WhatsApp Security Checklist

ACTIVIST CHECKLIST

Last updated on **October 22, 2026** Takes about **15 minutes**

WhatsApp messages are end-to-end encrypted, but Meta (the company that owns WhatsApp) still hands over a lot of metadata to law enforcement. If you're already organizing on WhatsApp (especially in immigrant communities), this checklist locks down backups, groups, AI features, linked devices, and notifications. For higher-risk political work, move sensitive conversations to Signal.

A lot of activism is already happening on WhatsApp, especially in immigrant communities. It isn't the most secure or private choice, but it's sometimes a useful tool for community organizing because people are already using it or requires features offered by WhatsApp (like Communities).

Your WhatsApp messages are end-to-end encrypted, which makes WhatsApp more secure than regular text messages for protecting what you say. If the cops subpoena your phone carrier for your regular texts, they can see the content of every message. If they subpoena Meta for your WhatsApp messages, they cannot see the content (as long as you don't have Chat Backups enabled).

> **Think of doing large group organizing WhatsApp the same way you would social media:** Assume that bad actors (government, right-wing) could join and monitor any large-unvetted group just like they could join and monitor large groups on social media. Assume they can also see who is in the group in the same way they could see who is following you on social media.

Even with the protections in this guide, there are a number of things WhatsApp will always be able to turn over to law enforcement:

- Your entire contact list (if you have ever given the app access to your contact list, they will always have it, even if you disable it later)
- All the other WhatsApp users who have YOU in their contact list (source)
- The names of all groups you are in
- The members of all the groups you're in
- Which phone numbers you're messaging and when (they can even get this information in real-time, which most other tech companies don't provide to law enforcement)
- If you enable chat backups, Google or Apple can be compelled to turn them over, and they contain all of your messages. See Securely back up your WhatsApp chats for how to use backups safely.

Brand new to WhatsApp? See this guide on how to use WhatsApp.

Baseline WhatsApp protections

EVERYONE This section is for anyone doing activism or advocacy work.

If you only have 10 minutes, start here.

Important Disable WhatsApp chat backups (and ask your contacts to do the same)

WhatsApp backups are not encrypted by default and can be turned over by court order.

The default backups that WhatsApp creates to iCloud or Google Drive are NOT end-to-end encrypted. That means a court can compel Apple or Google to turn over your entire chat history. Even though your messages were sent securely, the backup defeats that protection by providing an easy way for your entire chat history to be revealed.

Disabling backups also protects you if a hacker breaks into your iCloud or Google account through phishing or a reused password.

HOW TO DISABLE BACKUPS ENTIRELY

IPHONE

WhatsApp → Tap **You** in the bottom bar → **Chats** → **Chat Backup** → set **Auto Backup** to **Off**

ANDROID

WhatsApp → ⋮ → **Chats** → **Chat Backup** → set **Auto Backup** to **Off**

Tell your friends: Even if your backups are locked down, people you chat with may be backing up unencrypted. Their backup includes your messages. Ask contacts to lock down their backups too. You might want to send them this guide.

If you absolutely need backups, see Securely back up your WhatsApp chats for how to do this safely.

Hide your "Last seen & online" time on WhatsApp

Stops strangers and group members from tracking when you are using WhatsApp.

By default, anyone you've ever exchanged messages with can see when you were last on WhatsApp. For activists, that's a low-effort way for someone to map your patterns of activity.

HOW TO HIDE YOUR LAST SEEN AND ONLINE STATUS

IPHONE

WhatsApp → Tap **You** in the bottom bar → **Privacy** → **Last seen & online** → Select **Nobody**

ANDROID

WhatsApp → ⋮ → **Privacy** → **Last seen & online** → Select **Nobody**

The "Strict Account Settings" toggle locks this setting, so change Last seen first if you want a custom value.

Enable Strict Account Settings on WhatsApp

Turns on two-step verification, security notifications, unknown-sender blocking, link preview disabling, and silenced unknown callers in one step.

Enabling Strict Account Settings turns on a number of protections at once. It's a good default for anyone doing activism.

