Help Contents

[Using the HideThat Screen Saver](#)
Step-by-step instructions to help you fully utilize HideThat

[General Computer Security Information](#)
Tips and guides to computer security by best-selling author of the NCSA Guide to PC and LAN Security, and Certified Information Systems Security Professional, Stephen Cobb

[Technical Support](#)
Available support to help you get the most from your CobWeb Applications product

Using the HideThat Screen Saver
see also

 About HideThat Screen Saver

Selecting HideThat Screen Saver

Setting HideThat Password

Closing HideThat Screen Saver

Customizing HideThat

Leaving and Retrieving Messages

Setting Mouse Hot and Cold Spots

Using Spot Watcher

Securing your computer during start up

Using controls in Windows 95

Registering HideThat

UnInstalling HideThat and Spot Watcher

Acknowledgments

General Computer Security Information

see also

You might want to combine screen saving with security awareness.   You can use HideThat as a theft deterrent by using either the Scrolling Message or the Bouncing Picture options.   For example, HideThat can display security reminders as a Bouncing Picture and several examples can be downloaded from http://www.cobweb.co.uk.   You could enter your Scrolling Message as: "Alarm On, Motion Detector Armed!".   Such text scrolling across the screen in a dark office is quite impressive.

All forms of password protection share a common weakness, soft passwords.   These are passwords that are easy to guess.   Most of us are familiar with the soft password problem, whether it is the pin number for our cash card or the combination for our bike lock.   We have a natural tendency to choose something that is easy to remember, like the last four digits of our home phone number, or letters and digits from dates, like birthdays, and so on.   Unfortunately, such numbers are directly associated with us.   Someone pretending to be us will most likely know those numbers.

On the other hand, if we have to use a password that is decreed by someone else and means nothing to us, which is the case with some banks and bike locks, we may well feel compelled to write it down somewhere, thus exposing it to other people.

The same problem arises when we use computers and a program asks us to pick a password.   We tend to pick a word or string of characters that are somehow related to us, and thus guessable by someone pretending to be us.   Or we use a word that is entirely random, in which case we will feel obliged to write it down in order to remember it, thus exposing it to possible discovery (taping the password to the underside of the keyboard, is NOT recommended).

Commonly used passwords such as "pass" or the last four digits of your home phone number might defeat an inexperienced user who has inadvertently stumbled on a protected file.   They will not present a problem for the experienced and determined interloper.   Indeed, you can easily acquire extensive lists of commonly used passwords, compiled by experienced hackers.

The ideal password is easy to remember and hard to guess. What makes a password difficult to guess?. Consider the following criteria:

1. There should be no logical connection between password and the user.
2. There should be no logical connection between password and the protected resource (building, system, file, etc.).
3. If permitted, the password should contain a mixture of characters, both uppercase and lowercase, plus numbers, punctuation, and special symbols.
4. The password should not be identical to any string of characters that appears as a word in a dictionary.
5. The password should be at least eight characters long.

Adhering to the first two criteria will decrease the threat from an attacker who knows things about the protected resource, or the person to whom it belongs, and so use that information to guess the password. The last three criteria ensure that the interloper cannot simply try a series of ordinary words.

Encryption systems that can use punctuation and "special characters" allow for stronger passwords. For example, there are 256 characters in ASCII and only 62 of these are letters and digits (26 uppercase and lowercase plus 0-9). That leaves 194 other characters. Using an eight character password that can contain any one of 256 codes gives an incredible 256^8 possible combinations.   It can greatly enhance the power of passwords.   HideThat allows "special characters" and up to 20 characters in its password.

Password systems that accept spaces, such as HideThat, allow you to use phrases as keys. A phrase like "Time after time" is easy to remember and not difficult to type.   However, it is quite difficult to guess because there are 15 characters.   If you cannot use spaces in the password, try underlines or hyphens,

as in Blue_Suede_Shoes, or simply run the words together, as in TimeafterTime.

Of course, just as words associated with the file's creator or its contents should be avoided, so should popular phrases and inside jokes.   Don't use BlueSuedeShoes if you have a picture of Elvis on your desk.   Adding numbers and other characters can strengthen the password as in: "Chinatown, 1975".   Yet another method of password selection is to use acronyms for sentences, phrases, quotes, song titles, and so on.   For example, the fairly obscure password YoLoThLoFe is short for "You've Lost That Loving Feeling."

If you have to come up with a lot of passwords, for example, where a whole department is using passwords, then it might be necessary to adopt a centralized system where passwords are given to users, rather than chosen by the users themselves.   Indeed, if employees are required to use passwords on files or systems that management will need to access, then a management-controlled password selection system becomes essential.

