Whether you work on a desktop, a workstation, or a notebook, at home, in the office, or school, there is always the risk of your computer being infected by a computer virus. Some computer viruses are harmless and don't corrupt any of your data. However, more and more viruses contain destructive routines that, when activated, cause irreversible damage to your computer system, including destroying all of the information on your hard disk.

PC-cillin 97 is the ideal solution for protecting your system from the harmful affects of a computer virus attack. PC-cillin 97 incorporates advanced anti-virus technology, including powerful features such as 32-bit processing, on-line protection, and protected mode real-time scanning. Which simply means, PC-cillin 97 will find those viruses, before they find you.

See Also

Features and Benefits

What Is PC-cillin 97?

Why You Need PC-cillin 97

PC-cillin 97 is an anti-virus utility that provides a complete system of virus protection features that are specifically designed to protect Windows systems from new virus sources and increasingly sophisticated types of viruses. PC-cillin 97 constantly monitors all potential virus sources to trap viruses before they can infect a system.

PC-cillin 97's SmartMonitor™ automatically adjusts protection levels, detects and eliminates unknown viruses, scans Internet transfers and e-mail attached files, and keeps your virus protection up-to-date with easy, one-button virus pattern updates.

The emergence of macro viruses, found in Microsoft Word and Excel documents, has created an increased threat with the proliferation of e-mail to send files. If not detected, these new virus strains have been known to infect an entire network in less than an hour. This can be avoided with continuous, powerful protection. PC-cillin 97 maximizes protection for Windows 95 and on-line services without compromising speed or ease of use.

See Also

Features and Benefits

Why You Need PC-cillin 97

Automatic, On-line Pattern Updates

Up-to-the-Minute Virus Protection: Keeping your virus pattern file up-to-date is the key to detecting and cleaning many of the newest viruses. Now PC-cillin 97 does this updating for you automatically by downloading the latest virus pattern files as they become available. PC-cillin 97 keeps your protection current 24 hours a day!

Clean Wizard -- Your Built-in Virus Expert:

Automatic virus removal! Every time PC-cillin 97 nabs a virus, our one-of-a-kind Clean Wizard instantly springs into action to automatically remove the virus for you step-by-step, without harming your valuable data. It's the virus expert so you don't have to be.

MacroTrap -- The Only True Macro Virus Defense:

New macro viruses are being created at a blinding pace. Not only are they extremely difficult to catch before they cause damage, but they can be produced in a matter of minutes by practically anyone. PC-cillin 97 blocks macro viruses before they have a chance to infect your system. Plus, our patented MacroTrap not only detects and cleans known macro viruses, but will even catch new strains that have yet to be identified.

On-line Protection -- Stops the Cyberspace Virus Invasion:

Thousands of viruses are lurking throughout the Internet, just waiting to infect your computer. But have no fear PC-cillin 97 stops them cold!

- Scans all Internet and on-line service downloads
- Checks incoming e-mail and attached files
- Scans more types of compressed files than any other anti-virus

Since so much information is stored and accessed through computers, new viruses are a constant threat. Network connections, file sharing, and computer-to-computer file transfers bring a variety of infection possibilities. The emergence of macro viruses has created an increased threat of infection for any system sharing documents over the Internet or e-mail.

Viruses are programs designed to replicate and damage your computer system without your knowledge or permission. A virus may attach itself to another program or to the partition table and boot sector of your hard disk. A virus will wait for a certain event before executing its programmed routine.

A virus may be categorized by the type of damage it does. Some so-called “viruses” are actually harmless; they may only show a message on the screen or change the colors. A malicious virus, on the other hand, will destroy data once it is activated. It may format your hard drive or secretly change the values in a database file.

The two main transmission mediums for viruses are; electronic networks (i.e., Bulletin Board Systems), and files and software exchanged on disk or tape. Be on alert anytime you use a modem to download files, put new software or files on your computer, or open an e-mail attached file. Keep PC-cillin 97 active to scan the new files for viruses.

One characteristic of most successful viruses is that they do not immediately begin destroying data. This behavior, called “dormancy,” is necessary for long-term survival. While these viruses are dormant, they scan events, such as the system date, or user behavior (such as the number of keystrokes entered), then activate when certain conditions are met. This set of conditions is called the “catalyst.”

Avoiding the catalyst is not a good way to avoid a virus. Even if you manage to dodge it once, you will likely have the same conditions again in the future. You still need to find and remove the virus.

Boot Sector Viruses

The boot sector is the portion of a hard or floppy disk that controls how your operating system starts when you turn on your computer. When you start your computer, it tries to read the boot sector in your A: drive (if the startup can't read the A: drive, it moves to the C: drive). A boot sector virus replaces the disk's original boot sector with its own and loads the virus into memory. Once in memory, the virus can easily spread to other disks.

Macro Viruses

A macro virus originates in documents or spreadsheets made in applications that use macros to perform tasks, such as Microsoft Word, Microsoft Excel, and Lotus AmiPro. Macro viruses can cross platforms, meaning a virus created on an IBM compatible system can infect a Macintosh and vice versa.

Macro viruses are capable of renaming, deleting, or altering the content of files. This widespread virus type is the newest and fastest growing threat to your computer.

File Viruses

This type of virus attaches to executable files, such as .COM, .EXE, .SYS, or .DLL programs. When the "host" file is run, the file virus will either infect other executable files or install itself into memory and interfere with other memory-resident programs. In Windows 95, opening a DOS application can cause a file virus to activate. Many file viruses are written specifically to run under 32-bit operating systems like Windows 95.

Computer viruses fall into two categories; known viruses and unknown viruses. PC-cillin 97 detects and removes both known and unknown viruses on your computer.

A known virus is one that has been identified. Once identified, statistics about the virus (virus signature) are stored in a virus pattern (definitions) file. When PC-cillin 97 scans your disks and files, it searches your files for these signatures. If a file is infected with one of these viruses, PC-cillin 97 walks you through the process of destroying it.

When a new virus is discovered, its virus definition (signature) must be added to the virus pattern file. For this reason, you should update your virus pattern file regularly. This added protection provides you with necessary information to find all known viruses.

An unknown virus is one that has not been discovered and therefore does not yet have a virus definition.

PC-cillin 97 looks for programs that have been modified without your knowledge. PC-cillin 97 detects unknown viruses by constantly monitoring activity on your system for behaviors that viruses usually perform when replicating or attempting to damage your files. When a suspect activity is detected, PC-cillin 97 stops the program from running and initiates corrective action.

When you install PC-cillin 97 and accept the preset (default) options, your computer is safe. As part of the installation, your startup disk is scanned for viruses. After installation, the SmartMonitor's smart protection features provide you with constant protection while you work. The SmartMonitor checks programs for viruses when they are being used. If a virus is found, PC-cillin 97's "Clean Wizard" walks you through the removal process.

Listed below are some common questions that pertain to where viruses can hide:

CMOS Memory

Q: Can a virus hide in a PC's CMOS memory?

A: No. The CMOS RAM in which system information is stored and backed up by batteries is ported, not addressable. That is, in order to get anything out, you use I/O instructions. Anything stored there is not directly sitting in memory. Nothing in a normal machine loads the data from there and executes it, so a virus that "hid" in the CMOS RAM would still have to infect an executable object of some kind in order to load and execute whatever it had written to CMOS. A malicious virus can of course alter values in the CMOS as part of its payload, but it cannot spread through or hide in the CMOS.

Extended or Expanded RAM

Q: Can a virus hide in Extended or Expanded RAM?

A: Theoretically yes, although no such viruses are known yet. However, even if they are created, they must partly resident in conventional RAM; they cannot reside entirely in Extended or Expanded RAM.

Upper or High Memory

Q: Can a virus hide in Upper or High Memory?

A: Yes, it is possible to construct a virus that resides in Upper Memory (640K to 1024K) or High Memory (1024K to 1088K). A few currently known viruses (e.g., EDV) do hide in Upper Memory.

