**WhatsApp Encryption**

WhatsApp is an extremely popular mobile messaging service with over 1 billion daily users. That's an amazing figure, and the company prides itself in the apparent security it affords all of those users. WhatsApp 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.

As a user, you don’t have to turn this feature on, nor can you turn it off. You should receive a message within your chats if you are using the latest version of the app to let you know the change has been implemented for you.

Encryption is the scrambling of messages from the sender on their journey to the recipient, largely to discourage the interception and reading of those messages by other parties. 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 too 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, and other users – can intercept and read your messages.

**BIOS**

BIOS (Basic Input/output System) are a program for the initial boot of a computer, equipment adjustment and input/output functions support. BIOS is recorded on the flash-memory microcircuit which is located on the mainboard. Initially, the main purpose of BIOS was input/output devices maintenance (keyboard, screen and disk drives); that is why it was called “Basic Input/output System”.

**Purpose of BIOS for a Computer**

* **Boot and procedure of self-testing (Power-On Self-Test, POST).**A program, located in BIOS microcircuit, loads the first after computer power-up. It detects and examines the installed equipment, adjusts it and prepares for the future operation. If the equipment failure occurs, POST procedure will stop operating and corresponding message or alarm will be revealed.
* **System parameters setting with the BIOS Setup program assistance.**During the procedure POST equipment adjusts within the parameters that are stored in the specific CMOS-memory. Users can configure separate devices and entire system at their own discretion by violating these parameters which are edited in a special program called BIOS Setup or CMOS Setup. The majority of our articles will be dedicated to a system setup with the assistance of BIOS Setup program.
* **Input/output functions support with the assistance of BIOS program interrupts.**System BIOS comprised of built-in functions for the manipulation with keyboard, video display adapter, disk drive mechanisms, hard disk drives, input-output ports, etc. These functions have been used in such operation systems as MS-DOS, and they are almost not used in Windows modern versions.

**Booting Process of Computer**

* 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 are 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 manipulated 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 losing 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. |