If you go to the trouble and expense of instituting a password system, you will want to make sure that it is not simply put in place and left to run itself.   Password systems quickly lose their effectiveness if they are not enforced, maintained, and monitored.   Consider the following points when checking up on password-based security systems:

* Make sure employees are properly instructed in proper password selection and password rules such as minimum length.
* Develop a list of prohibited passwords to cross-check against those in use.   Update the list regularly, and perform the cross-check at random intervals.
* Check that procedures are in place to promptly remove passwords assigned to persons who leave the organization.   Check that procedures have been complied with, removing all redundant passwords.
* Check procedures to revoke the password of an employee who has been transferred from one department to another.
* If your password system does not have a minimum length requirement, verify the length of passwords being used. The minimum length password for HideThat is 5 characters.
* Some password systems can be activated by macros or scripts, which means that the user's password is kept in a file that might not be protected.   Check whether users are employing such systems and verify that they are secure.
* Maintain a log of previously used passwords, listed by employee name.
* Check that you have a readily available up-to-date list of authorized users.
* If users are having difficulty remembering passwords, check the security of procedures for assigning new passwords and coach employees of safe methods of recording passwords.
* Monitor the number of illegal attempts to access files and note any increases.
* Compare passwords used by employees within a single department.   Make sure everyone is not using the same password.

An ongoing effort is required to maintain the effectiveness of a password system.   Reminding users of the rules and their responsibilities should not be something you do only after a major intrusion reveals a problem.   While maintenance operations are somewhat repetitive and boring, they are essential to maximize security.

About BIOS Passwords

The ability to make booting of a computer dependent upon the user entering the correct password has been around for many years.   The simplest system is a single password, established via the same Setup program that allows changes to BIOS settings, such as hard drive parameters, which are stored in CMOS.   Once a password has been established, any attempt to boot the machine will halt until the correct password has been supplied in response to a simple, on-screen prompt.   Any attempt to change the password will be denied unless the user already knows the correct password.

Some PC vendors such as Apricot and DEC offer constructive variations on the basic BIOS password

scheme.   These use custom BIOS chips to provide for multiple user accounts with different passwords. Thus a master account can be created which prevents alterations by users who don't know the master password.   Different access controls can also be set for different users, such as the ability to read or write floppy disks. More personal computer manufacturers need to follow this example.

You can thwart BIOS-based access control.   Resetting the CMOS back to default values will erase the password, but this requires disconnecting or draining the battery that supports the CMOS storage.   This in turn requires access to the case that contains the motherboard.   In other words, one more reason that all of your system cases should have locks, that are locked with keys that are properly managed.   One weakness of BIOS-based access control systems is that they tend to offer limited length passwords.   Be sure to use the full length allowed in order to defeat guessing attacks.   Some BIOS password systems reboot the machine after three wrong passwords, which is a nice added margin of safety.

The information above should have provided you with some ideas on how to instigate a more secure computer environment.   Happy and safe computing.

Note

For more computer security information visit:
http://www.cobweb.co.uk
or
http://www.ncsa.com

Technical Support

The HideThat Screen Saver version 1.1 and Spot Watcher version 1.1 were developed by CobWeb Applications.
Copyright © 1996 CobWeb Applications

CobWeb Applications is run by Mike Cobb and is based in Surrey, England.

CobWeb's web page address is http://www.cobweb.co.uk.
If you have any queries or comments, or are interested in a special edition of HideThat, Mike can be emailed at mikec@cobweb.co.uk
or CompuServe 100664,2225

Other CobWeb Applications' products can be downloaded for free evaluation from
http://www.cobweb.co.uk

CobWeb Applications

Cherry Tree Cottage
Leatherhead Road
Great Bookham
Surrey
England
KT23 4SS

Unauthorized reproduction is strictly forbidden.

About HideThat Screen Saver   -   Version 1.1

Windows 95 supports special applications called screen savers which start when the mouse and keyboard have been idle for a period of time. Screen savers exist for two main reasons:

·   To avoid phosphor burn caused by static images on a screen
·   To conceal sensitive information left on a screen

The term "screen-saver" comes from the days of monochrome monitors which suffered "burn-in" if the same image remained on the screen for too long.   You can still find old green screens that bear the outline of the 1-2-3 spreadsheet because of this.   The answer was to use a screen blanker or screen saver, a program that, instead of sending an image to the screen sends either no image at all, or one that changes to avoid "burn in".   This nicely coincides with a solution to the problem of people reading what you have on your screen while you are away from the computer.

The main idea of the HideThat Screen Saver is to blank the screen on command or after a certain amount of time (set by the user) during which there is no mouse movement or keyboard input, in order to protect your computer's software and to hide work in progress while the computer is left unattended.   Moving images are used more often than complete blanking since they let you know that the machine is still turned on.

The use of password protection on a screen saver means that when the screen saver has been activated and someone presses a key or moves the mouse, a password is requested.   Failure to provide the correct password means that the screen stays locked.   This helps prevent one of the most common forms of network hacking, a person inside the company using someone else's workstation while they are logged onto the network.

