

CMOS PASSWORD RECOVERY

Mark E. Donaldson

BIOS PASSWORD AND LOCKED HARD DISK RECOVERY

If your computer won't boot without a password or you need a password to enter the computer set-up or change the settings, then you have a BIOS password set. BIOS is an acronym for basic input/output system. The BIOS is the basic instruction set that "teaches" the computer how to access disk drives, keyboard, display, etc. The BIOS is typically placed on a ROM chip in the computer, hence the term ROM BIOS. The ROM BIOS allows the computer to boot itself. The BIOS is required to boot the computer. Thus, if the BIOS is password protected, the computer will not boot (or you will not be able to enter or change the BIOS settings.)

There are a number of different BIOS types, but most PC's have a BIOS supplied by one of four companies: American Megatrends, Inc. (AMI), Award, Inc., Phoenix Technologies, Inc. or IBM. Award Software became part of Phoenix Technologies in September 1998 – their main website is the Phoenix Technologies site.

Additional security features have been built into laptop computers. These usually include a hard disk password and a more secure BIOS system. For more information about laptop BIOS passwords, review our security chips page here.

BIOS passwords can be set to require the password before booting the computer or to require the password only to enter and/or change the BIOS set-up (which might be required in order to upgrade the computer.)

Recovery If You Can Boot The System

If you can boot the system, BIOS password recovery is usually easy. The first thing you will want to do is to use a BIOS password cracker to recover the actual password. There are a large number of BIOS password crackers available from a variety of sources. Some BIOS crackers only work with certain BIOS versions and some work better than others. You may have to try a number of crackers before you find one that works.

Some BIOS' have pre-installed backdoor passwords that enable access to the system if you have lost or forgotten your password. Attempting to regain access to the computer by using one of the following backdoor passwords should be your first step if you have lost or forgotten your BIOS password and cannot boot your computer. If you are able to regain access to your system by using a backdoor password, you can then use a password cracker to reveal the stored password or enter the BIOS setup to change the password. These backdoors are more likely to work on older desktop systems. We are not aware of any name brand laptops or notebooks that have backdoor BIOS passwords.

At boot-up note the BIOS provider (Award, AMI, Phoenix, IBM, etc.)

For Award BIOS' try these backdoor passwords:

AWARD_SW
j262
HLT
SER
SKY_FOX
BIOSTAR

ALFAROME
Lkwpeter
j256
AWARD?SW
LKWPETER
syxz

ALLy
589589
589721
awkward
CONCAT
d8on

CMOS PASSWORD RECOVERY

Mark E. Donaldson

CONDO
j64

szyx

For AMI BIOS' try these backdoor passwords:

AMI
BIOS
PASSWORD

HEWITT RAND
AMI?SW
AMI_SW

LKWPETER
A.M.I.
CONDO

For PHOENIX BIOS' try this backdoor password:

phoenix

These backdoor passwords have been provided to you free of charge. If you have attempted to use these backdoor passwords on a system (even just as a test), we would appreciate knowing whether these backdoors have worked for you. This information will help us assist others in the future. The AMI or Award BIOS ID appears at the bottom of the screen after power on.

In BIOS' with a release date of December 19, 1996 or later, Award required OEM customers to configure their own security default BIOS passwords using the Award MODBIN.EXE utility, version 4.50.60. If you are aware of any other backdoor BIOS passwords please let us know at pwcrack@pwcrack.com.

If you are unable to recover the password with a BIOS password cracker or a backdoor there may still be options available. However, we recommend that the additional work only be attempted by a qualified technician.

Recovery If You Cannot Boot The System

If you cannot boot the system without the BIOS password, then using a BIOS password cracker is not going to work (since you cannot run the program.) You should first attempt to gain access to the system by using the backdoor passwords listed above. For many desktop type PC's, BIOS passwords can be reset by removing the CMOS battery for a number of hours. However, care should be taken when attempting recovery in this way since this method may also clear any BIOS customizations and render PC components inoperable.

Laptop And Notebook Recovery

Most laptop manufacturers have provided additional safeguards for their computers. We are not aware of any simple BIOS recovery program that works on laptops, nor are we aware of any simple backdoor passwords for these machines. BIOS passwords in most laptops are stored in a special chip on the motherboard and the only way to bypass this password is to replace this laptop security chip. Laptop BIOS passwords cannot be bypassed or reset by removing or shorting the CMOS battery. Further, doing this may cause other system errors and complicate the recovery of your system.