It might be thought that there is no point in scanning in these areas for any viruses other than those that are specifically known to inhabit them. However, there are cases when even ordinary viruses can be found in Upper Memory. Suppose that a conventional memory-resident virus infects a TSR program and this program is loaded high by the user (for instance, from AUTOEXEC.BAT). Then the virus code will also reside in Upper Memory. Therefore, an effective scanner must be able to scan this part of memory for viruses, too.

Listed below are some common questions that pertain to what components of your computer can be infected by a virus:

Infecting Windows 95

Q: Can DOS and Windows 3.1 viruses infect a Windows 95 system?

A: Yes. Currently about 70-80% of the existing DOS and Windows 3.1 virus can infect Windows 95 system.

Infecting Non-Bootable Disks

Q: Can boot sector viruses infect non-bootable floppy disks?

A: Any diskette that has been properly formatted contains an executable program in the boot sector. If the diskette is not "bootable," all that the boot sector does is print a message like *"Non-system disk or disk error; replace and strike any key when ready,"* but it's still executable and still vulnerable to infection. If you accidentally turn on your machine with a "non-bootable" diskette in the drive, and see that message, it means that any boot virus that may have been on that diskette has run and had the chance to infect your computer. So when thinking about viruses, the word "bootable" or "non-bootable" is really misleading. All formatted diskettes are capable of carrying a virus.

Infecting Data Files

Q: Can a virus infect data files?

A: Some viruses (e.g., Frodo, Cinderella, DataCrime) modify non-executable files. However, in order to spread, the virus must be executed. Therefore, the "infected" non-executable files cannot be sources of further infection.

Note that it is not always possible to make a sharp distinction between executable and non-executable files. One person's code is another person's data and vice versa. Some files that are not directly executable contain code or data that can, under some conditions, be executed or interpreted.

Some examples from the PC world are OBJ files, libraries, device drivers, source files for any compiler or interpreter, macro files for some packages like MS Word and Lotus 1-2-3, and many others. Currently, there are viruses that infect boot sectors, master boot records, COM files, EXE files, BAT files, and device drivers, although any of the objects mentioned above can theoretically be used as an infection carrier. PostScript files can also be used to carry a virus, although no known viruses that currently do so.

Infecting Cross Platforms

Q: Can viruses spread from one type of computer to another (e.g., from a PC to

a Mac)?

A: The simple answer is that no currently known virus can do this. Although the disk formats may be the same (e.g., Atari ST and DOS), the machines interpret the code differently. For example, the Stoned virus cannot infect an Atari ST as the ST cannot execute the virus code in the boot sector. The Stoned virus contains instructions for the 80x86 family of CPUs, which the 680x0-family CPU (Atari ST) can't understand or execute.

The more general answer is that such viruses are possible, but unlikely. Such a virus would be quite a bit larger than current viruses and might well be easier to find. Additionally, the low incidence of cross-machine sharing of software means that any such virus would be unlikely to spread -- it would be a poor environment for virus growth.

Running on Non-DOS Machines

Q: Can DOS viruses run on non-DOS machines (e.g., Mac, Amiga)?

A: In general, no. However, on machines running DOS emulators (either hardware or software based), DOS viruses, just like any DOS program, may function. These viruses would be subject to the file access controls of the host operating system. An example is when running a DOS emulator such as VP/ix under a 386 UNIX environment, DOS programs are not permitted access to files that the host UNIX system does not allow them to. Thus, it is important to administer these systems carefully.

Infecting Mainframe Computers

Q: Can mainframe computers be susceptible to computer viruses?

A: Yes. Numerous experiments have shown that computer viruses spread very quickly and effectively on mainframe systems. However, to our knowledge, no non-research computer virus has been seen on mainframe systems. (The Internet worm of November 1988 was not a computer virus by most definitions, although it had some virus-like characteristics.) Computer viruses are actually a special case of something else called "malicious logic," and other forms of malicious logic -- notably Trojan horses -- are far quicker, more effective, and harder to detect than computer viruses. Nevertheless, on personal computers, many more viruses are written than Trojans. There are two reasons for this: (1) Since a virus propagates, the number of users to which damage can be caused is much greater than in the case of a Trojan; (2) It's almost impossible to trace the source of a virus since it's not attached to any particular program.

DOS Viruses Working Under Windows

Q: Can normal DOS viruses work under MS Windows?

A: Most of them cannot. A system that runs exclusively MS Windows is, in general, more virus-resident. Viruses are not compatible with the memory management in Windows. Furthermore, most of the existing viruses will damage

the Windows applications if they try to infect them as normal EXE files. The damaged applications will stop working and this will alert the user that something is wrong.

Don't mistake being virus-resistant for being virus-proof, though. For instance, most of the well-behaved resident viruses that infect only .COM files (Cascade is an excellent example) will work perfectly in a DOS window. All non-resident COM infectors will be able to run and infect, too. And currently there exists at least one Windows-specific virus that is able to properly infect Windows applications (it is compatible with the new EXE file format). This virus is named WNVIR14.

Any low level trapping of Interrupt 13, as by resident boot sector and MBR viruses, can also affect Windows operations, particularly if protected disk access (32BitDiskAccess=ON in SYSTEM.INI) is used.

It's impossible to give an exact number because five to seven new viruses are literally created every day. Furthermore, different anti-virus researchers use different criteria to decide whether two viruses are different or the same. Some count viruses as different if they differ by at least one bit in their non-variable code. Others group the viruses in families and do not count the closely related variants in one family as different viruses.

Making a rough estimate, as of summer of 1997, there were about approximately 20,000+ IBM PC viruses, about 150 Amiga viruses, about 100+ Macintosh viruses, about a dozen Acorn Archimedes viruses, several Atari ST viruses, and a few Apple II viruses.

However, very few of the existing viruses are widespread. For instance, only about three dozen of the known IBM PC viruses are causing most of the reported infections. The virus that most people are concerned about the "in the wild virus" or "common virus."

This is a very complex issue. Most viruses don't spread very quickly. Those that do spread widely are able to do so for a variety of reasons. A large target population (i.e., millions of compatible computers) helps. A large virus population helps. Vendors whose quality assurance mechanisms rely on, for example, outdated scanners help. Users who insert new software into their systems without making any attempt to test for viruses help. All of these things are factors.

Word macro viruses spread quickly due to the fact that many people share .DOC files throughout an organization on a network or by e-mail.

There are a few quick and easy things you should do from time to time, especially right after installing PC-cillin 97:

Update the Virus Pattern File

Because virus pattern files are constantly being updated to accommodate newly created viruses, the pattern file that you installed with PC-cillin 97 is already out of date. This does NOT mean that you are not protected from virus infections. It merely means that some new viruses may have come on the scene since PC-cillin 97 was shipped and, to get the most effective protection against those viruses, you need a new pattern file. For more information on updating your virus pattern file, see Updating via the Internet, Modem, or Floppy.

Scan All Local Drives

It's always a good idea to periodically scan the local drives on your computer, especially after you update your virus pattern file. PC-cillin 97 will catch viruses when you activate them (e.g., opening the file that they are attached to). But, to be safe, we highly recommend performing the scan. For more information on scanning your local drives, see Using the Scan Tab.

To provide continuous protection against infection, the SmartMonitor maintains a constant watch for virus-like activity. It monitors every action that occurs on your computer and, when something suspect appears to happen (like a virus activating), PC-cillin 97 pounces.

To start the SmartMonitor

There are two ways to access the SmartMonitor:

1. **Choose the PC-cillin 97 SmartMonitor command from the Start menu. By default, this command is under the PC-cillin 97 group under Programs in the Start menu.**
2. **Double-click PC-cillin 97's application icon on the taskbar (a red ball with a yellow lightning bolt in the system tray). Another related way of opening PC-cillin 97 is right-clicking on icon in the taskbar, then choosing the Show SmartMonitor command.**

See Also

PC-cillin 97's SmartMonitor

Exclusion List for the SmartMonitor

Monitoring Options for the SmartMonitor

Virus Found Action for the SmartMonitor

PC-cillin 97's SmartMonitor automatically adjusts protection levels, detects and eliminates unknown viruses, and keeps your virus protection up-to-date with easy, one-button virus pattern updates.