HOW TO ENABLE STRICT ACCOUNT SETTINGS

IPHONE

WhatsApp → Tap **You** in the bottom bar → **Privacy** → **Advanced** → **Strict account settings** → **Next** → **Turn on**

ANDROID

WhatsApp → ⋮ → **Privacy** → **Advanced** → **Strict account settings** → **Next** → **Turn on**

If you want to enable each setting manually instead of using Strict Account Settings, here are the steps

Remember to save your two-step verification PIN somewhere safe, like your password manager. If you lose it, you can be locked out of your account.

Enable disappearing messages by default on WhatsApp

Protects you and your contacts if anyone's phone is ever confiscated or breached.

Enabling disappearing messages by default keeps you and your contacts safer if a phone is ever confiscated or breached. We don't know whose phone will be seized by law enforcement. Even if you believe you're talking about perfectly legal things, the government can find ways to twist your words.

WhatsApp's options are 24 hours, 7 days, or 90 days. 7 days is a good default to choose, and then you can manually set a shorter timeframe for more sensitive conversations.

HOW TO ENABLE DISAPPEARING MESSAGES BY DEFAULT

IPHONE

WhatsApp → Tap **You** in the bottom bar → **Privacy** → **Default Message Timer** → pick your duration

ANDROID

WhatsApp → ⋮ → **Privacy** → **Default message timer** → pick your duration

The default timer only applies to **new chats you start**. If someone else starts a thread with you, the timer is not applied. To set it on an existing thread, open the chat > tap the name at the top > **Disappearing messages**.

Ongoing WhatsApp security practices

EVERYONE This section is for anyone doing activism or advocacy work.

Don't share anything on WhatsApp that you wouldn't also post on social media

WhatsApp is good for mobilizing large numbers of people, but not good for higher-risk planning

DO: Use WhatsApp for mass mobilizing (in a similar way that you'd use social media)

DO NOT: Plan ICE watch shifts, election defense, or direct actions on WhatsApp

Be aware that discussions around political or strategic topics may be monitored by far-right actors, especially in groups or channels used for mass communication/mobilization where you don't fully control who joins.

Avoid saying anything on WhatsApp that you wouldn't publish openly on social media.

If you're planning sensitive actions among trusted folks, use Signal.

Don't "chat" with Meta AI on WhatsApp

Anything you ask Meta AI about your organizing, contacts, or plans gets stored and could be exposed to law enforcement.

For activists, Meta AI is a data collection feature dressed up as a helpful assistant. Anything you ask it about your organizing, your contacts, your locations, or your plans gets stored, profiled, and potentially exposed to law enforcement.

Tagging @MetaAI in a group chat pulls the surrounding messages into Meta's systems, even if you only meant to ask a quick question. Once Meta AI is in the conversation, that history is no longer just between the people in the chat.

> You can't entirely disable Meta AI in WhatsApp. The best protection is to never use it, and to never tag **@MetaAI** in a group chat.

To keep Meta AI out of specific chats and groups, also turn on Restricted chat on those chats.

Never enter a pairing code or scan a QR code under "Linked devices"

Attackers trick you into pairing their browser to your account, giving them full access to your chats.

DO: Only scan a WhatsApp QR code when YOU yourself opened WhatsApp Web or Desktop

DO NOT: Enter a pairing code or scan a QR code because a website or person asked you to

What is "Linked Devices"? WhatsApp lets you use your account on other devices (a computer, a tablet, a second phone) by linking them through a QR code or pairing code. Most people never use this feature. See WhatsApp's official explainer if you want more background.

Attackers have figured out that they can trick you into linking *their* device to your account. If a website or stranger walks you through "verifying" by entering a code in WhatsApp, that's not verification. That's you giving them full access to your chats. The same trick works with QR codes.

So: **never enter a pairing code or scan a WhatsApp QR code because a website or person asked you to.** Only scan a WhatsApp QR code when **you yourself** just opened WhatsApp Web or Desktop.

You can audit your account at any time. See Check Linked Devices regularly.

Never send anyone your WhatsApp PIN or 6-digit verification code

Not even to someone claiming to be "WhatsApp Support". That's how account takeovers happen.

Your WhatsApp PIN and the 6-digit verification code WhatsApp texts you are the keys to your account. Anyone who gets them can take it over.

Never share these codes with anyone, for any reason. This applies even if the person says they're from "WhatsApp Support" or "WhatsApp Security". WhatsApp will never DM you, call you, or text you asking for your PIN or verification code. If someone asks, it's a phishing attempt.

