WHAT'SAPP ENCRYPTION?

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 are communicating with can read what is 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 a 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. End-to-end encryption is always activated. There is no way to turn off end-to-end encryption.

What is 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 do not worry, it is not the actual key itself, that has 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.

If you and your contact are not physically near each other, you can send them the 60-digit number. Let your contact know that once they receive your code, they should write it down and then visually compare it to the 60-digit number that appears in the contact info screen under **Encryption**. For Android, iPhone and Windows Phone, you can use the **Share** button from the **Verify Security Code** screen to send the 60-digit number via SMS, email, etc.

Are my messages and calls with businesses end-to-end encrypted?

All WhatsApp messages and calls are secured with end-to-end encryption. It is important to remember, however that when you contact a business, several people in that business might see your messages. A business may employ another company to manage its communications - for example, to store, read or respond to your messages.

The business you are communicating with has a responsibility to ensure that it handles your messages in accordance with its privacy policy.

WHAT IS BIOS?

BIOS (basic input/output system) is the program a personal computer's microprocessor uses to get the computer system started after you turn it on. It also manages data flow between the computer's operating system and attached devices such as the hard disk, video adapter, keyboard, mouse and printer.

PURPOSE OF BOOTING

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 start-up 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?

6 Steps Your Computer Goes Through While Boot Up:

Unlike other electronic devices, a computer follows several steps in order to boot up .The boot up process is completely dependent on the BIOS chip and hence could possibly vary a little between manufacturers.

1. ***Hardware Start –Up:***

Once you have pressed the power button, the power supply is to be distributed among all the various hardware components present within your computer including the BIOS and processor.

It may happen that the power received by components isn't at the required level due to which the hardware remains unresponsive. In such cases, a signal, which signifies a power failure, is sent and the user has to power off and then later begin the startup process. In every other case, the hardware is ready and an LED usually lights up signifying proper hardware startup.

2. ***The Processor's First Process:***

Now that reliable power is supplied to all the components including the motherboard's chipset and processor. The processor is ready to start its first process. But since there is no memory, the processor is caught up not knowing what to execute and from where. So as pre-designed by manufacturers, the control shifts to that little code present in the BIOS chip.

This code is very small and is present in the default memory location from where the processor starts booting up the operating system. In the meanwhile since the BIOS chip is ON, it performs the power on self test.

3. ***BIOS: Power-On Self Test***

Like already mentioned, BIOS performs the power on self test (POST) at the very early stages of your computer startup. It is to let you (the users) know if there are any fatal system errors. It works like a diagnostic tool.

In motherboards featuring built –in speakers, the end or success of the POST is signified by a beep. If your system isn't beeping at startup then you have the opposite kind where you receive that beep in case of any system error.

By the end of the POST, all the devices and interrupts are checked, identified and properly initiated.

4. ***The post-POST part:***

By now the BIOS is aware of all the devices attached to the motherboard. Now the code present in the BIOS starts executing; and tries to communicate with the other BIOS chips present in the devices.

First the video card BIOS is communicated with and it then makes the video card display the first screen. (Usually the information of graphic card or motherboard is displayed). Later the other BIOS codes are also executed one after the other.

5. ***The Next Phase – Searching…***

Now that one half of the entire process is done, the BIOS now searches for a drive to boot the operating system. Usually it looks to boot from a floppy disk and if its not available, it proceeds to the hard drive.

All this searching is defined within the code present in the system BIOS. Once the drive is selected, the BIOS now looks for information required to boot operating system into that drive. For this it goes through the master boot record.

6. ***The Final Take-down:***

The information present in the master boot record is verified and the booting of operating system begins. In the meanwhile, the boot sector loads this code into memory at the location 0000:7C00. Once this is done, the computer now hands over the control from the BIOS to the operating system.

Once all the files in your operating system are loaded into memory, you are displayed the operating system screen and there you go, everything you need is prepared by the operating system itself.

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 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.

SERVER HARDENING

Server Hardening is the process of enhancing **server** security through a variety of means which results in a much more secure **server** operating environment. This is due to the advanced security measures that are put in place during the **server hardening** process.

Mainly involve:

- OS Hardening
- Web Server Hardening
- Database Hardening

Some common server handling tips and tricks:

- Physical System Security
- Disk Partitions
- Minimize Packages to Minimize Vulnerability
- Check Listening Network Ports
- Use Secure Shell(SSH)
- Keep System updated
- Lockdown Cronjobs.
- Disable USB stick to Detect.

- **CentOS**

  CentOS is a Linux distribution that provides a free, enterprise-class, community-supported computing platform functionally compatible with its upstream source, Red Hat Enterprise Linux.

- **Apache**

  The Apache HTTP Server, colloquially called Apache, is free and open-source cross-platform web server software, released under the terms of Apache License 2.0. Apache is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation.

- **MongoDB**

  MongoDB is a cross-platform document-oriented database program. Classified as a NoSQL database program, MongoDB uses JSON-like documents with schemata. MongoDB is developed by MongoDB Inc. and licensed under the Server Side Public License.