Many screen savers have password protection but this can be overridden by using Alt+Tab or Ctrl+Alt+Del key combinations.   HideThat stops anyone from moving to another program on the computer until they have entered the correct HideThat password.

You have a choice of five HideThat screen savers, from just a blank screen to one that enables you to choose which picture you want to bounce around the screen.   You can also customize the password dialog boxes so that the screen saver appears to be your own.

With the Scrolling Message screen saver you can leave a message for people passing your work place.

Anyone passing your workplace can leave you messages that will be hidden until your return. (Password Protection must be enabled in order to use this feature.)

By using the Hot and Cold Spots you can start the screen saver immediately, or stop HideThat activating at all.

HideThat works in conjunction with Spot Watcher, which appears as a pair of eyes in the corner of your Task Bar and enables you to quickly change HideThat settings without having to open the Control Panel. In order to help protect your computer's software, Spot Watcher can be launched at Windows startup.   If Spot Watcher is running you can use Hot and Cold spots, and choose to have HideThat start automatically on system start up or if Windows 95 is not shut down correctly (e.g. someone reboots your PC to try and bypass HideThat). This provides additional password protection. Read the topic secure your computer during startup before selecting these options.
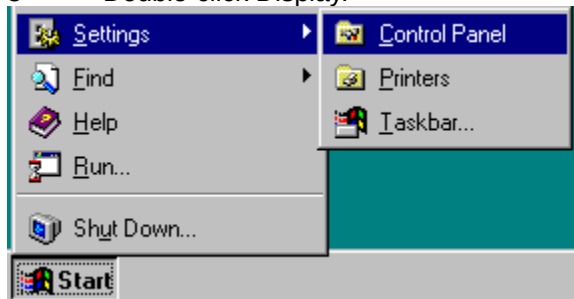
Selecting HideThat Screen Saver

To protect your screen using the HideThat screen saver

1   Double-click the My Computer icon on the desktop.
2   Double-click the Control Panel folder.
3   Double-click Display.

or
1   Click Start.
2   Select Settings, Control Panel.
3   Double-click Display.
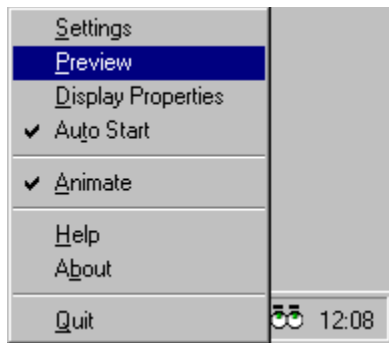

4   In the list box in the Screen Saver area, select the HideThat screen saver.
5   To customize the HideThat screen saver, click Settings.

Tips

The screen saver starts if your computer is idle for the number of minutes specified in the Wait box. To clear the screen saver after it has started, move your mouse or press any key.

To quickly change HideThat settings, right mouse click Spot Watcher and select Settings from the Pop-up menu.

Settings	
Preview	
Display Properties	
✔ Auto Start	
✔ Animate	
Help	
About	
Quit	👓 12:08

To quickly change other display properties, right mouse click Spot Watcher and select Display Properties from the Pop-up menu.

Setting the HideThat Password
see also
General Computer Security Information

To protect your files by assigning a HideThat password

1   Select Control Panel, Display.
2   In the list box in the Screen Saver area, select the HideThat screen saver.
3   Make sure Password Protected is checked, and then click Change Password.

6   First, type in your existing password.   **If you have not set a HideThat password before, then Tab to the New Password box**.   Type your password in the New Password box, and then confirm the password by typing it again in the Retype New Password box.   A HideThat password has to be at least 5 characters long and can be up to 20 characters long.   Passwords can include letters, numbers, punctuation, and special characters such as Alt+0169, the © symbol. As you type the password, HideThat displays an asterisk (*) for each character you type. **HideThat passwords are case-sensitive**.

Note

If you assign a password to HideThat screen saver, people who do not know the password cannot clear the screen saver, and therefore cannot easily gain access to your computer.   The HideThat password is encrypted using the Blowfish algorithm, and stored separately to other Windows passwords, due to concerns over their security.   The password for the standard Windows screen saver is stored with relatively weak encryption, meaning that it is easily decrypted.   Since users have a tendency to employ the same password in different applications, discovering the Windows screen saver password might also reveal other key passwords.

HideThat meets these guidelines for password protection systems laid out in The NCSA Guide to PC and LAN Security (McGraw-Hill, 1996):
* Uses a wide variety of characters, including uppercase and lowercase characters, punctuation, spaces, or ASCII codes.
* Requires a minimum key length to prevent short passwords.
* Disguises the actual password as it is entered.
* Limits the number of failed attempts at password entry, locking the system to deter brute force attacks.