There has been an increase in fake messages claiming to be from "WhatsApp Support" that try to hijack your account this way. If you're not sure whether a message is legit, don't reply, don't tap any links, and don't enter any codes. Instead, contact WhatsApp through the in-app **Help** section.

Enhanced WhatsApp protections

MEDIUM-THREAT

This section is for you if you are in a leadership role or you are doing activism that is more likely to be targeted by the state or your opposition.

Turn on Restricted chat for sensitive WhatsApp chats and groups

Blocks Meta AI, chat export, auto-saving media to the camera roll, and access from linked devices like WhatsApp Web in that chat.

Restricted chat is a per-chat setting. When it's on, nobody in that chat can:

- Export the chat
- Have photos and videos from the chat automatically saved to their camera roll
- Use Meta AI features in the chat
- Open the chat on a linked device, like WhatsApp Web, WhatsApp Desktop, or a tablet

A restricted chat won't show up on your computer. Once it's on, you and everyone else in the chat can only read and send messages in it from your main phone. The chat won't be available in WhatsApp Desktop, WhatsApp Web, or on a tablet, for anyone in the chat.

This is meant to keep AI agents and unofficial WhatsApp apps out of your chats. These tools connect to someone's WhatsApp account as a linked device. If anyone in your group has connected one, it can read every chat on their account, including your group's. Turning on Restricted chat blocks them from reading that chat. It also helps if an attacker tricks someone in the chat into linking the attacker's device to their account (see Check WhatsApp's Linked Devices list regularly).

You must turn it on for each sensitive chat. It can't be set automatically across all chats, and you can only change it from your main phone.

HOW TO TURN ON RESTRICTED CHAT

For a one-on-one chat (either person can turn it on):

IPHONE

Open the chat → tap the contact's name at the top → **Restricted chat** → toggle on

ANDROID

Open the chat → ⋮ → **View contact** → **Restricted chat** → toggle on

For a group (only group admins can turn it on):

Open the group → tap the group name at the top → **Restricted chat** → toggle on

If you're not an admin, ask an admin of the group to turn it on.

IF YOU ALREADY TURNED ON ADVANCED CHAT PRIVACY

Restricted chat replaces an older setting called Advanced Chat Privacy. Chats where you turned on Advanced Chat Privacy **won't switch to Restricted chat automatically**, and they can still be opened on linked devices until you upgrade them.

Open the chat → tap the chat name at the top → **Advanced chat privacy** → **Upgrade** → **Continue**

Restricted chat only fully works if everyone in the chat is on the latest version of WhatsApp. Someone on an older version may still be able to read the chat on a linked device, an unofficial app, or an AI agent, and WhatsApp won't tell you. Ask everyone in sensitive groups to keep WhatsApp updated. It also doesn't stop anyone from taking screenshots or forwarding individual messages.

Stop WhatsApp from auto-saving photos and videos to your camera roll

Keeps sensitive images out of iCloud or Google Photos backups where they can be subpoenaed.

Photos and videos you receive on WhatsApp can end up in more places than you think. By default, WhatsApp may save them straight to your camera roll, and iCloud or Google Photos will then back those up to the cloud automatically.

That means sensitive images (protest footage, photos of organizers, anything that could expose your community) and their metadata (such as the location and time the photo was taken) can sit in a Google or Apple account where law enforcement can subpoena them. Deleting every copy later becomes much harder.

HOW TO DISABLE AUTO-SAVE FOR ALL CHATS

IPHONE

WhatsApp → **Settings** → **Chats** → disable **Save to Camera Roll**

ANDROID

WhatsApp → **Settings** → **Chats** → disable **Media Visibility**

HOW TO DISABLE AUTO-SAVE FOR A SPECIFIC CHAT OR GROUP

IPHONE

Open the chat → tap the chat name at the top → **Save to Camera Roll** → choose **Default**, **Always**, or **Never**

ANDROID

Open the chat → tap the chat name at the top → **Media visibility** → choose **Default**, **Yes**, or **No**

Don't use your real name or photo on your WhatsApp profile

Helps protect you from cops or attackers who want to de-anonymize you. Especially useful if you are in unvetted WhatsApp groups.

