

Break Through the BIOS Password

The BIOS is the basic instruction set that "teaches" the computer how to access its media. If the BIOS is password protected, the computer will not function without the password. BIOS passwords are used in two ways: To prevent modification of the BIOS settings and to completely stop the computer from booting.

Accessing the BIOS

Below is a list of common key combinations to access the BIOS on specific computers.
(Courtesy of cybertechhelp.com)

Acer:	Ctrl+Alt+Esc	PS/2:	Ctrl+Alt+Ins after Ctrl+Alt+Del
ALR PC:	F2 , Ctrl+Alt+Esc	PS/2 (reference partition):	Press Ins during boot
AMI BIOS:	Del, F1 or F2	Some PS/2s, such as 75 and 90:	Ctrl+Alt+?
AST:	Ctrl+Alt+Esc	Some PS/2s when pointer at top right of screen:	Ctrl+Ins
Award BIOS:	Del or Ctrl+Alt+Esc		
Compaq:	F10		
Dell:	Del, F1 or Some require pressing reset twice	NEC:	F2
DTK BIOS:	Esc	Packard Bell:	F1 or F2
Gateway 2000:	F1	Phoenix BIOS:	F1, F2, Ctrl+Alt+Esc, Ctrl+Alt+S, Ctrl+S, Ctrl+Alt+Ins
Hewlett Packard:	F1	Sharp 9020:	F2
IBM:		Sony:	F3 while you are starting the PC, then F2 or F1
Older Models - In order to get into the configuration of the IBM setup screen (CMOS) screen you need to hold down both mouse buttons during boot up.		Tandon:	Ctrl+Shift+Esc
Aptiva: Press F1		Toshiba:	Esc, F1
		Olivetti PC Pro:	Shift+Ctrl+Alt + Num Pad Del
		Zenith:	Ctrl+Alt+Ins

Bypassing the BIOS

If you forgot the BIOS password, try some of the backdoor passwords that might be in place for some BIOS versions. Following is a list of potential passwords that may or may not work. There's no harm in trying 'em out.

AWARD BIOS

_award	AWARD?SW	J256	shift + syxz
01322222	AWARD_PW	j256	SKY_FOX
589589	AWARD_SW	j262	SYXZ
589721	AWKWARD	j322 KDD	syxz
595595	awkward	j332	szyx
598598	BIOSTAR	J64	TTPTHA
ALFAROME	CONCAT	j64	ZAAADA
ALLY	CONDO	LKWPETER	ZBAAACA
ALLy	Condo	Lkwpeter	ZJAAADC
aLLy	d8on	PINT	
aLLY	djonet	pint	
aPAf	HLT	SER	

AMI BIOS

589589	AMI	BIOS	LKWPETER
A.M.I.	AMI?SW	CONDO	PASSWORD
AAAMMMIII	AMI_SW	HEWITT RAND	

PHOENIX BIOS

Phoenix , phoenix, PHOENIX, CMOS, BIOS

IBM APTIVA

According to DigiSign Data Security, if you have an IBM Aptiva, you can clear the BIOS information by holding down both mouse buttons until the computer boots.

According to LabMice.net: Press both mouse buttons repeatedly during the boot

MISC. COMMON PASSWORDS

ALFAROME	buisstar	LKWPETER	setup
BIOSTAR	CMOS	lkwpweter	Syxx
biostar	cmos	SETUP	Wodj

OTHER 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, Toshy99, 24Banc81

PASSWORD RESOURCE FROM THE INTERNET

<http://www.cirt.net/cgi-bin/passwd.pl>

Dell Laptop

Have "Num Lock" light on

Have "Caps" light on

Have "Scroll Light" on

Now Press "Alt + E then Alt + F then Alt + W.

TOSHIBA LAPTOPS

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

Toshiba BIOS Clearing Dongle

The below wiring for a Toshiba laptop BIOS clearing dongle was posted by Shawn Patrick. Steve Guest says it works fine on every Toshiba laptop he's have tried it on.

Toshiba Dongle:

Use a DB-25 male connector (Cut one off an old printer cable)

Connect:

1-5-10

2-11

3-17

4-12

6-16

7-13

8-14

9-15

18-25 tied together (soldered)

Place in printer port and power up.

ALTERNATIVE TOSHIBA METHOD

The one and only way to bypass the Power On BIOS password of a Toshiba Notebook. This method works on all models.

This is what you need:

1. Your notebook
2. An empty formatted diskette (720 kb or 1,44 MB)
3. A second computer (e.g. a DOS desktop PC)
4. A hex-editor (e.g. Norton DiskEdit or HexWorks)

This is what you have to do:

1. Start the desktop PC and start the hex-editor
2. Put the disk in drive A:
3. Change the first five bytes of sector 2 (boot sector is sector 1) to: 4B 45 59 00 00
4. Save it! Now you have a KEYDISK
5. Remove the disk from drive A:
6. Put the disk in the notebook drive
7. Start the notebook in Boot Mode (push the reset button)
8. Press Enter when asked for Password:
9. You will be asked to Set Password again. Press Y and Enter.
10. You now see the BIOS configuration where you can set a new password.

If you can't get in with one of the backdoor passwords, it's time to open up your computer.

Remove a jumper

There's a jumper on your motherboard that you'll need to identify and remove. Most motherboards make your job easier by actually labeling the correct jumper as "BIOS config" or something similar.

Remove the jumper, and then turn the computer on. In some cases, you will have to remove the jumper while the system is powered up, though to minimize risk, try doing this first with the computer off.

-WARNING: This method will clear information stored in the BIOS including date and time settings

Remove the internal battery

If you are not able to locate the jumper or believe it doesn't exist, your next option is to remove the internal battery (usually looks like some variation of watch battery) from the motherboard, and unplug the computer.

Without power to retain the CMOS information, most computers will clear it anywhere between 10 seconds to 24 hours. Be sure and let the computer rest without any power whatsoever for the duration of this period before ruling out that this method will not work.

-WARNING: This method will clear information stored in the BIOS including date and time settings

Overload the keyboard buffer

Overloading the keyboard buffer can crash the password routine and let the computer boot. Try this by pressing the ESC key repeatedly, possibly more than 100 times.

Remove the hard drive

If you've got crucial data on your system, need it urgently, and can't get past the BIOS. Remember that you can always remove the hard drive with the data and access it from another system. The BIOS password (typically) only pertains to the motherboard. There are some

manufacturers, IBM and Dell included, who are encrypting the HDD to the motherboard. If this is the case, try contacting the manufacturer for a password to unlock the HDD.

This document has been the culmination of tips/techniques I have come across during my time as a computer crime specialist. Unfortunately, I have not kept close track of the numerous contributors so they could be properly recognized. A majority of information in this document came from members of IACIS (International Association of Computer Investigative Specialists) and assorted web sites dealing with hacking techniques.

Below is my contact information if you have anything that could be included for follow up, additions, or updates.

**Sergeant Frank P. Higgins
Bomb Technician, CFCE
Flagstaff Police Department
911 E Sawmill Rd
Flagstaff AZ 86001
(928) 779-2701
fhiggins@coconino.az.gov**
