

PC Security for Windows



Copyright Tropical Software, 1995. All Rights Reserved.

[Disclaimer](#)

[How to order PC Security for Windows](#)

[Introduction](#)

[Main Screen](#)

[Stealth File Encryptor](#)

[Encryptor Browser](#)

[Window Lock](#)

[File Lock](#)

[File Shredder](#)

[Keyboard Monitor](#)

[Program Manager Control](#)

[Important Files Backup](#)

[System Lock](#)

[Settings Screen](#)

[Password Settings Screen.](#)

[Master Password Settings Screen.](#)

[Intruder Detection Settings Screen.](#)

[System Lock Settings Screen.](#)

[Activation Screen](#)

[View menu](#)

[Help menu](#)

[Activate menu](#)

[Some data security topics](#)

[Large Scale Installations](#)

[Technical Information](#)

[Technical Support](#)

View menu commands

The View menu offers the following commands:

Icon Titles	Shows or hides the Icon Titles
<u>Status Bar</u>	Shows or hides the status bar.

Help Menu commands

The Help menu offers the following commands, which provide you assistance with this application:

<u>Index</u>	Offers you an index to topics on which you can get help.
<u>Using Help</u>	Provides general instructions on using help.
<u>About</u>	Displays the version number of this application.

Activate Menu

This menu item only exists on unregistered demo versions of this software.
It starts the Activation Screen

Status Bar command (View menu)

Use this command to display and hide the Status Bar, which describes the action to be executed by the selected menu item or depressed toolbar button, and keyboard latch state. A check mark appears next to the menu item when the Status Bar is displayed.

See [Status Bar](#) for help on using the status bar.

Status Bar



The status bar is displayed at the bottom of the PC Security window. To display or hide the status bar, use the Status Bar command in the View menu.

The left area of the status bar describes actions of menu items as you use the arrow keys to navigate through menus.

The right area of the status bar indicates whether the Keyboard Monitor is active or not:

Index command (Help menu)

Use this command to display the opening screen of Help. From the opening screen, you can jump to step-by-step instructions for using PC Security and various types of reference information.

Once you open Help, you can click the Contents button whenever you want to return to the opening screen.

Using Help command (Help menu)

Use this command for instructions about using Help.

About command (Help menu)

Use this command to display the copyright notice and version number of your copy of PC Security.

Context Help command



Use the Context Help command to obtain help on some portion of PC Security. When you choose the Context Help button, the mouse pointer will change to an arrow and question mark. Then click somewhere in the PC Security window, such as another button. The Help topic will be shown for the item you clicked.

Shortcut

Keys: SHIFT+F1

Title Bar



The title bar is located along the top of a window. It contains the name of the application and document.

To move the window, drag the title bar. Note: You can also move dialog boxes by dragging their title bars.

A title bar may contain the following elements:

- Control-menu button
- Maximize button
- Minimize button
- Restore button

Size command (System menu)

Use this command to display a four-headed arrow so you can size the active window with the arrow keys.



After the pointer changes to the four-headed arrow:

1. Press one of the DIRECTION keys (left, right, up, or down arrow key) to move the pointer to the border you want to move.
2. Press a DIRECTION key to move the border.
3. Press ENTER when the window is the size you want.

Note: This command is unavailable if you maximize the window.

Shortcut

Mouse: Drag the size bars at the corners or edges of the window.

Move command (Control menu)

Use this command to display a four-headed arrow so you can move the active window or dialog box with the arrow keys.



Note: This command is unavailable if you maximize the window.

Shortcut

Keys: CTRL+F7

Minimize command (application Control menu)

Use this command to reduce the PC Security window to an icon.

Shortcut

Mouse: Click the minimize icon  on the title bar.
Keys: ALT+F9

Maximize command (System menu)

Use this command to enlarge the active window to fill the available space.

Shortcut

Mouse: Click the maximize icon  on the title bar; or double-click the title bar.
Keys: CTRL+F10 enlarges a document window.

Next Window command (document Control menu)

Use this command to switch to the next open document window. PC Security determines which window is next according to the order in which you opened the windows.

Shortcut

Keys: CTRL+F6

Previous Window command (document Control menu)

Use this command to switch to the previous open document window. PC Security determines which window is previous according to the order in which you opened the windows.

Shortcut

Keys: SHIFT+CTRL+F6

Close command (Control menus)

Use this command to close the active window or dialog box.

Double-clicking a Control-menu box is the same as choosing the Close command.



Note: If you have multiple windows open for a single document, the Close command on the document Control menu closes only one window at a time. You can close all windows at once with the Close command on the File menu.

Shortcuts

ALT+F4 closes The PC Security for Windows upon the entry of the right password.

Restore command (Control menu)

Use this command to return the active window to its size and position before you chose the Maximize or Minimize command.

Switch to command (application Control menu)

Use this command to display a list of all open applications. Use this "Task List" to switch to or close an application on the list.

Shortcut

Keys: CTRL+ESC

Dialog Box Options

When you choose the Switch To command, you will be presented with a dialog box with the following options:

Task List

Select the application you want to switch to or close.

Switch To

Makes the selected application active.

End Task

Closes the selected application.

Cancel

Closes the Task List box.

Cascade

Arranges open applications so they overlap and you can see each title bar. This option does not affect applications reduced to icons.

Tile

Arranges open applications into windows that do not overlap. This option does not affect applications reduced to icons.

Arrange Icons

Arranges the icons of all minimized applications across the bottom of the screen.

Some data security topics

Interrupting the Boot process:

When Windows is booting up, first some DOS commands are processed through autoexec.bat and then Windows comes up. Processing the DOS commands can be interrupted by pressing F5 or F8 thus getting control before PC Security can take over. To avoid this, put the following command in the config.sys:
switches=/n

The problem of booting from the floppy drive:

The biggest break in security, comes from the fact that anyone can put a bootable diskette in the a: drive, reboot the machine, and take total control.

Some modern machines offer the capability of disabling booting from the a: drive as a BIOS setup.

