IF A VIRUS KILLS THE BIOS, YOUR PC DIES TOO

What is the BIOS? Click here: What is BIOS? - A Word Definition From the Webopedia Computer Dictionary

Question: "It seems incongruous that a virus program can rewrite the BIOS chip, but there's no other program available to put the BIOS instructions back onto the chip. Is this chip programmable or isn't it?"

Answer: The problem arises if the CIH **virus program overwrites the BIOS program code (but with no effect on the chip itself). The user could flash the chip again--there's** nothing physically wrong with it. One could even restore the BIOS program with a disk image copy of it (made in advance or obtained from the manufacturer), along with the software to reflash it onto the chip.

The BIOS program is vital, because it directly accesses the PC's hardware to test system memory and disk drives at boot-up, and it accesses the disk to load the operating system. Most PCs store the BIOS code on a flash (write-enabled) RAM chip to allow updates--if the PC is running normally.

However, CIH makes that task difficult if not impossible, because CIH's overwriting process temporarily disables the PC. Without the BIOS program, the PC will not start, even from a floppy disk or CD, and that means you can't access the disk image copy of the BIOS code (assuming you even have that), nor can you flash the program onto the chip again.

In those few cases where a skilled user has a second (identical) machine running and both machines have removable chips, the user could switch the chips (with extreme care, of course). But in many cases, the chip is soldered to the motherboard. You could in theory send the board back to the factory--but most people give up and replace it to get the PC up and running.

Note: The original CIH virus spread under the Portable Executable file format under Windows 95, Windows 98, and Windows ME. For a long time, CIH did not spread under Windows NT, Windows 2000, Windows XP or Windows Vista or MAC OS.

However, The CIH got a new look, while scanning the security holes inside the Windows Networks. Windows XP got prone to it when some people disliked the windows validation tool. CIH caused IP Conflicts, Font removal, System Netbios Conflicts on the many windows xp/server systems.

Most Anti-virus programs today will see the CIH and remove it….IF…IF you're running a reputable anti-virus program and if it has been updated regularly.

Revised 6/13/2008 JMM