locations where your files are physically stored on the drive. Files can either be stored in contiguous locations or scattered in pieces in different places. Since files are not always stored contiguously, the FAT information becomes even more indispensable than if files were stored one after another, end to end. If a drive's file allocation table becomes corrupt or scrambled (such as may be caused by a virus), your computer will be unable to find and assemble all the pieces of your files. This is true even if all the files' data still exists.

Protected Volume Files (The Ultimate Backup Protection)

Safe & Sound's Retake utility allows you to create backup sets in protected volume files, which is the safest and preferred type of backup, and is unique to Safe & Sound. A *protected volume file* is a sectioned off portion of the drive, sometimes called a logical drive. Retake's protected volume files have some very special characteristics that let Retake reconstruct backup files sector by sector, even if the drive's standard FAT is damaged or completely lost. In fact, files can be largely reconstructed even if large parts of the drive are unreadable or erased.

The protected volume file also includes enough information in each directory entry to completely reconstruct a file's entire directory tree even if all its parent nodes are erased.

Retake provides internal redundancy in the protected volume file backups you create. It does this by marking each sector of each file that it backs up with identifying information about the sector's contents and the file that sector belongs to. Each sector in a protected volume file contains enough information to allow files to be reconstructed from their individual sectors.

Why You Should Make Regular Backups With Retake

Your data is very valuable and costly to recreate. This means that making frequent or even mirror backup copies of the important data on your drives is *crucial*. A *mirror* backup copy is always identical to the original information on the source drive.

Retake automates the back-up process, doing the time-consuming and repetitive work for you. It lets you decide which types of files to back up, how often to save them, and where you want the backup set located (on the same drive, another local drive, or on a shared network drive). With Retake, you can create mirror backup sets that are, at any given time, an exact replica of the files you've selected to back up on the source drive. You can also specify a short time delay in the backup, or back up manually by copying files to the backup set on your drive if you prefer.

All forms of data storage are susceptible to losing the information they hold. The most common types of data storage—hard drives, 3.5-inch disks, ZIP disks or SyQuest tapes—are often called *permanent storage* (thus differentiating them from the volatile storage in your computer's RAM, random access memory). Permanent storage means the information remains intact even when you turn off your computer. Permanent storage does not mean *eternal* storage.

Many things can cause the data on disks, tapes or drives to become garbled or lost: hardware malfunctions, worn out media, electrical storms, excessive heat, static electricity, magnets, loose cable or power cord connections, and so on. CD discs, though durable, can become scratched enough to damage their data. Human actions can also cause lost data, such as deleting the wrong folder or formatting the wrong drive. Even a well-designed application can sometimes cause its own files to become corrupt.

With so much at risk, you have everything to gain by letting Safe & Sound's Retake utility automatically make backup copies for you. You simply decide what information is important to you, how you want it to be backed up, and where you want the backup copy to be stored. Retake takes care of the rest!

How Retake Creates Automatic Backups

When you select to have Retake automatically create a backup set for you, it creates the first backup set while you are stepping through the Retake Wizard. Thereafter, while the Enable Automatic Backup option is selected, it continues to update your backup set at the time delay you've specified. If you chose to make Mirror backups, Retake updates your backup set at the same time that you resave the original source files.

If you select a write-behind delay longer than zero seconds (a Mirror backup), Retake updates the backup set at any time after the specified time delay when your PC is idle. This allows Retake to work in the background so that it does not interrupt the work you are doing. This is a good option to use with the protected volume file backup type since it eliminates any speed loss due to more frequent disk accesses and larger file sizes associated with the protected volume file backup type.

What you're about to learn:

- How to define your backup strategy
- What backup settings you can select
- How to create, modify and delete a backup set
- How to restore a protected volume file
- How to repair and rebuild a backup set

Defining Your Backup Strategy

After you decide which backup type you want to use (either a protected volume file or a directory backup set), the most important questions you must answer when defining your own backup strategy are:

- Where will you store the backup set?
- What files are important (which files must be backed up)?
- How often should you or Retake make these backups?


Where Will You Store the Backup Set?

If the survival of your business depends upon your PC being up and running at all times (and if money is not an object), the ultimate way to protect the data on your PC would be to set up a redundant PC with identical sized drives. This backup PC's only job would be to mirror the data on your primary PC. It would be waiting in the wings should your first PC fail for any reason. And if that happened, you could simply switch your work to the second PC while the first one is repaired.


Often money is a consideration in deciding where you'll store your backup sets. The least expensive way of making backups has traditionally been to copy data to 3.5-inch disks, though this is the most labor intensive way of storing backups because it requires you to switch disks by hand.

In today's computer marketplace, you may discover that it is as cost effective to acquire a separate backup hard drive where you can keep a current mirror backup copy of one or more other drives that you use on your PC.

In addition, you may want the backup copy to be stored at a remote location, for increased protection. As long as Retake can access a logical drive mapped on your PC, it can store the backup set there. That is, the backup set can be stored on a shared network drive.

 *You can use the Map Network Drive command, available by Right-clicking My Computer, to assign (map) a drive letter to a location on a network drive. This makes that location a "logical drive" on your PC. For more details, see your Windows online Help.*

Even if you cannot invest in another drive or disks for storing your backups, you can still create a backup copy of your data on the same drive. This offers the least protection should that drive fail, but the potential for data recovery is increased by having two sets of your most important information stored there. It is further enhanced if you select the protected volume file backup type, which allows recovery in many circumstances even with the drive physically damaged.

 *If your data usually resides on a server, you can make a local copy so you can access data even when the server goes down.*


What Files are Important to You?

Retake automatically selects files that are typically important to include in a backup set. However, you can select other files or types of files to include in your backup set.

In addition, you can create multiple backup sets of data for particular purposes. Each of these backup sets can be created when and where you specify. They can each include exactly the files or types of files that you choose. For example, you might create individual backup sets for each of your clients if you produce data for clients that is stored on your computer, such as advertising layouts, graphic images, books, or accounting data.

How Often Should You or Retake Make Backups?

The more recent your backup set, the happier you'll be if your PC does encounter a problem that compromises the data on your primary drives. However, you may want to keep the default Write-behind Delay of 20 minutes to give you time to recover a previous version of a file if you ever need to.

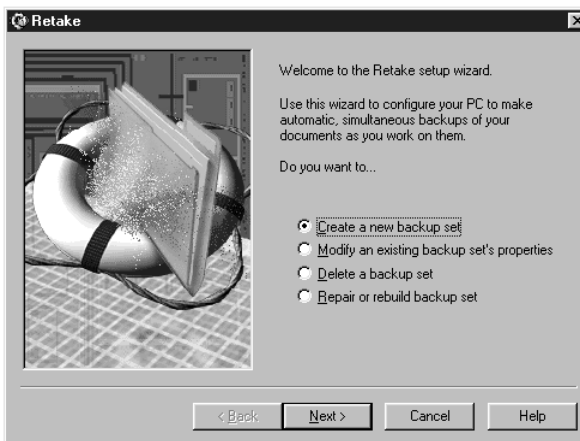
 *Save early, save often. While working in applications, you can almost always press **CTRL-S** to save your work as you go. The more often you save your work, the less you have to lose at any given point in time. You may also want to be sure the auto-save option is selected in your applications for more frequent backups.*

Creating a Backup Set

Creating a backup set, either manually or to be updated automatically, in Retake is very easy. Retake's default choices should work fine, though you may want to add additional folders or file types to your backup list.


To create a backup set:

1. Click the Start button and do one of the following:
 - Choose the Safe & Sound command from the Start menu and click the Retake button.
 - Choose the Programs > Safe & Sound > Retake command.



2. Click the Next > button while the Create a New Backup Set radio button is selected.
3. Select whether to back up to a Protected Volume File or a Directory. Then click Next >.

