Signal Verification

Signal actually has **two completely different "verification" concepts**, and people often mix them up:

1) Account verification (SMS code when you sign up)

When you first install Signal:

- You enter your phone number
- Signal sends you a **one-time SMS or call code**
- You type that in to confirm you control the number (Signal Support)

That's just **account registration**, not related to verifying other users.

2) Contact verification (the important security feature)

This is what most people mean by "verification" in Signal.

How it works

For every **1-to-1 chat**, Signal creates a unique:

Safety number (a long numeric code + QR code) (Signal Support)

This number is derived from encryption keys and acts like a **fingerprint of your secure connection**.

What you do

To verify someone:

Open the chat → view safety number

Compare it with your contact:

- Best: scan QR in person
- Or: read/compare digits via another trusted channel

If they match → tap **"Mark as verified"** (Signal Support)

If they match, you know:

- You're talking to the real person
- No one is intercepting messages (no "man-in-the-middle" attack)

Signal Verification

Important: verification is per conversation

- Each pair of users has its **own safety number** (Signal Support)
- Verifying Alice does nothing for Bob
- Group chats don't use a single shared safety number

Do you "continue verification" with other users?

Short answer: **No, not automatically.**

- You must verify **each contact separately**
- There is **no global trust system** or carry-over
- Signal itself explicitly says it **does not verify identities for you** (Signal Support)

Also important (many people misunderstand this)

- Verification is **only visible to you**
- The other person:
  - **Does NOT get notified**
  - Doesn't know if you verified them (Signal Support)

What happens if something changes?

If your contact:

- reinstalls Signal
- switches phones
- or changes keys

The safety number may change

Then:

- Signal warns you

- You should **re-verify before trusting again** (Signal Support)

Bottom line

Account verification (SMS) = proves you own

Here's a simple **step-by-step walkthrough** to verify a contact in the Signal app:

How to verify a contact in Signal

1) Open the conversation

- Launch Signal
- Tap the chat with the person you want to verify

2) Go to contact info

- Tap their **name at the top** of the chat screen
- This opens the contact settings

3) Find the safety number

- Tap **"View Safety Number"**

You'll now see:

- A long **60-digit number**
- A **QR code**

4) Compare with your contact

You have a few options:

✅ **Best (in person)**

Tap **"Scan QR code"**

Scan the code on their phone

✅ **Remote (still good)**

- Read the numbers aloud over a **trusted channel** (phone call, in person, etc.)
- Or send a screenshot via a **different secure platform**

5) Mark as verified

If everything matches, tap **"Mark as Verified"**

✔️ You'll now see a small checkmark or verification indicator in that chat

When should you re-check?

You should verify again if Signal shows a warning like:

- "Safety number has changed"

This can happen if they:

- Switch phones
- Reinstall Signal
- Change devices

⚠️ **Tips most people miss**

- Verification is **per person** (you must do it for each contact)
- It's **optional**, but strongly recommended for sensitive conversations
- The other person **won't know** you verified them

Verify a contact on iPhone (step-by-step)

1) Open the chat

- Open Signal
- Tap the conversation with the person

2) Tap their name

- At the very top of the screen, tap the **contact's name or profile photo**

This opens the contact details page. (This may vary depending which iOS you are using.) [Sorry, I don't use Android]

3) Tap "View Safety Number"

- Scroll a bit if needed
- Tap **"View Safety Number"**

4) What you'll see

You'll get a screen with:

- A long **60-digit number**
- A **QR code**
- Option to **scan** or **share**

5) Compare (best methods)

- **In person (most secure)**
  - Tap **"Scan Code"**
  - Scan their QR code directly from their phone

Not in person

Compare numbers via:

- A phone call
- FaceTime
- Any **separate trusted channel**

⚠️ Avoid comparing inside the same Signal chat you're trying to verify—that defeats the purpose.

6) Mark as verified

Tap **“Mark as Verified”**

Once done:

You’ll see a **verification checkmark** in the contact screen

Messages are now confirmed to be end-to-end secure with that person

What to watch for later

If you ever see:

“Safety number has changed”

That means:

They switched devices, reinstalled, or keys rotated

Go back and repeat the same steps before trusting again.

iPhone-specific tips

- You can take a screenshot of the safety number (for backup comparison), but don’t store it somewhere public
- Face ID / passcode lock on Signal adds another layer of protection (worth enabling in Settings → Privacy)

Here’s a practical way to think about verification in Signal:

When verification actually matters

You should verify when **identity really matters**, not just privacy.

1) Sensitive or high-stakes conversations

- Sharing passwords, recovery codes, or financial info
- Discussing legal, medical, or confidential work topics
- Anything where impersonation would be a big problem

Example: If someone pretending to be your coworker asks for sensitive info, verification would catch that.

2) First time talking to someone important

- New business contact
- Online acquaintance you haven't met
- Someone introduced digitally

This prevents "wrong number" or impersonation attacks.

3) You suspect something is off

- Messages feel unusual
- Tone suddenly changes
- They ask for unusual favors

Verification is your **reality check**.

4) After a "safety number changed" alert

- This is the **big one most people ignore**

Signal is basically saying:

"Hey, this *might* still be them—but you should confirm."

When it's probably overkill

You usually don't need to verify for:

- Close friends you talk to casually
- Family chats about normal day-to-day stuff
- Group chats that aren't sensitive

Signal is already encrypted—verification just adds **identity certainty**, not basic privacy.

When skipping verification can actually hurt you

Signal Verification

Real-world scenarios where people get burned:

- **SIM swap attacks** (attacker takes over a phone number)
- Someone reinstalling Signal and you assuming it's still the same device
- Social engineering ("Hey it's me, I lost my phone, send me X")

Verification would immediately reveal:

> "This is not the same cryptographic identity"

Simple rule of thumb

Use this:

"Would it be a problem if this person wasn't actually who I think they are?"

- If **yes** → verify
- If **no** → don't worry about it

Reality check (important)

Verification is powerful, but:

- It's **manual** (you have to remember to do it)
- Most people **never do it consistently**
- It protects against **very specific attacks**, not everyday risks

Smart, low-effort strategy

If you don't want to overthink it:

> Verify:
>
> - Your **top 3–5 important contacts**
> - Anyone you exchange sensitive info with
>
> Re-verify only when Signal warns you

That gives you **90% of the benefit with almost no hassle**.

Groups

Signal doesn't have a built-in "verified members only" setting for group chats. But it does have a few controls that get you close.

In Signal groups, you can:

Require admin approval for new members

- If someone joins via a group link, an admin must approve them first
- Control who can add members
- Admins can restrict adding people to admins only
- Review and remove members
- Admins can see all members and remove anyone
- These features let you "manually vet participants", which is the closest thing to a "verified-only" group.
- There's no way to enforce "only verified users can join or participate" in a group automatically
- Verification is "manual and individual", not a group-level rule

To simulate a "verified-only" group:

1. Turn on "admin approval for joins"
2. Only approve people after:
    - verifying them in person, or
    - confirming their safety number
3. Periodically review the member list