



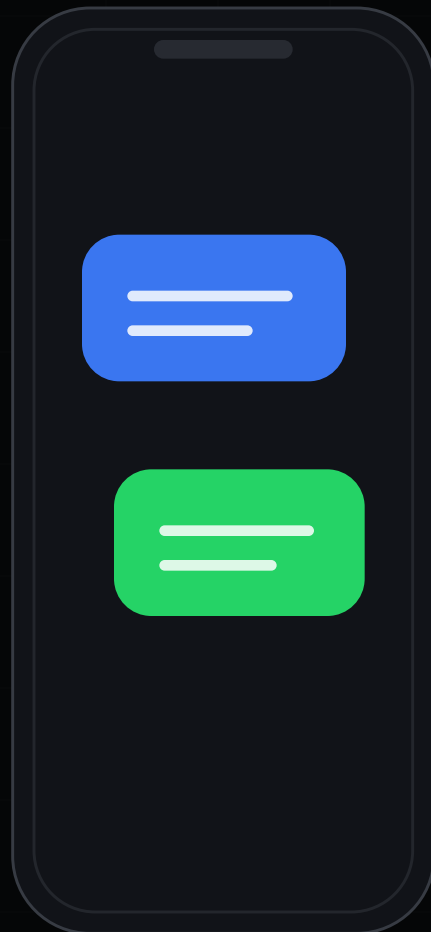
2026 FIELD GUIDE

RED.ONE SECURE COMMUNICATIONS

MESSAGING PRIVACY & SECURITY

SIGNAL + WHATSAPP

A practical guide to stronger account protection, visibility controls, call privacy, message retention, and device-level access.



COMBINED GUIDE

Two apps. One disciplined posture.

Signal and WhatsApp both protect message content with end-to-end encryption. The practical privacy posture, however, also depends on account security, visibility, call routing, backups, app locks, and retention settings.

01

SIGNAL

CONFIGURATION FOCUS

- Signal PIN and Registration Lock
- Phone number privacy
- Read receipts and disappearing messages
- App lock and switcher privacy
- Call relaying and sealed sender controls

02

WHATSAPP

CONFIGURATION FOCUS

- Privacy Checkup and visibility
- App Lock and Chat Lock
- Call IP and link-preview protection
- Media and encrypted backups
- Two-step verification and passkeys

Review both configurations periodically, especially after app updates or changes in operational needs.

01

Signal

ENHANCED SECURITY AND PRIVACY SETTINGS

Why these settings matter

Signal is widely regarded as one of the most secure messaging apps available today, offering end-to-end encryption, minimal data retention, and strong privacy protections.

To get the maximum benefit, users should take a few minutes to configure the app's privacy and security settings. This section walks through each key area and explains how to optimize it.

01

Signal PIN and Account Security

Signal uses a private PIN to protect profile data, settings, and identity information. This PIN is never shared and cannot be recovered by Signal, so choosing one that is memorable yet strong is essential.

KEY RECOMMENDATIONS

- Enable Signal PIN and use a 6 digit PIN.
- Turn on Registration Lock to prevent someone else from registering your number on another device without the PIN.

WHY IT MATTERS

These features ensure that even if someone gains access to your phone number, they cannot take over your Signal account.

02

Phone Number Privacy

Signal allows you to choose who can view your phone number and who can find you by searching for your number, an important control for limiting contact from unknown individuals.

RECOMMENDED SETTINGS

- Set "Who Can See My Number" to Nobody.
- Set "Who Can Find Me By Number" to Everybody only if you rely on coworkers or clients finding you. Otherwise, choose Nobody for maximum privacy.

WHY IT MATTERS

This approach ensures your number will not be exposed to users who do not already have it saved.

03

General Privacy Settings

Signal includes a variety of privacy-related toggles that allow you to control read receipts, typing indicators, and message disappearance timers.

WHAT TO CONFIGURE

- Disable Read Receipts and Typing Indicators if you prefer not to share usage behavior.
- Set a default disappearing message timer. Four weeks is common, but consider shorter intervals for sensitive conversations.
- Review your blocked contacts list periodically.

WHY IT MATTERS

These settings reduce digital traces and prevent others from monitoring when or how you use the app.

04

App Security Features

Beyond messaging privacy, Signal includes app-level security options such as Face ID or biometric lock and hiding the app screen in the app switcher.