Protected Volume File—The Protected Volume File is the preferred backup type. A protected volume file is a sectioned off portion on the drive. It has special characteristics to ensure that even if organizational structures, such as the file allocation table on the drive is corrupted or lost, or the data becomes scrambled, the files in the backup set can be reconstructed. Retake stores extra information (in each sector for each file and also in a separate directory) to provide this level of protection. For details, see the “Protected Volume Files (The Ultimate Backup Protection)” section on page 17.

 *You can copy files into a protected volume file manually using My Computer or Windows Explorer to add them to your backup set and instantly protect them.*

There are two drawbacks to using a protected volume file backup type. The first drawback is that three percent more storage space is required for the extra information that will be used to reconstruct the files in the event of a problem. The second drawback is that a protected volume file is slightly slower because it has to manipulate more information in more areas on the disk and more disk accesses are required. This is a marginal performance degradation, which you can eliminate by also selecting a Write-behind Delay of seconds or minutes.


Directory—The Directory backup type makes another copy of the files and directories selected for backup in a different location. This type of backup creates no performance drain on the system and it's simple to manage the backup area. You can use My Computer or Windows Explorer to cut or copy files in or out of the backup location or delete the files. The drawback of selecting a directory backup type is that the files are no more protected than if you had created a backup copy yourself.

4. Specify the target destination where the backup set will be created and click Next >.
5. Click the Settings button if you want to customize any of the settings for this backup set.

Volume Settings

- **Backup Type**—Displays the currently selected backup type (Protected Volume File or Directory).

- **Enable Automatic Backup**—While this check box is selected, Retake automatically updates this backup set as you update the files it contains based on the time delay you specify.
- **Name of Backup Set**—If you are saving this backup set to a non-Windows 95/98 or NT drive (such as to a UNIX server on your network) be sure to follow the 8.3 naming convention for this name.
- **Write-behind Delay**—Select the Mirror (0) write-behind delay if you want your backup set to remain in constant synchronization with the original files as you change them. Select a write-behind delay in seconds or minutes if you want your backup to be created during times when your PC is idle starting at any time after the time delay you select.

 *A write-behind delay in seconds or minutes is recommended if you are using the protected volume file backup type and want to eliminate the slight speed reduction caused by extra disk accesses in more locations on the drive.*

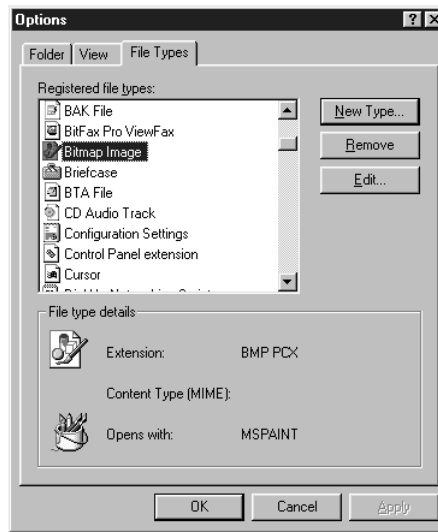
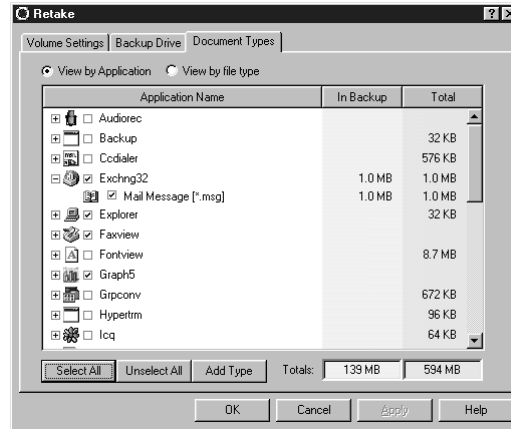
- **Protected Volume Drive Letter**—(available only for backup sets stored as a Protected Volume File). The drive letter you want to use for the Protected Volume File backup set.
- **Keep Deleted Files For**—Select how long you want the backup set to keep files whose original counterparts have been deleted from your system.
- **Limit Size of Backup Volume**—Drag the slider left to reduce the backup volume size limit or right to increase the backup volume size limit.

Backup Drive

Drive and Directory Folders appear in the Backup Drive list so you can select any of the ones you want to add to your backup set. Click folders to open and close them. Click the check boxes to place a check mark beside the drives or directories that you want to back up.

Document Types

You can select groups of files that you want to include in your backup set by selecting their file type. The file type, such as TXT (for a text file), indicates the file's purpose. Retake displays a list of all the registered file types in Windows 95/98. The file types with check marks show the types of files that will be included in your backup set.




Retake obtains its list of registered file types from Windows. You can view or add registered file types in My Computer or Windows Explorer.

If you are not yet familiar with file types and want to see them, you can open My Computer or Windows Explorer, choose the Options command from the View menu, and click the File Types tab.

In the Options dialog box you will be able to examine the list of the registered file types on your system. These are the file types that will be available to you in Retake. You can add new registered file types in the Options dialog box to make them available to Safe & Sounds' Retake utility the next time you run it.

Many file types are standard, such as BMP and PCX which are used by paint applications like Microsoft Paint, or TIF which is a standard file type used for TIF or TIFF graphic image files.

Each application's documents typically have a file type (which may or may not be registered in Windows). For example, Microsoft Word document files may be stored using the registered file types of DOC, RTF or TXT, depending upon the file type you select when saving the document.

 *You can also view file types directly in My Computer or Windows Explorer. Choose the Options command from the View menu, click the View tab, and make sure the HIDE MS-DOS FILE EXTENSIONS FOR FILE TYPES THAT ARE REGISTERED check box is deselected. Registered file types are also listed in the File Types tab in the Options dialog box. The other place where file types appear is in the Save As dialog box of Windows applications.*

6. Click Apply to apply changes to a tab of information. Then click OK when you are done.


If you want to make a backup set manually, deselect the Enable Automatic Backup check box.

If you've selected your 3.5-inch drive or a removable media drive that provides less space than you'll need for your backup set, you'll need to follow the instructions on the screen and switch disks or tapes when instructed.

7. Click Next >, enter a name for your backup volume, and click Next > again.
8. Click OK.

Restoring Files from a Backup Set

If you encounter a problem with the information on your drive, you can restore one or more of the files in your Retake backup sets.

 ***Unless you create a backup set that contains the entire contents of a drive, you should never drag and drop, or copy and paste, the contents of a Retake backup set's <drive letter> folder directly into your drive's window. Though the folder names match between a Directory type backup set and the folders on the drive, the contents of the two are most likely very different. By default, Retake only backs up files it considers essential and important, such as INI, TXT, RTF, DOC, and WRI files. It backs them up using the original hierarchical directory structure from the source drive. You will know where to restore each file, if you need to, based on its location in the backup set. It does not automatically back up your application files or DLL files, nor does it back up your Windows directory without your explicit instructions to do so.***

To restore a backup set:

1. Open Windows Explorer or My Computer and open the backup set.

If the backup set is a Directory type backup, the folder name (by default) is Backup_1, Backup_2, and so on. If the backup set is a Protected Volume File, it is located at the same level as your physical drives.

2. Find the files you want to restore and use Drag and Drop or Copy/Paste to copy files from your backup set to the location where you want them.

Modifying or Deleting Backup Sets

Modifying an Existing Backup Set

To modify a backup set:

1. Click the Start button and do one of the following:
 - Choose the Safe & Sound command from the Start menu and click the Retake button.
 - Choose the Programs > Safe & Sound > Retake command.
2. Select the backup set to modify and click the Properties button.
3. Change the settings and click OK when you are done. Then click Finish.

Deleting a Backup Set

If you created a Retake backup set as a protected volume file, you cannot delete it in My Computer or Windows Explorer. You can *only delete the protected volume file* using Retake.

If you created a Retake backup set as a directory, you should still delete it using Retake; however, you can delete the backup directory via My Computer or Windows Explorer.