If your machine doesn't offer this capability, locking the whole machine in a cabinet could be the only solution. (be careful with ventilation issues)

Data backup:

It is never too much to stress the need for frequent data backup.

Although the features of PC Security for Windows were tested and found to be bug free, external faults can cause encryption, file locking and others to lose data. Never use any of the PC Security features on files which you don't have a RECENT unencrypted Backup.

Not only PC Security for Windows is vulnerable to external faults, any program like the word processor, the backup programs, even the operating system itself is vulnerable.

These external faults could be intentional or not, some examples are:

Turning off, rebooting, pulling the plug, current surge, etc., while in operation, will have unpredictable results.

The hard disk keeps the information(including program code and the operating system) in the form of minuscule magnetic fields. With time, the magnetism fades out or is modified by the proximity of strong magnetic fields generated by telephone sets, speakers, magnetic business cards, even the earth's magnetic field. Because of these factors, one day one bit might change, causing unpredictable results.

As one can see, the computer is usually accurate but it is not always accurate!

How to manage back-ups:

There are two types of backup:

- The frequent backup is the one that is done frequently (recommended daily) for the case when the computer crashes and the data becomes unrecoverable. This is the backup that is worth more than gold sometimes. For this backup, avoid using the same media (diskette, tape, etc.) over and over again. Have ten and rotate them. Try to backup with a verify option for enhanced safety.

- The permanent backup, is a backup copy that is done once in a while (recommended monthly) and sent off site, possibly to a locked safe.

This is necessary for the case of fire and burglary, in these cases, both the data within the computer and the backed up one might be lost at the same time.

Also, because the hard drive can be corrupted little by little with time, the permanent backup will have the original data before the corruption.

This usually happens with files that are not used for a long period of time, therefore it's corruption is not detected.

Disclaimer

PC Security for Windows is supplied as is without warranty of any kind.

Tropical Software hereby disclaims all warranties and guarantees regarding the use, or the results of use, of PC Security for Windows in terms of correctness, accuracy, reliability or otherwise.

Tropical Software will not be responsible for any incidental, consequential, direct or indirect damages, including but not limited to damages for loss of profits, business interruption and loss of information resulting from the correct or otherwise use of PC Security for Windows even if Tropical Software has been advised of the possibility of such damages.

By installing PC Security for Windows, you acknowledge that you have read this limited warranty, understand it, and agree to be bound by its terms and conditions.

You also agree that the limited warranty is the complete and exclusive statement of agreement between the parties and supersedes all proposals or prior agreements, oral or written, and any other communications between the parties relating to the subject matter of the Limited warranty.

Order Form

When you order PC Security for Windows, you receive an "Activation Code" so you can start using the program immediately. You also receive the release package containing an installation disk that doesn't require activation for use in the case of changing computers. (it is not necessary to install the contents of that disk over the activated program)

Have the following information ready:

Installation Code (From the Activation screen)

Name _____

Company _____

Street _____

City _____

State _____ ZIP _____

Country _____

Telephone Number _____

E-Mail _____

Comments/Suggestions _____

Price:

PC Security for Windows (in US\$)..... 29.00 (or site license)

Florida residents add 6.5% sales tax..... _____

Shipping and handling..... 4.00
=====

Total in US\$..... _____

Site License:

2 to 9: \$22.00 each.
10 to 24: \$17.00 each.
25 to 49: \$14.00 each.
50 to 99: \$10.00 each.
100 to 199: \$ 7.00 each.
200 and up: \$ 5.00 each.

Ordering by check: To order by check send this order form and a check to:

Tropical Software
27 Georgetown Dr.
Eatontown, NJ 07724

Checks can be in US\$ or the equivalent in a foreign currency + 10% (bank charges).

Ordering by credit card: For information on ordering by Master Card, Visa, American Express, or Discover by phone, FAX, email, or postal mail, click here:

[Credit Card Ordering Information](#).

Ordering via Compuserve: Compuserve users can order PC Security for Windows on-line. Enter the command GO SWREG and follow the instructions. The PC Security for Windows **registration id is 9305**. The ordering price will be added to your Compuserve bill. When ordering more than 1 copy, search on PC Security for the right registration id.

PC Security for Windows is only shipped on 3.5 inch disks.

To contact Tropical Software:

- Compuserve - 73742,1104
- Internet - sales@tropsoft.com
http://www.tropsoft.com/tropsoft
- Mail - 27 Georgetown Dr.
Eatontown, NJ 07724

Credit Card Ordering

Credit Card Ordering

Master Card, Visa, American Express, and Discover orders for PC Security for Windows must be placed through PsL, a credit card order taking service. You can reach PsL 24 hours a day 7 days a week by fax at 1-713-524-6398, by Compuserve mail to 71355,470, or Internet mail to 71355.470@compuserve.com. You can also call PsL at 1-800-242-4PsL(4775) or 1-713-524-6394 between the hours of 7:00 am and 6:00 pm CST Monday-Thursday and 7:00 am and 12:30 pm CST on Fridays, except holidays.

Credit card orders can be mailed to PsL at P.O. Box 35705, Houston, TX 77235 USA.

Ask for Order # 14389

PsL requires the following information:

Credit Card: [] Master Card [] VISA [] AMEX [] Discover

Credit Card Number:

Expiration Date:

Name On Card:

Billing Address:

Tropical Software cannot be reached at the numbers above.

These numbers are for PsL, a credit card order taking service only.

Any questions about the status of the shipment of an order, refunds, registration options, product details, technical support, volume discounts, dealer pricing, site licenses, etc., must be directed to Tropical Software:

- Compuserve - 73742,1104

- Internet - sales@tropsoft.com

<http://www.tropsoft.com/tropsoft>

- Mail - 27 Georgetown Dr.

Eatontown, NJ 07724

Technical Information

Unlike other security programs, PC security for Windows doesn't install any special device driver. It performs its security functions by using the standard features provided by the operating system. This makes PC Security for Windows very reliable and trustworthy. It won't mess up the system and it's compatible with all the standard Windows installations.

