**What is BIOS? Explain its purpose?**

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

BIOS is an integral part of your computer and comes with it when you bring it home. (In contrast, the operating system 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 you turn on your computer, the microprocessor passes control to the BIOS program, which is always located at the same place on EPROM.

When BIOS boots up (starts up) your computer, it first determines whether all of the attachments are in place and operational and then it loads the operating system (or key parts of it) into your computer's random access memory ([RAM](https://searchstorage.techtarget.com/definition/RAM-random-access-memory)) from your hard disk or diskette drive.

With BIOS, your operating system and its applications are freed from having to understand exact details (such as hardware addresses) about the attached input/output devices. When device details change, only the BIOS program needs to be changed. Sometimes this change can be made during your system setup. In any case, neither your operating system or any applications you use need to be changed.

Although BIOS is theoretically always the intermediary between the microprocessor and I/O device control information and data flow, 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.

Purpose of BIOS

POST

The first job of the BIOS after you switch your computer on is to perform the Power OnSelf Test. During the POST, the BIOS checks the computer's hardware in order to ensure that it is able to complete the startup process. If the POST is completed successfully, the system usually emits a beep. If the test fails, however, the system generally emits a series of beeps. You can use the number, duration and pattern of these beeps to identify the cause of the test failure.

**Startup**

With the POST completed, the BIOS then attempts to load the operating system through a program known as a bootstrap loader, which is designed to locate any available operating systems; if a legitimate OS is found, it is loaded into memory. BIOS drivers are also loaded at this point. These are programs designed to give the computer basic control over hardware devices such as mice, keyboards, network hardware and storage devices.

**Security**

The BIOS can also play a role in computer security. Most BIOS software versions have the option to password-protect the boot process, which means that you must enter a password before any BIOS activity can take place. With the BIOS performing virtually all of its functions during startup, this effectively password-protects the operation of the whole computer. However, resetting a lost BIOS password can be time-consuming and involve working on some of the computer's most sensitive components.

**Hardware**

The BIOS software itself generally resides on a Read-Only Memory, or ROM, or a flash memory chip attached to your computer's motherboard. The location of the BIOS software on the chip is important, as it is the first software to take control of your computer when you turn it on. If the BIOS was not always located in the same place on the same chip, your computer's microprocessor would not know where to locate it, and the boot process could not take place

Differentiate between RAID and LVM

**RAID**

* RAID is used for redundancy.
* A RAID device is a physical grouping of disk devices in order to create a logical presentation of one device to an Operating System for redundancy or performance or a combination of the two.
* RAID is a way to create a redundant or striped block device with redundancy using other physical block devices.
* RAID is either a software or a hardware technique to create data storage redundancy across multiple block devices based on required RAID levels.
* RAID is NOT any kind of Data backup solution. Its a solution to prevent one of the SPOFs (Single Point of Failure) i.e. DISK failure. By configuring RAID you are just providing an emergency substitute for the Primary disk. It NEVER means that you have configured DATA backup.

**LVM**

* LVM is a way in which you partition the hard disk logically and it contains its own advantages.
* LVM is a logical layer that that can be anipulated in order to create and, or expand a logical presentation of a disk device to an Operating System.
* LVM usually sits on top of RAID blocks or even standard block devices to accomplish the same result as a partitioning, however it is much more flexible than partitions. You can create multiple volumes crossing multiple physical devices, remove physical devices without loosing data, resize the volumes, create snapshots, etc
* LVM is a software tool to manage large pool of storage devices making them appear as a single manageable pool of storage resource. LVM can be used to manage a large pool of what we call Just-a-bunch-of-Disk (JBOD) presenting them as a single logical volume and thereby create various partitions for software RAID.
* LVM is a disk management approach that allows us to create, extend, reduce, delete or resize the volume groups or logical volumes.
* Unified Extensible Firmware Interface (UEFI) is a specification for a software program that connects a computer's firmware to its operating system ([OS](https://whatis.techtarget.com/definition/operating-system-OS)). UEFI is expected to eventually replace [BIOS](https://whatis.techtarget.com/definition/BIOS-basic-input-output-system).
* Like BIOS, UEFI is installed at the time of manufacturing and is the first program that runs when a computer is turned on. It checks to see what hardware components the computing device has, wakes the components up and hands them over to the operating system. The new specification addresses several limitations of BIOS, including restrictions on [hard disk](https://searchstorage.techtarget.com/definition/hard-disk) [partition](https://searchstorage.techtarget.com/definition/partition)size and the amount of time BIOS takes to perform its tasks.
* Because UEFI is programmable, original equipment manufacturer ([OEM](https://searchitchannel.techtarget.com/definition/OEM)) developers can add applications and drivers, allowing UEFI to function as a lightweight operating system.
* The Unified Extensible Firmware Interface is managed by a group of chipset, hardware, system, firmware, and operating system vendors called the UEFI Forum.The specification is most often pronounced by naming the letters U-E-F-I.

Encryption in whatsapp

The term 'end-to-end encryption' (E2EE) has entered the common lexical use and is no more restricted to the geeks, thanks to WhatsApp which popularised it and brought it to over a billion users globally. It has become the part of our daily digital life as it is the definitive security mechanism that protects our personal data (messages etc.) such that it can only be read on by the sender, and by the recipient on the other end. No one else, including the hackers or the government, can snoop and read the encrypted data.

**How does end-to-end encryption work?**

WhatsApp's end-to-end encryption ensures that only you and the person you're communicating with can read what's sent. Nobody in between, not even WhatsApp, can read the messages. The messages are secured with locks, and only the recipient has the special key to unlock and read the messages. WhatsApp uses Signal Protocol developed by Open Whisper Systems. The following steps describes the working of E2EE when two people communicate on WhatsApp.

1. When the user first opens the WhatsApp, two different keys (public & private) are generated. The encryption process takes place on the phone itself.
2. The private key must remain with the user whereas the public key is transferred to the receiver via the centralised WhatsApp server.
3. The public key encrypts the senders message on the phone even before it reaches the centralised server.
4. The server is only used to transmit the encrypted message. The message can only be unlocked by the private key of the receiver. No third part, including WhatsApp can intercept and read the message.
5. If a hacker tries to hack and read the messages, they would fail because of the encryption.