HideThat allows three attempts at entering the password. After three incorrect passwords HideThat will disable the keyboard and mouse. You can set the number of minutes your computer is locked up, from between zero which gives no protection against repeated attempts, to 30 minutes.

Administrators

HideThat provides **STRONG** password protection. If a user forgets his password or for example a system crash corrupts the password (highly unlikely but not impossible), you can use the following steps to clear the password:

If you are locked out by HideThat start the computer in Safe Mode.
Run regedit.exe - usually located in the Windows directory
Open
        HKEY_CURRENT_USER
                Software
                        CobWeb
                                HideThat
                                        Settings
Right click on the name Password in the right hand list and select Modify

Delete the Value data
Click OK
Password now looks like this ""
Close regedit.

You have now set the password to blank i.e. nothing.
(Using regedit is not recommended for inexperienced users).

If you have disabled the F Keys during start up, start from your Windows 95 system recovery disk. See
Securing your computer during start up.

Closing the HideThat Screen Saver
see also
Leaving and Retrieving Messages

To close HideThat screen saver after it has started, move your mouse or press any key.   If Password Protection is on, type your password in the Password box and press Enter or click the OK button.

If you have any messages waiting they will be displayed before HideThat closes.

Note

You have three attempts to enter the correct password.   If the third attempt is also incorrect, HideThat will lock the mouse and keyboard for the number of selected minutes.

Customizing HideThat

To set your preferences for HideThat screen saver

1	Click Start.
2	Select Settings, Control Panel.
3	Double-click Display.
4	Select the Screen Saver page.
5	In the list box in the Screen Saver area, select the HideThat screen saver.
6	To customize the HideThat screen saver, click Settings.

or

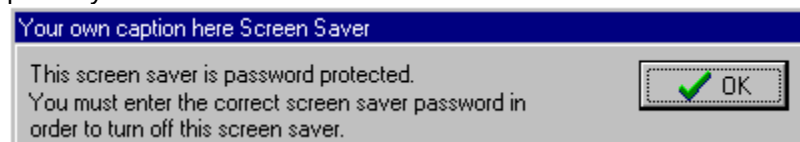To quickly change HideThat settings, right mouse click Spot Watcher and select Settings from the [pop-up menu](#).

Select the screen saver you would like to run from the list box at the top of the Settings form.
You have a choice of five screen savers

1	Blank Screen
2	Patrolling Eyes
3	[Scrolling Message](#) - Leave a message for passers-by.
4	[Your Bouncing Picture](#) - Select a picture to patrol your screen.
5	[Your Scrambled Picture](#) - Select a picture to be slowly scrambled.

To fully customise the HideThat screen saver, enter the caption that you would like to appear in the password dialog boxes, by typing the text in the 'Dialog Box Caption' box.   This text can be up to 38 characters long.
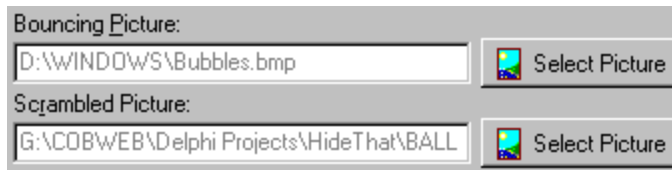

This caption is then prefixed to the words Screen Saver so that the HideThat dialog boxes appear to be part of your own screen saver.

Confirm your settings by clicking OK.

Bouncing Picture

Bouncing Picture:
D:\WINDOWS\Bubbles.bmp   [icon] Select Picture
Scrambled Picture:
G:\COBWEB\Delphi Projects\HideThat\BALL   [icon] Select Picture

 To select a picture to patrol your screen, click the first Select Picture button or press Alt+P.   This opens the Select Bouncing Picture dialog box, which enables you to search your files for a picture.   The picture must be of the bitmap picture type, usually denoted by the file extension BMP.   Once you have selected your picture, click the Open button.   This will enter the file path into the Bouncing Picture box for you. You cannot type in the file path yourself.

When you now select the 'Bouncing Picture' screen saver from the list box at the top of the Settings form, your picture will move around the screen.

Note

If the picture you select is larger than the actual screen, the picture will not necessarily appear to move around the screen.

Scrambled Picture

 To select the picture that you would like HideThat to scramble, click the second Select Picture button or press Alt+R.   This opens the Select Scrambled Picture dialog box, which enables you to search your files for a picture.   The picture must be of the bitmap picture type, usually denoted by the file extension BMP.   Once you have selected your picture, click the Open button.   This will enter the file path into the Scrambled Picture box for you.   You cannot type in the file path yourself.
When you now select the 'Scrambled Picture' screen saver from the list box at the top of the Settings form, your picture will be displayed and scrambled by HideThat.

Note

HideThat restores your picture every five minutes.   Choose as large a picture as possible for the best effect.

