**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 (provided they are running the latest version of the app).

Below is our guide on how to ensure your WhatsApp messages are fully end-to-end encrypted. However it's also good to be aware that not everyone trusts the company's word, in part because of privacy issues surrounding its parent company Facebook and also its implementation of encryption.

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) 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's very good. It may not be as obsessed with multimedia sharing as WhatsApp but its basic functions are the same - and fully end-to-end encrypted.

WhatsApp has taken a few hits and been in the news recently, and the somewhat limited understanding of encryption means it can be a bit confusing. Here are a few examples of WhatsApp in the news, and what it really means.

WhatApps 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 (which is required) to let you know the change has been implemented for you.

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 to 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.

Now that WhatsApp has end-to-end encryption, it means that they and no party – governments, police, hackers, other users – 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 (basic input/output system)**

BIOS (basic input/output system) is the program a personal computer's [microprocessor](https://whatis.techtarget.com/definition/microprocessor-logic-chip) uses to get the computer system started after you turn it on. It also manages data flow between the computer's [operating system](https://whatis.techtarget.com/definition/operating-system-OS) and attached devices such as the [hard disk](https://searchstorage.techtarget.com/definition/hard-disk), [video adapter](https://whatis.techtarget.com/definition/video-adapter), [keyboard](https://whatis.techtarget.com/definition/keyboard), [mouse](https://whatis.techtarget.com/definition/mouse) and [printer](https://whatis.techtarget.com/definition/printer).

BIOS is an integral part of your computer and comes with it when you bring it home. (In contrast, the operating system can either be pre-installed by the manufacturer or vendor or installed by the user.) BIOS is a program that is made accessible to the microprocessor on an erasable programmable read-only memory ([EPROM](https://whatis.techtarget.com/definition/EPROM)) chip. When you turn on your computer, the microprocessor passes control to the BIOS program, which is always located at the same place on EPROM.

When BIOS boots up (starts up) your computer, it first determines whether all of the attachments are in place and operational and then it loads the operating system (or key parts of it) into your computer's random access memory ([RAM](https://searchstorage.techtarget.com/definition/RAM-random-access-memory)) from your hard disk or diskette drive.

With BIOS, your operating system and its applications are freed from having to understand exact details (such as hardware addresses) about the attached input/output devices. When device details change, only the BIOS program needs to be changed. Sometimes this change can be made during your system setup. In any case, neither your operating system or any applications you use need to be changed.

Although BIOS is theoretically always the intermediary between the microprocessor and I/O device control information and data flow, in some cases, BIOS can arrange for data to flow directly to memory from devices (such as video cards) that require faster data flow to be effective.

# Purpose of BIOS

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.

**The Booting 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. The invention of integrated circuit Read-only memory (ROM) of various types solved the paradox by allowing computers to be shipped with a start up program that could not be erased, but growth in the size of ROM has allowed ever more elaborate start up procedures to be implemented.

There are numerous examples of single and multi-stage boot sequences that begin with the execution of boot program(s) stored in boot ROMs. During the booting process, the binary code of an operating system or runtime environment may be loaded from nonvolatile secondary storage (such as a hard disk drive) into volatile, or random-access memory (RAM) and then executed. Some simpler embedded systems do not require a noticeable boot sequence to begin functioning and may simply run operational programs stored in read-only memory (ROM) when turned on.

**The order of booting –**

In order for a computer to successfully boot, its BIOS, operating system and hardware components must all be working properly; failure of any one of these three elements will likely result in a failed boot sequence.

When the computer’s power is first turned on, the CPU initializes itself, which is triggered by a series of clock ticks generated by the system clock. Part of the CPU’s initialization is to look to the system’s ROM BIOS for its first instruction in the startup program. The ROM BIOS stores the first instruction, which is the instruction to run the power-on self test (POST), in a predetermined memory address. POST begins by checking the BIOS chip and then tests CMOS RAM. If the POST does not detect a battery failure, it then continues to initialize the CPU, checking the inventoried hardware devices (such as the video card), secondary storage devices, such as hard drives and floppy drives, ports and other hardware devices, such as the keyboard and mouse, to ensure they are functioning properly.

Once the POST has determined that all components are functioning properly and the CPU has successfully initialized, the BIOS looks for an OS to load.

The BIOS typically looks to the CMOS chip to tell it where to find the OS, and in most PCs, the OS loads from the C drive on the hard drive even though the BIOS has the capability to load the OS from a floppy disk, CD or ZIP drive. The order of drives that the CMOS looks to in order to locate the OS is called the boot sequence, which can be changed by altering the CMOS setup. Looking to the appropriate boot drive, the BIOS will first encounter the boot record, which tells it where to find the beginning of the OS and the subsequent program file that will initialize the OS.

Once the OS initializes, the BIOS copies its files into memory and the OS basically takes over control of the boot process. Now in control, the OS performs another inventory of the system’s memory and memory availability (which the BIOS already checked) and loads the device drivers that it needs to control the peripheral devices, such as a printer, scanner, optical drive, mouse and keyboard. This is the final stage in the boot process, after which the user can access the system’s applications to perform tasks.

## Difference between RAID and LVM

|  |  |
| --- | --- |
| **RAID** | **LVM** |
| RAID is used for redundancy. | LVM is a way in which you partition the hard disk logically and it contains its own advantages. |
| 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. |
| 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. |
| 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. |
| 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. |