A lot of community organizing happens in unvetted groups on WhatsApp where you don't know how much you can trust everyone in the group. These groups can be infiltrated by right-wing adversaries and law enforcement.

Using a fake name or just your first name prevents someone from finding your real identity through a Google search. Using a photo that isn't your face prevents someone from finding your social profiles based on image search or facial recognition. Both steps help defend you against doxxing and online harassment.

> It's very hard to be fully anonymous on WhatsApp because your phone number is visible to anyone you message and anyone you're in a group with. If a group has a bad actor, they can easily use your phone number to deanonymize you. Setting up a WhatsApp username hides your number from people who don't already have it.

HOW TO CHANGE YOUR PROFILE DISPLAY NAME

IPHONE

WhatsApp → Tap **You** in the bottom bar → Tap your name → Tap your name again → edit your name to be a fake name or just your first name → Tap **Save**

ANDROID

WhatsApp → ⋮ → **Settings** → Tap your name at the top → Tap your name again → edit your name to be a fake name or just your first name → Tap **Save**

HOW TO CHANGE YOUR PROFILE PHOTO

IPHONE

WhatsApp → Tap **You** in the bottom bar → Tap your profile picture → Tap **Edit** underneath the profile picture → Upload a generic photo that you found online that doesn't relate to your identity, preferences, interests, or location

ANDROID

WhatsApp → ⋮ → **Settings** → Tap your profile picture → Tap **Edit** underneath the profile picture → Upload a generic photo that you found online that doesn't relate to your identity, preferences, interests, or location

Remind people in your groups to do this as well. Security is a team sport.

Set up a WhatsApp username to hide your phone number

People who don't already have your number see your username instead. Useful in large or unvetted organizing groups.

WhatsApp now lets you pick a username. Once your username is active, people who don't already have your phone number saved see your username instead of your number. You can also give someone your username instead of your phone number when you want to connect with them.

This matters most in large or unvetted organizing groups, which can be infiltrated by bad actors. Your phone number is one of the easiest ways for someone to find out who you are.

WhatsApp is turning usernames on country by country. If usernames aren't active where you live yet, you can still reserve one now so it's ready when they are.

HOW TO SET UP A USERNAME

WhatsApp → **Settings** → **Account** → **Username** → pick a username

Pick a username that you don't use anywhere else and that doesn't include your real name. If you reuse a handle from Instagram, X, or another site, anyone can connect your WhatsApp account to that profile.

Optional: add a username key. **Username** → **Username key**. This is an extra code people need along with your username to message you for the first time, so strangers can't just guess your username and contact you. If you start getting unwanted messages, reset your key.

A username doesn't make you anonymous.

- You still need a phone number to use WhatsApp, and Meta can still hand it over to law enforcement.
- Anyone who already has your number saved, and anyone you've already chatted with by phone number, can still see it.
- Meta still knows who you talk to and which groups you're in.

Check that you're not sharing your live location in any WhatsApp chats

Live location sharing can be left running by accident. Audit it occasionally so you don't broadcast your movements to a chat.

WhatsApp lets you share your real-time location with a person or group for a set amount of time. It's easy to turn on and forget about, especially if you started sharing with someone hours ago.

For activists, an open live-location share is a direct map of your movements that anyone in the chat can see.

HOW TO REVIEW AND STOP LIVE LOCATION SHARING

IPHONE

WhatsApp → **Settings** → **Privacy** → **Live location** → review the list and tap **Stop sharing** on anything you no longer need

ANDROID

WhatsApp → ⋮ → **Settings** → **Privacy** → **Live location** → review the list and tap **Stop sharing** on anything you no longer need

Securely back up your WhatsApp chats (only if you absolutely need backups)

If you absolutely need backups, turn on WhatsApp's end-to-end encrypted backup so Google or Apple can't hand them over.

The safest option is to leave backups off entirely (see Disable WhatsApp chat backups). Only enable backups if you actually need them, for example if you're transferring devices or crossing a border and need to temporarily delete WhatsApp.

If you do need backups, turn on WhatsApp's built-in end-to-end encrypted backup. Without this, Google or Apple can be compelled to hand your entire chat history over to law enforcement.

