

Here's a DOS trick for Windows 9x, that will reset (delete) your motherboard's BIOS password (aka CMOS password) without any need to open up your computer to remove the battery or mess with jumpers.

-----  
-----  
//////////\*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @  
TekGyd | itechacks | Mukeshtricks4u\*////////  
-----  
-----

This method can come in very handy in the event you ever lose and forget your BIOS password or if you acquire used computers where the unknown previous owners had BIOS passwords set (in fact, this happened to me long ago—I was given a used computer, but there was no way I could enter the CMOS to make changes). It's important to note here that the password we are talking about is only the one that prevents a user from entering the BIOS setup at bootup, not the one that stops you from getting past the boot.

Normally, at bootup you can press a key (usually the DEL key) to access your BIOS allowing you to view it or make changes. With a password set, there is no way to enter setup. Though a password can provide a basic and very effective level of PC security, losing it can be a real headache if you don't know how to fix the problem.

The MS-DOS command that will makes this trick possible is the DEBUG command (debug itself is a utility—debug.exe—which is located in your Windows Command folder). This is not a command to be taken lightly—in other words, it's not a command to play with! You can cause serious corruption with this command and can end up not being able to even boot your computer! Debug is used to work with binary and executable files and allows you to alter (hex edit) the contents of a file or CPU register right down to the binary and byte level.

To begin debug mode, type debug at a MS-DOS prompt or you can specify a file, i.e., DEBUG FILE.EXE. There is a difference in screen output between the two methods. When you type DEBUG alone, debug responds with a hyphen (-) prompt waiting for you to enter commands. The second method, with a file specified, loads the file into memory and you type all the commands on the line used to start debug. In this tip, we will be writing to the BIOS, so the first method is the one that would be used. All debug commands can be aborted at any time by pressing CTRL/C.

#### Accessing BIOS with DEBUG

The basic trick will be to fool the BIOS into thinking there is a checksum error, in which case it resets itself, including the password. This is done by invalidating the CMOS and to do that we must know how to access the BIOS and where the checksum value of the CMOS is located so that we can change it. Access to the BIOS content is via what are known as CMOS Ports and it's Port 70 and 71 that will give us the needed access. On almost all AT motherboards, the checksum is located at hexadecimal address 2e and 2f and filling the address 2e with ff is all you should have to do to invalidate the checksum.

Here's what to do if you ever need to reset the password and have no other method, and you don't want to open up your computer to remove the battery or jumpers.

Note! Do this at your own risk. I can only tell you that it has worked for me more than once and has worked for others as well. But I cannot make any guarantees. When I did this, I took a willing risk. The BIOS was Award Modular BIOS v4.51PG

Restart your computer in MS-DOS mode.

When you get to the C:\> or C:\WINDOWS> prompt, type DEBUG and press Enter.

A hyphen (-) prompt will appear waiting for you to enter commands.

Enter the following commands, pressing Enter after each one. Note: the o is the letter o and stands for OUTPUT.

o 70 2e

o 71 ff

q

After the q command (which stands for QUIT), enter Exit.

Then try to enter your BIOS at bootup. The password prompt should now be gone and you should now have full access to it again. However, you will now be at the default BIOS settings and may want to change them to your preference. You may also want to have your drives autodetected again.

In closing, I should state that in the case of a lost BIOS password, your first step should always be to contact your manufacturer to see if a backdoor password is available that will allow you to bypass the forgotten password.

There are many sites on the net that list backdoor passwords you can try, but beware that some BIOS that are set up to lock up if you enter the wrong password more than a certain number of times, usually only 3 times!