Scrolling Message

To leave a message for people passing your work place select the 'Scrolling Message' screen saver from the list box at the top of the Settings form.

In the Message Text box type the message you want to appear on the screen.   This can be up to 200 characters long.   Select the Font by clicking the Format Text button and choose a background color from the Background Color list box.

You can further customize the Scrolling Message by selecting its Position on the screen.   Centred will scroll it across the middle of the screen whereas Random will change its position each time HideThat starts.   Speed adjusts how quickly the message moves across the screen.

Note

To stop and hide the scrolling message, or to restart it, press M.

Leaving and Retrieving Messages
see also
Closing HideThat Screen Saver

To leave a message for people passing your work place, select the 'Scrolling Message' screen saver from the list box at the top of the Settings form.

People passing your work place can leave a message for you by moving the mouse or pressing any key. This will bring up the Enter Password dialog box, the lower half of which contains the Message box. People wishing to leave a message must leave their name as well as a message.   The message can be as long as they like.   To post the message to you, they click the Post It button.   To clear an error they click the Clear button.

Once you have entered your password, any messages (up to 20) will be displayed along with the time they were left.   The names are listed on the left-hand side.   Select a name by clicking on it and the message will be displayed on the message pad.

Note

Password Protection must be on, in order for HideThat to take messages.

Setting Mouse Hot and Cold Spots
see also
Using Spot Watcher

Mouse Hot and Cold Spots enable you to immediately start the HideThat screen saver or to prevent it starting, without having to change your settings via the Control Panel. To set your Hot and Cold spots

1   Select Control Panel, Display.
2   In the list box in the Screen Saver area, select the HideThat screen saver.
3   Click Settings.
4   Select the Security page.

Left mouse click within the picture of the computer screen to select which corner is to be the Hot Spot.
Left click the Hot Spot again to clear it.   Confirm these settings by clicking OK.
If you now move the cursor to the Hot Spot, the screen saver will be activated immediately.

Right mouse click within the picture of the computer screen to select which corner is to be the Cold Spot.
Right click the Cold Spot again to clear it.
If you now leave the cursor in the Cold Spot, the screen saver will be prevented from activating.

To set the Hot and Cold Spots using the menu, right click the middle of the picture of a screen on the Security page of HideThat Settings, or use the Application key if available, to access the pop-up menu

Note

By setting a Hot spot, you can hide your work immediately if you leave your desk or to prevent a passerby from seeing your work.   By setting a Cold spot you can prevent HideThat screen saver activating while you are working at your computer.

Using Spot Watcher
see also

Start Spot Watcher from the Start menu or select Auto Start from the pop-up menu to start Spot Watcher automatically when you switch on your computer.   By right mouse clicking on the eyes, a pop-up menu allows you to quickly change HideThat settings.   You can also stop the Spot Watcher eyes from revolving.

If you have selected the pop-up menu but decide not to make a selection, just click anywhere on the desk top to close the menu.
Selecting Quit closes Spot Watcher until you next switch on your computer or until you select Spot Watcher from the Start Programs menu
If Spot Watcher is closed, the Hot and Cold Spots will not operate.
If you have selected the option to start HideThat if Windows 95 is not shut down correctly and Spot Watcher is running, Spot Watcher will start HideThat immediately when the computer is restarted and provide password protection.
If you have selected Start Screen Saver on System Startup, Spot Watcher will start HideThat when Windows 95 starts. This can provide password protection if you do not want, for example, the cleaner, the cat or the children accessing your files.
HideThat will also be displayed on your Task Bar, to indicate that Spot Watcher activated the screen saver on startup.

Note

Read the section on securing your computer during start up.

HideThat Security

On how to use the HideThat screen saver - see: [Selecting HideThat Screen Saver](#)

On how to assign a password - see: [Setting HideThat Password](#).

On how to use Hot and Cold Spots - see: [Setting Mouse Hot and Cold Spots](#).

On using Spot Watcher - see: [Using Spot Watcher](#).

On how to secure your computer during startup - see: [Securing your computer](#) during start up.

For information on general computer security - see: [General Computer Security Information](#).

Securing your computer during start up
see also
General Computer Security

Below is a list of measures you can take to help secure your computer during startup, using mainly software based techniques.

Access limitation schemes endeavor to ensure only authorized people can reach and use the data and programs on your PC.   Windows 95 is particularly insecure when it comes to controlling access.   If you are using Windows 95 do not rely on the primary Windows Logon or Network logon as a means of securing access to your system.   Anyone can usually get past it by pressing the Escape key!   Also Windows 95 allows most Windows-based startup protection to be thwarted by experienced hackers.