To delete a backup set:


1. Start Retake.
2. Click the Next > button while the Delete a Backup Set radio button is selected.
3. Select the backup set to delete and click Finish. Then click Yes to confirm the deletion.

Repairing and Rebuilding a Backup Set

If you encounter a problem with the backup set itself, you can repair or rebuild it. For example, if your computer crashes while the backup is being created or updated automatically, the contents of the backup may be incomplete or damaged. Retake automatically checks the integrity of your backup when you start Windows. If it is damaged, Retake starts and asks if you want to repair the backup set.

To repair or rebuild a backup set:

1. Start Safe & Sound's Retake utility and click Next > while the Repair or Rebuild Backup Set radio button is selected.
2. Do one of the following:
 - Click the Repair button and click Next > if you can see the backup set in My Computer or Windows Explorer, but the information is somehow damaged. For example, if a backup was not finished due to a power outage or computer crash.
 - Click the Rebuild button and click Next > if you can no longer see the backup set (for example if the protected volume file is no longer visible in My Computer or Windows Explorer).


 *Performing a Rebuild is a time-consuming process because Retake searches your entire system to find all backup sets that are stored there.*

3. Select the drives that contain a protected volume file you want to restore. Then click Next >.

Wait while the Restore utility searches the selected drives for protected volume files or backup directories. If it finds a protected volume file, a message appears asking if you want to Save As, Ignore, or Ignore All.

4. Click the Save As button and select where you want the restored volume file to be placed. Then click Save.

Viruses can infect any computer and cause serious damage. A virus is a small program that, when it is inadvertently run, takes control of the infected computer. This gives the virus the opportunity to perform destructive actions, like deleting or writing over files or changing random bits of data.

 *New viruses are continually being propagated, so it is important to stay informed and to keep your Safe & Sound software updated. Network Associates' Internet website offers a wealth of excellent information about computer viruses, including antivirus technical support; a Virus Info Library that defines individual viruses, hoaxes, research, and technical information; and White Papers that describe viruses and the countermeasures you can take to combat them. To access this information, point your web browser to: <http://www.nai.com/vinfo/>*

What is a Virus?

A *virus*, like its biological namesake, replicates itself and attaches to another program, or any file that can be run (such as a word processing or spreadsheet macro). When you run the infected program or macro, you unknowingly run the virus.

While the virus is running, it has the opportunity to clone itself, thus spreading from one disk or drive to another. It also has a chance to damage or destroy your valuable information.

Anyone can write a computer virus, even people who are not programmers, so viruses can either do no damage at all or far more damage than intended. Few viruses are written to be destructive, but the simple fact that a virus takes control of your computer—sometimes as soon as you start your computer—makes viruses a serious threat. Worst of all, if even a single copy of a virus remains “in the wild” (that is, lying dormant on anyone’s computer without their knowledge), then it may be able to quickly spread from one machine to another.

How Are Viruses Transmitted?

Any software interaction with another computer gives a virus a possible entry point to your system. The most common method of getting a virus is from an infected disk, such as when you install software (even shrink-wrapped software) from either 3.5-inch disks or CDs. Software manufacturers check for viruses when creating *golden masters* (the master disk set used for creating all other copies of their software). This does not mean that they will always detect and clean every virus. A new virus could easily evade detection, or one disk might be accidentally missed in the virus scanning process.

Furthermore, viruses can be designed to avoid detection in a number of ways. Viruses are written, with varying degrees of success, to hide from detection when examined using standard file handling software (such as My Computer or Windows Explorer). For example, when a virus clones itself, it can save a copy of the information it overwrites including file size, creation and modification dates, and so on. When Windows Explorer attempts to read this information, these viruses (called *stealth* viruses) simply supply the pre-infected information. This means that you cannot always tell whether your computer has a virus just by checking program information to watch for sudden changes.


Your computer can also become infected when you connect to another computer via modem (direct, Internet, BBS or online service connections) or any form of network connection. A virus can be copied to your machine, but until you perform the action that triggers that virus, it stays inactive. A trigger event could be running the program the virus has attached itself to, a particular date or time, or even certain characters you type.

What Types of Viruses Can I Encounter?

There are three major categories of viruses: boot sector, file and macro. Safe & Sound's Virus Scanner checks for all of these types of viruses.

Boot Sector Viruses

Boot Sector viruses copy themselves to the boot sector of a disk. The *boot sector* is the first sector on a disk that contains special information used to startup (or boot) your computer. A boot sector virus gains control of your computer from the moment you start your machine. Typically, this virus becomes resident in your computer's memory the same way Bomb Shelter does when it is active.

 *Bomb Shelter does protect certain critical areas of your computer's RAM from being overwritten by applications (including virus programs). However, it is aimed at securing your system against system crashes rather than against virus attacks.*

File Viruses

To perform any action, a virus must be run. With this in mind, a file virus attaches itself to a file it knows can be run, which includes COM, EXE, SYS or BAT files. File viruses sometimes also attach themselves to OVL or OVI overlay files. Once the virus is attached to a file, it will be run the next time you start that program or run the macro. When this happens, the file virus can propagate itself and cause damage to your computer's information.

File viruses are the most common type of virus, but because they overwrite part of the original program, they usually cause the program to fail in some way. This provides a warning signal that makes file viruses easier to detect.

Macro Viruses

Macro viruses take advantage of the power of macro languages offered by application programs, such as Microsoft Word or Excel. A macro virus uses macro commands to perform undesirable actions on your computer when they are run from within the application that supports them. It doesn't take a programmer to write a macro virus.

Externally, a macro virus looks like a regular document, and until recently, regular documents were considered safe from virus infections. This means that macro viruses can spread very quickly.

Logic Bombs, Trojans, and Worms

There are other kinds of programs that can be written to damage your computer, but that are not viruses because they either cause damage but do not replicate themselves, or vice versa.

A *logic bomb* is a program that stays on your computer and remains inactive until some trigger event. When that trigger takes place, the logic bomb performs some destructive action. For example, a logic bomb might be copied to a computer by a disgruntled employee. The logic bomb has a particular target and does not clone itself.

A *trojan*, like the trojan horse which is its namesake, delivers a destructive program (a logic bomb or virus). A trojan goes in the guise of an attractive, or seemingly useful program (such as a game or utility program).

A *worm* is a program whose sole purpose is to clone itself, without taking any other form of destructive action. By itself, a self-replicating program can bring a computer or even a network to a standstill by stealing exponentially increasing amounts of CPU time and storage space.

How Can You Combat Viruses?

Virus Scanner checks for viruses in your computer's memory, in the boot sector and in files. It does this using a sophisticated, algorithmic checking process. Simply start Safe & Sound and click the Virus Scanner button. Follow the instructions on your screen and Virus Scanner examines your computer's memory, boot sector and files for viruses. If it finds them, it gives you a report of them so that you can clear them from your system. For more information, see "Recovering From a Virus Attack" on page 35.

Thereafter, you should also follow some preventive guidelines to help ensure that viruses have a more difficult time gaining access to your computer. For example, you should write-protect the disks you use whenever possible. Also, you should only run a macro when you know exactly where it came from and who created it.

Recovering From a Virus Attack

Once a virus has already attacked your system, Virus Scanner cannot perform the kind of repairs that may be necessary. To help you repair a damaged computer, run Safe & Sound's System Checker or Disk Minder for DOS.

If the virus has deleted files from your drive, you may need to recopy these files from your latest Retake backup set. If the damage to your drive is severe, you may need to reformat the drive and reload your latest complete backup set. As soon as you finish this process, be sure to rerun Virus Scanner to catch the virus before it has a chance to destroy your data again.

If none of these things work, you can contact Network Associates' Technical Support department for assistance with your particular virus and how to recover from the attack. Late-breaking information is also offered at the Network Associates' <http://www.nai.com/> website.