Files:

SECURITY.EXE	The PC Security for Windows main program.
WINSECHK.DLL	Utilities used by PC Security for Windows.
SECURITY.HLP	The on-line user's guide and help file.
INSTALL.EXE	Found in the installation disk, provides Install and Uninstall functions
DEFPWD.INI	Used by automated Installations to create passwords other than SECURITY
SECURITY.INI	Located in the Windows directory, contains settings information.

The following line must be present in the config.sys for proper File Lock operation:

```
install=c:\dos\share.exe /F:16384 /L:130
```

(make adjustments for DOS's drive and directory)

Installation notes:

The installation program was designed to provide both single user interactive installation and automated installations.

See [Large Scale Installations](#) for more details.

To uninstall PC Security for Windows, run the installation program from a diskette, press Cancel at the installation settings screen and select the Uninstall menu.

Technical Support

- CompuServe - 73742,1104

- Internet - support@tropsoft.com
<http://www.tropsoft.com/tropsoft/techsprt.htm>

- Mail - 27 Georgetown Dr.
Eatontown, NJ 07724

If desired, include your phone # with the problem description and we'll call back.

While technical support is offered free of charge, the associated telephone costs are significant in relation to the cost of this product, therefore we will call collect. (reversed charges)

Introduction

In this era of inter networking, work groups and digital highway, it becomes more and more important to protect personal sensitive data from malicious or unintended harm. More and more documents and information are migrated to the computer in the form of files stored in the hard disk. More and more computers are linked together, exposing those files to dangers of being destroyed, examined, or adulterated intentionally or not by other users (hackers) of the network.

The PC Security for Windows utilities are custom designed to help you protect your system against such intrusions. The PC Security for Windows offers comprehensive data security protection by performing the following functionality:

- Stealth File encryption
- Window locking
- File locking
- System locking
- File Shredder
- Keyboard Monitor
- Program Manager Control
- Important Files Backup with auto encryption
- Intruder Detection with Alarm
- Flexible and complete password protection
- Drag and Drop support

You can try PC Security for Windows with no fear as it doesn't change any system configuration. If you decide not to use it, it has an uninstall feature that removes it completely from your machine!

Unlike other security programs, PC security for Windows doesn't install any special device driver. It performs it's security functions by using the standard features provided by the operating system. This makes PC Security for Windows very reliable and trustworthy. It won't mess up the system and it's compatible with all the standard Windows installations.

PC Security for Windows is widely distributed in the form of "Activationware". The public copy has full functionality for evaluation purpose but all the passwords and the encryption keys are disclosed. By "Activating" PC Security for Windows, it enters normal operation, DES* encryption becomes available while maintaining all of the current settings. No reinstallation required. Activation is accomplished by selecting the Activate menu, contacting Tropical Software with the displayed Installation Code and entering the given Activation Code.

Hardware/Software Requirements:

- Computer: IBM or compatible
- Processor: 80386 or higher
- Operating System: Windows 3.1 or higher

Large Scale Installations

PC Security allows for easy large scale installations.

The installation program was designed to provide both single user interactive installation and automated installations.

Usually, the Installation program displays screens for directory input and creates "SECURITY" as the default passwords.

The Installation program can also be run with command line parameters. In this case, the input screens are not displayed and it uses the values passed by the parameters:

SETUP TargetDirectory yes/no

Where:

SETUP is the name of the installation program.

TargetDirectory is the directory to install PC Security for Windows. The target directory must have only one level from the root.

yes/no refers to Start Security With Windows. It is necessary for relocking files, windows and the system in case of reboot.

Example:

SETUP c:\security yes

The default passwords can be modified by changing the values in DEFPWD.INI prior to installations.

Other settings can be replicated by copying the file SECURITY.INI from one machine to another.

Once you have completely configured a machine, for example locked all the necessary groups with the Window Lock, make a copy of the file security.ini that is located in the Windows directory. Right after a new installation, copy this file to the target machine's Windows directory. When PC Security starts, it will be already configured and it will behave exactly like the master machine.

Please contact [technical support](#) for more details on large scale installation.



Window Lock

With the Windows Lock, all individual windows and even the Program Manager itself can be locked so that they don't respond to mouse or keyboard input.

This feature is specially useful for limiting someone's access to a particular window or a group of windows.

There are two different ways of locking a window:

1. Disable the window so that it gets "frozen".
2. Make it invisible and disabled.

Controls:

Disable

Disable the selected window, it will still show on the screen but all mouse and keyboard operations will be disabled.

Invisible

Disable and hide the selected window from the screen.

Lock

By pushing this button (or Alt+L), the mouse pointer turns into a key. Aim the key to the desired window and click the left mouse button in order to lock it.

Unlock

Press this button (or Alt+U) to unlock all the windows selected from the locked list.

Close

Press this button (or Alt+C) to close the Window Lock screen.

Procedure:

To lock window(s), first select the lock mode between disable only or invisible. Then press the lock button.

At this point, the mouse pointer changes to a key. Put this key in front of the desired window (preferably at the title bar) and push the left mouse button.

The name of the window will be added to the locked list.

To unlock the windows, select one or more windows from the locked list and then press unlock.

If the system is shutdown (or turned off) and some windows were locked, PC Security will try to lock them again the next time it starts.

Tips:

- You can also lock minimized windows by pointing the key to the icon and pressing the left mouse button..
- PC Security will only be able to relock the windows that restart when the system is booted.



PC Security Settings

The Settings Screen is the platform to control all PC Security for Windows settings.

Start Security when Windows starts

Check this option to have PC Security for Windows start when Windows start. This option is highly recommended as it provides continuous protection.

This option must be selected if PC Security for Windows is to relock files or windows when the system is rebooted.

Passwords

Press this button (or Alt+P) to start the Password Settings Screen.

Master Password

Press this button (or Alt+M) to start the Master Password Settings Screen.

Intruder Detection

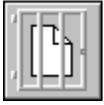
Press this button (or Alt+I) to start the Intruder Detection Settings Screen.

