How to Bypass BIOS Passwords

BIOS passwords can add an extra layer of security for desktop and laptop computers. They are used to either prevent a user from changing the BIOS settings or to prevent the PC from booting without a password. Unfortunately, BIOS passwords can also be a liability if a user forgets their password, or changes the password to intentionally lock out the corporate IT department. Sending the unit back to the manufacturer to have the BIOS reset can be expensive and is usually not covered in the warranty. Never fear, all is not lost. There are a few known backdoors and other tricks of the trade that can be used to bypass or reset the BIOS

DISCLAIMER
This article is intended for IT Professionals and systems administrators with experience servicing computer hardware. It is not intended for home users, hackers, or computer thieves attempting to crack the password on a stolen PC. Please do not attempt any of these procedures if you are unfamiliar with computer hardware, and please use this information responsibly. LabMice.net is not responsible for the use or misuse of this material, including loss of data, damage to hardware, or personal injury.

Before attempting to bypass the BIOS password on a computer, please take a minute to contact the hardware manufacturer support staff directly and ask for their recommended methods of bypassing the BIOS security. In the event the manufacturer cannot (or will not) help you, there are a number of methods that can be used to bypass or reset the BIOS password yourself. They include:

Using a manufacturers backdoor password to access the BIOS

Use password cracking software

Reset the CMOS using the jumpers or solder beads.

Removing the CMOS battery for at least 10 minutes

Overloading the keyboard buffer

Using a professional service

Please remember that most BIOS passwords do not protect the hard drive, so if you need to recover the data, simply remove the hard drive and install it in an identical system, or configure it as a slave drive in an existing system. The exception to this are laptops, especially IBM Thinkpads, which silently lock the hard drive if the supervisor password is enabled. If the supervisor password is reset without resetting the and hard drive as well, you will be unable to access the data on the drive.

Backdoor passwords

Many BIOS manufacturers have provided backdoor passwords that can be used to access the BIOS setup in the event you have lost your password. These passwords are case sensitive, so you may wish to try a variety of combinations. Keep in mind that the key associated to "_" in the US keyboard corresponds to "?" in some European keyboards. Laptops typically have better BIOS security than desktop systems, and we are not aware of any backdoor passwords that will work with name brand laptops.

WARNING: Some BIOS configurations will lock you out of the system completely if you type in an incorrect password more than 3 times. Read your manufacturers documentation for the BIOS setting before you begin typing in passwords

Award BIOS backdoor passwords:

ALFAROME ALLy aLLy aLLY ALLY aPAf _award AWARD_SW AWARD?SW AWARD SW AWARD PW AWKWARD awkward B CONDO Condo d8on djonet HLT J64 J256 J262 j332 j322 KDD Lkwpeter LKWPETER PINT pint SER SKY_FOX SYXZ syxz shift + syxz TTPTHA ZAAADA ZBAAACA ZJAAADC 01322222
589589 589721 595595 598598

AMI BIOS backdoor passwords:

AMI AAAMMMIII BIOS PASSWORD HEWITT RAND AMI?SW AMI_SW LKWPETER A.M.I. CONDO

PHOENIX BIOS backdoor passwords:

phoenix, PHOENIX, CMOS, BIOS

MISC. COMMON PASSWORDS

ALFAROME BIOSTAR biostar biosstar CMOS cmos LKWPETER lkwpeter setup SETUP Syxz Wodj

OTHER BIOS PASSWORDS BY MANUFACTURER

Manufacturer Password
VOBIS & IBM merlin
Dell Dell
Biostar Biostar
Compaq Compaq
Enox xo11nE
Epox central
Freetech Posterie
IWill iwill
Jetway spooml
Packard Bell bell9
QDI QDI
Siemens SKY_FOX
TMC BIGO
Toshiba Toshiba

TOSHIBA BIOS

Most Toshiba laptops and some desktop systems will bypass the BIOS password if the left shift key is held down during boot

IBM APTIVA BIOS

Press both mouse buttons repeatedly during the boot

Password cracking software

The following software can be used to either crack or reset the BIOS on many chipsets. If your PC is locked with a BIOS administrator password that will not allow access to the floppy drive, these utilities may not

work. Also, since these utilities do not come from the manufacturer, use them cautiously and at your own risk.

Cmos password recovery tools 3.1
!BIOS (get the how-to article)
RemPass
KILLCMOS

Using the Motherboard "Clear CMOS" Jumper or Dipswitch settings

Many motherboards feature a set of jumpers or dipswitches that will clear the CMOS and wipe all of the custom settings including BIOS passwords. The locations of these jumpers / dipswitches will vary depending on the motherboard manufacturer and ideally you should always refer to the motherboard or computer manufacturers documentation. If the documentation is unavailable, the jumpers/dipswitches can sometimes be found along the edge of the motherboard, next to the CMOS battery, or near the processor. Some manufacturers may label the jumper / dipswitch CLEAR - CLEAR CMOS - CLR - CLRPWD - PASSWD - PASSWORD - PWD. On laptop computers, the dipswitches are usually found under the keyboard or within a compartment at the bottom of the laptop.
Please remember to unplug your PC and use a grounding strip before reaching into your PC and touching the motherboard. Once you locate and rest the jumper switches, turn the computer on and check if the password has been cleared. If it has, turn the computer off and return the jumpers or dipswitches to its original position.

Removing the CMOS Battery

The CMOS settings on most systems are buffered by a small battery that is attached to the motherboard. (It looks like a small watch battery). If you unplug the PC and remove the battery for 10-15 minutes, the CMOS may reset itself and the password should be blank. (Along with any other machine specific settings, so be sure you are familiar with manually reconfiguring the BIOS settings before you do this.) Some manufacturers backup the power to the CMOS chipset by using a capacitor, so if your first attempt fails, leave the battery out (with the system unplugged) for at least 24 hours. Some batteries are actually soldered onto the motherboard making this task more difficult. Unsoldering the battery incorrectly may damage your motherboard and other components, so please don't attempt this if you are inexperienced. Another option may be to remove the CMOS chip from the motherboard for a period of time.
Note: Removing the battery to reset the CMOS will not work for all PC's, and almost all of the newer laptops store their BIOS passwords in a manner which does not require continuous power, so removing the CMOS battery may not work at all. IBM Thinkpad laptops lock the hard drive as well as the BIOS when the supervisor password is set. If you reset the BIOS password, but cannot reset the hard drive password, you may not be able to access the drive and it will remain locked, even if you place it in a new laptop. IBM Thinkpads have special jumper switches on the motherboard, and these should be used to reset the system.

Overloading the KeyBoard Buffer

On some older computer systems, you can force the CMOS to enter its setup screen on boot by overloading the keyboard buffer. This can be done by booting with the keyboard or mouse unattached to the systems, or on some systems by hitting the ESC key over 100 times in rapid succession.

Jumping the Solder Beads on the CMOS

It is also possible to reset the CMOS by connecting or "jumping" specific solder beads on the chipset. There are too many chipsets to do a breakdown of which points to jump on individual chipsets, and the location of these solder beads can vary by manufacturer, so please check your computer and motherboard documentation for details. This technique is not recommended for the inexperienced and should be only be used as a "last ditch" effort.

Using a professional service

If the manufacturer of the laptop or desktop PC can't or won't reset the BIOS password, you still have the option of using a professional service. Password Crackers, Inc., offers a variety of services for desktop and laptop computers for between $100 and $400. For most of these services, you'll need to provide some type of legitimate proof of ownership. This may be difficult if you've acquired the computer second hand or from an online auction.