The BIOS, short for Basic Input/Output Services, is the control program of your PC, stored in a chip inside the computer.   It is responsible for starting up your computer, transferring control of the hardware to your operating system, and for handling other low-level functions, such as disk access.   A convenient feature that most BIOS manufacturers include is a startup password.   **This prevents access to the system until you enter the correct password.   If you have this facility, it is recommended that you use it**. If your system allows, you may set up a BIOS password for both the Setup screen and access to the system.   It will protect your software from all but the determined thief.

If your BIOS supports any of the following, make these changes to your BIOS setup:

1. Change boot sequence to "C: only" or "C: then A:" - this option prevents the easy bypass of the password program by booting from a floppy.
2. Disable BIOS setup prompt on startup - this option prevents the display of the key presses needed to enter the BIOS utility.

If someone has access to your computer when it is already turned on, they could use a utility program to override the BIOS settings.   However, using HideThat to protect your system will prevent this type of access.   Also, it is possible to alter the BIOS settings and remove the password protection by tampering with the computers internal battery.   For this reason I recommend you always use a case locking device to prevent such tampering.   For about such protection devices see:htpp://www.ncsa.com/pclan/chap04.html

Next it is necessary to disable the bypass of any startup files.   When you switch on your computer, a "Starting Windows 95" message appears on the screen before Windows 95 continues to boot.   By pressing either the F4, F5, F6 or F8 keys at this point, you can either bypass or step through commands in your start up files.

This is a very useful feature.   If you are having problems with your computer, you can start Windows 95 in Safe mode (F5), start Windows 95 in Safe mode with network (F6), a previous version of MSDOS (F4), or select from the StartUp Menu (F8).   This will allow you to start the computer without installing troublesome software or hardware.
It does, however, allow someone to bypass any security programs by rebooting your computer.

By disabling the F4, F5, F6 and F8 keys during start-up, you will prevent anyone overriding your usual start-up files.   This increases protection of your software but should not be used if you are suffering from configuration problems.
Add the following line to your 'MSDOS.SYS' file under [OPTIONS] to disable the F keys during startup:
BootKeys=0
 As MSDOS.SYS is a system file, you will first have to change its properties to allow you to make the above change. Right click the file in Windows Explorer and select properties, then deselect the Read-only box.   Remember to change the file back to Read-only, once you have finished.   MSDOS.SYS is located in your root directory e.g. C:\.
Do not change this file yourself, unless you are an experienced user.

To enable the F keys during startup write:
BootKeys=1

Microsoft PowerToys is a freeware product provided by Microsoft that contains a tool called Tweak UI. Tweak UI's Boot tab enables you to customize your boot options easily.   Also the Paranoia tab enables you to clear all the file histories stored in the Start menu Documents etc. when anyone logs on to the computer. PowerToys can be downloaded from:
http://www.microsoft.com/windows/software/powertoy.htm.

If you have upgraded from Windows 3.x, you can disable the F5 and F8 keys during start up of a previous windows version, by adding the following line to your CONFIG.SYS file:
SWITCHES= /F /N
The CONFIG.SYS file is located in your root directory e.g. C:\.

From the HideThat Settings, you can choose to have HideThat start as soon as Windows 95 starts. Also you can have HideThat start as soon as Windows 95 starts, if the computer was not shut down correctly, e.g. someone reboots while Windows 95 is still running. Spot Watcher must be running for this option to be able to operate.

IMPORTANT: CHECK YOUR PASSWORD AND THAT YOUR RECOVERY PROCEDURE WORKS BEFORE USING THE ABOVE SETTINGS.

HideThat provides **STRONG** password protection. If you forget your password or for example a system crash corrupts the password (highly unlikely but not impossible), you can use the following steps to clear the password:

If you are locked out by HideThat start the computer in Safe Mode.
Run regedit.exe - usually located in the Windows directory
Open
      HKEY_CURRENT_USER
         Software
            CobWeb
               HideThat
                  Settings
Right click on the name Password in the right hand list and select Modify
Delete the Value data
Click OK
Password now looks like this ""
Close regedit.

You have now set the password to blank i.e. nothing.
(Using regedit is not recommended for inexperienced users).

If you have disabled the F Keys during start up, start your computer from your Windows 95 system recovery disk.
If you have changed the boot sequence from A to C, enter BIOS setup and change the sequence to A then C, and boot from your recovery disk.

For more information on computer security, visit:
http://www.cobweb.co.uk
or
http://www.ncsa.com

If your computer does not support a BIOS password, registered users of HideThat can obtain a free program on request, called PassThat.   PassThat provides password protection that will prevent access to your system until you enter the correct password.