System Locker

Press this button (or Alt+y) to start the System Lock Settings Screen.

Close

Press this button (or Alt+C) to close Settings screen.



File Lock

The File Lock, locks up to 50 selected files by requesting exclusive use from the operating system.

It is therefore impossible for any other program or even a network system to have access to that file.

Controls:



Press this button (or Alt+L) to start a multi-file selection screen. Select all the files to be locked from that screen.



Press this button (or Alt+U) to unlock all the selected files from the locked files list.



Press this button (or Alt+C) to close the File Lock screen.

Procedure:

Press the Lock Files button, select drive, directory, one or more files and press the Lock button.

The selected files will show in the main list.

More files can be added to this list by repeating the above procedure.

To unlock, select one or more files from the locked files list and press the Unlock Files button.

Attention:

The following line must be present in the config.sys for proper File Lock operation:

```
install=c:\dos\share.exe /F:16384 /L:130
```

(make adjustments for DOS's drive and directory)

Tips:

- To select all the files in a list, press *Ctrl + ** when the list has the focus. To unselect all files press *Ctrl + *.
- If the system is shutdown (or turned off) and files were locked, PC Security will lock them again the next time it starts.
- You can drag files directly from the File Manager to this screen. To do this, highlight the files, press the left mouse button, move the cursor anywhere in this screen and release the mouse button.
- If you can, lock the file *command.com* located in the dos directory. This file is the preferred hacker back door access.

Warning - NEVER lock any file for which you don't have a recent unencrypted backup. (See the backup discussion later in this manual)



Keyboard Monitor

The Keyboard Monitor, when active, records up to 20,000 alphanumeric characters that are typed on the keyboard.

Controls:



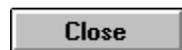
Select this option to start monitoring.



Press this button to clear the monitored text.



Press this button to save the monitored text to a file.



Press this button to close the Keyboard Monitor screen. It will continue monitoring the keyboard if active.

Procedure:

To start the Keyboard Monitor press the Active checkbox. At this point, any key pressed will start to show in it's screen.

The information can at any time be deleted by the Clear button or Saved to a file by using the Save button and either entering the file name or selecting (overwriting) an existing file.

Tips:

- *The Keyboard monitor continues to monitor even when it's screen is closed.*
- *The intruder detection can also start the Keyboard Monitor. Read about the Intruder Detection later in this manual.*
- *If the system is shutdown (or turned off) and the Keyboard Monitor was active, PC Security will make it active again the next time it starts.*
- *The keyboard monitor can detect characters sent to any Window programs, but it doesn't work for DOS programs.*



Stealth File Encrypt/Decrypt - List Mode

Encryption is a very powerful way of protecting the information in a file from being examined by others. Encryption works by modifying the contents of the file according to a secret key word, making it impossible to read it unless it is again decrypted using exactly the same keyword.

By using the sophisticated stealth technique (file name disguise), you can effectively hide files in your disk.

There are two file encryption modes of operation:

- The List Mode (this screen) lets you maintain a list of selected files from different directories and perform encryption operations.

- The Browser Mode lets you navigate the disk and perform encryption operations.

A button on the lower left corner of the screen allows for switching between them.

Controls:



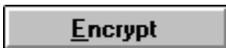
Press this button (or Alt+K) to start the Enter Key screen. The Enter Key screen is used for entering the initial working key and for changing the existing working key. For security reasons, the key is never stored in disk, therefore the key must be entered at least once per program run.

Unencrypted Files:

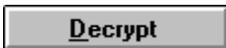
Shows a list of all the files that are not encrypted. Select from this list the files to be encrypted.

Encrypted Files:

Shows a list of all the files that are encrypted. Select from this list the files to be encrypted.



Press this button (or Alt+E) to will trigger the encryption of all the files that were selected from the unencrypted file list.



Press this button (or Alt+D) to trigger the decryption of all the files that were selected from the encrypted file list.



Press this button (or Alt+A) to add files to the lists by starting the select files screen. The selected files go to the respective list according to their encryption state, ie, the files that are encrypted go to the encrypted list and the ones that are not encrypted go to the unencrypted list.



Press this button (or Alt+R) to remove the selected files from the lists. Select unwanted files from one or both lists and press this button. Note that files that were encrypted will remain encrypted, they just don't show in the list

anymore.

Refresh list

Press this button (or Alt+H) to refresh the information contained in the directory list and file lists for that directory.

Fast Encryption

Select this option (or Alt+F) for fast encryption. Fast encryption is sufficient for most cases.

DES Encryption

Select this option (or Alt+S) for DES encryption. DES is the government's appointed encryption algorithm and stands for Digital Encrypting Standards. It is recommended for those very top secret files.

DES Encryption is subject to special export laws.

Both

Select this option (or Alt+B) for a combination of fast and DES encryption. This method provides for extra strength encryption because it defeats the "Text Attack" method of breaking encryption which is by far the most effective method.

Desguise Filename

When this option is selected (Alt+G), the filename is changed to a combination of random numbers. The real name will still show in the encrypted files list.

Browser Mode

Press this button (or Alt+W) to change to Browser Mode. The Encryptor in Browser Mode works similar to this screen but instead of a list of files it allows for disk navigation.

Close

Press this button (or Alt+C) to close the Encryptor screen.

The files that are encrypted will be displayed in the encrypted files list and the regular files will show in the unencrypted files list.

At this point files can be encrypted or decrypted by selecting one or more from one list and pressing the corresponding button.

Tips:

- You can drag files directly from the File Manager to this screen. To do this, highlight the files, press the left mouse button, move the cursor anywhere in this screen and release the mouse button. The files will be listed in the corresponding list according to their encryption state.

-When you start the Encryptor, a key must be entered. This can be done by pressing the key button.

- The Encryptor also offers the option of disguising the filename by changing it to a random number, while still showing the real filename within the encrypted list.

