Stealth Encryptor

Copyright © Tropical Software, 1996. All Rights Reserved.

Disclaimer

Introduction

How to order Stealth

About the demo version

Menus

> FileMenu
> View menu
> Help menu
> Activate

Functionality

> Stealth Encryptor List Mode
> Stealth Encryptor Browser Mode
> E-Mail Encrypt/Decrypt
> Important Files Backup
> File Shredder
> Encryption Setting
> Encryption Details Selection Bar
> Password Setting
> Key enter screen

Some data security topics
Technical Information
Technical Support

File Menu

The File menu offers the following commands:

Lock   Locks Stealth, a password is needed to unlock it.

Settings   The settings screen allows control of:
                                  - Encryption Setting
                                  - Password Setting

E-Mail Encrypt/Decrypt   The E-Mail Encrypt/Decrypt is a Wizard type operation that through the
use of the clipboard, makes it easy to encrypt and decrypt parts or the whole e-mail message.

Exit   Exits Stealth.

View menu commands

The View menu offers the following commands:

List Mode

Tougles the Encryptor in List Mode which allows for storing a list of frequent files for encryption.

Browser Mode

Tougles the Encryptor in Browser Mode which allows for navigating the disks for encryption.

Files Backup Mode

Tougles the Encryptor in files Backup Mode which allows for automatically backing up important files.

Files Shredder Mode

Tougles to the Files Shredder Mode which allows for permanent deletion of files.

Help menu commands

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

Help Topics   Offers you an index to topics on which you can get
                                                        help.
Order Information   Explains how to order Stealth
About   Displays the version number of this application.

Exit command (File menu)

Use this command to end your Stealth session.   You can also use the Close command on the application Control menu.

Shortcuts
    Mouse: Double-click the application's Control menu button.

Keys: ALT+F4

Status Bar

```
                                                    CAP  [  ] [  ]
```

The status bar is displayed at the bottom of the Stealth window.

The left area of the status bar describes actions of menu items as you use the arrow keys to navigate through menus.   This area similarly shows messages that describe the actions of toolbar buttons as you depress them, before releasing them.   If after viewing the description of the toolbar button command you wish not to execute the command, then release the mouse button while the pointer is off the toolbar button.

The right areas of the status bar indicate which of the following status's:

Indicator   Description
Stealth On/Off   Indicates that the file name disguise option is on/off.

Fast/DES/Both Indicates the currently selected encryption type.

Beginner/Level1/Level2/Advanced   Indicates the currently selected encryption level (see Encryption Settings for details).

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 Stealth 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 Stealth.

Context Help command

Use the Context Help command to obtain help on some portion of Stealth.   When you choose the Toolbar's Context Help button, the mouse pointer will change to an arrow and question mark.   Then click somewhere in the Stealth window, such as another Toolbar 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:
- Application Control-menu button
- Document Control-menu button
- Maximize button
- Minimize button
- Name of the application
- Name of the document
- Restore button

Scroll bars

Displayed at the right and bottom edges of the document window.   The scroll boxes inside the scroll bars indicate your vertical and horizontal location in the document.   You can use the mouse to scroll to other parts of the screen.

The scroll bar appears only when the Stealth screen is resized smaller than it's full view.

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 Stealth window to an icon.

Shortcut

 Mouse: Click the minimize icon on the title bar.

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.

Next Window command (document Control menu)

Use this command to switch to the next open document window.   Stealth 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.   Stealth 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.

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.

No Help Available

No help is available for this area of the window.

No Help Available

No help is available for this message box.

Technical Support

- Compuserve - 73742,1104

- Internet   - support@tropsoft.com
                http://www.tropsoft.com/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)

Technical Information

Unlike other security programs, Stealth Encryptor 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 Stealth Encryptor very reliable and trustworthy.   It won't mess up the system and it's compatible with all the standard Windows installations.

Files:
STEALTH.EXE	The Stealth Encryptor main program.
STEALTH.CNT	The on-line user's guide contents file.
STEALTH.HLP	The on-line user's guide and help file.
SETUP.EXE	Found in the installation disk, provides Install and Uninstall functions
ORDER.TXT	Form and information for ordering Stealth.
README.TXT	Install instructions and licensing information.