What this means is files are scanned for viruses before they are executed, copied, saved, or created. The SmartMonitor performs virus scans in the background without affecting normal operations. If a virus is detected, PC-cillin 97 stops the virus before it can do any harm.

The SmartMonitor window contains the following elements:

Monitored Threats

This sections displays a list of potential areas where a virus can enter your system from. If the "light" next to a specific area appears, the SmartMonitor is paying particular attention to this potential virus gateway.

Virus Pattern File

This section displays the current version of your virus pattern file and its creation date. Updating allows you to detect and clean the newest viruses as well as updating the types of files to be scanned.

Buttons

- **Scan Now:** Scans all the local drives on your computer.
- **Main**: Exits the SmartMonitor and displays the main program window.
- **Options:** Accesses an options screen where you can configure how the SmartMonitor detects viruses and what to do if an infection if found.
- **Update:** The Update button gives you access to the Update Options tab where you can download or copy the latest virus pattern files. For more information on updating your virus pattern files, see Updating via the Internet, Modem, or Floppy .
- **Help**: Displays on-line help for the SmartMonitor.
- **Unload**: Unloads PC-cillin 97, removing the SmartMonitor from the taskbar and disabling your protection.
- **Minimize**: Returns the SmartMonitor to the taskbar. The SmartMonitor continues to guard your system against viruses when minimized.

See Also

Exclusion List for the SmartMonitor

Monitoring Options for the SmartMonitor

Virus Found Action for the SmartMonitor

Why Is the SmartMonitor Important?

The Monitoring tab allows you to specify how and where the SmartMonitor checks your computer for viruses.

System Startup

- **System Startup Scan -** Scans the boot sector and partition table when the program loads, which should be when you start Windows.
- **Enable Screen Saver Scan -** Activates the screen saver scan that runs when, as you might have guessed, your screen saver is on.
- **Enable Floppy Shutdown Scan -** Initiates a scan of any diskette that is in the A: drive. This feature is especially important if you are booting from a floppy (you want to make sure that floppy is not infected). Otherwise, the next time you boot your system from that floppy, you will be infected.

Monitor Mode

Specify which files you want the SmartMonitor to check – all files or only the extensions listed in the Program File Extensions dialog (selected by default because it covers all currently known file types that are attacked by viruses).

Select the *Monitor All Files* check box to have PC-cillin 97 monitor every file you access on your computer. While this method may be the safest, it also increases system overhead (meaning your system runs slightly slower).

Deny File Modification

Denies access to a specified folder/sub-folder. This eliminates the possibility of writing a virus infected file into a particular folder and/or sub-folder by denying access to that folder/sub-folder. Choose the **Selected Folder** button to designate which folder and/or sub-folder you want to deny access to.

Advanced Monitoring

Determines which preventative actions to take based on the selections made in this group box. For example, if you only want PC-cillin 97 to scan executable and compressed files, select the appropriate check boxes.

Select the Use advanced settings checkbox to enable the advanced options, then select the ones you want:

- **Floppy Boot Sector** - monitors for viruses in the boot sector of a floppy disk you access
- **Execute Program** - monitors for viruses in executable programs only
- **File is Opened** - monitors for viruses when you open a file

- **File is Created** - monitors for viruses when you create a new file
- **Scan Archived Files** - monitors for viruses in compressed files

Show

Using the corresponding three checkboxes, you can decide whether or not to display the MacroTrap splash screen, Internet splash screen, and Unload confirmation. Two reasons you would consider removing these screens are that it saves a tiny amount of time when loading and, if you are frequently opening applications that activate these features, the screens can become annoying.

See Also

PC-cillin 97's SmartMonitor

Why Is the SmartMonitor Important?

By default, PC-cillin 97 scans .BIN, .COM, .DOC, .DOT, .DRV, .EXE, .OVL, .SYS, and .XLS files and .CLASS, .CLA (java class) files. You can use the Program File Extensions dialog box to add, delete or accept the default program file type extensions.

To Add Program File Extensions

1. **Click the Add button. The Add Program File Extension dialog appears.**
2. **Type the three-character file extension in the Extension to add text box.**
3. **To abort adding the program file type, click the Cancel button. To add the program file type, click the OK button. Control returns to the Program File Extension dialog box.**
4. **Click the OK button to confirm your selections.**

To Delete Program File Extensions

1. **Select the file type extension(s) you want to delete.**
2. **Click the Delete button. The selected file types are removed from the list.**
3. **To confirm the deletion, click the OK button.**

NOTE: The next time PC-cillin 97 scans your computer, the deleted program file extension is excluded from the scanning session. There must be at least one extension present for the scan to operate.

To Return to the Default Settings

1. **Click on the Default button.**
2. **Click on the OK button.**

This dialog, which is accessible via the Program File Extensions dialog in the Monitoring tab (part of the SmartMonitor options), lets you add a file type to PC-cillin 97's automatic scanning routine.

To Add a File Type

1. **Type in the three-character extension of the file type in the Extension to add field (for example, to add document files, type in "DOC"). No period is necessary before the extension (i.e. ".DOC").**
2. **Click on the OK button to accept the extension. To abort adding the program file type, click the Cancel button.**

When a virus is discovered, there are several courses of action you can take. You can delete, deny access and continue, rename, or move an infected file. An action is what you tell PC-cillin 97 to do with the infected file once it is found. The following actions are available:

Clean Infected Files Automatically

Selected by default, this option will attempt to clean infected files automatically (i.e. without user intervention), then inform you about the infection after it has been handled.

Deleting an Infected File

Deleting an infected file is the best option if the infected file is not important or if a clean backup is available. Since the virus is attached to the infected file, deleting the infected file will also delete the virus.

> **NOTE:** If a clean backup file is available, it is better to just delete the infected file. This is because viruses can damage parts of a file; using the clean backup would be much better than trying to clean the file.

Deny Access to the Infected Files and Continue

If Deny Access to the Infected Files and Continue is selected as the action, PC-cillin 97 will block any attempted access to the infected file, then continue the current process (for example, copying or opening the file). Any workstation with access to the file may be exposed to the virus. This can cause every server and workstation on a network to become infected. We recommend not using the Continue option unless you are sure that PC-cillin 97 scans are running across a series of false positives.

> **NOTE:** A false positive is when PC-cillin 97 thinks it is catching viruses when in fact it is just catching a lucrative pattern string in a file. False positives rarely occur, but one thing that occasionally turns up as virus activity is when a programmer compiles code. Any process that changes the size of an executable file (which is a common virus behavior) will cause a false positive.

Renaming an Infected File

Renaming an infected file is useful when you want to distinguish an infected file from other files within your directory or when you want to stop the infected file from executing and spreading the virus.

Renaming can also create a backup of the original file when you want to try to clean the original. When you rename an infected file, PC-cillin 97 changes the file's extension to .RB1 (unless you provide a different extension). If other files with the same name are infected, PC-cillin 97 assigns sequential extensions such

as .RB2, .RB3, etc.

WARNING! The renamed file is no longer executable unless you revert back to the original file extension (e.g. program.**rb1** back to program.**exe**).

Moving an Infected File

PC-cillin 97 defines a quarantine directory where all infected files can be moved. The default directory is **[PC-cillin 97's root]\VIRUS**. This directory is safe if the files within it are not opened or manipulated in any way. However, like renaming an infected file, this option should be considered a temporary solution to ridding your computer of a virus- the idea being that you hold onto the file until you can decide what do with it.

See Also

PC-cillin 97's SmartMonitor

Why Is the SmartMonitor Important?

Using the Exclusion tab, you can exclude certain directories from PC-cillin 97's scan. One reason to exclude a directory is if it contains something that yields a lot of Virus Found hits (for example, if you use the Move infected files to option under the Virus Found Action tab, there will be a directory that contains all the viruses that infect your computer).