- The key must be entered both in the enter field and verify field and they must match exactly to avoid mistyping. This is done because if the file is encrypted with an unknown key, it becomes UNRECOVERABLE (this is it's strength).

- If a file was encrypted with a key different than the current working key, it will be shown in the encrypted files list

anyway. If the file is decrypted with the wrong key, encrypt it back with that key again and than decrypt it with the original key.

- Keep all your important documents in the list, they can be encrypted or decrypted with the push of a button.

Warning - NEVER encrypt any file for which you don't have a recent unencrypted backup.(See the backup discussion later in this manual)



File Shredder

When a file is deleted in the computer, it is not really deleted.

For speed performance reasons, the computer only deletes the file indexing information saying that the disk space the file occupied is now free.

Only when another file is created using that space, will that information disappear.

This fact allows unerase utilities like Norton Utilities *, PCTOOLS * or the like to retrieve all or part of the information that the file contained.

The File Shredder overwrites the contents of a file with 2 complementary sequences of alternating bits, and then fills it with blank spaces prior to deleting it, thus completely erasing the contents of that file.

The File Shredder also changes the original name of that file so that all traces of it are eliminated.

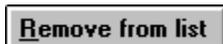
:Controls:



Click the arrow to select how many times the file should be overwritten prior to deletion. In most cases, one time is enough. The more times the harder it is to recover the files, the longer it takes to wipe them out.



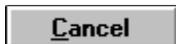
Press this button (or Alt+S) to bring the file selection screen.



Press this button (or Alt+R) to remove from the list any file that should not be shredded.



Press this button (or Alt+W) to wipe out all the listed files.



Press this button (or Alt+C) to close the File Shredder screen.

Procedure:

Press the select files button, select drive, directory, one or more files and press the OK button. (or drag files from the file manager)

The selected files will show in the main list.

More files can be added to this list by repeating the above procedure.

If it's desired to remove some files from the list, highlight the files and press the Remove from list button.

Press the Wipe Out button and the files are gone.

Tips:

- *You can drag files directly from the File Manager to this screen. To do this, highlight the files, press the left mouse button, move the cursor anywhere in this screen and release the mouse button.*
- *To select all the files in a list, press `Ctrl + /` when the list has the focus. To unselect all files press `Ctrl + \`.*

* Norton Utilities and PCTOOLS are registered trademarks of their respective companies.

WARNING - Once a file is shredded, it is GONE.

Key Enter Screen

This screen gets the key for the encryption operation.

A keyword is a word made of 1 to 8 characters and numbers.

For example:

magic

ANYTHING

12031980

key003

Controls:

Enter

Enter here the encryption working key.

Verify

Enter the key again for verification. This is done for extra protection because there is NO WAY of determining the key of an encrypted file.

OK

Press this button (or Alt+O) to accept the key.

Cancel

Press this button (or Alt+C) to cancel the enter key operation leaving the current key (if any) still active.

Tips:

- The encryption key is not case sensitive so the following keys are considered equal:

Tropical

TROPICAL

tropical

Close

Password Settings

The key to the PC Security for Windows protection is its rich and flexible password scheme.

A password consists of a string of 1 to 8 alphanumeric characters.

The case is ignored, making upper case and lower case the same, for example: TROPICAL, tropical and Tropical are considered equal.

Some other password examples:

protect

secure13

@#%\$^&*()

10apples

Controls:

Function Section:

- Selects the function for password maintenance.

Program Start

Select this button (or Alt+P) to set the Program Start password settings, this option is seldom used.

Encryptor

Select this button (or Alt+E) to set the Encryptor password settings.

File Locker

Select this button (or Alt+L) to set the File Lock password settings.

Window Locker

Select this button (or Alt+W) to set the Window Lock password settings.

File Shredder

Select this button (or Alt+F) to set the File Shredder password settings.

Settings

Select this button (or Alt+S) to set the Settings Screen password settings.

Keyboard Monitor

Select this button (or Alt+K) to set the Keyboard Monitor password settings.

Program Manager Control

Select this button (or Alt+M) to set the Program Manager Control password settings.

Files Backup

Select this button (or Alt+B) to set the Files Backup password settings.

System Locker

Select this button (or Alt+Y) to set the System Lock password settings.

Program Exit

Select this button (or Alt+X) to set the Program Exit password settings.

Setting Section:

Required

When this option is selected (or Alt+R), the corresponding application requires a password.

Global

When this option is selected (or Alt+G), the corresponding application's password is the global one.

Private

When this option is selected (or Alt+R), the corresponding application's password is private (i.e. applies only to that application).

Private Password:

Entry field for the private password

Global Password

Entry field for the global password

Close

Press this button (or Alt+O) to save the password settings.

Close

Press this button (or Alt+C) to close the screen without saving any changes.

Procedure:

For every function of the PC Security for Windows, a password is assigned by using the Password Maintenance screen.

On the left side, a list of all the protected features are displayed close to a radio button.

By pressing the button, that particular feature gets selected and then, on the right side, the settings for it are displayed.

Every feature can have it's own password by selecting the private radio button and filling in the private entry field, or it can accept the global password by selecting the global radio button.

The password for that feature can also be disabled by pressing the Required button and therefore unselecting it (doing this greatly diminish the security level).

After all the desired configuration is set, Press the Ok button to save it.

The cancel button will keep the settings as they were, ignoring all the changes.

The default configuration which is in effect when the program is initially installed is:

- SECURITY as global password
- Global password for all the features.
- No password required for Program Start.

Tips:

- *If the System Lock's password is not required, it becomes just a screen saver.*

Close

System Lock settings

The System Lock, locks the entire system by blanking up the screen.

No mouse or keyboard entry will be accepted until the right password is entered.

To unlock the system, move the mouse or press any keyboard key to bring up the Password Entry Screen, type in the password and press the enter button.

If the locked system is shutdown (or turned off), PC Security will lock it again the next time it starts.

The System Lock can be configured to activate automatically after a certain number of minutes that the machine is left inactive.(no mouse or keyboard input)

It can also be configured to always lock when PC Security starts.