Hardware/Software Requirements:
Computer: IBM or compatible
Processor: 80386 or higher
Operating System: Windows 95 or higher, Windows NT 4.0 or higher
At least 10Mb free hard disk space.

To uninstall Stealth Encryptor, run the installation program from a diskette, press Cancel at the installation settings screen and select the Uninstall menu.

In order to best fit Stealth in the screen, adjust the desktop resolution for at minimum of 800x600 with small fonts.   (Start, Settings, Control Panel, Display, Settings)

The Encryption details Toolbar is dockable , it can be removed from it's present position and placed either on the bottom of the screen or floating anywhere on the screen.

Stealth remembers its size and position, once adjusted it will always start that way.

Some data security topics

Data backup:

It is never too much to stress the need for frequent data backup.
Although the features of Stealth Encryptor were tested and found to be bug free, external faults can cause encryption to lose data. Never use any of the Stealth Encryptor features on files which you don't have a RECENT unencrypted Backup.
Not only Stealth Encryptor 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

Stealth Encryptor 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 Stealth Encryptor 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 Stealth Encryptor even if Tropical Software has been advised of the possibility of such damages.

By installing Stealth Encryptor, you acknowledge that you have read this limited warranty, understand it, and agree to be bound by it's terms and conditions.
You also agree that the limited warranty is the complete and exclusive statement of agreement between the parties and supersede all proposals or prior agreements, oral or written, and any other communications between the parties relating to the subject matter of the Limited warranty.

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 Stealth Encryptor utilities are custom designed to help you protect your system against such intrusions.
The Stealth Encryptor offers comprehensive data security protection by performing the following functionality:
Stealth File encryption
E-Mail encryption
File Shredder
Important Files Backup with auto encryption
Drag and Drop support

You can try Stealth Encryptor 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, Stealth Encryptor 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 Stealth Encryptor very reliable and trustworthy. It won't mess up the system and it's compatible with all the standard Windows installations.

Stealth Encryptor is widely distributed in the form of "Activationware". The public copy has full functionality for evaluation purpose but all the password and the encryption keys are disclosed.
By "Activating" Stealth Encryptor, it enters normal operation, DES* encryption becomes available while maintaining all of the current settings. No reinstallation required.
After purchasing Stealth, 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 95 or higher
Minimum 10MB free disk space when processing encryption.

Stealth File Encryptor was developed by Silvio Kuczynski.

To contact Silvio Kuczynski e-mail to silviok@tropsoft.com.

Tropical Software's address is http://www.tropsoft.com

About the demo version

The demo version of Stealth is released to the public for evaluation.

It performs all the functionality of the release version allowing for full evaluation before purchase with the following exceptions:
- DES encryption is not supported.
- The password is disclosed at the lock screen .
- The encryption key is disclosed as plaintext.

DES is not supported due to export restrictions since the demo can be freely distributed all over the world.
The password and key disclosures enable you to evaluate it fully with a lesser chance of losing files and information.
Once activated, the key and password are no longer disclosed.

Important: Do NOT rely on the demo for data privacy, please read the explanation above.

Files Backup

.

The Important Files Backup, used in combination with the File 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 lists. 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:

New

Press this button (or Alt+N) to create a new group of files list to be backed up.

Delete

Press this button (or Alt+D) to delete a group of files list to be backed up.

Add files

Press this button (or Alt+A) to add files to the current list.
You can also drag the files from the Explorer to this screen.
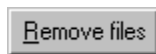
Remove files

Press this button (or Alt+R) to remove the selected files from the current list.
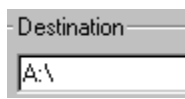
Destination
A:\

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**
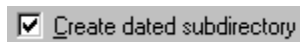
Select this option (or Alt+C) to automatically create a new subdirectory of the destination path for the backed up files. The new subdirectory's name will be composed as today's date using the following format: BKddmmyy, where dd is today's day, mm is the current month and yy is the current year. As an example, if today is 14/2/1997, the subdirectory will be BK140297.

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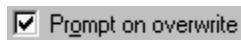
Select this option (or Alt+P) to be warned when a back up of a certain file already exists. If this option is not selected, the former back up is replaced without warning.
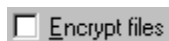
☐ **Encrypt files**

Select this option (or Alt+E) to cause the backup up files to be automatically encrypted. (see Encryptor for more details)
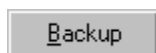
Backup

Press this button (or Alt+B) to perform the backup.

