***WhatsApp Encryption***

WhatsApp is an extremely popular mobile messaging service. WhatsApp messages are fully end-to-end encrypted. WhatsApp uses part of a security protocol developed by Open Whisper Systems, a company that has its own fully secure messaging app Signal (for [iOS](https://go.redirectingat.com/?id=803X112721&xcust=06-3637780-11-0000000&sref=https%3A%2F%2Fwww.techadvisor.co.uk%2Ffeature%2Finternet%2Fhow-secure-is-whatsapp-whatsapp-security-encryption-explained-3637780%2F&xs=1&url=https%3A%2F%2Fitunes.apple.com%2Fgb%2Fapp%2Fsignal-private-messenger%2Fid874139669%3Fmt%3D8" \t "_blank) and [Android](https://go.redirectingat.com/?id=803X112721&xcust=06-3637780-11-0000000&sref=https%3A%2F%2Fwww.techadvisor.co.uk%2Ffeature%2Finternet%2Fhow-secure-is-whatsapp-whatsapp-security-encryption-explained-3637780%2F&xs=1&url=https%3A%2F%2Fplay.google.com%2Fstore%2Fapps%2Fdetails%3Fid%3Dorg.thoughtcrime.securesms%26hl%3Den)). It may not be as obsessed with multimedia sharing as WhatsApp but its basic functions are the same - and fully end-to-end encrypted. WhatApp now securely encrypts every single message, call, picture, video or any other type of file you send so that the only person who can read or view it is the recipient. Not even WhatsApp has the ability to intercept and view those messages.

WhatsApp encrypting messages ‘end-to-end’ is a big deal because it means that the company itself has decided to run a system in which even it cannot intercept and read messages sent on its own platform. When you send a message, it can only be ‘unlocked’ by the intended recipient, thanks to a very complex code that took WhatsApp several years to develop. It’s no mean feat to achieve, particularly given that 1 billion people use the service. This differs from many messaging apps, which only encrypt messages between you and them. This means that your messages are stored on the services servers, usually not permanently, so hypothetically could be accessed and read.

WhatsApp has end-to-end encryption, it means that they and no party – governments, police, hackers, others – can intercept and read your messages. WhatsApp has done this because as a company they believe in your right to have private conversations when you use their service.

***BIOS***

BIOS Stands for Basic Input/Output System.  The BIOS is a program pre-installed on Windows-based computers (not on Macs) that the computer uses to start up. The CPU accesses the BIOS even before the operating system is loaded. The BIOS then checks all your hardware connections and locates all your devices. If everything is OK, the BIOS load the operating system into the computer's memory and finishes the boot-up process. Since the BIOS manages the hard drive, it can't reside on one, and since it is available before the computer boots up, it can't live in the RAM. It is actually located in the ROM (Read-Only Memory) of the computer. More specifically, it resides in an erasable programmable read-only memory (EPROM) chip. So, as soon as you turn your computer on, the CPU accesses the EPROM and gives control to the BIOS.

The BIOS also is used after the computer has booted up. It acts as an intermediary between the CPU and the I/O (input/output) devices. Because of the BIOS, your programs and your operating system don't have to know exact details (like hardware addresses) about the I/O devices attached to your PC. When device details change, only the BIOS needs to be updated. You can make these changes by entering the BIOS when your system starts up. To access the BIOS, hold down the delete or F2 key as soon as your computer begins to start up.

# *Purpose of BIOS for a Computer*

BIOS enables computers to perform certain operations as soon as they are turned on. The principal job of a computer's BIOS is to govern the early stages of the startup process, ensuring that the operating system is correctly loaded into memory. BIOS is vital to the operation of most modern computers, and knowing some facts about it could help you troubleshoot issues with your machine.

## *POST*

The first job of the BIOS after you switch your computer on is to perform the Power On Self 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.