Safe & Sound offers these tools to protect your system or help you recover from problems:


- **Bomb Shelter**—provides crash protection and recovery.
- **Discover**—offers extensive information about your hardware and software.
- **Rescue Disk**—lets you make a disk that you can use to boot your PC if you can't start from your system hard drive and begin recovery of your system.
- **McAfee Image**—saves an image copy of critical disk information in a special file, and restore that image later if your system becomes damaged.
- **Year 2000 Checker**—tests your PC for Year 2000 hardware compliancy. It provides a resident program (Y2Kfixer.com) that can fix problems with your PC's date handling at the transition to 01-01-2000 and beyond.

What you're about to learn:

- How to set up Bomb Shelter crash protection and recovery to safeguard your PC against application errors
- About the Discover window, its tabs of information and how to view detailed information for each tab
- How to create a Rescue disk and use the programs on it.
- How to create and restore an image copy of critical system information.
- How to check your computer system for Year 2000 compliance, what Year 2000 compliance means and some other things you'll want to check on your system before the year 2000 starts.

Bomb Shelter

Bomb Shelter is a Safe & Sound “crash protection and recovery” utility that prevents critical regions of your system’s RAM from accidentally being overwritten by misbehaving application programs. Bomb Shelter also lets you restart a *crashed application* (an application that has completely failed or stopped responding) in order to recover your data.

 *We recommend that you activate Bomb Shelter so it always runs when you run Windows. See “Starting Bomb Shelter” on page 39. By running Bomb Shelter, you ensure that application errors and faults do not cause you to lose data, and more importantly, that such problems do not cause any damage to your system.*

If an application tries to overwrite any critical system RAM regions, Bomb Shelter will produce a fault, an error condition, and display a dialog box, allowing you to selectively close the faulty application or reenter it so you can save your information before closing.

For a variety of reasons, PC users will, sooner or later, encounter faults and error conditions—usually caused by an errant application. In most circumstances, the application has to be closed, with a corresponding loss of any unsaved data. However on occasions, the problem can be more serious, requiring a complete system reboot.

In even rarer cases, the error can cause critical areas of your PC’s files to be overwritten or otherwise corrupted. To repair the damage created by such an error requires lengthy and complex diagnostics and repairs using other Safe & Sound utilities. Bomb Shelter is designed to reduce the severity of application errors, and to almost completely eliminate the most serious errors.


Bomb Shelter can coexist on the same PC with other protection programs. However, you won’t need to use another protection program because Bomb Shelter provides the most complete protection. It not only protects your system against high-level errors that other protection programs miss, but it also protects your system against more serious low-level errors.

Since Bomb Shelter operates at a lower system level than other crash protection programs, it will see errors only if any other protection program you use misses the error. So if you have Bomb Shelter loaded with another crash protection program, the other program will intercept some errors. This does not mean that the other program is superior—in fact, quite the reverse. Bomb Shelter catches errors at all levels, so though you can use other crash protection programs, you really don't need to.

Starting Bomb Shelter

When you start Bomb Shelter, it automatically activates so it can begin protecting your system's critical areas from being overwritten by applications and allow you to recover from crashes. Once loaded, Bomb Shelter remains active until you deactivate it.

To start Bomb Shelter:

1. Start Bomb Shelter by doing one of the following:
2. Click the Start button and choose the Programs > Safe & Sound > Bomb Shelter command.
3. Choose Safe & Sound from the Start menu, click the Tools button, and choose Bomb Shelter from the Tools menu.
4.  Open the Safe & Sound folder and double-click the Bomb Shelter icon in the Windows Explorer or My Computer window.

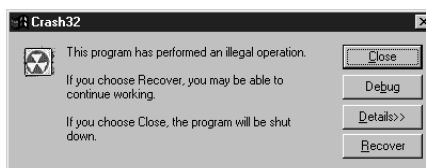


5. Click OK.

Bomb Shelter remains active, and automatically places itself in the StartUp folder so that it loads the next time you start Windows.

Recovering from an Application Error

Bomb Shelter continuously monitors your system to detect when an application tries to perform an invalid operation or damage any critical part of your system. When such a “Fault” condition occurs, Bomb Shelter suspends the application and displays the following dialog box.



When you see this dialog box, the application has caused an error which usually means it has gone astray. Therefore *your data may already be lost or damaged*. This dialog box lets you choose what to do with the faulty program. The following options are available:

- **Close**—closes the application that caused the error and allows you to continue working.
- **Recover**—reactivates the faulty program at a point that should let you save your data. *This procedure has some inherent risks* and you should follow the steps in the procedure below when trying to Recover a crashed program.

To attempt to recover your work:

1. Use Windows Explorer to make a backup copy of the open document you were working with in the application.
2. Click the Recover button in the Bomb Shelter dialog box.
3. Attempt to save your work in the application.

4. Exit the application immediately and restart Windows.

Recovering a Crashed, Locked-Up or Hung Application

Sometimes application errors cause programs to stop responding to the keyboard or mouse. In Windows 95, Bomb Shelter can “unlock” programs and allow you to try to recover any previously unsaved information in documents you had open in the application when it stopped responding.

To unlock a locked program:

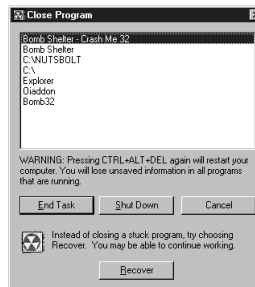
1. Hold down the **CTRL** and **ALT** keys and simultaneously press the **DELETE** key (sometimes labeled **DEL**).

Bomb Shelter displays the Close Program dialog box.

2. Select the application that has stopped responding.

Bomb Shelter tries to recognize the program and pre-select it for you.

3. Click Close to have Bomb Shelter close the program, or click Recover to have bomb shelter try to reactivate the program.



✍ An application that has stopped responding may have other problems as well. Therefore your data may already be lost or damaged. If you need to recover your work, follow the instructions in the following procedure.

To attempt to recover your work:

1. Use Windows Explorer to make a backup copy of the open document you were working with in the application.
2. Click the Recover button in the Bomb Shelter dialog box.
3. Attempt to save your work in the application.
4. Exit the application immediately and restart Windows.

Selecting Bomb Shelter Properties

Bomb Shelter lets you select a variety of properties that determine how the utility behaves and what kind of protection it gives you. You can also select Advanced properties, which provide settings for advanced users and for troubleshooting by Network Associates' Technical Support Engineers.

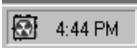
To select Bomb Shelter properties:

1. Click the Properties button in the Bomb Shelter Wizard.
2. Select the options in the Properties tab and the Statistics tab. Click a tab to bring it to the front.

The properties you can select in the Properties tab are:


- **Write protect System**— Activates Bomb Shelter's write protection option that protects various critical parts of your system RAM from being overwritten. If these areas become overwritten or corrupted, your system may lock up or worse.
- **Automatic Error recovery**— Activates Bomb Shelter's Program Fault dialog box that lets you re-activate crashed programs to try to save the data in them. If you disable this option, Bomb Shelter does not intercept application errors, and you get the regular Windows dialog box for these errors. The Windows dialog box does not have a recover option.

- **Use Ctrl-Alt-Del to unfreeze**—Activates Bomb Shelter's Close Program dialog box, which lets you re-activate programs that have stopped responding to attempt to save the data in them. If you disable this option, Bomb Shelter will not intercept the **CTRL-ALT-DELETE** key combination, and you will get the regular Windows Close Programs dialog box when you press **CTRL-ALT-DEL**. The Windows dialog box does not have a recover option.
- **Show icon in tray**—Tells Bomb Shelter to display the Bomb Shelter icon in the Windows taskbar tray. Double-clicking the tray icon activates the Bomb Shelter Wizard.



The Statistics Tab gives you an up-to-the-minute report on Bomb Shelter activity. The information contained in this tab is really only of interest to advanced users.

3. Click the Apply button when you finish selecting options for a tab so you can continue selecting options for another tab.
4. If you are an advanced user, or if you are working under the direction of a Network Associates' Technical Support Engineer, you can click the Advanced button to specify advanced properties for Bomb Shelter.