To Add a Directory

1. **Click on the Add button.**
2. **On the Browse window that appears, select the proper directory. If a directory contains subdirectories, they will be excluded as well.**
3. **Click the OK button**

To Remove a Directory

1. **Choose a directory from the exclusion list.**
2. **Click on the Remove button.**

See Also

PC-cillin 97's SmartMonitor

Why Is the SmartMonitor Important?

When you open PC-cillin 97's main program, the Scan tab is displayed.

The left side of the window displays the drive/folder tree listing that shows all the current drives/folders accessible by your computer. To select a drive/folder, click on the box next to the drive/folder name (selected drives/folders place a check mark in the box). Selecting a drive or folder also selects any existing sub-folders. To expand or compress the tree listing, click on the + (to expand) or - (to compress) sign.

The window also includes the following items:

- **Scan Now Button -** Starts scanning the selected drives/folders.
- **Options Button -** Opens an options screen where you can configure scanning options for your computer.
- **Refresh Button -** Clears the drive tree listing.
- **Last Full Local Scan -** Tracks the date and time that the last full scan occurred on your local drives.
- **Help Button -** Displays on-line help for the current item.
- **Exit Button -** Removes the current window from your desktop.
- **Quick Scan (Boot & Root Area) -** Scans memory, the boot sector, and the root directory (usually the C: drive).
- **All Local Drives in My Computer -** Scans all the local drives on your computer.
- **All Network Drives in My Computer -** Scans all the network drives on your computer.

Scanning a Drive

From the Scan tab, choose a drive/folder to scan. Be advised, depending on the size and number of drives on your computer, a scan of all your local drives may take a while.

Click the **Scan Drives** button to initiate the scan. The Scanner Report window appears informing you of the progression of the scan.

To Pause Scanning

1. **From the Scanner Report window, click the Pause button. This temporarily stops the scanning process.**
2. **To reactivate the scanning process, click the Continue button.**

To Stop Scanning

1. **From the Scanner Report window, click the Stop button.**

This action displays the *Do you want to stop the scan process?* message box.

2. **To continue scanning, click the No button. To halt the scanning session, click the Yes button.**

Scanning a Folder

1. **Drag and drop the folder onto the Scan tab. Or, choose Scan Page from the File menu.**
2. **To select every folder on a particular drive, double-click the drive(s) box you want to scan.**
3. **If necessary, you can de-select a folder within a folder. Expand the selected drive list by clicking the + sign (selected folders will have a check mark placed next to them).**
4. **Click the folder(s) you do not want to scan (clicking the folder(s) removes the check mark).**

See Also

Setting Scanning Options for the Main Program

Scheduling Scans on a Daily, Weekly, Monthly Basis

Windows Explorer Scanning

Using the SmartMonitor

In Windows Explorer, you can scan any drive, folder, or file by right-clicking the item you want to scan, then choosing the PC-cillin 97 command from the pop-up menu that appears. This action scans every file within a selected drive or folder. You can select multiple folders.

Clicking the **Scan Now** button on the SmartMonitor causes PC-cillin 97 to load the main program and automatically scan all the local drives on your computer.

You can fine-tune the way PC-cillin 97 scans your system to increase system security, reduce scanning time, and perform specific tasks. Certain options can be configured for the Virus Scanner -- for example, you can:

- scan the partition table and boot sector of your PC
- scan archived/compressed files
- scan all files
- scan specific files
- create a scan report
- view a scanned report
- select a word processor to view a report in

PC-cillin 97's default settings scan the boot area, every file (including compressed files) on your computer, and generates a scan report automatically. However, you can modify these default settings to fit your needs.

PC-cillin 97's Prescheduled Scan feature allows you to automate your scanning activities by selecting the scan destination, types of files, and the date, time and frequency for automatic scanning on your computer.

IMPORTANT: You can also schedule virus pattern updates from this screen. For more information, see Scheduling Daily, Weekly, or Monthly Updates.

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

To Schedule a Scan

1. **Choose Preschedule Options from the Options menu.**
2. **Or, from the Scan tab, click the Options button. The Options dialog box appears.**
3. **Click the Preschedule tab. The Preschedule page appears.**
4. **Type or select how often you want the scan to occur in the Frequency drop-down list box.**
5. **Type in or click the arrow button(s) to select the time in the hour/minute text boxes.**
6. **To scan on a weekly basis, select the day of the week in the Day of Month text box.**
7. **Or, to scan on a monthly basis, select the day of the week in the Day of Month text box.**
8. **Click the Select Drives to Scan button. The PreSchedule Browser dialog box appears.**
9. **Choose the drive(s) you want to scan.**
10. **To accept the selections made, click the OK button. Control returns to the Preschedule page.**
11. **To complete the scheduled event, click the OK button in the Preschedule page.**

    NOTE: Preschedule Options must be set and active before scheduled scans can run.

If a virus is discovered during an automatic scan performed by the SmartMonitor, a Virus Found warning message appears.

PC-cillin 97 will attempt to clean all the files it can on its own, then notify you of the infection. If there are any viruses that could not be cleaned, you should click on the **Clean Options** button, which will take you to PC-cillin 97's Clean Wizard. When you are done reviewing the list, click on the **OK** button to exit the window.

See Also

Dealing with Viruses from the Clean Tab

When PC-cillin 97 detects a virus during a manual scan performed from the main program, a Virus Found warning message appears.

At this point, you have two options -- go to the Clean tab (recommended for more-experienced users) or automatically clean the infected files.

To automatically clean the virus-infected file(s), click on the **Auto Clean Files** button.

If, during the automatic cleaning, an uncleanable file or one that requires special handling arises, PC-cillin 97 will display its Clean Wizard, which steps you through the entire process of cleaning and removing the virus(es) from your computer. To go to the Clean tab, click on the **Clean Options** button. For more information, see the next section Dealing with Viruses from the Clean Tab.

See Also

Dealing with Viruses from the Clean Tab

PC-cillin 97 offers you three methods in which to remove a virus: delete the infected file(s), rename the infected file(s), or clean the infected file(s). As you perform an action on a virus, that virus is removed from the list. When you have deleted, renamed, and cleaned all the detected viruses, the list box will be empty.

PC-cillin 97 includes a cleaning engine that attempts to remove the virus from an infected file, leaving the original file undamaged. However, some viruses damage files during the infection process. Therefore, you cannot safely clean some files.

When you select **OK**, PC-cillin 97 will begin cleaning the file(s). If the cleaning was successful, the file(s) will be removed from the infected files list box. However, if the cleaning was not successful, you will receive a warning prompt. At this point, you must delete or rename the infected file because it cannot be cleaned.

For less-experienced users, we highly recommend using the Clean Wizard, which is accessible by clicking on the **Clean Wizard** button. The Clean Wizard will lead you step by step through the process of getting rid of a virus.

To display a log of all the cleaning processes that have occurred, click on the **View Log** button.

Cleaning a virus-infected file “removes” the virus from the original file, leaving the original file undamaged. PC-cillin 97 includes a cleaning engine that attempts to remove the virus from the infected file leaving the original file intact (undamaged). However, some viruses damage files during the infection process; therefore, some files cannot be safely cleaned.

To Clean an Infected File

1. **From the Clean tab, under the Infected File Name list box, select the file(s) you want to clean.**
2. **Click the Clean button. The Clean 1 File(s) message box appears.**
3. **To abort cleaning the infected file(s), click the Cancel button. To clean the infected file(s), click the OK button.**
4. **If the cleaning operation is successful, the 1 file(s) have been cleaned message box appears.**
5. **To continue, click the OK button. PC-cillin 97 will begin cleaning the file(s). The file(s) are cleaned and removed from the infected files list box.**
6. **If the cleaning was successful, the file(s) will be removed from the infected files list box. However, if the cleaning was not successful, you will receive a warning prompt. At this point, you must delete or rename the infected file because the file cannot be cleaned.**

   WARNING!: Even if PC-cillin 97 "successfully" cleans an infected file, you should test the file before using it. The virus may have damaged the file in ways that PC-cillin 97 could not detect.