Tips:

- You can drag files directly from the Explorer 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.

- Please maintain a recent unencrypted back up copy of your files (locked in a safe maybe)..

- Press ESC to cancel backing up   all remaining files in the list.

Stealth Encryptor   List Mode

.

Encryption is a very powerful way of protecting the information in a file from being examined by others.
Encryption works by scrambling the contents of a 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.

Controls:

The encryption is performed according to the selections in the Encryption Details Selection Bar .
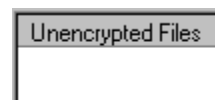
Unencrypted Files

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

| Encrypted Files	Disg. Name
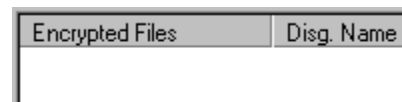
Shows a list of all the files that are encrypted and their corresponding disguised names. Select from this list the files
to be decrypted.
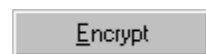
Encrypt

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

Decrypt

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

Add to lists
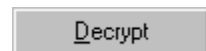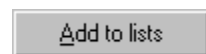
Press this button (or Alt+A) to add files to the lists. The selected files go to the respective list according to their
encryption state, i.e., the files that are encrypted go to the encrypted list and the ones that are not encrypted go to the
unencrypted list.
You can also drag the files from the Explorer to this screen.

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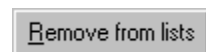
Press this button (or Alt+R) to remove the selected files from the lists. Select unwanted files from one or both lists
and press this button. Note that files that were encrypted will remain encrypted, they just don't show in the list
anymore.

Refresh

Press this button (or Alt+S) to refresh the information contained in the lists.

Operation:

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 Explorer 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. Feel free to rename it as you wish, Stealth will still keep track of the original name.
- 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).
- Keep all your important documents in the list, they can be encrypted or decrypted with the push of a button.
- A quick way of highliting a collection of files from the list is to left click on the right side of the files and drag enclosing the desired files in the square 'Rubber Band'.

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

Stealth Encryptor 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 Stealth Encryptor, you can immediately activate your copy. By "Activating" Stealth Encryptor, 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.
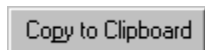
Controls:
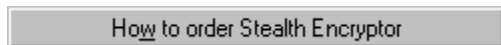
How to order Stealth Encryptor
Press this button (or Alt+W) to display the Order Form.

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.
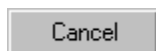
Copy to Clipboard
Press this button (or Alt+P) to copy the Installation Code to the clipboard making it easy to paste it into an e-mail or order form.

Enter Activation Code:
Enter the activation code here.
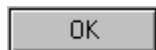
OK
Press this button (or Alt+O) to activate the program.

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

Order Information

When you order Stealth Encryptor, 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:

Stealth Encryptor (in US$)............................ 34.95 (or site license)

Washington residents add 8.25% sales tax................_____

Shipping and handling................................... 5.00

                                        ============

            Total in US$................................_____

Site License:

2   to 19: $30.00 each.
20 to 49: $20.00 each.
50 to 99: $15.00 each.
100 to 199: $10.00 each.
200 and up: Contact us.

The prices are subjected to change without notice, please visit our
WEB site for the latest information: http://www.tropsoft.com.

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 via CompuServe: CompuServe users can order Stealth Encryptor on-line. Enter the command GO
SWREG and follow the instructions.
The Stealth Encryptor **registration id is 13487**. The ordering price will be added to your CompuServe bill.

Ordering by credit card:
The easiest way of ordering by credit card is through our secured on-line order page. Your credit card information is
fully protected.
**The secure order form can be accessed at the bottom of the page in our WEB site at
http://www.tropsoft.com**

You can also mail this order form and credit card information to:
Tropical Software
27 Georgetown Dr.
Eatontown, NJ 07724

If you prefer to order by phone or fax, please use 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.
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.
Ask for Order # 14389
PsL requires the following information:
Credit Card [ ] MasterCard [ ] 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.**

To contact Tropical Software:
- CompuServe -   73742,1104

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

Stealth Encryptor is only shipped on 3.5 inch disks.

