Signal

PRIVACY GUIDE

Signal

The principles, in plain language

What it is, how it protects your messages and why it is so reliable.

01

What Signal is

Signal is a messaging and calling app designed so that only you and the person you are talking to can read what you say to each other. It is maintained by a non-profit foundation, carries no advertising, and its encryption protocols have become the industry reference.

END-TO-END ENCRYPTION

Messages and calls are encrypted on your phone and only opened on your contact's. Not even Signal can read them.

NO ADVERTISING

It is funded by donations and voluntary subscriptions, not by selling data or ads.

OPEN SOURCE

Anyone can read how it works, review it and propose improvements.

02

Four ideas first

If you already know how encryption works, skip straight to section 4.

1. **Keys.** You have two linked numbers. The public key is like your mailbox number: you can give it to anyone. The private key is the key that opens it, and it never leaves your phone.
2. **End-to-end encryption.** The message turns into unreadable data as it leaves your phone and only becomes readable when it reaches the recipient's. The servers it passes through see only noise.
3. **Metadata.** This is data about the conversation, not its content: who talks to whom, when and from where. Sometimes it matters as much as the message itself.
4. **Verification.** To be sure that the key you receive is really your contact's, you can both compare a number that depends on the two keys. If it matches, nobody has got in the middle.

03

The problem: hardly anyone knows where their messages pass through

A message travels through several computers before it arrives. If the service only encrypts the connection to its server, the company can read everything that passes through there, store it or hand it over if asked. And even if the content is protected, the company still knows whom you talk to and when: it is as if the envelope were sealed, but the postman wrote down every sender and every recipient in a notebook.

> **Why it matters.** Whoever knows your contacts and your schedules can deduce a lot about you without opening a single message. A good messenger has to protect the content and also reduce what it knows about people.

04

The three privacy principles

Signal protects three things at once, each with its own technique.

CONTENT

Only you read it

End-to-end encryption.

HISTORY

A new key for every message

The double ratchet.

METADATA

The server knows the minimum

Sealed sender and private contacts.

Content: only you read it

Before you write, your phone and your contact's agree on a secret key using their public keys, even if they have never met and even if someone listens to everything they say to each other. With that key, the message is encrypted on your phone. The server receives a closed package and keeps it until the recipient connects. It is like two people who, speaking aloud in a square, manage to agree on a code that nobody else can work out.

History: a new key with every message

The key is not always the same: it changes with every message and every time the conversation changes turn. It is called the double ratchet because, like a mechanical ratchet, it turns in only one direction: from today's key you cannot work out yesterday's. If someone stole your phone today, they could not read the old messages, and if they copied your keys, the conversation heals itself as soon as you write to each other again.

Metadata: the server knows the minimum

Signal reduces what its own server can see. With sealed sender, the server knows whom the message is for, but not whom it comes from. To find your contacts it uses a hardware-protected processor that looks up the numbers without anyone, not even Signal, seeing your address book. In groups, names and members are stored encrypted. And you can create a username so as not to give your phone number to strangers.

> The three mechanisms work together: the content is protected, the keys do not last and the server sees the minimum needed to deliver.

05

A message, step by step

1. Your app asks the server for your contact's public keys, which they left ready even though they are offline.
2. With them, your phone computes a shared secret key, reinforced with a post-quantum secret.
3. It encrypts the message with a one-time key and deletes it afterwards.
4. It sends it to the server inside a sealed envelope: the recipient is visible, the sender is not.
5. The server keeps it until your contact connects. It can never open it.
6. Your contact's phone decrypts it and the conversation moves on to a new key.

06

How to get the most out of it

A LONG PIN

It protects your account if someone tries to register your number on another phone. Also turn on registration lock.

A USERNAME

It lets you chat without giving your phone number and decide who can find you with it.

VERIFY CONTACTS

Compare the safety number or use automatic verification to know you are talking to who you think.

DISAPPEARING MESSAGES

They delete themselves after the time you choose, in your most sensitive conversations.

Signal is ready for the future: it already combines classical encryption with encryption that resists quantum computers, so that what you send today stays protected tomorrow. No system can protect a phone that is already in someone else's hands or infected, so keep your system up to date and lock your screen.

REFERENCE

Quick glossary

TERM	IN ONE SENTENCE
End-to-end encryption	Only the two ends of the conversation can read the message
Public and private key	Your mailbox, which is shared, and its key, which is not
Double ratchet	A mechanism that changes the encryption key with every message
Sealed sender	A technique so that the server does not know who sends each message
Metadata	Data about the communication: who, when and from where
Safety number	A number you compare to check that nobody is in the middle
Post-quantum	Encryption designed to resist future quantum computers
PIN	A code that protects your account and lets you recover your data

> **Next step.** The complete guide, "Signal in depth", explains each of these pieces in more detail and with their maths, chapter by chapter.

Sources: Signal documentation and blog (signal.org).