Deleting a virus infected file results in the virus, and the infected file, being deleted. This is the safest way to kill a virus, but it also destroys the infected file. However, if you have backups of the original file (or you can re-install the file), then using Delete is the best measure. If you can restore the infected file from a backup or installation disk, make sure that those disks are not infected, too. Otherwise, you'll just be loading the virus back onto your computer.

To Delete an Infected File

1. **From the Clean tab, under the Infected File Name list box, select the file(s) you want to delete.**
2. **Click the Delete button. The Delete 1 file(s) message box appears.**
3. **To abort deleting the infected file(s), click the Cancel button. To delete the infected file(s), click the OK button. If the deletion operation is successful, the 1 file(s) have been deleted message box appears.**
4. **To continue, click the OK button. The file(s) are removed from the source (i.e., floppy disk, etc.) and the infected files list box.**
5. **To continue, click the OK button.**

Control returns to the Clean tab.

Renaming an infected file is only a temporary measure—it does not clean the virus; it simply changes the filename so that the file cannot execute. If you select this action, the file will be renamed with a .VIR extension (i.e., test.exe becomes test.vir). However, if the same filename already exists with the .VIR extension, the filename is renamed with a .VR2 extension (i.e., test.**com** becomes test.**vr2**).

PC-cillin 97 does not limit you on the total number of files that can be renamed, but you are limited to renaming the same filename up to 10 times.

To Rename an Infected File

1. **From the Clean tab, under the Infected File Name list box, select the file you want to rename.**
2. **Click the Rename button. The Rename 1 File(s) message box appears. To abort renaming the infected file, click the Cancel button. To rename the infected file, click the OK button.**
3. **To rename additional files, repeats steps 1 and 2 above.**
4. **If the rename operation is successful, a message box appears telling you what the filename is. To continue, click the OK button. The renamed file is displayed in the infected files list box.**
5. **If the rename operation is not successful, a message box appears telling you there is a Rename error! To continue, click the OK button. The 0 file(s) have been renamed to xxxxxx.vir message box appears.**
6. **To continue, click the OK button. Control returns to the Clean tab.**

PC-cillin 97's Clean Wizard is designed for those who have never dealt with a computer virus. The Clean Wizard steps you through the entire process of cleaning and removing viruses from your system using the safest method possible.

To access the Clean Wizard, choose the **Clean Wizard** button from the Clean tab. To accommodate the different types of virus infections, there are variations in the Clean Wizard process:

- viruses that can be cleaned
- boot viruses

See Also

Eliminating Viruses That Can Be Cleaned

Removing Boot Sector Viruses

1. **Choose the Clean Wizard button from the Clean tab. The Welcome window appears.**

   The file name(s), type of virus, and relevant virus information are displayed.

2. **To continue the cleaning procedure, click the Next button.**

   After PC-cillin 97 acknowledges all of the infected files, the Ask for Cleaning window appears.

3. **To clean the virus from the file(s), click the Next button. The bar graph displays the progress of the cleaning procedure. PC-cillin 97 automatically backs up and renames the files in case you need to re-use them. Backup files have an RB0 extension.**

4. **When the cleaning procedure is completed, the Send E-Mail window appears. When you share your files with other users, the potential for re-infection by the same virus is very high. Therefore, we recommend either printing or sending an e-mail message to those people you share files with as a preventative measure to keep from re-infecting your computer with the same virus.**

5. **To send an e-mail message, click the Send E-Mail button. The Choose Profile dialog box appears. To accept the MS Exchange default setting, click the OK button.**

6. **To choose another profile, click the New button. For assistance on how to proceed from here, refer to your Windows documentation.**

7. **To print the virus information, click the Print It button. The print dialog box appears.**

8. **To complete the cleaning procedure, click the Finish button.**

   If you are cleaning more than one virus, PC-cillin 97 returns you to the Welcome window. Repeat steps 2 through 6. When PC-cillin 97 is finished cleaning the virus(es) from the file(s), the Scan Disk window appears.

   The Scan Disk window gives you the option of scanning your hard drive(s). We recommend scanning your local drives right away to ensure that no other files have been infected.

9. **To scan your hard drive(s) at a later time, select the *No, I will do it later* check box. Or, to scan your hard drive(s) now, select the *Yes, scan my local hard drive* check box.**

10. **The Scanner Report window appears displaying the progression of the scan. When the scanning session is completed, the Floppy window appears.**

NOTE: Floppy disks are carriers of computer viruses that can infect your system. For this reason, we strongly recommend that you scan any floppy diskettes you are currently working with. If you exclude this step, there is a good possibility you could re-infect your computer, especially if you re-use the floppy disk(s) that were initially infected.

---

11. **To scan your floppy disk(s), insert the questionable floppy(ies) and select the appropriate drive letter in the *Select a drive* text box.**
12. **To continue, click the Next button.**
13. **To scan another floppy diskette, insert the floppy disk and click the Scan Next Floppy button.**
14. **When you are finished scanning floppy disks, click the** Next **button. The Good-Bye window appears.**

    The Good-Bye window gives you an opportunity to go back and scan additional floppy disks, view a virus report log file of viruses cleaned from your computer, or complete the clean up procedure and get back to work.
15. **To scan additional floppy disks, click the Back button.**
16. **To view a virus report log, click the View Clean Log File button. The virus report appears on your desktop and can be printed.**
17. **To close the virus report window, double-click the notepad icon in the upper left corner of the window.**
18. **To exit the Good-Bye window, click the Finish or Cancel button.**

NOTE: Virus(es) that were removed using the Clean Wizard are removed from the Clean tab.

As a reference, the file name(s), type of virus, and relevant virus information are displayed.

To continue the cleaning procedure, click the **Next** button.

After PC-cillin 97 acknowledges all of the infected files, the Ask for Cleaning window appears.

To clean the virus from the file(s), click the **Next** button. The bar graph displays the progress of the cleaning procedure.

> **NOTE:** PC-cillin 97 automatically backs up and renames the files in case you need to re-use them. Backup files have an RB0 extension.

When the cleaning procedure is completed, the Send E-Mail window appears.

When you use PC-cillin 97's Clean Wizard to remove detected viruses, you can send an e-mail message to anyone you share files with. When you share your files with other users, the potential for re-infection by the same virus is very high. Therefore, we recommend either printing or sending an e-mail message to those people you share files with as a preventative measure to keep from re-infecting your computer with the same virus.

To Send an E-mail Message

1. **Click the Send E-Mail button in the Send E-Mail window. The Choose Profile dialog box appears.**
2. **To accept the MS Exchange default setting, click the OK button. To choose another profile button, click the New button. For assistance on how to proceed from here, refer to your Windows documentation.**

To Print an E-mail Message

1. **Click the Print It button in the Send E-Mail window. The Print dialog box appears.**
2. **Choose the printer and select the number of copies you want to print.**
3. **Click the OK button to print the message.**

To complete the cleaning procedure, click the Finish button.

If you are cleaning more than one virus, PC-cillin 97 returns you to the Welcome window. When PC-cillin 97 is finished cleaning the virus(es) from the file(s), the Scan Disk window appears.

The Scan Disk window gives you the option of scanning your hard drive(s).

NOTE: We recommend scanning your local drives right away to ensure that no other files have been infected.

To scan your hard drive(s) at a later time, select the *No, I will do it later* check box. Or, to scan your hard drive(s) now, select the *Yes, scan my local hard drive* check box.

The Scanner Report window appears displaying the progression of the scan. When the scanning session is completed, the Floppy window appears.

Anytime you system becomes infected with a virus, you should scan your floppy disks, especially since they too are carriers of computer viruses that can infect your system. For this reason, we strongly recommend that you scan any floppy diskettes you are currently working with. If you exclude this step, there is a good possibility you could re-infect your computer, especially if you re-use the floppy disk(s) that were initially infected.