Stealth Encryptor Browser Mode

▪

Encryption is a very powerful way of protecting the information in a file from being examined by others. Encryption works by scrambling the contents of a 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.

The encryption is performed according to the selections in the Encryption Details Selection Bar .

Controls:
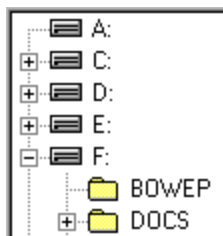
Navigate down the drive/directory tree and highlight the desired directory.

▪
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. The right column shows the disguised filename for each file that was encrypted with the Stealth option.

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

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

▪
Press this button (or Alt+S) to refresh the information contained in the file lists. To refresh the directory tree, close the branch by pushing the - box and then open it again by pushing the + box.

Operation:

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 corresponding button.

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. Feel free to rename it as you wish, Stealth will still keep track of the original name.
- 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).
- A quick way of highliting a collection of files from the list is to left click on the right side of the files and drag enclosing the desired files in the square 'Rubber Band'.

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.
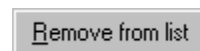

:Controls:
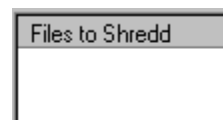
Files to Shredd

Shows a list of all the files that are ready to be shredded. Files can be added and   removed from this list with the following controls.
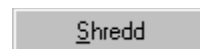
Select Files

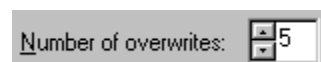Press this button (or Alt+E) to bring the file selection screen.
You can also drag the files from the Explorer to this screen.

Remove from list

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

Shredd

Press this button (or Alt+S) to shred all the listed files.

Number of overwrites: 5

Click the arrows 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.

Procedure:

Press the select files button, select drive, directory, one or more files and press the OK button. (or drag files from the Explorer)
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 Explorer 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.
- A quick way of highliting a collection of files from the list is to left click on the right side of the files and drag enclosing the desired files in the square 'Rubber Band'.
- Press ESC to cancel shredding of all remaining files in the list.

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

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

Password Setting

A password consists of a string of 1 to 12 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:
protection#1
secure13
@#$%^&*(
10apples

Controls:

Current Password	

Type here the current password.

New Password	

Type here the new password.

Verify New Password	

Type here the new password again for verification.

▪
Press this button to submit the change.

▪
Press this button to cancel the password change operation.

Encryption Setting

▪

Encryption is a powerful tool and like any powerful tool it can be dangerous leading to data loss if not used properly.

The most frequent cause for data loss is when files are encrypted with one key and then decrypted with a different key.

When the key is case sensitive, this problem becomes even more severe.

The encryption operation offers 4 different levels of functionality to let users get confortable with encryption while minimizing the chances of data loss:
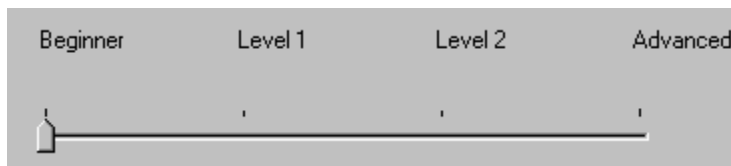
Beginner Level - The Key is case insensitive and an attempt to decrypt with a different key is aborted.
Key differences like apple and Apple are ignored and decryption with a misspelled key is aborted and doesn't corrupt the file.
This setting fully protects the information against misoperation.

Level 1 - The key is case insensitive and decrypting with a different key corrupts it.
Key differences like apple and Apple are ignored and decryption still works correctly. Misspelled key on the other hand will corrupt the file on decryption.

Level 2 - The key is case sensitive and an attempt to decrypt with a different key is aborted.
Key differences like apple and Apple are NOT ignored but decryption with a misspelled key is aborted and doesn't corrupt the file.

Advanced - The key is case sensitive and decrypting with a different key corrupts it.
No protection at all, should only be used when you feel very confortable with encryption.

As you progress towards the advanced level, the encrypted files become slightly more secure.

This settings acts on all encryption operations.

Always have all your files backed up!

Encryption Details Selection Bar

This toolbar's settings acts on all encryption operations except the e-mail encrypt/decrypt.

This toolbar is dockable, you can drag it out of it's position and make it float or dock it at the bottom of the screen.