HOW TO ENABLE ENCRYPTED BACKUPS

IPHONE

WhatsApp → Tap **You** in the bottom bar → **Chats** → **Chat Backup** → **End-to-end encrypted backup** → set a passkey or password

ANDROID

WhatsApp → ⋮ → **Chats** → **Chat Backup** → **End-to-end encrypted backup** → set a passkey or password

Save the password in a password manager. WhatsApp cannot recover it for you.

iPhone only: For extra protection on top of WhatsApp's encrypted backup, you can also turn on Apple's **Advanced Data Protection for iCloud**. This is a separate, iCloud-wide setting that end-to-end encrypts most of what's in your iCloud account.

For group organizers/admins

MEDIUM-THREAT This section is for you if you are in a leadership role or you are doing activism that is more likely to be targeted by the state or your opposition.

If you're running an organizing group, the settings on the group itself matter as much as your personal settings.

Lock down your WhatsApp organizing groups

Group privacy is only as strong as the least secure member.

If you're running an organizing group, the settings on the group itself matter as much as your personal settings.

Group chat privacy is only as strong as the least secure member. If one person is an infiltrator or has a compromised device, everything in the chat can be exposed. Support your group to follow norms together.

HOW TO LOCK DOWN YOUR GROUP SETTINGS

Recommended group setup:

- [ ] **Enable disappearing messages on the group from the start.** Pick the shortest timeframe the group can tolerate.
- [ ] **Turn on Restricted chat** on the group (only admins can do this). This disables chat export, prevents media from auto-downloading to everyone's camera roll, keeps Meta AI out of the chat, and keeps AI agents and unofficial apps out by blocking linked devices. Let members know the group will only work on their phones, not in WhatsApp Desktop or Web. If you turned on the older Advanced Chat Privacy setting before, upgrade it to Restricted chat, since it won't switch over automatically.
- [ ] **Make the group invite-only.** Open the group thread → tap the group name → **Group Permissions** → restrict who can edit info, add members, and send messages.
- [ ] **Agree on group norms up front:** no cloud backups, no discussion of high-risk actions on WhatsApp, don't add new people without approval. Make sure all new members agree to these norms, and remind existing members periodically.
- [ ] **Design a vetting practice that fits your needs and risk tolerance.** Larger groups are easier to infiltrate.

Use WhatsApp Communities to keep group members' phone numbers private

Communities hide members' phone numbers from each other, which helps when organizing in large or partially vetted groups.

WhatsApp has a newer feature called **Communities** that lets you create a parent group containing multiple subgroups.

The benefit for organizers is that Communities have a "phone number privacy" feature so that other members can't see each other's phone numbers.

> Phone number privacy in Communities has limits: group admins can still see your phone number, and so can anyone who already has it saved in their contact book.

If you're running a large organizing group on WhatsApp, consider migrating to a Community to reduce the risk of members being doxxed by other members or infiltrators.

Protections for higher-risk activists

HIGH-THREAT This section is for you are in a high-profile role or your activism involves high-risk work that could result in serious consequences or retaliation.

The checklist items in this section will help protect your data if your device is seized by law enforcement.

Enable Lockdown Mode (iPhone) or Advanced Protection (Google & Android)

Spyware is an advanced type of attack, exploiting sophisticated vulnerabilities on our devices. In response, Apple and Google have introduced an advanced security mode that offers enhanced protection against spyware.

On iPhones, it's called **Lockdown Mode** and on Android, it's called **Advanced Protection Program**. (You can also enable Advanced Protection Program on just your Google Account even if you don't have an Android phone.)

We have **no reports** of anyone getting infected with spyware who had Apple's Lockdown Mode enabled. Android's Advanced Protection is more recent and its effectiveness has yet to be tested.

Usability trade-offs: Both features come with some functionality sacrifices. See the full list of trade-offs. If you encounter issues that don't work for your needs, you can always disable the feature later.

HOW TO ENABLE LOCKDOWN MODE FOR IPHONES

IPHONE

Settings → **Privacy & Security** → **Lockdown Mode** → **Enable**

This feature is available for iOS version 16 and above.

HOW TO ENABLE ADVANCED PROTECTION ON ANDROID

ANDROID

Settings → **Security & Privacy** → under **Other Settings** tap **Advanced Protection**

Note: The location of this setting may vary between Android devices, so we recommend searching for 'Advanced Protection' in the Settings search bar.

