The WhatsApp Spam Dojo

A Comprehensive Guide for Admins

Change the Locks, Keep the Welcome Mat

If scam posts are flooding the group

Remove and report the offending accounts → Save relevant evidence → Delete offending posts → Audit "Group permissions" → Reset the join link → Share the replacement selectively → Update the validated blocklist → Review pending join requests.

> If messages are arriving faster than admins can remove them, temporarily set **Send messages** → **Only admins**. Restore **All members** when the disruption has passed.

The goal is to keep people talking and protect their ability to find recovery, while making repeat scam entry harder.

Why removal alone doesn't work

Removing a scam account from a WhatsApp group doesn't prevent it from returning. If the person still has a working join link, that route remains available. WhatsApp has no built-in, persistent group- or community-wide blocklist that automatically rejects previously removed numbers.

The practical defense is **controlled admission, precautionary link resets, and a shared record of verified scam activity**. These measures complement one another: the link reset closes an old route, approval checks new requests, and the blocklist helps admins recognize repeat accounts.

1. Lock down entry, not conversation

Go to **Group info → Group permissions** (labels vary by app version) and configure:

Control	Recommended setting	What
Add new members / Add other members	**Only admins**	Prevents ordinary members from directly adding people; WhatsApp also documents this setting as controlling who can create invitation links on some interfaces.
Invite via link / Invite via link or QR code (if shown)	**Only admins** (if shown)	Prevents members from creating or retrieving an invitation link through the group interface. If this permission does not appear, it is governed by the "Add new/other members" setting.
Require admin approval / Approve new members	**On**	Requires an admin to approve requests to join through an invitation link.
Edit group settings	**Only admins**	Prevents unauthorized changes to group information.
Send messages	**All members**	Keeps ordinary fellowship discussion open.

These controls cannot stop someone from forwarding an invitation link they already possess. Link resets and admin approval provide separate protections against that route of entry.

If you administer a WhatsApp Community

In **Community info → Community Settings**, set both available permissions:

Community permission	Recommended setting
Who can add new members	**Only admins**
Who can add new groups	**Only admins**

These are **community-level controls**, separate from the group permissions above. Configure both levels when a group belongs to a community.

For Communities: Have a **Community admin** remove an offending account **from the Community**, not just the group. This removes the account from **all groups in that Community**.

2. Reset join links when scams occur

If you see scam posts or receive credible reports of scam accounts that need to be removed, reset the affected group's join link as a precaution. You don't need to establish that the current link was how they entered.

In **Group info** → **Share** (labeled **Invite via link** on some versions), choose **Reset link**. Menu labels may vary by device. The old link stops working; people who have already joined aren't removed. If a **community** invitation link may also be providing access, reset that link too.

Replace the old link in meeting materials and other legitimate access points. Ask members **not to post join links in public group chats**. Sharing them in meetings, friend group chats, and direct messages is fine. Keep a straightforward way for newcomers to obtain the current link without making it publicly harvestable.

3. Maintain a shared, validated blocklist

Use a shared document that **authorized people can read and update**. People who review join requests need access to consult it. Designate **trusted points of contact** who can reliably receive reports, evaluate evidence, and add or correct entries. No particular document provider is required.

Validate before including a number on the blocklist. A request for financial assistance does not, by itself, establish a scam. But the circumstances surrounding a request, including evidence of deception, manipulation, or high pressure tactics, can be compelling. **One well-documented incident may be sufficient.** Judge the available conduct and evidence, not someone's character, presumed motives, or recovery status. Don't require proof of fraudulent intent when the conduct provides sufficient grounds for action.

Record-keeping recommendations:

- Record the **phone number in international format**, with its country code (for example, +1-888-555-5555); consider including the **date** and the **observed conduct**, and possibly a reference to the supporting evidence.
- **Group by country code in numerical order; sort numbers numerically within each country-code group.** Keep new entries in order as the document grows.
  - Keep incident notes factual. Share screenshots or other details only with people who need them, and do not include unrelated members' personal information.
- Treat the list as **correctable**: reports can be mistaken and phone numbers can be reassigned. Review or remove entries when warranted.
- Revisit read/write permissions when service responsibilities change.
- Don't publish the list.

Keep unverified concerns separate from validated blocklist entries. An unverified report may still warrant prompt, proportionate precautions, such as declining or delaying a join request while checking details. Protecting the group needn't wait for a committee decision or certainty about someone's motives.

3. Maintain a shared, validated blocklist (continued)

When reviewing a join request, consult the blocklist and any available evidence. A listed number may justify refusing entry, but consider the possibility of an error or reassigned number. Neither an unfamiliar number nor a financial request is proof of bad faith or not being a recovering addict. Avoid demanding unnecessary personal disclosures as a condition of ordinary access.

4. Coordinate incidents among trusted servants

Create a **private coordination chat** where admins and other relevant trusted servants can post reports, phone numbers, screenshots, timestamps, and actions taken. This gives blocklist maintainers evidence to work from.

Keep the conversation factual and the audience limited to people with a legitimate reason for access. **The chat is for coordination, not mandatory preapproval**: admins act promptly within their responsibilities and report back afterward.

Coordinating protective actions

Establish shared expectations for reviewing join requests, removing suspicious accounts, resetting invitation links, and maintaining the blocklist. These can evolve with experience and don't need to anticipate every situation.

Use your judgment when circumstances aren't covered. Sometimes prompt action is appropriate; sometimes consulting other trusted servants first makes sense. **You don't need perfect certainty to act responsibly.**

Use the coordination chat to share relevant evidence, document actions taken, discuss uncertainties, and learn from experience. Review and correct decisions when warranted.

5. Optional privacy safeguards

These controls reduce the amount of past conversation a newly admitted bad actor can quickly collect or feed into outside analysis. They do **not** make a WhatsApp group confidential to everyone already admitted.

Control	Recommended setting	What it accomplishes
Advanced Chat Privacy or Restricted Chat	**On**	Restricts WhatsApp's built-in chat export, automatic saving of media, and in-chat Meta AI features.
Send message history	**Only admins** (or disable member sharing, if shown as a toggle)	Prevents ordinary members from passing earlier group messages to newcomers.

5. Optional privacy safeguards (continued)

Recent-history sharing can provide a newcomer with earlier messages, and WhatsApp also permits history to be sent **after** someone joins. Admins retain the ability to send history and should use it thoughtfully. Advanced Chat Privacy and Restricted Chat do not stop screenshots, manual copying, photography of a screen, or all possibility of analysis outside WhatsApp. Neither setting hides messages posted after admission.

Members' phone numbers and messages may also be visible to others in the group. Admission checks and reduced history sharing lower exposure; they cannot guarantee privacy.

WhatsApp documentation

- Group permissions and admin settings
- Inviting people and resetting a group link
- Community invitation links
- Advanced Chat Privacy and Restricted Chat
- Adding or removing group members
- Group Message History

FTC resources: recognizing scam patterns

- Crypto investment scammers are targeting your community groups
- Did a new online friend ask for money? Odds are it’s a scam

November 2026. WhatsApp menu names and available settings may differ by device and app version.