Media Stealth

Select this option for an encryption algorithm specially developed for image and
multimedia files. It's repetitive sequence of random bursts render these files unreadable to virtually every existing
viewer with lightning speed. **Stealth Media uses only the first 40 bits (5 digits) of the key.**

Fast Encryption

Select this option for fast encryption. Fast encryption is sufficient for most cases.

DES Encryption

Select this option 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.

Stealth mode (Disguise Filename)

When this option is selected, the filename is changed to a combination of random numbers. The real name will still
show in the encrypted files list. Feel free to rename it as you wish, Stealth will still keep track of the original name.

Always ask for the key

Select this option to have Stealth ask for the key before every encryption or decryption operation. When this option
is not selected the key is memorized within the current run of he program but is not stored in disk (for security
reasons), therefore the first encryption/decryption operation will still ask for the key.

Encryption Key

Press this button to enter or change the current encryption key. This button is only valid when the Always ask for
key option is not selected.

Tips:
*- You can drag this toolbar out of it's position and make it float or dock it at the bottom of the screen. To drag, click
anywhere in the toolbar's body*

Browser Mode Button

This button tougles to the Encryption <u>Browser Mode</u>.

List Mode button

This button tougles to the Encryption <u>List Mode</u>.

Lock button

Press this button to lock Stealth, a password is needed to unlock it.

Shredder Mode button

This button tougles to the <u>File Shredder</u>.

Settings button

Press this button to start the settings screen.
The settings screen allows control of:
 - Encryption Setting
 - Password Setting

Files Backup button

This button tougles to the <u>Files Backup</u>.

E-Mail Encrypt/Decrypt Button

This button starts the E-Mail Encrypt/Decrypt

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
Good#@()

Stealth Media uses only the first 40 bits (5 digits) of the key.

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.

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

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

Tips:
- Use special characters like !@#$%&(and numbers and minimize the use of common English words to make it more difficult to guess the key.

E-Mail Encrypt/Decrypt

When you send an email, the text travels openly and unprotected through Internet connections (routers) until it reaches it's destination, anyone with technical knowledge can read it undetectedly.
Within a corporation, email is stored in disk, it's considered company property and it can be legally read and stored without your knowledge.
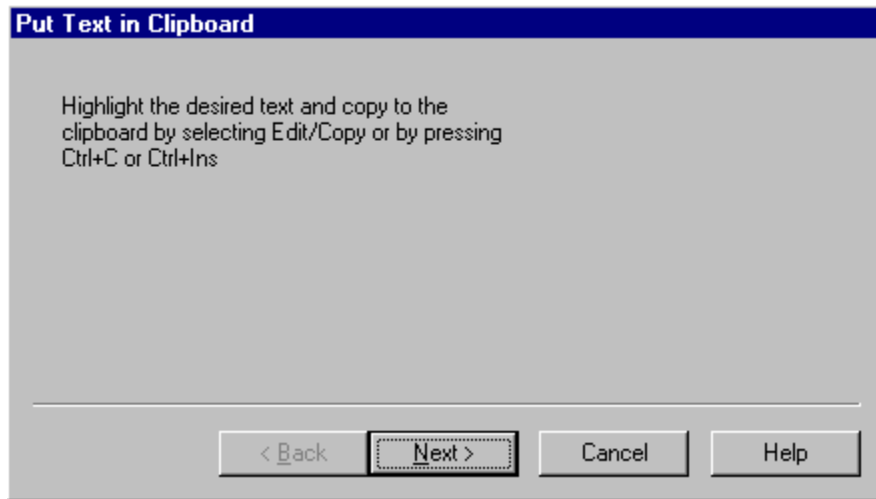When encrypted, the email can still be accessed as explained above but the contents can only be retrieved by decrypting with the exact same key.

The E-Mail Encrypt/Decrypt is a Wizard type operation that through the use of the clipboard, makes it easy to encrypt and decrypt parts or the whole e-mail message.