We offer a full-range of replacement laptop security chips. These chips will allow you to bypass the laptop BIOS password. Note that these chips will require soldering on the system board (a hot air soldering kit is also available.) Since these chips store the laptop BIOS passwords, replacing the laptop security chip will remove the BIOS password. However, if a hard disk lock password has been set, it will remain. Passwords can be recovered from the original chip removed from the system board using our Password Recovery Service (PRS) for an additional fee. Since the BIOS password and hard

CMOS PASSWORD RECOVERY

Mark E. Donaldson

disk lock passwords are usually the same, recovering the BIOS password from the old chip may allow you to access the hard disk. However, this is not guaranteed, since these passwords can be set independently. All replacement chips include detailed instructions. Password Crackers, Inc. cannot take any responsibility for damage to system boards, computers or data. More information about our security chips and our chip password recovery service are available on our security chips page.

One exception to the above chip information is the Toshiba Security Access Key. The Toshiba Key allows for the immediate bypass of the BIOS password from most Toshiba models without soldering. More information on the Toshiba Key is available on our Toshiba security chips page.

Hard Disk Locks

Some laptops provide a utility to lock a hard disk with a password. These passwords are not the same as BIOS passwords. Moving a locked hard disk to another machine will not unlock it, since the hard disk password is stored in the hard disk firmware and moves with the hard disk. Also, adding a new (unlocked) hard disk to a locked machine may cause the new hard disk to become locked. Also, note that hard disk lock passwords cannot be removed by reformatting the disk, fdisk or any other software procedure (since the disk will not allow and reads or writes to the disk, it cannot be reformatted.) Usually, the BIOS password and hard disk lock passwords are set the same by a user and we can recover the BIOS password directly from the laptop security chip (after it is removed from the system board.) However, it is possible that the BIOS password and hard disk lock passwords may be set different. In this case the BIOS password will not unlock the hard disk. You can test to determine if your hard disk is locked by attempting to access it in another laptop. Password Crackers, Inc. offers a service that can unlock most models of laptop hard disks. Detail are available on our hard disk page.

Removing a Bios - CMOS Password

Unfortunately, access to computers can, at times, be blocked for all of the wrong reasons. Sometimes this occurs due hardware related issues such as electrical problems or due to inadvertence, such as someone setting and then forgetting the password. It can happen as the result of accidental use of a Bios password by a new user. This also often occurs when an employee who is quitting or has been terminated, sets the Bios password as some form of retaliation against an employer. Reversing this can be time consuming as well as very frustrating depending upon the motherboard manufacturer and the make and model of the motherboard. Relax though, as it is possible to reset or disable the password.

Default Passwords

At times, and without any obvious reason, static discharges as well as other electrical problems can cause the PROM on the motherboard to reset the Bios (CMOS) to its default values and even cause the default Bios password to be set. These are some of the default Bios passwords used with different Bios's, give them a try first.

AMI	concat
Award	AMI_SW (case sensitive)
bios	AMI!SW/
setup	AMI?SW/
cmos	j262

CMOS PASSWORD RECOVERY

Mark E. Donaldson

NOTE: With respect to the Award BIOS, the "AWARD_SW" (use without quotes) and (is is case sensitive) password should even override a set password! If not, you may also want try j262 as the password

Removing Arbitrary or Revenge Passwords

Many times we have had customers contact us explaining that either an employee or family member has set a Bios password and then forgot what it was, making access to the computer impossible. A few times we have seen vindictive employees set Bios passwords as their way of getting even with their employer. Most times though, this is a well-meaning effort on the part of an employee to secure employer data, so don't punish the employee if this is the case. As far as family members are concerned, we have heard just about every explanation possible ranging from adults trying to regulate computer use by their children or one adult trying to curb computer use by his or her significant other. We have even had some reasons that we simply can't publish here. In any event, reversing the setting of this password is not impossible, it just takes some thought and some work.

If you have tried the passwords listed above and none have worked, then there are a few more options to try. You can attempt to erase the Bios/CMOS settings and have the Bios return to its default settings or you can use use a Bios/CMOS password utility (password crack) to try and erase or reset the password.

Forcing the Bios-CMOS to be Reset to Default Values

There are two ways to approach forcing the Bios/CMOS to be reset to its default values: Option #1: Mechanically, by removing all power to the Bios/CMOS thereby forcing it to reset itself to its stored defaults, which include no password or the default password employed by the Bios manufacturer, and Option #2: Using a program to either locate and identify the password and reveal it to you or erasing the password entirely. These are referred to as password by-pass utilities or cracks. Let's look at Option #1 first, and then move on to Option #2 if necessary.

Option #1: Mechanically Removing the Password

Most motherboards manufactured over the last decade or more use a battery to sustain the dynamic Bios/CMOS settings for the motherboards PROM chip. These dynamic settings are those manually set by either the computers manufacturer or you, the user. There are two ways to erase these dynamic settings, by either resetting a jumper on the motherboard itself (referred to as a "clear CMOS" jumper), or by physically remove the power from the computer (disconnecting the power plug) and then removing a battery (used to maintain power to the PROM chip that contains the Bios/CMOS information) from the motherboard.

