The Lock Security Wizard

This is the help file for The Lock Security Wizard for Windows 95 by CrashCourse Software.

.

topic 2

Jump back to topic 1

.

Securing the Windows Startup Process

The items listed in this section will help you to secure the initial startup of the Windows 95 environment only, and does not include system bootup. By having the system secure during this process, there is no chance of user intervention without the proper authorization.

Auto Run protection: to activate The Lock password protection automatically upon program startup.
Load The Lock with Windows: to automatically load The Lock upon Windows startup.

Note: Always be aware of any network connections made to the machine, and minimize the security risk by only allowing access to those resources that are needed by outside users.

Back to the top.

.

Securing the DOS Startup Process:

During the bootup process, the user may use the break key to stop the processing of the autoexec.bat. The installation of The Lock for DOS will prevent the unauthorized access to the system before the Windows 95 GUI is started. If the user has disabled the ability to system boot from the A: drive, the addition of The Lock for DOS will make the process even more secure. For the ultimate level of security, ensure that the hard drive is in a lock case, and that access to that lock is only available to the administrator.
Use Lock for DOS: This option will protect the system bootup while CONFIG.SYS and AUTOEXEC.BAT are being processed.
Lock Win95 Boot Keys: This option will disable the Windows 95 boot up keys (shift f5, shift f8, f5, f8, etc);
Lock DOS Boot Keys: This option will disable the DOS boot keys. (F5 and F8, etc.);

Back to the top.

.

Auto Insert Notification

This feature of Windows 95 can cause serious security issues...
Because auto insert notification will automatically load and run the AUTOLOAD.INF file on a CD, a user could write some custom code to a CD-R, and insert this disk into a machine. Auto insert notification will execute the code on the CD even if The Lock is enabled.

THIS FEATURE MUST BE DISABLED, OR SYSTEM SECURITY IS AT RISK.

Back to the top.

.

General Security Items:

These are features that enhance the security items included in The Lock.
Blank Screen on Protection: Select this item to blank the screen each time The Lock protection is started.
Activate after Idle Time: To automatically start The Lock's password protection after the system has remained idle for a certain length of time. Use edit box to adjust max idle time.

Back to the top.

System Monitor Security mode:

In System Monitor mode, the machine has a higher level of protection.

The Admin may select files based on Window name or Windows class, and monitor the system for these programs, and shut them down if they are started. This mode offers the system administrator the ability to monitor what programs are allowed run and what programs will be closed automatically by the System Monitor.

Under this mode, there is no way to change any of The Lock options, shut down The Lock or run any protected programs without using the Admin password.

Back to the top.

.

Passwords:

The Lock has 5 password modes.

The Admin password. The default for this is PassWordCrash. Make sure that this password is THE FIRST password you change. The Admin password will grant access to all secure Lock items, and is the password for The Lock for DOS.

The *user password* is the standard password used to exit Protection Mode. It is different for each user that logs into the system.
Novell server validation is a substitute for the user password. The current user logged into the machine will be validated against an NT server. This method does not require the user to be already entered into The Lock's Password system.
Sentry passwords may be used as temp timed login passwords for other users. These passwords are valid for a user defined number of times.
Temp master passwords will allow access to the machine for an Admin defined number of times. The system Admin may specify how many logins are available for this password.

Back to the top.

.

Bios Security Settings

The following items will add the highest level of security to the system:

The system BIOS can offer multiple levels of protection if the following items are addressed.

Always use a CMOS password to block any changes to the BIOS settings by anybody except the System Admin.

Always disable booting from the A: drive.

For Maximum Security, store the system in a secured case that has a physical locking mechanism. This will hinder the removal of the hard-drive to move it to another machine for bootup. A locked case will also deny access to the system board in order to reset, or remove the CMOS password.

Back to the top.

.