 *It is strongly recommended that you do not make Advanced selections unless you have a very clear understanding of error conditions, faults and Windows.*


The Bomb Shelter Advanced Properties dialog box appears. Select the options you want and click OK.

5. Click OK when you finish selecting properties.

The Bomb Shelter Wizard dialog box reappears.

Testing Bomb Shelter

The Bomb Shelter Wizard dialog box offers a testing option that lets you activate the Crash-Me test program. This test program lets you simulate common application error conditions to check how Bomb Shelter is working and verify that your system is protected.

 *The Crash-Me test program is provided for advanced users or for use by Network Associates' Technical Support Engineers. Avoid using the Crash-Me test program unless you suspect that Bomb Shelter is not working properly. **Bomb Shelter must be active when you perform tests.** Otherwise, your system will have no protection when you simulate error conditions and you may have to restart your PC.*

Network Associates' engineers have made every effort to ensure that Crash-Me crashes gracefully, particularly with any crash protectors other than Bomb Shelter, but *prior to running any crash tests*, ensure that you have saved all your work and have closed all other programs.

To simulate error conditions:

1. Click the Test button in the Bomb Shelter Wizard.

Bomb Shelter starts the Crash Me program, which displays a dialog box where you can choose the type of error to simulate.

The 11 fault types simulate different error conditions and faults that can be produced by higher-level applications (such as the General Protection Fault) or by low-level programs (such as the Stack Fault or Null Stack Pointer).

2. Select the test you want to perform and click the Test button to simulate the selected error or fault condition.

Bomb Shelter creates the desired fault/error conditions and displays the Bomb Shelter recovery dialog box.

3. Click the Close button to close the test program, or click the Recover button continue using the test program.

Deactivating Bomb Shelter

You can deactivate Bomb Shelter whenever you like without restarting Windows.

To deactivate Bomb Shelter:


1. Do one of the following to open Bomb Shelter:
 - Double-click the Bomb Shelter tray icon in the Windows taskbar.
 - Choose Safe & Sound directly from the Start menu, click the Tools button, and choose Bomb Shelter from the Tools menu
 - Click the Start button and choose Programs > Safe & Sound > Bomb Shelter.
2. Click the Deactivate button.

Bomb Shelter unloads from memory and removes itself from the StartUp folder so it does not load the next time you start Windows.

Discover

This topic shows you how to use Discover, a unique utility that lets you view a wealth of system information, as well as perform benchmark tests. Discover is your complete system analysis tool. It can help you understand PC hardware and software configurations, and is designed to help you use, analyze, and configure your PC. It provides all the information you need to make optimum use of all available memory.

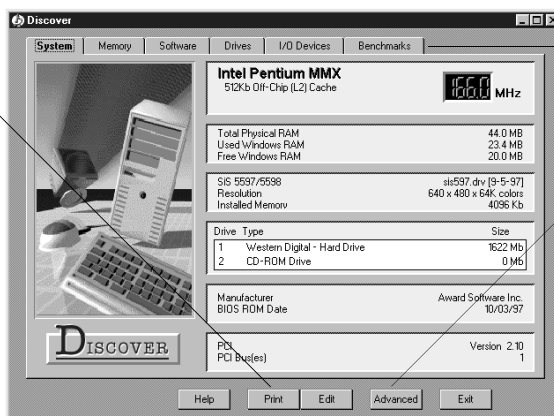
Unlike other system information tools, Discover doesn't simply display information that it obtained from Windows. Discover actually tests and measures the hardware and software in your system.

 You should have general knowledge of DOS and Windows memory architectures and terminology. See "Understanding Windows Memory" in the online Help.

The Discover Window

Discover is easy to use and most windows are self-explanatory. Click the Help button for context-sensitive help from any window.

Click Print to display the Print dialog box where you can decide which screens to print to your printer or save in a text file



Click a tab to bring it to the front, making it active

Click Advanced to view the Advanced window for the active tab, which shows details about that aspect of your system

Click Edit to edit an INI file

Discover lets you view information about your hardware and software. Each tab in the Discover window covers a specific aspect of your PC, ranging from a general overview of your system configuration through software to benchmark tests. You can click the Advanced button at any time to obtain a far more detailed analysis of the current tab's topic. Then click the Summary button to return to the Summary view illustrated above.

- **System tab**—shows information about the most critical hardware components of your system, including your CPU, RAM, video, hard drives, BIOS ROM and PCI Bus. You can confirm that your CPU conforms to the manufacturer's specifications; check your physical, used and free RAM; and confirm your video board type, resolution and installed video memory.
- **Memory tab**—gives information on Windows' usage of your PC's memory, via easy-to-understand pie charts and tables. You can identify RAM and resource usage for each application and task; view your physical RAM, User and GDI Resources free; and so on. Note that Discover reports on the actual physical memory (RAM) used by programs.
- **Software tab**—offers information about the software you are currently running and the software components of Windows, such as the numbers of virtual machines, threads, tasks, virtual device drivers and modules. It also shows whether tasks, or programs, are 16-bit or 32-bit, and gives details on your DOS program segments and bytes used.
- **Drives tab**—gives you a complete summary of any drive installed on your system and of all the directories (or folders) and files on that drive. You can immediately see the total size of each drive, the amount of free space, fragmentation levels and the size of your drive's file slack. An easy-to-understand pie chart gives you a visual overview of your drive's contents and free space.
- **I/O Devices tab**—shows information on the secondary and optional hardware devices installed on your PC, such as sound devices, serial and parallel ports, printers (including fax/modems) and network data including network type, driver, specification, version and user name.
- **Benchmarks tab**—an easy-to-use method to benchmark the performance of your CPU and compare it to average benchmarks for three other "commonly configured" PCs.

Working With Advanced Information


You can view detailed information about any of the tabs in the Discover window.

To work with advanced information:

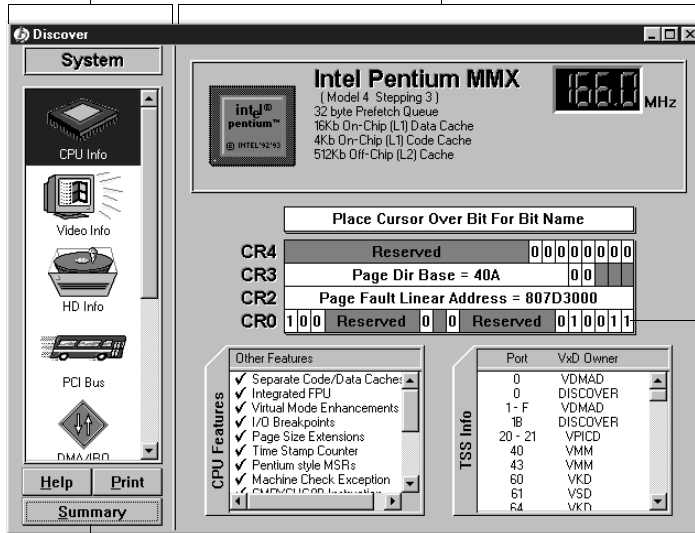
1. Click a tab to bring it to the front.
2. Click the Advanced button.

Discover displays the Advanced window for the active tab. All the Advanced windows have these elements in common:

- **Icon Panel**—Click any of the icons in the panel at the left to view that type of information in the panel at the right.
- **Detail Information Panel**—The detail information shown in the panel at the right is for the category indicated by the currently selected icon. The detail information is mostly self-explanatory with scrolling lists and buttons you can click to obtain additional information or perform related tasks, such as running or stopping benchmark tests.

 *In several of the detail information panels, you'll see legends with small color boxes showing the kind of information that is graphically represented in that color. If you click a Color box, the Color Change dialog box appears where you can select a different color to use for that legend item.*

Click an icon here and Discover changes the panel here.