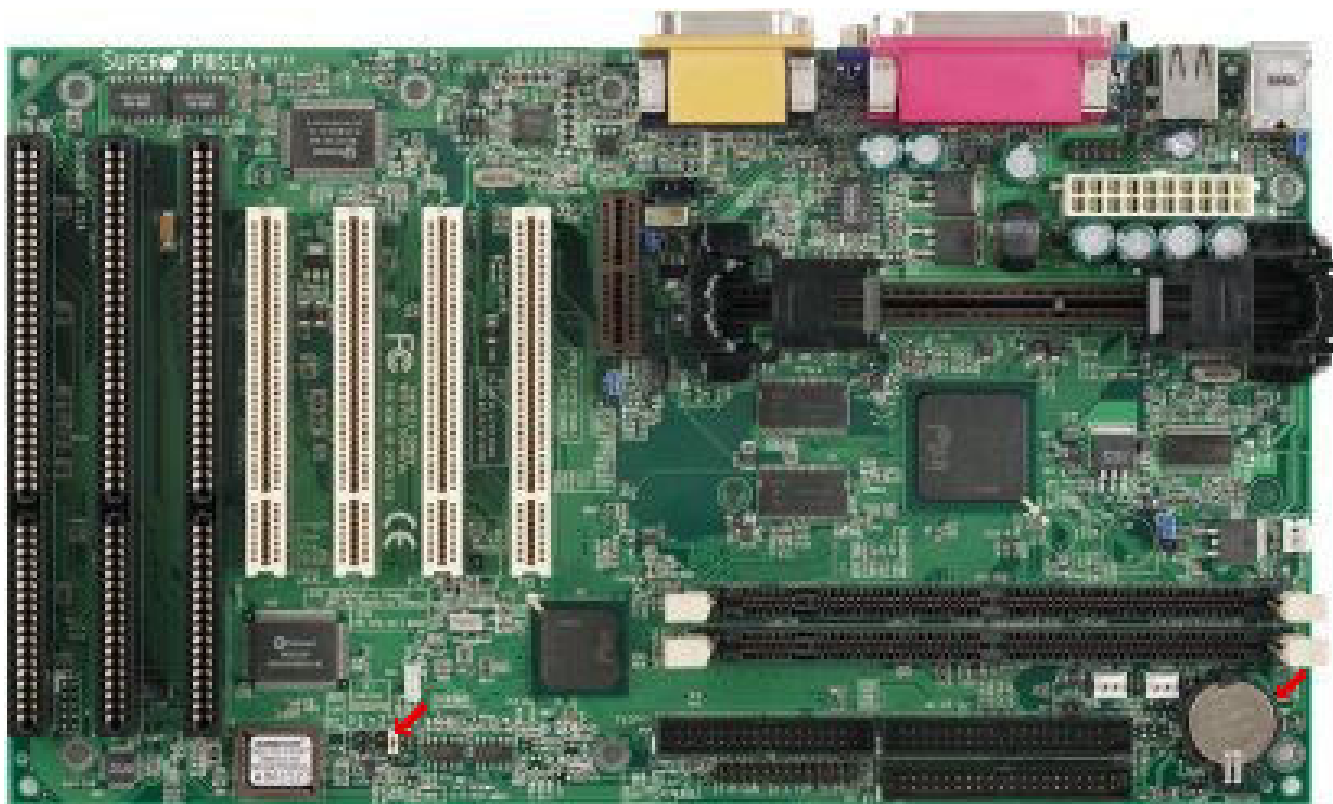
Motherboard Jumpers:

Some, but not all, motherboard manufacturers provide a set of three jumpers on their motherboards that provide you with the ability to clear the Bios/CMOS settings, thereby allowing them to be reset. For the most part this is used when the Bios/CMOS data becomes scrambled and you need to clear the Bios/CMOS in order to return the computer to a functional state. This same procedure, however, can be used to clear passwords from the Bios/CMOS setup. Typically a jumper will be found across pins #1 and #2 as the default position, and by shutting the computer down, unplugging the power cord and then moving the jumper so that it is across pins #2 and #3 will clear the Bios/CMOS settings.

Here's an example of a Supermicro PIIISEA motherboard.

CMOS PASSWORD RECOVERY

Mark E. Donaldson



As you can see from the picture, we have added two small red arrows. The arrow to the left denotes the location of the "Clear CMOS" jumpers, while the red arrow to the right denotes the location of the CMOS battery.