Controls:

Active

Select this option (or Alt+A) to set the System Lock as active. When active it monitors the system's mouse and keyboard for inactivity.

Timeout in minutes 

Click on the arrow and select the amount of inactive minutes that triggers the System Lock.

Lock on startup

Select this option (or Alt+L) to lock the system immediately every time that Windows starts.

Close

Press this button (or Alt+O) to save the System Lock settings.

Close

Press this button (or Alt+C) to close the screen without saving any changes.

Tips:

- See also System Lock

Close

Intruder Detection Settings

An important feature of the PC Security for OS/2 is the Intruder Detection.

When someone types a specified number of wrong passwords, the Intruder Detection takes control and triggers the following:

Close

Keyboard Monitor

Close

Alarm

Close

Desktop Lock

Close

Warning Message

Controls:

Active

Select this option (or Alt+A) to set the Intruder Detector as active. When active it monitors the validity of entered passwords.

Sound Alarm

Select this option (or Alt+S) to sound an alarm when an Intruder is detected.

Monitor Keyboard

Select this option (or Alt+M) to automatically make active the Keyboard Monitor when an Intruder is detected.

Lock the system

Select this option (or Alt+L) to activate the System Lock when an Intruder is detected.

Maximum password tries 

Click on the arrow and select the number of password entry mistakes before the intruder Detection triggers the selected actions.

Last detection:

Shows the date and time when the last intruder detection occurred.

Close

Press this button (or Alt+O) to save the Intruder Detection settings.

Close

Press this button (or Alt+C) to close the screen without saving any changes.

Procedure:

Press the Active checkbox to make it active or not.

All the features can be enabled or disabled by toggling on or off their respective checkboxes.

Select the number of password entry mistakes before the Intruder Detection triggers.

Press the Ok button to save the new settings or the Cancel button to cancel the operation.

Tips:

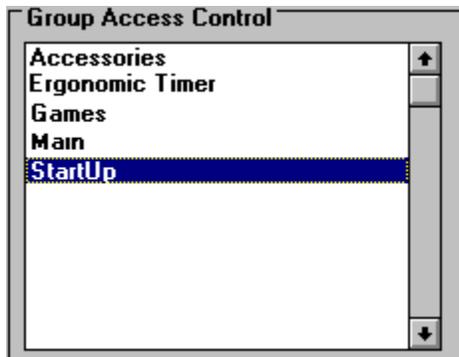
- To stop the Intruder Detector, simply type the right password in any password entry screen.



Program Manager Control

The Program Manager Control is a powerful desktop management tool that can completely limit the access of unauthorized users.

The Program Manager Control works by locking (and hiding) desired groups and by modifying the Program Manager's configuration and functionality.



Here all the current Program Manager groups get listed, highlight the groups that are to be locked.

The Highlighted groups are:

- L**ocked
- L**ocked and **H**idden

Select these options to either lock (Alt+L) the selected groups or lock and hide (Alt+H) them.

Level 1: Disable create, delete or change groups

Select this option (or Alt+1) to prevent the user from creating, deleting or changing group items.

Level 2: Disable create or delete program items

Select this option (or Alt+2) to prevent the user from creating, deleting or changing program items in addition to the former level.

Level 3: Disable modify command line of program items

Select this option (or Alt+3) to prevent the user from changing the command line of program items in addition to the former levels.

Level 4: Disable modify properties of program items

Select this option (or Alt+4) to prevent the user from changing the properties of program items in addition to the former levels.

No Close

Select this option (or Alt+N) to disable the Exit Windows menu item.

No Run

Select this option (or Alt+R) to disable the Run menu item, thus preventing users from running unauthorized programs.

No File Menu

Select this option (or Alt+F) to disable the File menu item altogether.

No Save Settings

Select this option (or Alt+S) to disable the Save Settings on Exit menu item, thus keeping the startup appearance of the Program Manager constant.

Close

Press this button (or Alt+O) to save the new settings.

Close

Press this button (or Alt+C) to close the screen without saving any changes.

Tips:

- *Disable the Shortcut key for all the items that you want locked (see Properties from the File menu).*
- *Use this to protect machines that are used by children.*
- *Very useful for maintaining a constant desktop in an organization.*
- *For maximum protection, open the groups before locking with the hide option. Also resize the groups to the minimum size possible to hide it's contents.*



Important Files Backup

The Important Files Backup, used in combination with the File Lock, File Shredder and the Encryptor, provide complete protection for your important documents.

The Important Files Backup was designed to backup important documents rather than whole directories or hard drives.

The documents to be backed up are kept in a list. These files can be backed up in their original format or they can all be automatically encrypted when backed up. The creation of a new sub directory for each different backup day is supported.

Controls:

Add files

Press this button (or Alt+A) to add files to the list

Remove files

Press this button (or Alt+R) to remove the selected files from the list.

Destination

C:\BACKUP

Fill in with the destination path for the backup up files. The stated path must exist prior to the back up operation.

Create dated subdirectory

Select this option (or Alt+S) to automatically create a new subdirectory of the destination path for the backed up files. The new subdirectory's name be composed as today's date using the following format: BKddmmyy, where dd is today's day, mm is the current month and yy is the current year. As an example, if today is 14/2/1995, the subdirectory will be BK140295.

Prompt on overwrite

Select this option (or Alt+P) to be warned when a back up of a certain file already exists. If this option is not selected, the former back up is replaced without warning.

Encryption Options (see [Encryptor](#) for more details):

Encrypt files

Select this option (or Alt+E) to cause the backup up files to be automatically encrypted.

Close

Press this button (or Alt+K) to enter the desired encryption key.



Select this option (or Alt+F) to use Fast encryption when backing up. This option requires that the Encrypt Files option be selected.



Select this option (or Alt+D) to use DES encryption when backing up. This option requires that the Encrypt Files option be selected.



Select this option (or Alt+T) for a combination of fast and DES encryption. This method provides for extra strength encryption because it defeats the "Text Attack" method of breaking encryption which is by far the most effective method.