To Scan Your Floppy Disk(s)

1. **Insert the questionable floppy(s) and select the appropriate drive letter in the *Select a drive* text box.**
2. **To continue, click the Next button.**
3. **To scan another floppy diskette, insert the floppy disk and click the Scan Next Floppy button.**
4. **When you are finished scanning floppy disks, click the Next button. The Good-Bye window appears.**

The Good Bye window gives you an opportunity to view, save and print a log of viruses cleaned from your computer.

Otherwise, you can click on the **Finish** button to exit the Clean Wizard.

To View a Clean Log File

1. **Click the View Clean Log File button in the Good Bye window. A copy of the report appears on your desktop displaying the name(s), date and time the virus(es) were cleaned.**
2. **To print or save the report, choose the desired option from the File menu.**

1. **To move onto the Send E-mail window, click the Next button. Otherwise, to deal with the virus immediately, click on the Enter the Virus Lab Now button in the middle of the window.**
2. **The Check-Up Center in the Internet Virus Lab opens. Instructions on what to do with the uncleanable virus will be provided. Mostly, this entails sending Trend the virus using the Virus Doctor window.**
3. **Use the Virus Doctor window to upload the virus to Trend's Virus Doctor staff (for more information, see Internet Virus Doctor). If there are multiple viruses, they will be uploaded in a single batch, meaning you will not have to repeat this process for each one.**

This screen notifies you that a virus was detected in the system memory. To proceed to the Good-Bye window, where detailed instructions are provided for getting rid of the infection, click on the **Next** button.

To exit the Boot Wizard, click on the **Cancel** button.

Boot sector viruses are difficult to eliminate. Thus, they cannot be automatically cleaned. You must perform a simple process to rid your computer of the virus. This process is detailed on the Good-Bye window.

You should write down or print (using the **Print It** button) the provided instructions, then follow them. You will need an Emergency Clean Disk (this dosk came in your PC-cillin 97 package).

When you are finished, click on the **Finish** button.

To Remove a Boot Sector Virus

If You Have NOT Created a Bootable Emergency Clean Disk

1. **Turn off the PC (shut down Windows first).**
2. **Insert a write-protected system boot disk.**
3. **Turn on the PC.**
4. **Wait for a DOS prompt.**
5. **Eject your system boot disk.**
6. **Insert the Emergency Clean Disk.**
7. **Type in SCAN, then press the Enter key.**
8. **Follow the on-screen prompts.**

If You Have Created a Bootable Emergency Clean Disk

1. **Turn off the PC (shut down Windows first).**
2. **Insert the Emergency Clean Disk.**
3. **Turn on he PC.**

   NOTE: If the Emergency Clean Disk isn't bootable, follow the instructions under If You Have NOT Created a Bootable Emergency Clean Disk.

---

4. **Type in SCAN, then press the Enter key.**
5. **Follow the on-screen prompts.**

Using PC-cillin 97, boot sector viruses can be destroyed before they have an opportunity to infect your system. However, some boot sector viruses cannot be cleaned from within Windows 95.

If the boot sector on a floppy disk is infected, PC-cillin 97 displays a message box indicating the floppy drive and the name of the file infected. However, if the boot sector on your hard drive becomes infected, PC-cillin 97's Boot Wizard steps you through the process of removing it.

PC-cillin 97's Boot Wizard appears when a boot sector (memory) virus is detected while you are starting up Windows 95. If the boot sector on your hard drive becomes infected, Boot Wizard steps you through the process of removing it. Listed below are instructions for getting rid of a boot sector virus:

To Remove a Boot Sector Virus

If You Have NOT Created a Bootable Emergency Clean Disk

1. **Turn off the PC (shut down Windows first).**
2. **Insert a write-protected system boot disk.**
3. **Turn on the PC.**
4. **Wait for a DOS prompt.**
5. **Eject your system boot disk.**
6. **Insert the Emergency Clean Disk**
7. **Type in SCAN, then press the Enter key.**
8. **Follow the on-screen prompts.**

If You Have Created a Bootable Emergency Clean Disk

1. **Turn off the PC (shut down Windows first).**
2. **Insert the Emergency Clean Disk.**
3. **Turn on the PC.**

   NOTE: If the Emergency Clean Disk isn't bootable, follow the instructions under If You Have NOT Created a Bootable Emergency Clean Disk.

4. **Type in SCAN, then press the Enter key.**
5. **Follow the on-screen prompts.**

PC-cillin 97 uses a virus pattern file to detect known computer viruses. By regularly updating your pattern file, you enable PC-cillin 97 to detect the newest viruses.

To prevent newly discovered viruses from invading your computer, you should periodically update your pattern files. PC-cillin 97 uses the information in these virus pattern files to detect and eliminate viruses found during scans. When new viruses are found, their virus definitions are added to the virus pattern files. To ensure that you have maximum security against acquiring virus infections, we recommend updating your virus pattern file on a monthly basis.

See Also

Updating via the Internet, Modem, or Floppy

Setting Update Options

Scheduling Daily, Weekly, or Monthly Updates

You can perform two distinct functions from the Update Pattern tab:

- Update your virus pattern file via the internet, modem, or floppy.
- Register PC-cillin 97 on-line.

See Also

Updating via the Internet, Modem, or Floppy

Registering PC-cillin 97

PC-cillin 97 offers you three ways to update your virus pattern files. As a registered owner, you have around-the-clock access to PC-cillin 97's BBS or World Wide Web server on the Internet to download the latest virus pattern. Choose the one most convenient for you.

- **Internet:** Downloads the latest virus pattern file from the Internet. To use our World Wide Web site, be sure you have an account set up with a service provider before selecting this option.
- **Modem:** Downloads the latest virus pattern file from the BBS. You can download virus pattern files for free.
- **Floppy:** Copies the latest virus pattern file from a floppy diskette, which can be purchased from Trend.

To Update Your Virus Pattern File

1. **Choose Update Pattern Page from the File menu.**
2. **Or, select the Update Pattern tab from PC-cillin 97's main program window.**
3. **Select the update method you want--click either the Internet, Modem, or Floppy button. If you select the Internet or Modem options, it automatically connects to PC-cillin 97's World Wide Web service forum or BBS and quickly downloads the latest virus pattern update.**

The Update Pattern Status group box displays the status of the current update action, and the bar graph indicator shows how far along the update pattern routine has progressed in terms of a percentage of completion.

See Also

Setting Update Options

Scheduling Daily, Weekly, or Monthly Updates

PC-cillin 97 allows you to change the Comm Port, Baud Rate, Dial Method and Outside Line Access options for your modem. By default, PC-cillin 97 includes the Internet, BBS/Modem and BBS Configuration settings, along with the necessary User IDs and Passwords required in order to access PC-cillin 97's BBS or World Wide Web site, so you do not need to worry about setting these options, it's done for you.

To Change Modem Settings

1. **Choose Update Pattern Options from the Options menu.**
2. **Or, choose the Update Options tab from the Options dialog box. The Update Options page appears.**
3. **Select the Comm Port, Baud Rate, and Dial Method settings appropriate for your modem. If you are not sure which COM port your modem is on, select the Auto Detection option from the Comm. Port drop-down list.**
4. **If necessary, enter the number required to access an outside line (i.e., 9).**
5. **If you are dialing into Trend's BBS, you should not need to change the settings under the BBS Configuration section.**
6. **Do not touch the Internet Settings section unless you know what you are doing. It is meant for users of a corporate proxy server.**
7. **When you're finished, click the OK button.**

See Also

Updating via the Internet, Modem, or Floppy

You can schedule updates to your virus pattern file that can be downloaded automatically on specific dates and times. If you are using the computer when the scheduled update begins, it runs in the background so that you do not have to stop working.