This feature is available for Android 16 and above.

Keep your phone (and laptop) updated to the latest operating system version

Protects you from hackers, spyware, and the phone hacking tools the cops use.

DO: Install updates as soon as you're prompted

DO NOT: Keep pushing the "update later" button

Every time a new operating system update comes out, it is fixing security holes. Each update you haven't installed represents a longer list of ways the cops can hack into your device. Think of it as a big building with more and more doors left unlocked.

If your operating system is not up-to-date, many of the other recommendations in this guide will not protect your data.

Start with your phone. If you're doing something higher risk, make sure to update all your devices.

HOW TO RUN UPDATES

Because security updates are so important, **we designed a tool to walk you through the process**.

Check your phone and computer updates →

HOW TO RUN UPDATES MANUALLY

If you prefer to run updates manually, here is how to do it for each device:

Click to show the manual steps

Disable face/fingerprint unlock (biometric)

You have stronger legal standing with a passcode than with biometric unlock. Cops can try to force you to unlock with biometrics.

HOW TO DISABLE FACE/FINGERPRINT UNLOCK

IPHONE

Settings → **Face ID & Passcode** → Disable **Use Face ID for iPhone Unlock**

(You can leave the rest enabled.)

ANDROID

Settings → **Lock Screen** (or **Security**) → **Biometrics and Security** → **Disable both Face Recognition and Fingerprint Unlock** for unlocking your phone

Caveat: Face and fingerprint unlock let you use stronger passwords without typing them all the time. If you have to choose, it's better to have a longer passcode than to turn off face/fingerprint unlock. If you leave biometrics on, make sure you know how to quickly turn them off if you're heading into a high-risk situation (see tips below).

Fully powering off your phone is the best way to temporarily disable biometrics because it also encrypts your data. The next unlock will require your passcode.

iPhone locking tip: If you leave face/fingerprint unlock on, you can force your passcode to be used for the next unlock by **pressing the side button 5 times**.

iPhone camera tip: You can take photos without unlocking your phone by **swiping left** on your home screen. (In case you get arrested while filming.)

Android camera tip: On many Android phones, you can launch the camera without unlocking by **pressing the side/power button twice**.

Set your phone passcode to 8 to 10 random digits

It takes years for cops to crack an 8-digit random passcode. They can probably guess your current passcode in less than 5 minutes with automated tools.

DO: Use a random passcode generator to create an 8 to 10-digit code

DO NOT: Use any passcode you thought of yourself (dates, patterns on the keyboard, etc.). Do not use 6-digit passcodes if possible.

HOW TO CHANGE YOUR PASSCODE

1. Generate a random 8 to 10-digit passcode using this random passcode generator. (Don't make one up yourself—humans are bad at choosing randomly!)
2. Change your passcode:

   IPHONE

   Settings → **Face ID & Passcode** → **Change Passcode** → **Passcode Options** → **Custom Numeric Code**

   ANDROID

   Settings → **Security** → **Screen Lock** → Enter Current Lock → **PIN/Password** → Enter a Passcode
3. **Practice the new passcode** at least 10 times in a row right now so you are more likely to remember it. (Disabling biometrics will force a passcode request every time you lock the phone.)
4. Write your new passcode on paper and keep it somewhere safe at home until you've memorized it. Then destroy it after 2–3 weeks. Setting a reminder on your phone can help.

How long does it take to crack a passcode?

TYPE	TIME IT TAKES TO CRACK (AVERAGE)	EXAMPLE
6-digit *easy-to-guess* pattern	**Less than 24 hours** to crack	*333666 (common pattern)* or *110585 (date pattern for Nov 5, 1982)*
6-digit *random* code	**200 days** to crack	*238253*
8-digit *random* code	**40+ years** to crack	*34780026*

Note: These times only apply to phones. Computers can be cracked much more quickly, and need much stronger passwords.

Sources: The estimates in the table above assume real-world observed attempts/second from police forensic hacking tools. If you need more security, use a 10-digit passcode, which will protect you even under the highest-possible cracking scenarios. See the sources linked in the passcode FAQ here.

☐ Only give WhatsApp access to specific photos from your photo library

Prevents WhatsApp from being able to see every image in your library, in case the company ever changes how that data is used.

