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.

Important: End-to-end encryption is always activated. There's no way to turn off end-to-end encryption.

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.

Note: The verification process is optional and used only to confirm that the messages you send 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.

If you and your contact aren't 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's 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're communicating with has a responsibility to ensure that it handles your messages in accordance with its privacy policy. For more information, please contact that business directly

Why does WhatsApp offer end-to-end encryption and what does it mean for keeping people safe?

Security is essential to the service WhatsApp provides. We completed the implementation of end-to-end encryption in 2016 for all messaging and calling on WhatsApp so that no one, not even us, has access to the content of your conversations. Since then, digital security has become even more important. We've seen multiple examples where criminal hackers illegally obtained vast sums of private data and abused technology to hurt people with their stolen information. So as we’ve introduced more features – like video calling and Status – we’ve extended end-to-end encryption to these features as well.

WhatsApp has no ability to see the content of messages or listen to calls on WhatsApp. That’s because the encryption and decryption of messages sent on WhatsApp occurs entirely on your device. Before a message ever leaves your device, it's secured with a cryptographic lock, and only the recipient has the keys. In addition, the keys change with every single message that's sent. While all of this happens behind the scenes, you can confirm your conversations are protected by checking the security verification code on your device.

Naturally, people have asked what end-to-end encryption means for the work of law enforcement. WhatsApp appreciates the work that law enforcement agencies do to keep people safe around the world. We carefully review, validate and respond to law enforcement requests based on applicable law and policy, and we prioritize responses to emergency requests. As part of our education efforts, we published information for law enforcement about the limited information we collect and how they can make requests of WhatsApp.

DIFFERENCE

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

BIOS

A computer's **Basic Input Output System** and **Complementary Metal-Oxide Semiconductor** together handle a rudimentary and essential process: they set up the **computer** and boot the operating system. The BIOS's primary function is to handle the **system setup process** including driver loading and operating system booting.

BIOS, which stands for Basic Input Output System, is software stored on a small memory chip on the motherboard. ... The **BIOS** firmware is non-volatile, meaning that its **settings** are saved and recoverable even after power has been removed from the device.

How to Configure the BIOS Using the BIOS Setup Utility

1. Enter the BIOS Setup Utility by pressing the F2 key while the system is performing the power-on self-test (POST). ...
2. Use the following keyboard keys to navigate the BIOS Setup Utility: ...
3. Navigate to the item to be modified. ...
4. Press Enter to select the item. ...
5. Use the up or down arrow keys or the + or – keys to change a field.