Using controls in Windows 95

If you are not sure how to interact with the various controls in Windows 95, below is a list of controls used in HideThat and how to access them using a mouse or keyboard.
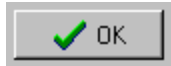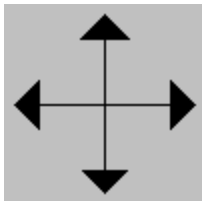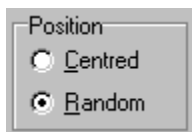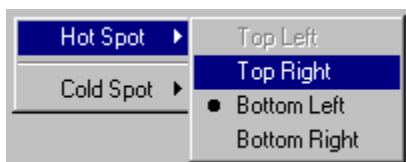
Buttons
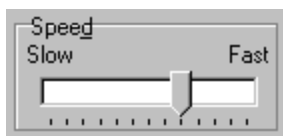
Context-Sensitive Help

Drop-down lists

Navigating controls

Option Buttons

Pop-up menus

Slider Control

Registering HideThat

HideThat and Spot Watcher are Shareware.   Both are fully functional for 30 days after installation, so that you can decide whether you wish to purchase them, the ultimate try before you buy.   If you have not registered HideThat after 30 days, all the security features of Spot Watcher and HideThat are still enabled, but HideThat will only display an "Unregistered Software"   message when it is activated.

If you wish to register HideThat and Spot Watcher, right click on the Spot Watcher eyes and select Register.   Write down the following details:

1   Computer Name
2   User Number
3   Computer Number

4   Email the above details to mikec@cobweb.co.uk or CompuServe 100664,2225 with the subject "Reg HideThat v1.1".
5   To pay via a secure credit card transaction on the internet, visit http://www.cobweb.co.uk and follow the registration links.
6   To pay via a CompuServe account, select SERVICES GO SHAREWARE.   Select Shareware Registration and then Register Shareware.   When prompted for search criteria, type "HideThat" in Keywords or "13014" in Registration ID, and follow the instructions.   Your CompuServe account will be debited with the equivalent of $25.
7   To pay by cheque, send the above details with your name, address or email address, along with a cheque, payable to "CobWeb Applications" for £16 or $25 to:

CobWeb Applications
Cherry Tree Cottage
Leatherhead Road
Great Bookham
Surrey
UK   KT23 4SS

On registration via credit card, CompuServe or clearance of your cheque, an Unlock Code will be sent to you.   Once you receive the Unlock Code, right click on the Spot Watcher eyes and select Register. Enter the Unlock Code in the box provided.

If you do not wish to continue using HideThat, you can uninstall it from your computer.

UnInstalling HideThat and Spot Watcher

The HideThat setup program installs the following files on your computer:
HideThat.scr, HideThat.hlp, HideThat.cnt, HotSpot.Ini and HotSpot.Ppp in your Windows directory,
Pppwin32.dll and Machnm1.exe in your Windows\System directory,
HotSpot.exe and Watch.dll in the HideThat directory.

To uninstall these files, firstly ensure Spot Watcher is not running.   Also ensure that the Start Screen
Saver on System Startup option is not selected in the Settings form.

1   Click Start.
2   Select Settings, Control Panel.
3   Double-click Add/Remove Programs.
4   Select HideThat.
5   Click Add/Remove.

The uninstall program does not always remove the following line from the [Boot] section of your system.ini
file:
SCRNSAVE.EXE=C:\WINDOWS\HIDETHAT.SCR
Windows 95 should ignore this line but if it does cause a problem during start up, just delete the above
line.

Acknowledgments

CobWeb Applications would like to thank the following for their technical help and expertise:

Stephen Cobb - author of PC and LAN Security,
Bruce Schneier - author of Applied Cryptography and the Blowfish algorithm,
BlowFish Implementation provided by Greg Carter, CRYPTOCard Corporation,
TeamB at the Delphi Forum,
All the people on the Net who share their knowledge, may bandwidth be with you.

Note

Windows 95 is either a registered trademark or trademark of Microsoft Corp. in the United States and/or other countries.

Buttons

You can activate a button by clicking on it with the mouse or by <u>moving the focus</u> to the button and pressing Enter.   A button becomes highlighted when it has the focus.

A button without the focus.
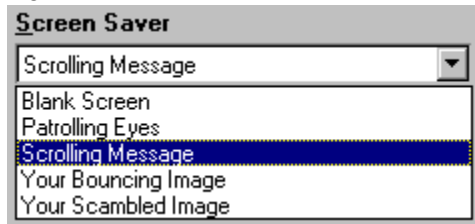
A button with the focus.

Drop-down lists

Drop-down list boxes provide for the selection of a single item from a list of items.
When closed, the control displays the current selection.

 A closed drop-down list.

To open a drop-down list, click the down arrow with the mouse, or using the keyboard, press Alt+Page Down.

 An open drop-down list.

To make a selection from the list, click the required item with the mouse, or using the keyboard, press the up and down arrows to move to the required item.

To close a drop-down list, click on the required item, or using the keyboard, press Alt+Page Up.

Note

When a drop-down list has the focus, pressing the up and down arrows will select the next item in the list.