Meta recently rolled out a feature in the Facebook app where all images in your photo library are sent to their servers and processed. This is a significant violation of privacy and could present legal risk to activists.

Meta (the parent company that also owns WhatsApp) has claimed that this kind of feature doesn't exist for WhatsApp. Even so, it's worth disabling broad photo access for WhatsApp, since the company rolled out the exact feature on Facebook.

HOW TO GIVE WHATSAPP LIMITED ACCESS TO YOUR PHOTO LIBRARY

Limited access adds one or two steps when you want to share a new photo, but it's simple.

IPHONE

Settings app → **Apps** → **WhatsApp** → **Photos** → select **Limited Access**

ANDROID

Settings app → **Apps** → **WhatsApp** → **Permissions** → **Photos and videos** → select **Select photos and videos every time** (or **Ask every time**, depending on your device)

Hide WhatsApp notification content on the lock screen

Stops message previews and sender names from showing up if your phone is seized.

If your phone is confiscated, your notification history can reveal message content and sender names, even after the messages themselves have disappeared. See the Prairieland case for why this matters.

Apple has fixed the issue that lead to incoming Signal notifications being stored even after messages were disabled in iOS/iPadOS 26.4.2 (and the older 18.7.8 maintenance branch). Even though they fixed that issue, it's unclear whether Android phones still present the same weakness, so it's worth hiding previews on either platform.

HOW TO HIDE WHATSAPP NOTIFICATION CONTENT

IPHONE

Settings app → **Notifications** → **WhatsApp** → set **Show Previews** to **Never**

ANDROID

Settings app → **Apps** → **WhatsApp** → **Notifications** → turn off **Show notification content on lock screen**

Disable AI notification summaries for WhatsApp

Apple Intelligence and Android notification summaries can send parts of your notifications to cloud servers.

Apple Intelligence and Android's notification summaries can send parts of your notifications to cloud servers. It's not fully clear what gets sent where, and the data could be compelled by a government request.

We have an article about this topic as it relates to Signal. The same reasoning applies to WhatsApp: Is Apple Intelligence reading my Signal messages?

HOW TO DISABLE AI NOTIFICATION SUMMARIES FOR WHATSAPP

IPHONE

Settings app → **Notifications** → **Summarize Notifications** → toggle off **WhatsApp**

ANDROID

Settings app → **Notifications** → **Notification summaries** → add **WhatsApp** to the excluded list

Check WhatsApp's Linked Devices list regularly

You can protect your account from being hijacked by occasionally reviewing your linked devices.

WhatsApp's multi-device feature is a major pathway for an attacker to takeover your account. Attackers trick you into scanning a QR code or entering a pairing code, and their computer can start seeing all the messages you send and receive.

The same multi-device infrastructure has also been used by mercenary spyware to target journalists and organizers. See our spyware page for more.

HOW TO CHECK YOUR LINKED DEVICES

IPHONE

WhatsApp → Tap **You** in the bottom bar → **Linked Devices**

ANDROID

WhatsApp → ⋮ → **Linked Devices**

Log out anything you don't recognize. If you don't use WhatsApp Web or Desktop, log out of everything.

For your most sensitive chats and groups, turning on Restricted chat keeps those chats off linked devices entirely, so a hijacked linked device can't read them.

Other resources

- How to use WhatsApp guide — Electronic Frontier Foundation
- Upgrading WhatsApp security — Freedom of the Press Foundation

Frequently asked questions

What is this 'verify encryption key' option I see under each chat?

What about the 2026 lawsuits claiming WhatsApp created a 'backdoor' to bypass end-to-end encryption?

Is WhatsApp safer than regular text messages (SMS)?

Can law enforcement read my WhatsApp messages?

Do WhatsApp usernames hide my phone number from law enforcement?

When should I use Signal instead of WhatsApp?

Keep learning with these related guides

Signal security
Secure your Signal messaging app for safer communications.

Security essentials
Core security practices every activist should follow.

Spyware protection
Protect yourself from spyware and surveillance software.

Doxxing defense
Protect yourself from doxxing and online harassment.

VPNs for activists 14 min read · Security update checker · How to use Proton safely 15 min read

Remove link tracking 3 min read · Is Signal secure? 4 min read

Is Apple Intelligence reading my Signal messages? 5 min read