**BIOS**

BIOS (basic input/output system) is the program a computer's [microprocessor](https://whatis.techtarget.com/definition/microprocessor-logic-chip) uses to start the computer system after it is powered on. It also manages data flow between the computer's operating system (OS) and attached devices, such as the hard disk, video adapter, keyboard, mouse and printer.

**History of BIOS**

The term BIOS was first coined in 1975 by American computer scientist Gary Kildall. It was incorporated into IBM's first personal computer in 1981 and, in the years to come, gained popularity within other PCs, becoming an integral part of computers for some time. However, BIOS' popularity has waned in favor of a newer technology: Unified Extensible Firmware Interface ([UEFI](https://whatis.techtarget.com/definition/Unified-Extensible-Firmware-Interface-UEFI)). Intel announced a plan in 2017 to retire support for legacy BIOS systems by 2020, replacing them with UEFI.

**Uses of BIOS**

The main use of BIOS is to act as a middleman between OSes and the hardware they run on. BIOS is theoretically always the intermediary between the microprocessor and I/O device control information and data flow. Although, in some cases, BIOS can arrange for data to flow directly to memory from devices, such as video cards, that require faster data flow to be effective.

**How does BIOS work?**

BIOS comes included with computers, as firmware on a chip on the [motherboard](https://whatis.techtarget.com/definition/motherboard). In contrast, an OS like Windows or iOS can either be pre-installed by the manufacturer or vendor or installed by the user. BIOS is a program that is made accessible to the microprocessor on an erasable programmable read-only memory ([EPROM](https://whatis.techtarget.com/definition/EPROM)) chip. When users turn on their computer, the microprocessor passes control to the BIOS program, which is always located at the same place on EPROM.

When BIOS boots up a computer, it first determines whether all of the necessary attachments are in place and operational. Any piece of hardware containing files the computer needs to start is called a *boot device*. After testing and ensuring boot devices are functioning, BIOS loads the OS -- or key parts of it -- into the computer's random access memory ([RAM](https://searchstorage.techtarget.com/definition/RAM-random-access-memory)) from a hard disk or diskette drive (the boot device).

**The 4 functions of BIOS**

BIOS identifies, configures, tests and connects computer hardware to the OS immediately after a computer is turned on. The combination of these steps is called the *boot process*.

These tasks are each carried out by BIOS' four main functions:

1. **Power-on self-test (**[**POST**](https://whatis.techtarget.com/definition/POST-Power-On-Self-Test)**).** This tests the hardware of the computer before loading the OS.
2. [**Bootstrap loader**](https://searchdatacenter.techtarget.com/definition/boot-loader-boot-manager)**.** This locates the OS.
3. **Software/drivers.** This locates the software and drivers that interface with the OS once running.
4. **Complementary metal-oxide semiconductor (CMOS) setup.** This is a configuration program that enable users to alter hardware and system settings. CMOS is the name of BIOS' non-volatile memory.

**Accessing BIOS**

With BIOS, the OS and its applications are freed from having to understand exact details, such as computer hardware addresses, about the attached I/O devices. When device details change, only the BIOS program needs to be changed. Sometimes, this change can be made during system setup.

Users can access BIOS and configure it through BIOS Setup Utility. Accessing BIOS Setup Utility varies somewhat depending on the computer being used. However, the following steps generally enable users to access and configure BIOS through Setup Utility:

* Reset or power off the computer.
* When the computer turns back on, look for a message that says "entering setup" or something similar. Accompanying that message will be a key that the user should press to enter system configuration. Here's an example message a user might see: "Press [key] to enter BIOS setup." Some keys often used as prompts are Del, Tab, Esc and any of the function keys (F1-F12).
* Upon seeing the prompt, quickly press the key specified.

Once in BIOS Setup Utility, users can change hardware settings, manage memory settings, change the boot order or boot device, and reset the BIOS password, among other configuration tasks.

**BIOS security**

[BIOS security](https://searchsecurity.techtarget.com/answer/How-to-bolster-BIOS-security-to-prevent-BIOS-attacks) is a somewhat overlooked component of cybersecurity; however, it should still be managed to prevent hackers from executing malicious code on the OS. Security group Cylance, in 2017, showed how modern BIOS security flaws could enable ransomware programs inside a motherboard's UEFI and exploit other PC BIOS vulnerabilities.

Another unique exploit involving the manipulation of BIOS was [Plundervolt](https://searchsecurity.techtarget.com/definition/Plundervolt). Plundervolt could be used to mess with a computer's power supply at the time data was being written to memory, causing errors that lead to security gaps. Intel released a BIOS patch to defend against it.

**BIOS manufacturers**

BIOS, in its beginnings, was originally owned by IBM. However, some companies, such as Phoenix Technologies, have reverse-engineered IBM's original version to create their own. Phoenix, in doing this, allowed other companies to create clones of the IBM PC and, more importantly, create non-IBM computers that work with BIOS. One company that did this was Compaq.

Today, many manufacturers produce motherboards with BIOS chips in them. Some examples are the following:

* AMI
* Asus
* Foxconn
* Hewlett Packard (HP)
* Ricoh

Knowing the motherboard manufacturer is important because users may want to update their BIOS and chipset drivers -- the drivers that enable the OS to work with other devices in the computer, such as a video card -- to the most recent versions. Driver updates may improve computer performance or patch recent BIOS-level security vulnerabilities. Each manufacturer has a unique way of updating these drivers.