Navigating controls

To select different controls with a mouse, move the pointer over the required control and click on it.
To move to another control using the keyboard, press the Tab key.   To move backwards press Shift+Tab.
To change pages in a tabbed dialog box, click on the required tab with the mouse, or using the keyboard, press Ctrl+Tab.

If a control has a caption that contains an underlined letter, (an accelerator key), you can move to that control by pressing Alt+ the underlined letter.

 Alt+S takes you to the Screen Saver drop-down list.

Note

When entering text in a control box, use the Tab key not the Enter key, to move to the next control.
(Pressing Enter will usually activates the button that has the default focus.)

Pop-up menus

Pop-up menus are activated by clicking with the right mouse on an object, or pressing the Application key available on some keyboards.

HideThat uses one pop-up menu.

 Right click within the picture of a screen on the Security page of HideThat Settings, or use the Application key.   The pop-up menu enables you to set the Hot and Cold Spots.

Spot Watcher uses one pop-up menu.

 Right click on the revolving eyes.   The pop-up menu enables you to change your HideThat settings, request help or quit Spot Watcher.

To select a menu item, click on it with the mouse, or press the accelerator key or the up and down arrow keys.   A check mark will appear.
To close a menu, click anywhere outside it or press Esc.

Option Buttons

HideThat uses two kinds of option button, radio buttons and check boxes.

 Radio buttons allow only one option to be selected, indicated by the dot in middle of the circle.   Here Random has been selected.   To make your selection, either click it with the mouse, or move the focus to the option group, and using the up and down arrow keys make your selection.

 Check boxes support options that are either on or off.   When the choice is set, a check mark appears in the box. To make your selection, either click it with the mouse, or using the keyboard, move the focus to the check box.   Press the space bar to toggle on and off.   Here the check box has the focus, indicated by the dotted line and the check box is checked. i.e. Password Protection is on.

Slider Control

A slider control is used to adjust values on a continuous range of values.
HideThat uses a slider to adjust the speed of the message text across the screen.

 Click and drag the slide indicator to the required setting, or click the required location.   Using the keyboard, move the focus to the slider control, and then use the left and right arrow keys to move the indicator.

Context-Sensitive Help

Click the Help buttons, or select Help from the pop-up menus.
While changing HideThat settings or the HideThat password, context-sensitive help is available for any control by pressing the F1 key while the control has the focus.   Context-sensitive help is not available while HideThat screen savers are running.
Tooltips are displayed when the mouse moves to a control and stops.

Lists the available HideThat screen savers.   A screen saver displays moving images,   which prevent damage to your screen and hide your work.   The screen saver starts automatically if your computer is idle for a specified amount of time.

Enables you to assign a password to your HideThat screen savers.   A password protects your computer from unauthorized use. HideThat will not clear a screen saver until this password is typed correctly.   To assign a password, click Change Password.

Click this to assign a new password or change an existing HideThat password.

Displays the message in the center of your screen or in different places.

Adjusts the speed at which the message moves across your screen.

Lists the background colors on which you can display your message.

Provides a place for you to type the message you want to display.   To change the font, formatting, or color of your message text, click Format Text.

Click this to change the font, size, or color of your message text.

Provides a place for you to type the Caption you want to display.

Click this to choose which picture you want to bounce around the screen.

Click this to choose which picture you want to scramble.

Click this to close this dialog box and save any changes you have made.

Click this to close this dialog box without saving any changes you have made.

Click this for comprehensive help on using HideThat.

Choose the HideThat settings and options.

Click this to set Hot and Cold Spots.

Provides a space for you to type a new password. For security, asterisks (*) will appear as you type.   The password must be between 5 and 20 characters long.   After you have typed your password, type it again in the Retype New Password box.

Provides a space for you to type the password again. If what you type matches what you typed in the New Password box, HideThat changes the password. For security, asterisks (*) will appear as you type.

Provides a space for you to type your current HideThat password. If what you type matches your existing password, HideThat will allow you to change the password.   For security, asterisks (*) will appear as you type.   If you have not set a HideThat password before, then tab to the New Password box.

Click this to select the HideThat settings and options.

Click this to change HideThat password and set Hot and Cold Spots.

Click this to automatically start HideThat when your computer is started.

Click this for help on registering HideThat and Spot Watcher.

Click this to close this dialog box without entering an Unlock Code.

Enter the Unlock Code and register HideThat and Spot Watcher.

Enter the Unlock Code provided by CobWeb Applications.

Enter the number of minutes, between 0 and 30, that you want your PC to lock up for, after three incorrect passwords.

Click this to automatically start HideThat when your computer is started after an uncontrolled shut down.

HideThat will not start

You must run Spot Watcher before using the HideThat screen saver for the first time.

If HideThat continues to ask you to run Spot Watcher before running HideThat for the first time, it means that file 'HotSpot.Ppp' located in your Windows directory has become corrupted or deleted inadvertently. If this is the case reinstall HideThat.