Select this option (or Alt+F) to have the filename disguised when backing up. This option requires that the Encrypt Files option be selected.



Press this button (or Alt+B) to perform the backup and save the current settings.



Press this button (or Alt+C) to close the screen without saving any changes.

Tips:

- You can drag files directly from the File Manager to this screen. To do this, highlight the files, press the left mouse button, move the cursor anywhere in this screen and release the mouse button.

Close

Set Master Password

The Master Password acts like a master key and will always satisfy any password entry screen.

The initial master Password is SECURITY and **must be changed immediately**.

Controls:

New Password

Enter here the new master password.

Verify Password

Enter the same new master password for verification. This is done because if the master password is miskeyed or forgotten it can **never** be changed again.

Close

Press this button (or Alt+O) to save the new master Password.

Close

Press this button (or Alt+C) to close the screen without saving any changes.

Enter Password

Enter here the required password and press Ok.

The Master Password will always satisfy any password entry screen.

Press Cancel to cancel the requested operation.

Close

Stealth File Encrypt/Decrypt - Browser Mode

Encryption is a very powerful way of protecting the information in a file from being examined by others. Encryption works by modifying the contents of the file according to a secret key word, making it impossible to read it unless it is again decrypted using exactly the same keyword. By using the sophisticated stealth technique (file name disguise), you can effectively hide files in your disk.

There are two file encryption modes of operation:

- The List Mode lets you maintain a list of selected files from different directories and perform encryption operations.
- The Browser Mode (this screen) lets you navigate the disk and perform encryption operations. A button on the lower left corner of the screen allows for switching between them.

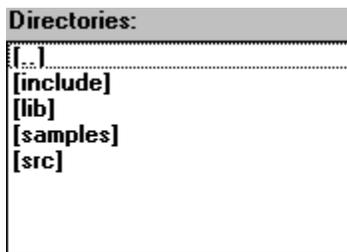
Controls:

Close

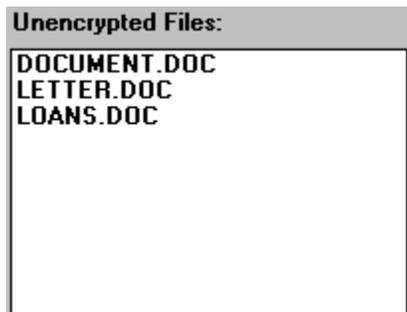
Press this button (or Alt+K) to start the Enter Key screen. The Enter Key screen is used for entering the initial working key and for changing the existing working key. For security reasons, the key is never stored in disk, therefore the key must be entered at least once per program run.

Close

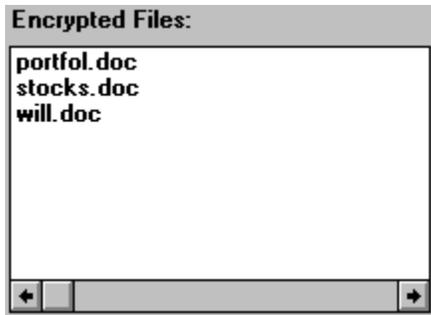
Click on the arrow and select the desired drive.



Shows all the directories for the current selected path. Double click on the desired directory. Note that [..] means parent directory.



Shows a list of all the files in the current path that are not encrypted. Select from this list the files to be encrypted.



. Shows a list of all the files in the current path that are encrypted. Select from this list the files to be decrypted. Slide the scrollbar to the right to see the disguised filename for each file that was encrypted with the disguise option.



Press this button (or Alt+>) to trigger the encryption of all the files that were selected from the unencrypted file list.



Press this button (or Alt+<) to trigger the decryption of all the files that were selected from the encrypted file list.



Press this button (or Alt+H) to refresh the information contained in the directory list and file lists for that directory.



Select this option (or Alt+F) for fast encryption. Fast encryption is sufficient for most cases.



Select this option (or Alt+D) for DES encryption. DES is the government's appointed encryption algorithm and stands for Digital Encrypting Standards. It is recommended for those very top secret files. DES Encryption is subject to special export laws.



Select this option (or Alt+B) for a combination of fast and DES encryption. This method provides for extra strength encryption because it defeats the "Text Attack" method of breaking encryption which is by far the most effective method.



When this option is selected (or Alt+G), the filename is changed to a combination of random numbers. The real name will still show in the encrypted files list.



Press this button (or Alt+C) to close the Encryptor screen.

List Mode

Press this button (or Alt+L) to change to List Mode. The File Encryptor in List Mode works similar to this screen but instead of disk navigation it maintains for a list of files.

For every selected directory, the Encryptor will list all the files containing in that directory.

The files that are encrypted will be displayed in the encrypted files list and the regular files will show in the unencrypted files list.

At this point files can be encrypted or decrypted by selecting one or more from one list and pressing the button that points to the other list.

There are two Encryptor modes of operation.

The List Mode lets you maintain a list of files from different directories and perform encryption operations.

The Browser Mode (this screen) lets you navigate the disk and perform encryption operations.

Tips:

- When you start the Encryptor, a key must be entered. This can be done by pressing the key button.
- The Encryptor also offers the option of disguising the filename by changing it to a random number, while still showing the real filename within the encrypted list.
- The key must be entered both in the enter field and verify field and they must match exactly to avoid mistyping. This is done because if the file is encrypted with an unknown key, it becomes UNRECOVERABLE (this is it's strength).
- If a file was encrypted with a key different that the current working key, it will be shown in the encrypted files list anyway. If the file is decrypted with the wrong key, encrypt it back with that key again and than decrypt it with the original key.
- Keep all your important documents in the list, they can be encrypted or decrypted with the push of a button.

Warning - NEVER encrypt any file for which you don't have a recent unencrypted backup.(See the backup discussion later in this manual)

Activation Screen

PC Security for windows is widely distributed in the form of "Activationware".

The public copy has full functionality for evaluation purpose but all the passwords and the encryption keys are disclosed.