Click Summary to go back to the Discover summary window

Point to a bit (bits are ones or zeros) to see its name

Rescue Disk

Rescue Disk lets you create an emergency boot disk that you can use to boot up your PC if you encounter a problem that prevents you from starting the computer from the system hard drive. The *system hard drive* is the hard drive that contains your Windows directory or folder.

You can use the Rescue disk that is created by default. Or if you are an advanced user, you can customize your Rescue disk to add the most important files that you may want to use when recovering a failed hard drive. For example, you might want to add your CD drive's driver software so you can also access that drive during the recovery process.

To create a Rescue Disk:

1. Click the Next > button in the Rescue Disk Wizard.
2. Do one of the following:
 - Go to step 3 if you want to use the default Rescue disk.
 - Click Advanced if you are an advanced user and want to add additional files to (or remove them from) the Rescue disk.
3. Click Next >. Then click Finish.
4. Insert a disk into drive A and click OK.

Rescue Disk formats the disk and copies critical startup files to it, as well as any files you added. When the process is complete, Rescue Disk exits and returns to the desktop.

Using a Rescue Disk

Insert your Rescue disk into drive A, reboot your computer (or turn on the power). If your system doesn't boot, access CMOS and make sure the Booting From Floppy option is enabled. Then follow the on-screen instructions.

Disk Minder in DOS

Disk Minder in DOS lets you repair disks even if you cannot start Windows. It resolves most disk-related problems such as missing drives, inability to access drives, or errors accessing drives.

To use Disk Minder in DOS:

1. Type the following:

```
C:\WINDOWS\DMDOS
```

and press **ENTER**.

Disk Minder searches your PC for drives and then asks you to select the drives you want to check from the Drives list.

2. Press the **TAB** key to change the drives that are currently selected to be scanned. Selected drives have an **x** beside them in the list.
3. Press the **UP ARROW** and **DOWN ARROW** keys to highlight a drive and press **ENTER** to select it.
4. Press the **RIGHT ARROW** key to move the cursor back to the buttons.

You can select Disk Minder options if you like. Your options are:

- **Fix Errors Automatically**—fixes any data or disk errors automatically. This is the same as selecting the Fix Errors Automatically Using Default Values check box in the Disk Minder window. If you deselect this check box, Disk Minder will let you fix errors interactively.
- **Test Drive Surface**—performs read/write tests of the recordable surface media on a disk. This process may take some time because the entire disk is read and then rewritten. If a sector is damaged, Disk Minder relocates the information, saving it elsewhere on the disk so you can try to recover the information later. Then it maps out the bad sector so it won't be used for storing data in the future.

- **Check DxSpace Host Drive First**—checks the physical drive where DriveSpace or DoubleSpace compressed volume files are stored. Then it checks the compressed volume files, or logical disks.
 - **Check for Valid File Names**—verifies that filenames use acceptable characters. Valid characters for filenames are numbers 0-9, letters A-Z, and basic symbols excluding the backslash (\), greater than (>), less than (<), colon (:), double quotations ("), and bar or pipe (|). Disk Minder also checks long filenames as well as short filenames that follow the 8.3 filename convention.
 - **Check for Duplicate File Names**—checks the selected drives for duplicate filenames (files with the same name in the same directory).
 - **Check Reserved Attribute Bits**—flags files that have any of the unused (by Windows/DOS) file attribute bits set. These bits may be set on a drive that is shared by OS/2, but otherwise you should most likely leave this option deselected.
 - **Display Summary for Each Drive**—The Summary report tells you how many errors were found on the scanned drive. It also gives you complete information about the status of clusters (the smallest storage units of information on a PC drive) on the drive.
5. Select Start and press **ENTER** to start checking the drives.

Disk Minder displays a screen showing the kind of data it is checking and the options in effect. If the Display Summary for Each Drive option is set, Disk Minder displays a summary message showing the total number of errors found on each drive, if any. It also shows information about the clusters on the drive.

Image/Restore in DOS

Image/Restore can recover from drives that have been accidentally formatted or completely erased, if Image was recently run.

SysRecover

SysRecover can restore several of the Windows 95/98 startup files, such as SYSTEM.INI and the Windows Registry. You should choose this option only if Disk Minder finds no problems on your drives and you cannot start Windows even in Safe mode.

Recover Backup

Recover Backup can restore files from Retake protected volumes file backup sets on drives that have been damaged, erased or accidentally formatted.

Unformat

Unformat can restore entire drives that have been recently formatted.


Image



Although it happens rarely, data stored on a hard drive can become damaged in several ways. For example, the electric company may be working down the street and accidentally send a spike, or power surge, to your PC. Even if you use a surge protector and connect all the computer's power cords and the modem's phone line to a surge protector (instead of connecting them directly to wall connectors), power surges can still reach your PC and cause lost or corrupted data.

An important step in preventing disaster is using Safe & Sounds' Image to make a "snapshot" of the most critical areas on your hard drives. Since even a recent backup copy is still not as good as recovering your current data, you'll want to try to recover the latest data first if anything goes wrong. If you use Image to make a snapshot of the most crucial information on your drives, then if a drive becomes corrupted, you can use Restore to restore the most current version of your data.

Rescue Disk saves information that you'll need if your hard disk ever fails, including the boot record, partition tables and FAT information. It's a good idea to run Rescue Disk daily, as well as whenever you've reorganized a disk's files using a defragmenter. This ensures that you can use Image's Restore option to restore the latest states of your files and folders (or directories). Image stores its information in a file on your hard drive. This file is stored using a special, patent-pending method that allows the file to be recovered even if the hardware is severely damaged.

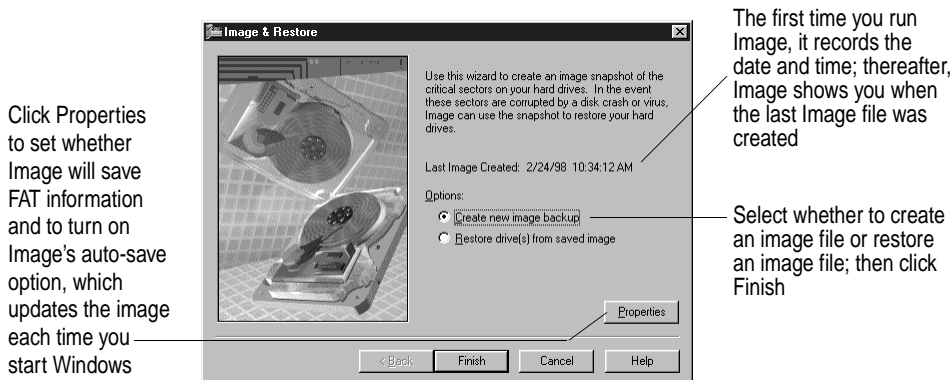
 *Set the Image Properties sheet option to run Image automatically each time you start Windows. Image will examine your system and update the image only if needed. Doing this ensures you always have the latest data saved for your disks.*

Creating an Image of Your Disks

Creating an image copy of your hard disks as a file (`nbimage.dat`) only takes a moment. You should create a new image file any time you've rearranged files or added many new files to your hard drive.

To create an image of your hard drives, select the Create a New Image Backup option, as illustrated on page 55, and click Finish. Image saves the `nimage.dat` file on your system hard drive, and displays a message letting you know the process is complete. Click OK.

Be sure to create a Rescue disk using Safe & Sound's Rescue Disk. Rescue Disk places some Image information on your 3.5-inch disk.




Setting Image Properties

You can set Image Properties to specify whether Image saves the *File Allocation Tables* (FAT), which is a roadmap or index to where all the pieces of files on a disk drive are located. Most likely, you'll want to keep this check box selected. You can also have Image create a new image copy of your hard disks each time you start Windows (recommended).

