Someone May Be Reading Every WhatsApp You Send. These 5 Settings Stop That.

WhatsApp is encrypted in transit — but that's only half the story. Your account, your backup, and your phone can all be compromised.

Mayank Jain · mayankjain.io

A WhatsApp account can be taken over without touching your phone — a SIM swap, a forgotten linked device, or an unencrypted backup sitting in Google Drive is all it takes. These five settings close the gaps that WhatsApp's end-to-end encryption does not cover.

1

Turn on Two-Step Verification — your real WhatsApp password

WhatsApp accounts are tied to your phone number, not a password. Two-Step Verification adds a 6-digit PIN that must be entered when your number is registered on any new device — so even if someone does a SIM swap, they cannot take over your account without this PIN.

WHERE TO FIND IT (iPhone & Android):

WhatsApp → Settings → Account → Two-Step Verification → Turn On → set a 6-digit PIN → add a recovery email address

2

Enable App Lock — biometric protection for WhatsApp itself

Your phone's screen lock protects the whole phone, but App Lock means WhatsApp requires Face ID or fingerprint every time it opens — even if your phone is already unlocked. Anyone who picks up your unlocked phone cannot read your messages.

WHERE TO FIND IT (iPhone & Android):

WhatsApp → Settings → Privacy → App Lock → toggle ON → set "Require Touch ID / Face ID" to Immediately

3

Audit your Linked Devices — the silent spy in your account

WhatsApp lets you stay logged in on up to four devices at once. An old laptop, a tablet you sold, or a device someone else connected can receive every message you send and receive — indefinitely, without any notification. Review this list now and remove anything you do not recognise.

WHERE TO FIND IT (iPhone & Android):

WhatsApp → Settings → Linked Devices → tap each device → Log Out of any you do not recognise or no longer use

4

Turn on End-to-End Encrypted Backup — protect what is at rest

WhatsApp's encryption protects messages while they travel, but your backup in iCloud or Google Drive is stored without encryption by default. If your iCloud or Google Drive account is ever hacked — through a phishing attack or a weak password — the attacker gets a complete copy of your messages. E2E Encrypted Backup means only you, with your password, can ever open it.

WHERE TO FIND IT (iPhone & Android):

WhatsApp → Settings → Chats → Chat Backup → End-to-End Encrypted Backup → Turn On → create a strong password and save it safely

5

Control who can add you to groups — stop strangers and scammers

By default, anyone with your number can pull you into a WhatsApp group. Scammers use this to add people to groups full of strangers and then push fake offers, investment schemes, and fraud — a tactic that particularly targets older people and children who may not recognise the manipulation. "My Contacts" means you get an invite first and can choose to join or decline.

WHERE TO FIND IT (iPhone & Android):

WhatsApp → Settings → Privacy → Groups → change from "Everyone" → select "My Contacts"

■ WhatsApp's encryption protects messages in transit — but not your account, your backup, or your linked devices. These five settings cover what encryption alone cannot. Set them once and you are covered.

Want more guides like this?

Sign up free to receive new guides, checklists,
and plain-language tips straight to your inbox.

mayankjain.io

No spam. Unsubscribe any time.