Here are the procedures if the jumpers are present on the motherboard:

- Locate, if possible, the instruction booklet for your motherboard. If you cannot locate the booklet, then use the motherboard references on this site to locate the manufacturer and see if a manual is available there. You may also want to closely examine the motherboard itself.
- Shut down your computer and disconnect the power plug.
- Now identify where the jumpers are located, then check the present pin location and the location of the jumper on those pins to determine their default location. As an example, the default location on the above motherboard is to have the jumper across pins #1 and #2. Write it down!
- Next, move the jumpers from the their default location (Example: from across pins #1 and #2 as above) and then place the jumper across pins #2 and #3.
- Leave the jumper in place for 20 to 30 seconds and then return it to its default location.
- Now plug the power cord back in and restart the computer.

CMOS PASSWORD RECOVERY

Mark E. Donaldson

- When the computer begins its startup (boot) process, tap the DEL, F10 or F1 key, (whichever is appropriate for your computer) to get into the Bios/CMOS setup. If you need more detailed information as to how to get to the Bios/CMOS setup, follow this link. [Bios Basics](#)
- Once into the Bios/CMOS setup, look for a section or area to set the Bios/CMOS to its default settings. This will return the motherboard to either its basic or optimum settings depending upon the motherboard manufacturer's settings. You will then need to verify certain settings, such as CPU and memory as well as hard drive type and size recognition. If you need more information regarding these settings, follow either of these links: [For an AMI Bios](#) or [for an Award Bios](#).
- After making any final adjustments, save your settings and restart the computer. The Bios password should be gone and the Bios set to its optimum settings.

If the "Clear CMOS" jumpers are not present or not available:

The procedures for clearing a Bios/CMOS without jumpers is essentially the same as those given above when they are present, it just takes a little more effort.

- Shut down the computer and disconnect the power plug.
- Locate, if possible, the instruction booklet for your motherboard. If you cannot locate the booklet, then use the motherboard references on this site to locate the manufacturer and see if a manual is available there. You may also want to closely examine the motherboard itself.
- Now identify where the battery is located on the motherboard. It will be approximately 1/2 inch in diameter.
- Normally these batteries are held into place with one or more small clips over the face of the battery.
- Carefully lift the battery out of its socket and set it aside. Note: Some batteries are actually soldered to the motherboard, so take that into consideration and be careful.
- Leave the battery out of the computer for about 20 to 30 minutes and then return it to its socket.
- Now plug the power cord back in and restart the computer.
- When the computer begins its startup (boot) process, tap the DEL, F10 or F1 key, (whichever is appropriate for your computer) to get into the Bios/CMOS setup. If you need more detailed information as to how to get to the Bios/CMOS setup, follow this link. [Bios Basics](#)
- Once into the Bios/CMOS setup, look for a section or area to set the Bios/CMOS to its default settings. This will return the motherboard to either its basic or optimum settings depending upon the motherboard manufacturer's settings. You will then need to verify certain settings, such as CPU and memory as well as hard drive type and size recognition. If you need more information regarding these settings, follow either of these links: [For an AMI Bios](#) or [for an Award Bios](#).
- After making any final adjustments, save your settings and restart the computer. The Bios password should be gone and the Bios set to its optimum settings.

CMOS PASSWORD RECOVERY

Mark E. Donaldson

Option 2: What to do if changing jumpers or removing batteries doesn't work:

On some motherboards there are no jumpers to be moved and the battery may be soldered into place and cannot be removed. There may also be those occasions where moving jumpers or removing batteries just won't work. This is often the case on early motherboards.

In these instances, there are three additional options to be considered.

Option #1:

You can physically remove the Bios/CMOS PROM chip from the motherboard and send it either to the motherboard manufacturer or a Bios developer for replacement of flashing. You can also send the entire motherboard to a facility experienced in these operations.

Option #2:

If the motherboard has a flash updateable Bios/CMOS PROM chip, then you can download a fresh Bios update and re-flash the PROM to eliminate the password.

Option #3:

As mentioned earlier, there are programs (utilities) and (cracks) that can be used to try and either identify the password or remove it forcibly from the PROM chip. Utilities to recover passwords are extremely expensive and are usually only sold to manufacturers and others involved in hardware and software development.

Smaller utilities and those referred to as Bios crack programs are readily available. These, however, are used at your own risk. Please read and understand our disclaimer before downloading any of these types of utilities. By downloading any of these utilities you are agreeing to the terms of our disclaimers.

AMI Password Viewer with Source Code	Award Flash Utility in zip format
AMI 1 Zip (Early Password Viewer - 1994 version)	Award Zip - Early password viewer
AMI 2 Zip (Password Viewer - 1995 and later)	Award1 Zip - Later password viewer
Remove Password Tool	Award 2 Zip - Latest password viewer

Notice: Any or all of the above files should only be used by those professionals completely familiar with motherboard and Bios/CMOS issues and recovery. We make no warranty of any type as to any of these files, including their usability for a particular purpose. Using these files is at your own risk!