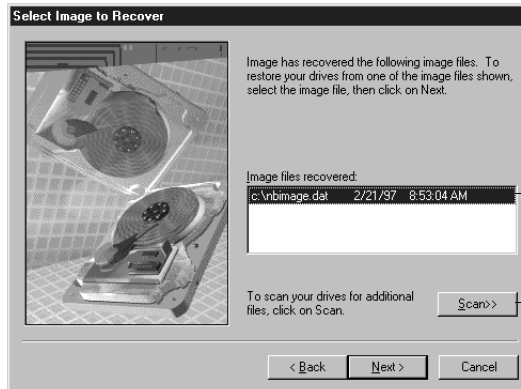
Restoring Drives From an Image File

When all else fails, you can restore the critical information on one or more drives from an image file. Restoring an image file *does NOT* recover deleted files. If you have deleted data files that you need, you can restore a copy of them from your last backup set (protected volume file or directory) created with Retake.

 *Do not restore an image, except as a last resort. The Image file does not contain your data files, those are located in your Retake backup set.*

To restore one or more drives from an image file:

1. Start Image (click the Tools button in Safe & Sound Central and choose Image/Restore), select the Restore Drive(s) From Saved Image radio button, and click Next >.



Select an image file from the list and click Next > to begin restoring your hard disks

Click Scan >> to locate image files stored on any disk drive on your PC; you can restore image files from any drive, even damaged hard drives


2. Do one of the following and click the Next > button:
 - Select an image file to use for restoring your drives from the list of those found on your system hard drive.
 - Click the Scan >> button to look for additional image files if you don't see the one you want to use. Image scans your hard drives for image files. Select one of them and click Next >.
3. Select the hard drives you want to restore and click Next >.
4. Select the kinds of information you want to restore.

Image defaults to restoring the master boot sector, partitions and the File Allocation Tables. In most cases, you should use the Image default settings. If you are an advanced user, you may want to only restore one or two of the options:

- **Master boot sector**—Select this option if you cannot start the PC from your system hard drive. The master boot sector is the sector on your system hard disk that contains boot information with instructions for starting up your PC.

- **Partitions**—Select this option if you cannot find a logical drive on your PC. *Partitions* subdivide a physical drive into multiple logical drives. Each partition has its own drive letter.
- **File allocation tables**—Select this option if your files are corrupted and you have been unable to repair them using Disk Minder. Often much or all of your data may be intact on the disk, but the file allocation tables (FATs) may be damaged. By restoring the most current copy of a disk's FAT, you can often recover files that would otherwise be lost.

5. Click Finish to restore the drives with the specified kinds of data.

 *If your Image file is more than a day or two old, or if you have optimized your hard disk and have not run Image, try using Disk Minder to repair the hard drive first.*

Year 2000 Checker

The countdown is on to the year 2000. So what's all the hubbub about this date in the computer world?

What is the Year 2000 Problem?

For nearly a millennia, we have been abbreviating the year to simply two digits in date notations. Almost universally, people understand that 12/01/98 means December 1, 1998. Unfortunately, most computers and software followed suit. For details about why this happened, see "Why Do We Have Y2K Problems With Our Computers?" section on page 59.

The problem in a nutshell is simple math (which is the language of computers). Computers and software most often allocate two digits for the year, both when storing the information and when displaying it on the screen. Starting in the year 2000, our data will span two centuries. For that reason, four digits must be used to accurately sort, calculate and compare years in the 1900s and 2000s.

The human eye can instantly recognize that 00 means the year 2000 and 95 means 1995. Therefore on screen displays, dates are likely to still only show two-digit years. But the underlying storage and calculation of dates must change.

Using two digits for the year works fine when all the dates are in the same century. However, when dates span centuries, calculation problems can arise unless computers use four-digit years. For instance, when subtracting 06/01/95 from 06/01/05 to determine a person's age, a computer using two digits would produce an incorrect result of -90 instead of 10 (the accurate result).

Why is the Y2K Issue so Urgent?

The year 2000 is the beginning of the Gregorian calendar year that culminates with the start of a new century and a new millennium. It is also the year whose first tick of our clock's second hand will test the date handling of computers and software worldwide. What makes this issue urgent is that the deadline for bringing computers and software into Year 2000 (Y2K) compliancy is fixed. We simply cannot turn back the clock and still have meaningful data.

So will our computers and software accurately handle this transition from dates in the 1900s to dates in the 2000s? Or will our computers suddenly miscalculate the date and reset computer clocks to some date only meaningful to the developers, such as January 1, 1990 or January 4, 1980? Or worse yet, will our computer systems stop working entirely? These situations are all possible. And the Y2K problem is massive, affecting governments, private sector business and home users alike.

For this reason, U.S. Government agencies estimate they will spend \$2.3 billion between the 1996 and 2000 fiscal years bringing government computer systems into compliancy before the beginning of the year 2000. Solving the Y2K issue is the most massive example of human cooperation and teamwork to date. In that respect, achieving total compliance before 2000 will be something to celebrate in itself.

Why Do We Have Y2K Problems With Our Computers?

The Year 2000 issue is a problem now, because of design decisions made two or more decades ago by engineers and programmers. These people knew that the turn of the century loomed only 20 years in the future. However, they were confident that their products would only have a five to ten year lifespan. Hardware wears out, and software is enhanced (at that time approximately once every year a new release of software was made available).

There were other factors involved in those early decisions to use a two-digit year. Screen “real estate” (or the area on the screen available for displaying information) has always been a precious commodity. Also the standard method of noting dates by hand and in printed forms used only the last two digits of the year. For these reasons, and for reasons associated with the storage space needed to store dates, developers opted to go with only two digits to represent the year (that is, 93 is 1993, 86 is 1986, and so on).

These developers were confident that their products would be “wall art” long before the next century commenced. In that regard, they were right. The earliest microcomputers (such as Z80 and 8080 CPUs) and their software have long been obsolete and are now in some cases collectors items.

What these developers did not predict was that the standard methods of storing dates that they defined would become “etched in stone.” They did not foresee that their hardware and software, although long out of production, might remain in use long into the future due to replacement costs. Neither did they expect that using two-digit years would start a chain reaction of backward compatibility and design stasis that has caused developers to scramble en masse to find and fix every single occurrence of Y2K non-compliance in hardware and software alike.


What are the RTC, BIOS, DOS, and Windows Clocks?

Safe & Sound's Year 2000 Checker can test the four clocks on your PC. They are the RTC, BIOS, DOS and Windows clocks.

The *RTC (Real Time Clock)* is a device in your computer that maintains the time (measuring elapsed time) even when you turn off or unplug your PC. Accurate time measurement is needed on your PC, and not just so that you can use your computer as a timepiece either. Your PC uses accurate time to perform a flow of computing tasks. The RTC clock gives your computer the ability to perform tasks in order.

The *BIOS (Basic Input/Output System) clock* is stored in firmware, such as PROM (Programmable Read Only Memory) or EPROM (Erasable Programmable Read Only Memory). When you start your computer, the BIOS reads the date and time from the RTC. The BIOS is your PC's “traffic cop,” which dictates how software interacts with all the peripheral devices in your computer, including the RTC clock. Most software gets the date and time from the BIOS, DOS, or Windows clocks. Non-compliant BIOS clocks have reset themselves from 12/31/1999 to 01/01/1900 when the year 2000 begins.

The *DOS (Disk Operating System) clock* gets its date and time from the BIOS clock, and then makes the current date and time available to you or to any application that requests it. You can change the DOS date and time in an MS-DOS Prompt window using the DATE or TIME commands. Non-compliant DOS clocks have reset themselves from 12/31/1999 to 01/04/1980 (the date when DOS was originally released, and before which it did not need to support a current date).

 *Although seemingly transparent, MS-DOS still runs underneath Windows 95, so the Year 2000 Checker fixes the DOS date if it is non-compliant.*

The *Windows clock* gets its information from the DOS clock, and makes the date and time available to Windows applications, or to you via the Date/Time control panel. Non-compliant Windows clocks have also reset themselves from 12/31/1999 to 01/04/1980.