To Schedule an Update

1. **Choose Preschedule Options from the Options menu. Or, from the Scan tab, click the Options button to display the Options dialog box, then select the Preschedule tab. The Preschedule tab appears.**
2. **On the right side of the screen, under Preschedule Pattern Update, select how often you want the scan to occur in the Frequency drop-down list: Every Day, Once A Week, or Once A Month.**
3. **In the hour/minute text boxes, enter the time or click the arrow button(s) to select the time you want the update to occur.**
4. **To update on a weekly basis, select which day of the week you want the update to occur. Or, to update on a monthly basis, in the Day of Month field, enter or select which day of the week you want the update to occur.**
5. **Choose method by which updates will be obtained by selecting either the Update Using Internet or Update Using BBS radio button.**
6. **When you are finished scheduling the update, click the OK button.**

If you are after an update to your virus pattern file, look for a file called "LPT$VPN" followed by a three-digit extension, which is the version of the file. The version numbers are sequential, meaning LPT$VPN.202 is newer than LPT$VPN.178.

Also, some files are self-extracting or self-installing. This means that when you download the file, you need to copy it to the PC-cillin 97 folder, then run extraction or installation process. You can do this through the Run command in the Start menu or by double-clicking on the file in Windows Explorer.

To download a file, click on its name, which is a link. The download will then commence. If you are downloading a self-extracting or self-installing file, you will need to provide a destination directory before the file is actually transmitted.

Be advised that depending on the speed of your modem or Internet connection and the size of the file, your download time may vary substantially.

PC-cillin 97 includes a database listing of all the viruses it recognizes (common, boot, or file). Each virus is listed by its more common name, with known aliases shown under the name. The virus encyclopedia also specifies the type of virus, the size of the virus code, the type of damage the virus causes, and the infection method of the virus.

To View Information About a Virus

1. **Choose Virus Information from the File menu.**
2. **Or, choose the Virus Information tab from PC-cillin 97's main program window. The Virus Information window appears.**
3. **From the Virus Type drop-down list, select the virus type you want information about.**
4. **Scroll through the Virus Name List and select the virus name you want information about. Information about the virus you selected appears in the Type of File Virus, Memory Resident Type and Description areas.**

To view a list of all the viruses that PC-cillin 97 detects, you can access its list of detectable viruses. To do so, click on the Detectable List command in the Help menu in the Main Program. The list appears. Boot viruses are displayed, followed by file viruses.

NOTE: When you take into account all the variations and mutations, the number of viruses that PC-cillin 97 actually detects far-exceeds what is listed.

- To save the list to a text file, click on the **Save as…** button. This opens a standard Windows save dialog.
- To print the list, click on the **Print** button
- To close the window, click on the **Close** button.

Creating an Emergency Clean Disk is an important part of virus protection. It stores critical system information and the programs necessary to start your computer. A clean disk is the only means to restore your computer's configuration from certain types of boot viruses.

> **NOTE:** You can create an Emergency Clean Disk at any time. We recommend making a clean disk whenever you update your virus pattern file. This way, you will have the most current version of the pattern file in the case of an especially harmful virus infection.

To Create an Emergency Clean Disk

To create an Emergency Clean Disk, you can use the Emergency Clean Disk that is provided in the PC-cillin 97 package (which we recommend) or a blank 3½-inch high density floppy disk. With a disk in hand, perform the following steps:

1. **Choose Create Emergency Clean Disk command line from the Start menu. By default, this command should be under the PC-cillin 97 group in the Program group. The following dialog box appears.**
2. **Insert the Emergency Clean Disk or blank 3½-inch high density diskette to selected target drive (A or B) and click Start. When the Emergency Clean Disk is successfully created, the Create Clean Disk message box appears.**
3. **Click the OK button to conclude the procedure.**
4. **Label the disk to identify the computer for which it was created along with the date the disk was made.**
5. **Write-protect the Emergency Clean Disk by adjusting the disk's write-protect tab in the corner, then store it in a safe place.**

There may be times when you will want to unload PC-cillin 97 from your computer. For example, you may want to unload the program if you experience any conflicts with another system, or your system slows down from having too many windows open. However, remember that when you unload PC-cillin 97 from your computer, you eliminate your protection, and increase your risk of acquiring a virus until you reload the program.

To Unload PC-cillin 97

1. **Right-click the mouse on PC-cillin 97's icon on the taskbar, then choose Unload PC-cillin 97 from the pop-up menu.**
2. **Or, click the Unload button from the SmartMonitor window. The Do you really want to exit PC-cillin 97? message box appears.**
3. **To abort exiting the program, click No. Control returns to PC-cillin 97's main program window.**
4. **To continue and exit the program, click Yes.**

See Also

Removing PC-cillin 97

Uninstalling PC-cillin 97 from your computer is fairly easy. However, before you can remove PC-cillin 97 from your computer, you must unload the program (for more information, see Disabling PC-cillin 97).

To Remove PC-cillin 97

1. **Choose Settings, Control Panel from the Start menu.**
2. **Double-click the Add/Remove Programs icon. The Add/Remove Program Properties dialog box appears.**
3. **Select PC-cillin 97, then click the Remove button.**
4. **Or, choose Programs, and PC-cillin 97's Uninstall applet from the Start menu. The Confirm File Deletion message box appears.**
5. **To abort the operation, click the No button. To proceed with the removal of the application, click the Yes button. The Remove Programs from your Computer message box appears.**
6. **To complete the uninstall procedure, click the OK button. The uninstall program removes PC-cillin 97 from your system.**

In addition to our World Wide Web site, www.antivirus.com, technical support is available to all registered users through Trend Micro's network of local business offices and authorized resellers. Technical support is also available via the Internet , FaxBack service, and telephone and fax in most areas. To contact a technical support representative in your area, browse through the listings below. If Trend does not maintain an office in your area, please contact the location where you purchased the product from or the North American headquarters for assistance.

- North America
- Latin America
- South America
- Europe
- Asia
- Australia

Area	**North America**
Address	**Trend Micro Incorporated** **10101 N. De Anza Blvd., Suite 400** **Cupertino, CA., 95014-9985 USA**
Web (virus center)	**http://www.antivirus.com**
Web (corporate)	**http://www.trendmicro.com**
Email	**support@trendmicro.com**
BBS Private/Public	**Baud rate 9600-28800, Z-modem protocol** **+1 408-255-5221 / 2054** **CompuServe: 72662,432 or** **GO TRENDMICRO**
Toll Free	**+1 800-228-5651 (from within the US)**
Telephone	**+1 408-257-1500**
Fax	**+1 408-257-2003**

Return to Technical Support page

Area	**Latin America**
Address	**Trend Micro Latin America** **Holbein (eje 6 sur) 217, oficina 803,** **Col. Nochebuena, CP 03720, Mexico DF**
Web (virus center)	**http://www.antivirus.com**
Web (corporate)	**http://www.trendmicro.com**
Email	**Hernan_Armbruster@trendmicro.com**
Telephone	**+(525) 598 0668 / (541) 816-1663**
Fax	**+(541) 941-7916**

Return to Technical Support page

Area	**Argentina**
Address	**Trend Argentina (de Gustavo Moroni)** **Viamonte 1646, Piso 8, Dpto 61, 1055** **Buenos Aires - Argentina**
Web (virus center)	**http://www.antivirus.com (English)**
Web (corporate)	**http://www.trendmicro.com**
Email	**pccillin@sminter.com.ar**
Telephone/Fax	**+541 816 0525** **+541 816 0537** **+541 816 0539**

Area	**Brazil**
Address	**Trend Micro do Brazil, Ltda.** **Av. Sao Gabriel, 555-3 conj. 305/306,** **Sao Paulo –SP, Brazil 01435-001**
Web (virus center)	**http://www.antivirus.com (English)**
Web (corporate)	**http://www.trendmicro.com.br**
Email	**trend.suporte@trendmicro.com.br**
Telephone	**+55 11 282 8000**
Fax	**+55 11 881 4046**

Return to Technical Support page

Area	**France**
Address	**Trend Micro France S.A.** **Tour Aurore, 18 Place des Reflets** **92975 PARIS LA DEFENSE 2 France**
Web (virus center)	**http://www.antivirus-fr.com**
Web (corporate)	**http://www.trendmicro.fr**
Email	**marc_blanchard@trendmicro.fr**
Telephone	**+33-1-47-78 62 62**
Fax	**+33-1-47-78 68 99**

