**Basic Input/output System (BIOS)**

A basic input/output system (BIOS) is a preinstalled program used during start-up on Windows-based computers. The CPU initially accesses the BIOS, after which the operating system is loaded.

The BIOS is built-in software that contains generic code required to control the keyboard, display screens, disk drives and other functions. The primary purpose of the BIOS is to set up hardware and further load and start an operating system. BIOS is placed in a non-volatile ROM chip inside the computer, ensuring the availability of BIOS at all times and preventing accidental disk failure. The BIOS checks every hardware connection and locates the devices, after which the operating system is loaded into computer memory.

BIOS software is designed to work with the various devices that make up a complimentary system chipset. The BIOS library has certain functions used to operate and control system peripherals, which can be initiated by an external software.

Users using the BIOS user interface can perform functions such as:

* Setting the system clock
* Enabling and disabling certain system components
* Hardware configuration
* Selecting boot drives
* Set password prompts for secured access to BIOS user interface function

Booting Process

**Booting a computer** refers to the process of powering on the computer and starting the operating system. The **operating system** is the program that makes all your software applications and hardware work together, so you can do the work you want to do. Once you hit the power button, it's all automatic from there. The boot process loads the operating system into main memory or the random access memory (RAM) installed on your computer. Now let's learn a little more about the boot process.

Booting (also known as booting up) is the initial set of operations that a computer system performs when electrical power is switched on. The process begins when a computer that has been turned off is re-energized, and ends when the computer is ready to perform its normal operations. On modern general purpose computers, this can take tens of seconds and typically involves performing power-on self-test, locating and initializing peripheral devices, and then finding, loading and starting an operating system. Many computer systems also allow these operations to be initiated by a software command without cycling power, in what is known as a soft reboot, though some of the initial operations might be skipped on a soft reboot. A boot loader is a computer program that loads the main operating system or runtime environment for the computer after completion of self-tests.

The computer term boot is short for bootstrap or bootstrap load and derives from the phrase to pull oneself up by one’s bootstraps. The usage calls attention to the paradox that a computer cannot run without first loading software but some software must run before any software can be loaded. Early computers used a variety of ad-hoc methods to get a fragment of software into memory to solve this problem.

**Unified Extensible Firmware Interface (UEFI)**

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.

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 partition size and the amount of time BIOS takes to perform its tasks.

## 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 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. It’s 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. |

**Whatsapp Security**

# End-to-end encryption

Privacy and security is in our DNA, which is why we have end-to-end encryption. When end-to-end encrypted, your messages, photos, videos, voice messages, documents, status updates and calls are secured from falling into the wrong hands.

WhatsApp end-to-end encryption ensures only you and the person you're communicating with can read what's sent, and nobody in between, not even WhatsApp. Your messages are secured with locks, and only the recipient and you have the special keys needed to unlock and read your messages. For added protection, every message you send has an unique lock and key. All of this happens automatically: No need to turn on settings or set up special secret chats to secure your messages.

### What's the "Verify Security Code" screen in the contact info screen?

Each of your chats has its own security code used to verify that your calls and the messages you send to that chat are end-to-end encrypted.

This code can be found in the contact info screen, both as a QR code and a 60-digit number. These codes are unique to each chat and can be compared between people in each chat to verify that the messages you send to the chat are end-to-end encrypted. Security codes are just visible versions of the special key shared between you - and don't worry, it's not the actual key itself, that's always kept secret.

### To verify that a chat is end-to-end encrypted

1. Open the chat.
2. Tap on the name of the contact to open the contact info screen.
3. Tap **Encryption** to view the QR code and 60-digit number.

If you and your contact are physically next to each other, one of you can scan the other's QR code or visually compare the 60-digit number. If you scan the QR code, and the code is indeed the same, a green check mark will appear. Since they match, you can be sure no one is intercepting your messages or calls.

If the codes don't match, it's likely you're scanning the code of a different contact, or a different phone number. If your contact has recently reinstalled WhatsApp or changed phones, we recommend you refresh the code by sending them a new message and then scanning the code.