RECOMMENDED CONFIGURATION

- Enable "Hide Screen in App Switcher" to prevent message previews from appearing in multitasking view.
- Use screen lock if your device does not have a feature to require biometric protection to open the app, like an iPhone.
- Turn on Payments Lock if you use Signal Payments.

WHY IT MATTERS

These features prevent unauthorized access to your conversations if someone temporarily handles your device.

05

Advanced Protections

Signal's advanced settings offer additional layers of protection, especially for users who prioritize anonymity.

KEY OPTIONS

- Enable "Always Relay Calls" to hide your IP address from call recipients.
- Enable the "Sealed Sender" status icon to verify that messages use Signal's most private delivery method.
- Leave "Allow from Anyone" off unless you want to accept sealed-sender messages from people who are not already connected to you.
- Proxy settings can be used in regions where Signal is blocked, though they are not needed in most cases.

WHY IT MATTERS

These advanced options help shield metadata and reduce exposure during calls and message delivery.

● Configuration takeaway

Configuring Signal properly ensures that you benefit from its strongest privacy protections. The app provides granular control over your visibility, data retention, and communication security, controls that most messaging platforms do not offer. By following the recommendations above, you can tailor Signal to match your personal privacy needs.

02

WhatsApp

PRIVACY AND SECURITY: A PRACTICAL GUIDE

Why these settings matter

If privacy matters to you, be intentional about how WhatsApp handles your messages, calls, and profile metadata. This section explains each setting in plain language and provides a clear implementation sequence.

WhatsApp includes strong protections by default, such as end-to-end encryption for message content, but privacy is more than encryption. Newer features provide control over what others can see, how calls expose information, how backups are handled, and how well your account is defended.

01

Privacy Checkup: Your Starting Point

Open the "Privacy Checkup" tool in Settings to review your current configuration. It walks you through the key privacy pillars: contact access, visibility, conversations, and account protection.

02

Visibility Controls: Defining Your Public Footprint

In the Privacy menu, decide who can see your profile photo, "About" status, last seen or online presence, and group assignments. Restrict these to "My Contacts" or "Nobody" if you want to minimize exposure.

03

Access Controls: App Lock and Chat Lock

App Lock places a biometric or passcode barrier at WhatsApp launch. Chat Lock goes further by hiding chosen conversations behind a second barrier and masking their notifications, ideal for highly sensitive content.

04

Call and Link Privacy Enhancements

In the Advanced settings, you will find two important toggles:

- Protect IP Address in Calls: Routes calls through WhatsApp servers to prevent IP leaks.
- Disable Link Previews: Stops WhatsApp from fetching link metadata that could expose your IP or browsing patterns.

WHY IT MATTERS

Consider enabling "Block unknown account messages" if unsolicited messages are a concern.

05

Media, Chats, and Backups

In Chats settings, keep "Save to Photos" off if you do not want media saved automatically to your camera roll. In Chat Backup, activate end-to-end encryption so backups stored in the cloud are also protected.

Review settings like voice message transcription and private processing, which let you control how much processing is done on your device.

06

Reinforcing Your Account

In Account settings, enable two-step verification, adding a PIN required to re-register your number. Activate security notifications to be alerted when keys change. If your phone supports it, use passkeys for stronger authentication.

If you change phone numbers, migrate your account securely using the built-in option.

07

Step-by-Step Guide: Locking Down WhatsApp

- 1 Open Privacy Checkup and review all categories.
- 2 In Privacy > Visibility, restrict "Last Seen," profile photo, "About," and group settings to tighter audiences.
- 3 Enable App Lock and apply Chat Lock to your most sensitive chats.
- 4 In Privacy > Advanced, activate Protect IP Address in Calls and Disable Link Previews. Optionally enable blocking for unknown message senders.
- 5 In Chats, disable automatic media saving, and in Chat Backup enable end-to-end encrypted backups. Adjust transcription and processing preferences.
- 6 In Account, turn on two-step verification, security notifications, and passkeys if available. Confirm your recovery email.
- 7 Periodically revisit these settings, especially after updates or new feature releases.

● Configuration takeaway

WhatsApp now offers a sophisticated toolkit for privacy-conscious users. With thoughtful setup, you can preserve the ease and reliability of the app while minimizing what you expose, intentionally and unintentionally. Use this guide as your template, adapt it to your needs, and treat your configuration as evolving, not fixed.