How to Ensure Y2K Compliancy of Your PC's Clocks

Safe & Sound's Year 2000 Checker can instantly determine exactly what the four primary clocks on your computer will do on certain milestone dates without some form of correction or intervention. It can also bring these clocks into compliancy by installing the Y2Kfixer.com program, and adding a line to your AUTOEXEC.BAT file that causes this program to run each time you start your computer. Even if you uninstall Safe & Sound, the Y2Kfixer.com program remains on your system so it continues to be Y2K compliant.

What Dates Does Year 2000 Checker Test and Why?

The Safe & Sound Year 2000 Checker tests each of the four clocks for the following dates. In each case, it starts the tests a few seconds before the date and verifies that the transition to the next day's date is accurate.

01/01/2000

This date is the 2000 rollover. In some applications that perform forecasting or handle future dates, this date will be reached before the actual calendar date. Examples of this include banking, accounting and project management software. In many cases, these programs may begin using 01/01/2000 when the previous year begins on 01/01/1999 or even earlier. The Year 2000 Checker tests to make sure that all four clocks transition accurately from a few seconds before 01/01/2000 into the next day.

02/29/2000

The year 2000 is a leap year, so the Year 2000 Checker verifies that this date is accurate.

The rule for determining leap years is:

- Years divisible by 4 are leap years except for years ending in 00.

- Years ending in 00 that are divisible by 400 are leap years.

Reports have been made of computers failing to accurately consider 2000 a leap year (and instead making the year 2001 a leap year).

03/01/2000

Some BIOS clocks go correctly to February 29, 2000 but then continue to an inaccurate date of 02/30/2000. So the Year 2000 Checker tests not only 02/29/2000, but also that it then moves accurately to the first day of March (03/01/2000).

01/01/2002

The Year 2000 Checker tests 01/01/2002 to ensure that farther down the road your clocks are still handling dates accurately. It also confirms that the clocks do not consider the year 2002 to be a leap year.

What Other Y2K Problems Must You Resolve?

After you ensure that your PC's clocks are Y2K compliant using Safe & Sound's Year 2000 Checker, you still need to verify that the software you use, and your data itself, is also Y2K compliant.

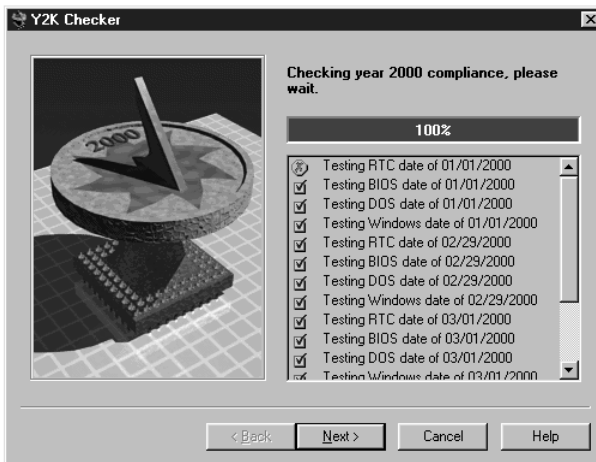
Check the ways that you use dates in your data (such as embedding dates in identifiers like serial numbers). Also check with your computer vendors for Year 2000 compliance in all new products or updates you acquire. If you are using older software, it is an excellent idea to update it.

If you have custom software, its programmers must examine the source code, looking for not only two-digit dates, but also for obscure times when dates, week counts, or even day of the week calculations are performed. If an inaccurate calculation of leap years is made, even the day of the week can be thrown off.

If your PC is connected to a LAN, be aware that networking software synchronizes the server clock with your PC's clock whenever you connect to a server. This means that LAN servers must be accurate, or they could update workstation clocks resetting them all to the wrong date.

To determine if your system is Year 2000 hardware compliant:


1. Click the Start button and do one of the following:
 - Choose the Safe & Sound command from the Start menu, click the Tools button and choose the Year 2000 Checker command.
 - Choose the Programs > Safe & Sound > Year 2000 Checker command.
2. Click Next >.



Y2K Checker tests your computer system for compliance. It displays a circled red X beside the dates that are non-compliant and a check mark in a green box for those dates that are compliant.


3. Click Next >.

If the Y2K Checker finds dates that are non-compliant, it copies the Y2Kfixer program to your Windows directory and adds a line to your AUTOEXEC.BAT file that causes this program to run each time you start your PC. The Y2Kfixer program ensures that your PC's dates remain accurate after January 01, 2000.

 *If the RTC clock fails, but the BIOS clock checks out okay, the Year 2000 Checker indicates that your PC is year 2000 hardware compliant because the BIOS contains a fix.*

4. Click Finish.

If your system clocks were inaccurate, the Y2Kfixer.com program is installed on your PC. Each time you start your computer, this program runs to correct the date as necessary. Even if you uninstall Safe & Sound later, the Y2Kfixer.com program remains installed so it can continue to protect your system's dates each time you start your PC.

 *You should leave the Y2Kfixer.com program on your system if it is installed to ensure on-going protection of your PC clock dates.*

A

Application
 recover from error 40
AUTOEXEC.BAT 61

B

Back Up 17–29
Backup
 Retake 8
 strategies 20–21
 Type 23
Backup Set
 creating 22–26
 deleting 28
 modifying 28
Backups
 automatic 19
 frequency of saving 21
 where to store them 20
 why you need them 18
Benchmarks information 47
BIOS (Basic Input/Output System) clock 60
bomb 34
Bomb Shelter 8, 38–45
 deactivate 44
 Properties 42, 43
 testing 43
Boot Sector Viruses 33

C

Clocks
 RTC, BIOS, DOS and Windows 60

D

Diagnosis and repair
 standard 14–16
Directory backup type 23
Discover 8, 46–49
Disk Minder in DOS 51–52
Document Types 25
DOS (Disk Operating System) clock 60
Drives information 47

E

emergency boot disk 50
Enable Automatic Backup 24

F

File
 Allocation Table 55
 view and add registered types 26
Viruses 33

I

I/O Devices information 47
Image 8, 54–57
 Properties 55
Instant Update 8

K

Keep Deleted Files For 24

L

Limit Size of Backup Volume 24

M

Macro Viruses 33
Map Network Drive 20
Memory information 47
mirror backup 18

N

Name of Backup Set 24
Network Associates
 website 35

P

- Partitions [57](#)
- PC Checkup [8](#), [13–16](#)
- permanent storage
 - definition [18](#)
- Protected Volume
 - Drive Letter [24](#)
 - Files [17](#), [18](#), [23](#)

R

- Rebuilding backup files [29](#)
- registered file types [26](#)
- Repairing backup files [29](#)
- Restore image [8](#)
- Restoring backup files [27](#)
- Retake [8](#), [17–29](#)
- RTC (Real Time Clock) [60](#)

S

- server
 - backup a local copy of files [21](#)
- Software information [47](#)
- System
 - hard drive [50](#)
 - information [47](#)

T

- trojan [34](#)

U

- URL
 - Network Associates [35](#)
- Utilities
 - Bomb Shelter [8](#), [38–45](#)
 - Discover [8](#), [46–49](#)
 - Image [8](#), [54–57](#)
 - Instant Update [8](#)
 - PC Checkup [8](#)
 - Retake [8](#)
 - Retake backup [8](#)

V

- Virus Scanner [31–35](#)
- Viruses
 - boot sector [33](#)
 - combatting [34](#)
 - definition [31](#)
 - file [33](#)
 - macro [33](#)
 - recovering from an attack [35](#)
 - transmission methods [32](#)
 - types of [33](#)

W

- website
 - Network Associates [35](#)
- Windows
 - clock [61](#)
- worm [34](#)
- Write-behind Delay [23](#), [24](#)

Y

- Y2Kfixer.com [61](#)
- Year 2000 (Y2K)
 - dates tested and why [61](#)
 - deadline-driven problem [58](#), [59](#)
 - definition of problem [58](#)
 - testing your system [62](#)
 - why computers fail the transition [59](#)
- Year 2000 Checker [58–64](#)