## *Booting Process of Computer*

#### **Booting Process of Computer Step by Step :-**

* When you turn on the PC’s power switch, the internal power supply initializes itself. The power supply does not provide power to the rest of the PC immediately. As soon as the power supply is able to supply reliable power to the motherboard, it transmits a “good power” signal to the motherboard’s chip set , which sends a system reset command to the processor . At this point, from all outward appearances, the PC looks as if it is still powered off.
* The system reset command sent by the motherboard’s chip set causes the CPU to read its first instruction from what is called the jump address. The jump address is always located in a fixed preset location, typically address FFFF0h in system memory. The jump address contains the physical address of the BIOS’ boot program on the ROM BIOS chip.
* The CPU executes the first instruction, which copies the BIOS programs into system memory and starts the BIOS running.
* The BIOS next performs the POST (Power-On Self-Test) process. The POST verifies and tests the hardware configuration stored in the BIOS configuration information. Should the POST detect any problems, it sounds beep codes, one or more beeps through the system speaker to indicate the nature of the problem, or displays an error message, and the boot process stops.
* If the POST finds no problems, the boot process continues. At this point, the system BIOS (the one booting the PC) looks for the video adapter’s BIOS and starts it. Virtually all peripheral devices on the PC have their own BIOS. This is the first time, aside from the noises of the disk drives and a single beep indicating all is well, that you will know the PC is booting. Information about the video card is displayed on the monitor’s screen.
* The display of the video adapter’s information is followed by information about the system BIOS itself. This usually includes information on the manufacturer and version of the BIOS program.
* Any device BIOS routines are started. The video card’s BIOS starts first to turn on the display, then information about the system BIOS and the other BIOSs is displayed as they are started.
* Next, the BIOS begins a series of tests on the system, including the amount of memory detected on the system. This test is usually displayed on the screen as a run-up counter showing the amount of memory detected and tested. Because the BIOS now has use of the monitor, it displays error messages for any problems detected instead of the beep codes that it had to use prior to the display being available.
* With the device BIOSs loaded, the system BIOS checks if the devices listed in the CMOS configuration data (see “Complementary Metal-Oxide Semiconductor (CMOS)” later in the chapter) are present and functioning, including their speeds, access modes, and other parameters. In this sequence, the serial and parallel ports are assigned their identities (COM1, COM2, LPT1, etc.). As each device is passed, a message is displayed that it was found, configured, and tested.
* If the BIOS supports Plug and Play (PnP) technology, any PnP devices detected are configured. Information on each PnP device is displayed on the screen, although it typically goes by much too fast to read.
* At the end of the test and configuration sequence, the BIOS should display a summary data screen that details the PC as the BIOS sees it and indicating that the system is verified and ready for use.
* To start the operating system running, the BIOS must first find it. Included in the CMOS data is a parameter that indicates the disk drives (floppy, hard, or CD-ROM) and the order in which they should be accessed to find the operating system. In most cases, the boot sequence parameters will be set to look for the operating system on first the floppy disk drive, then the hard disk drive, and perhaps, if all else fails, the CD-ROM drive.
* This sequence can be changed to reflect the sequence desired. If the first boot device is the hard disk, the BIOS looks for the master boot record (MBR) to use to start the operating system. If the boot disk is a floppy disk, the BIOS looks at the first sector of the disk for the OS boot program. If the boot program is not found on the first device listed, then the next device is searched and so on until the boot program is found. If no boot device is found, the boot sequence stops and an error message (“No boot device available”) is displayed.

***Difference Between RAID and LVM***

|  |  |  |
| --- | --- | --- |
| **S.No** | **RAID** | **LVM** |
| 1. | RAID is used for redundancy. | LVM is a way in which you partition the hard disk logically and it contains its own advantages. |
| 2. | 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. | 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. |
| 3. | RAID is a way to create a redundant or striped block device with redundancy using other physical block devices. | 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 |
| 4. | RAID is either a software or a hardware technique to create data storage redundancy across multiple block devices based on required RAID levels. | 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. |
| 5. | 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 is a disk management approach that allows us to create, extend, reduce, delete or resize the volume groups or logical volumes. |