Instructions:

Have your email program ready and the desired message open.
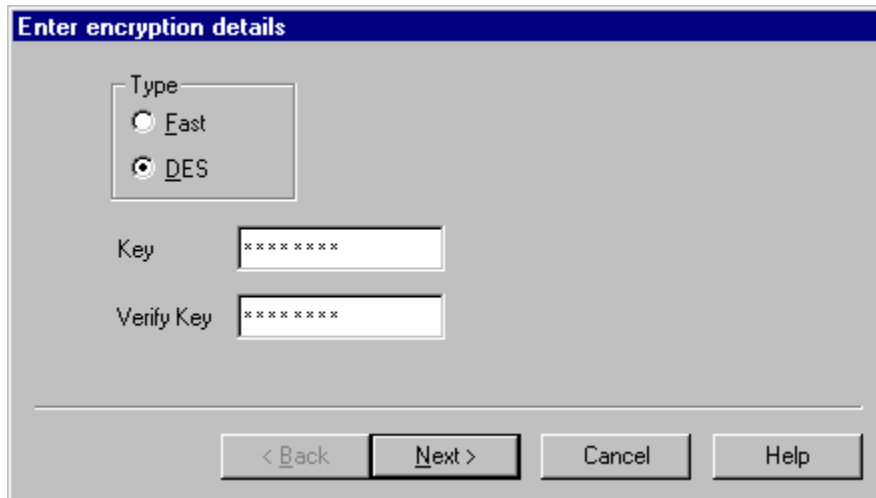
Select the desired operation and press next.

Put Text in Clipboard

Highlight the desired text and copy to the
clipboard by selecting Edit/Copy or by pressing
Ctrl+C or Ctrl+Ins

< Back | Next > | Cancel | Help

Highlight the desired text, copy (or cut) it into the clipboard and press next.
If you are decrypting, highlight the encrypted text from (including) the beginning asterisks to the ending asterisks.

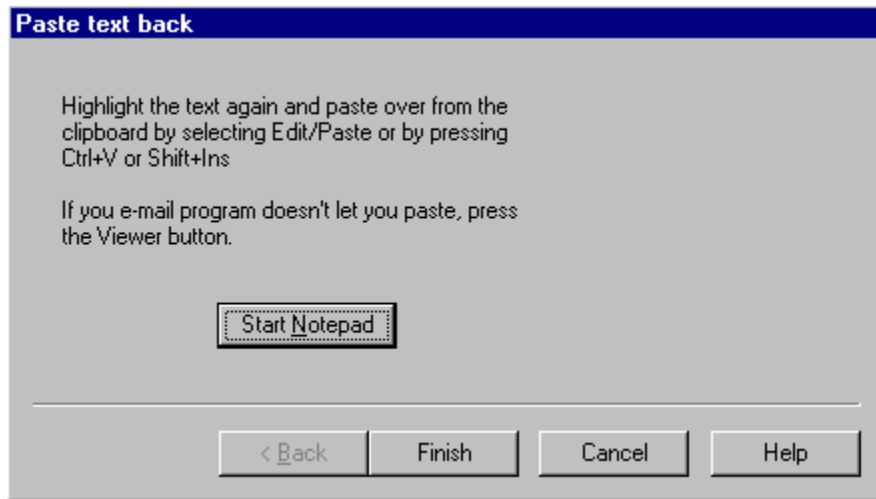**Enter encryption details**

Type
○ Fast
◉ DES

Key   [* * * * * * * *]

Verify Key [* * * * * * * *]

< Back | Next > | Cancel | Help

Enter the key and press next.
The encryption type used is the one selected in the Encryption Details Selection Bar
The encryption level (from beginner to advanced) applies to this operation as well.

Paste text back

Highlight the text again and paste over from the
clipboard by selecting Edit/Paste or by pressing
Ctrl+V or Shift+Ins

If you e-mail program doesn't let you paste, press
the Viewer button.

[Start Notepad]

[< Back] [Finish] [Cancel] [Help]

Paste now the result of the operation back into the document. Some e-mail programs don't let you modify the text on a received mail screen, in this case, press the Start Notepad button and paste it there for viewing and saving to disk.

Tips:
- You can use this function to encrypt any kind of text, not only e-mail.
- When you exchange the encryption key with your partner(s), do it using a media different than the Internet like a phone call or fax or personally. If you must use the Internet, send it in a different message and preferably in a different day.

Encryption Action Screen

This screen shows when Stealth is encrypting or decrypting a list of files.

It shows the number of files already processed, the total number of files and the name of the file that is currently being processed.

pressing the Cancel button gives you a chance to cancel the operation for all the remaining files. (After it completes the operation on the current one).