When you order PC Security, you can immediately activate your copy. By "Activating" PC Security for windows, it enters normal operation while maintaining all of the current settings. No reinstallation required.

Activation is accomplished by selecting the Activate menu, contacting Tropical Software with the displayed Installation Code and entering the given Activation Code.

Controls:

How to order PC Security for Windows

Press this button (or Alt+W) to display the Order Form.

Installation Code:

An unique installation code is assigned to your system. Take note of this code, it is upon this code that the activation code is generated.

Enter Activation Code:

Enter the activation code here.

Close

Press this button (or Alt+O) to activate the program.

Close

Press this button (or Alt+C) to close the screen without activating.

Main Screen

The main screen provides the means of accessing the different security tools.

There are three ways to access a tool:

1. Push the appropriate button.
2. Select the corresponding menu selection item from the menu bar.
3. Press the accelerator key which is displayed by the menu options.

An optional password entry screen might have to be entered.



Press this button or F2 to start The File Encryptor. The File Encryptor encrypts files in a way that makes it impossible for anyone to read or understand them.



Press this button or F3 to start The Window Lock. The Window Lock locks windows, and Program Manager Groups. It is useful when someone should have limited access to the desktop.



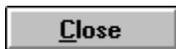
Press this button or F4 to start The File Lock. The File Lock locks files so that no other program or network hacker can access it. It can also be used to protect important files from accidental deletes, overwrites, etc. Locking system files like autoexec.bat and config.sys is highly recommended.



Press this button or F5 to start The File Shredder. The File Shredder deletes files in a way that makes it impossible for anyone to recover them.



Press this button or F6 to start The Keyboard Monitor. The Keyboard Monitor, when active, records every character that is typed on the keyboard.



Press this button or F7 to start The Program Manager Control. The Program Manager Control has the ability to limit the options of modifying it's settings, creation and/or destruction of group and program items.



Press this button or F8 to start The Important Files Backup. The Important Files Backup lets you have a list of important documents to be backed up with the push of a single button. The files can also be encrypted as they are backed up.



Press this button or F9 to start The System Lock. The system Locker, locks the whole desktop. Only the right password can unlock it, rebooting won't do it!



Press this button or F10 to start The Settings Screen.

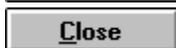
The Settings Screen is the platform to start:



The Password Settings Screen.



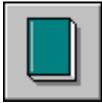
The Master Password Settings Screen.



The Intruder Detection Settings Screen.



The System Lock Settings Screen.



Press this button or F11 to start The PC Security On Line Manual.



Press this button or Ctrl+F4 to exit The PC Security for Windows. Exiting the program will unlock all locked windows and files and stop the Keyboard Monitor if it was active. The files and windows that were locked when it exited will be locked again the next time the program starts and the Keyboard Monitor will resume monitoring if it was active when the program last exited.



Press this button or Shift+F1 to start the Context Help.

Tips:

- The main screen always remembers its size and position , the next time PC Security starts it will be placed exactly like before. If it was minimized when you last exited Windows, it will start minimized again.
- Try hiding the icon titles (from the View menu) for a cleaner and nicer looking screen.
- The advertisement bar and the Activate menu go away when the software is activated.

Exit Button



Press this button or Alt+F4 to exit The PC Security for Windows upon the entry of the right password.

Tips:

- *Exiting the program will unlock all locked windows and files and stop the Keyboard Monitor if it was active.*
- *The files and windows that were locked when it exited will be locked again the next time the program starts and the Keyboard Monitor will resume monitoring if it was active when the program last exited.*

Encryptor Button



Press this button or F2 to start The File Encryptor .The File Encryptor encrypts files in a way that makes it impossible for anyone to read and understand them.

There are two file encryption modes of operation:

- The List Mode lets you maintain a list of selected files from different directories and perform encryption operations.
 - The Browser Mode. lets you navigate the disk and perform encryption operations.
- A button on the lower left corner of their screen allows for switching between them.

Window Lock Button



Press this button or F3 to start The Window Lock. The Window Lock locks windows, and Program Manager Groups. It is useful when someone should have limited access to the desktop.

File Lock Button



Press this button or F4 to start The File Lock. The File Lock locks files so that no other program or network hacker can access it. It can also be used to protect important files from accidental deletes, overwrites, etc. Locking system files like autoexec.bat and config.sys is highly recommended.

File Shredder Button



Press this button or F5 to start The File Shredder. The File Shredder deletes files in a way that makes it impossible for anyone to recover them.

Keyboard Monitor Button



Press this button or F6 to start The Keyboard Monitor. The Keyboard Monitor, when active, records every character that is typed on the keyboard.

Settings Button



Press this button or F10 to start The Settings Screen.
The Settings Screen is the platform to start:



The Password Settings Screen.



The Master Password Settings Screen.



The Intruder Detection Settings Screen.



The System Lock Settings Screen.

Program Manager Control Button



Press this button or F7 to start the Program Manager Control. The Program Manager Control works by locking (and hiding) desired groups and by limiting the options of modifying it's settings, creation and/or destruction of group and program items.

Files Backup Button



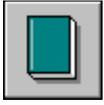
Press this button or F8 to start the Important Files Backup. The Important Files Backup lets you have a list of important documents to be backed up with the push of a single button. The files can also be encrypted as they are backed up.

System Lock Button



Press this button or F9 to start The System Lock. The system Lock, locks the whole desktop. Only the right password can unlock it, rebooting won't do it!

User's Manual Button



Press this button or F11 to start The PC Security On Line Manual.

View Icon Titles Menu

This option toggles the icon titles on and off.



System Lock

The System Lock locks the entire system by blanking up the screen.

No mouse or keyboard entry will be accepted until the right password is entered.

To unlock the system, move the mouse or press any keyboard key to bring up the Password Entry Screen, type in the password and press the enter button.

Tips:

-If the locked system is shutdown (or turned off), PC Security will lock it again the next time it starts.

- If the System Lock's password is not required, it becomes just a screen saver.

- See [System Lock Settings Screen](#). for more information