Area	**Germany**
Address	**Trend Micro Deutschland GmbH** **Unterfeldstr. 19** **85238 Peterhausen Germany**
Web (virus center)	**http://www.antivirus.com (English)**
Web (corporate)	**http://www.trendmicro.de**
Email	**support@trendmicro.de**
BBS Private/Public	**Private/Public: Baud rate 28800, 8 N 1 protocol** **+49 8137-99030**
Telephone	**+49-0-8137 99027**
Fax	**+49-0-8137 3865**

Area	**Italy**
Address	**Trend Micro Europe S.R.L.** **Via Ponchielli 4, 20063** **Cernusco Sul Naviglio (MI) Italy**
Web (virus center)	**http://www.antivirus.com (English)**
Web (corporate)	**http://www.trendmicro.com (English)**
Email	**assistenza@trendmicro.it**
BBS Private/Public	**Baud rate 28800, Z-modem protocol** **+39-2-92-11 80 07**
Telephone	**+39-2-92 11 18 47**

Fax **+39-2-92 11 18 53**

Return to Technical Support page

Area	**Hong Kong**
Address	**Trend Micro Limited** **Unit A, 17/F, Southern Commercial Building** **11-13 Luard Road** **Wanchai, Hong Kong**
Web (virus center)	**http://www.antivirus.com (English)**
Web (corporate)	**http://www.trendmicro.com (English)**
Email	**Anthony_Fung@trendmicro.com**
Telephone	**(852) 2866 4362**
Fax	**(852) 2866 4363**

Area	**Japan**
Address	**Trend Micro** **Saisho Bldg, 3F, 8-1-14, Nishi-Gotanda** **Shinagawa-Ku, Tokyo 141 Japan**
Web (virus center)	**http://www.antivirus.co.jp**
Web (corporate)	**http://www.trendmicro.co.jp**
Email	**support@trendmicro.co.jp**
Telephone	**+81 3-3493-5850**
Fax	**+81 3-3493-5188**
FaxBack service	**+81 3-3861-8089 code 42**

Area	**Korea**
Address	**#661, Daeyoung Bldg, 44-1, Youido-Dong** **Youngdeong po-Ku, Seoul 150-010** **Korea**
Web (virus center)	**http://www.antivirus.com (English)**
Web (corporate)	**http://www.trendmicro.com (English)**
Email	**support@trendmicro.co.kr**
BBS Private	**Baud rate 9600, Z-modem protocol** **+82-2-780-2086 / +82-2-782-1786** **chollian = GO TREND**

BBS Public	**nownuri = GO TRENDK**
	unitel = GO TREND
	hitel = GO TRENDK
Telephone	**+82 2-7821784**
Fax	**+82 2-786-5792**

Area	**Malaysia**
Address	**1F, No. 4, Jalan SS2/61** **47300 Petaling Jaya, Selangor,** **Malaysia**
Web (virus center)	**http://www.antivirus.com (English)**
Web (corporate)	**http://www.trendmicro.com (English)**
Email	**Kenny_Ooi@trend.com.tw**
Telephone	**+60 3 773-9533 / 9544**
Fax	**+60 3 773-9500**

Area	**Philippines**
Address	**Computex Industries Inc.** **Unit 7M, 7th Floor, Vernida 1 Building** **120 Amorsolor Street, Legaspi Village** **Makati City, Philippines**
Web (virus center)	**http://www.antivirus.com (English)**
Web (corporate)	**http://www.trendmicro.com (English)**
Email	**computex@mnl.sequel.net**
BBS Private	**+63 2-812-4606**
Telephone	**+63 2-817-2555 /813-2909 /813-2970**
Fax	**+63 2-818-2406**

Area	**Singapore**
Address	**7 Temasek Boulevard** **#29-01 Suntec Tower 1** **Singapore 038987**
Web (virus center)	**http://www.antivirus.com (English)**
Web (corporate)	**http://www.trendmicro.com (English)**
Email	**Charlene_Jan@trend.com.tw**

Telephone	**+65 3349912**
Fax	**+65 3345474**

Area	**Taiwan**
Address	**Trend Micro Incorporated** **11F, No.319, Tun Hwa S. Rd., Sec. 2** **Taipei, Taiwan**
Web (virus center)	**http://www.antivirus.com (English)**
Web (corporate)	**http://www.trend.com.tw**
Email	**support@trend.com.tw**
BBS Public	**+ 886-2-923-3233**
Telephone	**+ 886 2-378 9666**
Fax	**+ 886 2-377 9749**
Faxback	**+ 886 2-874 0302 ext. 222**

Area	**Thailand**
Address	**66/165 Ban Yai City, Karnjanapiset Road** **Tumbol Sao Tong Hin, Umber ban Yai** **Nontaburi 11140 Thailand**
Web (virus center)	**http://www.antivirus.com (English)**
Web (corporate)	**http://www.trendmicro.com (English)**
Email	**thanavat@classic.asianet.co.th**
Telephone	**+ 661 939-5994**
Fax	**+ 661 903-0745**

Return to Technical Support page

Area	**Australia**
Address	**Trend Micro Australia Pty. Ltd.** **14th Floor, 33 Berry Street** **North Sydney, NSW 2060** **Australia** **PO BOX 1727,** **North Sydney, NSW 2060, Australia**
Web (virus center)	**http://www.antivirus.com**
Web (corporate)	**http://www.trendmicro.com.au**
Email	**Mark_Misallef@trendmicro.com.au**
Telephone	**+61 2-9959 1970**
Fax	**+61 2-9959 1016**

Return to Technical Support page

Trend`s FaxBack Service is a 24-hour automated customer support service that can instantly send you the latest information about Trend`s products. You can order product brochures and price lists, extensive compatibility notes (the same information Trend`s Customer Support staff uses), installation, and troubleshooting instructions, and more.

Currently, the FaxBack Service is only available in Taiwan and Japan.
The number in Taiwan is +886-2-8740303 ext. 222
The number in Japan is +81 3-3861-8089 code 42

See Also

Technical Support

Trend maintains a comprehensive virus information web site including the latest news about viruses, product upgrades, and virus pattern files. Visit Trend at:

www.antivirus.com

See Also

Technical Support

PC-cillin 97 includes a feature that allows you to perform an automatic online registration. Registering your product entitles you to technical support as well as information about new products and services.

To Register On-line

1. **Choose Update Pattern Page from the File menu.**
2. **Or, click the Update Pattern tab from the main program window. The Update Pattern tab appears.**
3. **Click the Register button.**
4. **Fill in the fields and checkboxes. Keep in mind that the fields with asterisks are required.**
5. **When you're finished, click the OK button.**

The next time you download a virus pattern file, your registration will be uploaded automatically.

To Register by Mail

1. **Choose Update Pattern Page from the File menu.**
2. **Or, click the Update Pattern tab from the main program window. The Update Pattern tab appears.**
3. **Click the Register button.**
4. **Fill in the fields and checkboxes. Keep in mind that the fields with asterisks are required.**
5. **When you're finished, click the Print button.**
6. **Click the OK button.**
7. **Send the completed form to the Trend office nearest you. For a list of Trend's world wide locations, click here.**

See Also

Technical Support

PC-cillin 97 includes a database listing of all the viruses it recognizes (common, boot, or file). Each virus is listed by its more common name, with known aliases shown under the name. The virus information tab also specifies the type of virus, the size of the virus code, the type of damage the virus causes, and the infection method of the virus.

To View Information About a Virus

1. **Choose Virus Information from the File menu.**
2. **Or, choose the Virus Information tab from PC-cillin 97's main program window. The Virus Information window appears.**
3. **From the Virus Type drop-down list, select the virus type you want information about.**
4. **Scroll through the Virus Name List and select the virus name you want information about. Information about the virus you selected appears in the Type of File Virus, Memory Resident Type and Description areas.**