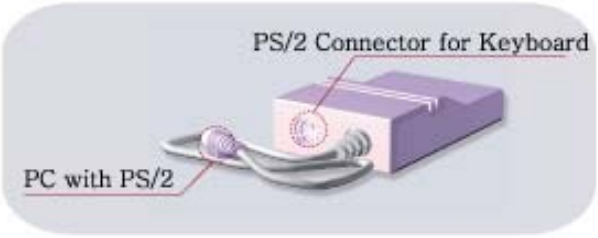

CompuSafe
BTC Secu
Installation Guide
Main features
◆ Prevents Keystroke Data Hacking using Stream Cipher Encryption
◆ Encryption can be toggled off and on by the user
◆ Quality Compact Designs
◆ Compatible with most Windows applications

CompuSafe Hardware Products

Keyboard Type



Add on Type

COMPUSAFE OFFERS TWO TYPES OF HARDWARE FOR ENCRYPTION, KEYBOARDS OR MODULES, PLEASE
NOTE : YOU DO NOT NEED BOTH TO BE ENCRYPTED.

* Photos shown in this manual may vary slightly from actual product.

Keyboard

The CompuSafe keyboard has a Gold button to control activation.

Pushing the secure button will change the mode on & off(encrypted/un-encrypted)

If the CompuSafe mode is set to secure, (encrypted), *the red LED light will illuminateon the keyboard indicating encryption.*

secure mark

Module(Add on)

· The optional module has two LED Indicators (Green & Red) to show status.

When the module is correctly connected to the PC, the green LED light will illuminate.

When the module is set to secure mode, the *red LED light will illuminate.*
on the module indicating encryption protection.

Toggle encryption on & off by clicking on the icon on the bottom right side of your screen.

CompuSafe User's Manual

Installation

Before installing CompuSafe software close all open applications.

1. Turn off the PC before connecting any hardware.
   Connect CompuSafe hardware to the PS/2 port on the PC.
2. Turn on the PC and insert the CompuSafe CD that came with your new hardware into your CD-ROM drive. Setup will begin automatically. If setup does not automatically begin, please execute "Setup.exe" from the CD-ROM drive.
3. Click "Setup" button to start installation
4. Read all information, and then click "Setup" button.
5. After installation, your PC will automatically reboot.

- Do not connect CompuSafe hardware to the mouse port on the PC.

User's Manual

Please refer to the User's Manual for additional information on CompuSafe hardware.

Refer to the following steps to start User's Manual.

Start - Programs- Safetek - CompuSafe - Help

How to use CompuSafe

A. Secure mode / Normal mode

- **Secure Mode (red LED lit)**

  This mode means the keyboard or module encrypts all keyboard input data.

- **Normal Mode (red LED *NOT* lit)**

  This mode means that the secure functions of the hardware are *not activated*.

B. Mode Switching

You can change the encryption mode by using the keyboard or mouse. The mode can be toggled on & off by a double click of the CompuSafe icon on the lower right side of the screen.

C. Smart Upgrade

CompuSafe program checks the need to upgrade periodically. If an upgrade of this program is needed, the following tray icon will flicker. Double clicking the Smart Upgrade icon will cause the program to download the necessary files and upgrade itself.

* Please refer to the User's Manual for additional information on CompuSafe products'

Further Information & Features

- To avoid collision with encrypted keyboard data, do NOT use two CompuSafe hardware products at the same time.

- CompuSafe protects keyboard input data in 3 ways:

  1) Hardware oriented hacking.
  2) Driver oriented hooking
  3) Windows message hooking
  4) New techniques introduced by hackers can be protected through on-line updates

- In the Secure mode, CompuSafe is compatible with most Windows applications. If you are not concerned about security while playing games, chat rooms, debugging programs, etc.., turn the encryption off.

- In MS-DOS mode and Dos prompt, keyboard hacking is not protected from Windows hacking. In this case, keyboard input data is protected and supported under the driver.

- Some games supporting DirectInput™ has to use in Normal Mode.

- Encrypted keyboard input data can occasionally collide in some special cases when in Windows mode such as the power saving mode. When you wake the computer up, the encryption will automatically turn off. Be sure you turn the encryption back on.

FCC Information

This device complies with Part 15 of the FCC Results. Operation is subject to the following two conditions:

(1) This Device may not cause harmful interface, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for CLASS B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try correct the interference by one or more of the following measures:

1.1. Reorient or relocate the receiving antenna.
1.2. Increase the separation between the equipment and receiver.
1.3. Connect the equipment into an outlet on a circuit different from that to which receiver is connected.
1.4. Consult the dealer or experienced radio/TV technician for help.

WARNING

Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

Specifications subject to change without notice.

BTCSECU CO., Ltd
For USA help contact :
CompuSafe Tech
214 Third Ave
Waltham Ma. 02451
877-242-6266