Signal Security Checklist

ACTIVIST CHECKLIST

Last updated on **April 3, 2026** Takes about **15 minutes**

This copy was made on November 6, 2026. We update our guides often as threats change and as better ways to protect yourself become available. For the latest version, visit **activistchecklist.org/signal/**

Signal is currently the most secure mainstream messenger, but only if you configure it. This checklist covers the changes that protect your messages and your organizing network if your phone is seized at a protest or your group is infiltrated. Includes deeper settings for organizers and frequent ICE observers.

This guide helps you take control of your private conversations on Signal[1]. While Signal already encrypts everything you send, these extra steps ensure your chats stay private, even if your phone is lost, taken, or compromised. You'll learn simple ways to protect your messages, notifications, and identity.

Brand new to Signal? Check out this beginner's guide to using Signal[2].

Tip: Signal setup works well as a group session with friends[3]. Most items take 5 to 10 minutes once you sit down and do them.

Hide your identity on Signal

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

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

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

A lot of community organizing happens in unvetted groups on Signal where you don't know how much you can trust everyone in the group. These groups can be infiltrated by right-wing adversaries[4] and law enforcement[5].

Using a fake 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 an image match or facial recognition.

Both steps help defend you against doxxing[6] and online harassment.

HOW TO CHANGE YOUR PROFILE

1. **Change your profile display name:** Open Signal → Tap your profile picture → **Settings** → Tap on your name/icon near the top → Click the top item with the silhouette of a person → Edit your profile display name
2. **Change your profile photo:** Open Signal → Tap your profile picture → **Settings** → Tap on your name/icon near the top → **Edit photo** → upload a generic photo that you found online that doesn't relate to your identity/preferences/interests/location.

The same principle applies even more strongly to social media. If your Instagram, Facebook, or LinkedIn profile pairs your full real name with a clear photo of your face, attackers can easily identify you even if the rest of your profile is private. See Lock down social media for more.

Remind people in your groups to do these things too. Security is a team sport.

Enable username and hide phone number

If you want to have the option to be anonymous on Signal, protecting your phone number helps protect your identity.

If you installed Signal before March 2024 when they introduced usernames[7], your phone number may still be set to be visible to others.

HOW TO ENABLE USERNAMES AND HIDE YOUR PHONE NUMBER

1. Make sure you first change your profile display name (see the above item). If your Signal profile display name is your full name, then hiding your phone number will only be slightly helpful.
2. **If you want to change your username:** Open Signal → Tap your profile picture → **Settings** → Tap on your name/icon near the top → Tap the **@** symbol → **Edit username** → set the username to something **completely unrelated** to your identity, or any usernames you've used anywhere before. It must end in at least 2 numbers.
3. **Hide your phone number:** Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Phone Number** → Under **Who Can See My Number** → Select **Nobody**.
    1. Optionally, you can change "Who Can Find Me By Number." But this will mean that none of your existing contacts will know that you're on Signal already unless you message them first. Only change this to "Nobody" if you need very high levels of privacy.
4. **Share your username instead of your phone number:** If you're connecting with someone new for political purposes, share your username. Open Signal → Tap your profile picture → **Settings** → Tap on your name/icon near the top → **QR Code or Link** → share either the QR code or the link with someone you want to be in contact with. Or more simply, just tell them your username.

Disable link previews

Can protect you against your approximate location being revealed

This protects you from certain attacks. But make sure you always take a close look at the URL that you're being sent to see if it's from a site you feel comfortable opening.

HOW TO DISABLE LINK PREVIEWS

Open Signal → Tap your profile picture → **Settings** → **Chats** → **Disable Generate Link Previews**

Technical Background: An attack was published[8] in 2025 that allows an attacker to estimate your location within about 250 miles.

Enable "Always Relay Calls"

By default, Signal calls connect directly between you and the other person. This means the other person's device can see your IP address. With a court order to your internet provider, your IP address can be used to identify you specifically.

Enabling "Always Relay Calls" routes your calls through Signal's servers, hiding your IP address from the other party. (If you already use a VPN[9], your IP address is already masked.)

HOW TO ENABLE ALWAYS RELAY CALLS

Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Advanced** → Toggle on **Always Relay Calls**

Protect your messages & calls

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

- [ ] Important **Change your default settings so all new Signal threads have disappearing messages enabled**

  This keeps everyone safer if someone's phone is ever confiscated or breached.

The best upgrade everyone can make to their use of Signal is to make sure that disappearing messages[10] are enabled ***by default***. Most activists we talk to haven't enabled this by default. (And most people forget to enable it manually for each new thread.)

This keeps you safe and other people safe. We don't know who's phone will be seized by law enforcement. Even if we believe we're talking about perfectly legal things, the government can find ways to twist our words to attempt to make a case against us for our dissent

There are two things to track related to disappearing messages:

1. **First, change your default** so any thread you make has this feature enabled.
2. **Second, make sure it is enabled for threads that other people start:** if someone else starts the thread, it may not have disappearing messages enabled. You may need to enable it.

HOW TO ENABLE DISAPPEARING MESSAGES

1. **To change the default:** Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Disappearing Messages** → set to your desired time (longer or shorter depending on your risk tolerance).
2. **(Android-only) Change your message retention limit:** This will delete messages on threads even that don't have disappearing messages turned on. (They will only be deleted on your device.) Open Signal → Tap your profile picture → **Settings** → **Data and storage** → **Manage storage** → **Keep Messages** → set to your desired max timeframe. Go back a screen and enable **Apply limits to linked devices**.
3. **To change existing threads:** Signal → Open the message thread you want to change → Click on the person's name (or group name) at the top of the screen → **Disappearing Messages** → set to your desired time.
4. **Delete old messages/threads:** Disappearing messages does NOT apply retroactively. So you may want to delete old threads on your phone. This will not delete them on other people's phones, unfortunately. So if it is very sensitive, you may need to ask them to also manually delete the thread. (And while you're at it, encourage them to turn on disappearing messages by default!)

Choosing your disappearing message time: How long you set your disappearing times depends on the sensitivity of your messages. A question you might ask yourself is "if someone's device was confiscated or hacked, how important is it that these messages are not accessible?"

- For chatting about low-risk things with friends, you might choose 4 weeks.
- For standard political organizing, you might choose 1 week.
- For a higer-risk actions, you might set it to 1 day or 1 hour or 5 minutes, so the messages are gone before the action starts.

Note: Messages only disappear after the message has been read. So if the recipient doesn't read it for 2 weeks, and you have disappearing messages set to 4 weeks, it will actually disappear 6 weeks after you sent it.

Hide message preview and sender name for Signal notifications

If your phone is confiscated, the cops can get access to your noficiation history.

If your phone is confiscated, there are two ways the cops can get access to your notification history:

1. They can see the notifications on your home screen without unlocking your phone.
2. If they use hacking tools, they can get access to the log of notifications your phone has received. (Example from the Prairieland case[11].)

This only applies to incoming messages. And this is a risk even after the message has disappeared from Signal (if you have disappearing messages enabled).

HOW TO DISABLE SIGNAL NOTIFICATIONS

IPHONE

Open Signal → Tap your profile picture → Settings → Notifications → Notification Content → **Select "No Name or Content"**

ANDROID

Open Signal → Tap your profile picture to open Settings → Notifications → Show → **Select "No name or message"**

If you disable Signal notifications at the phone operating system level, you won't be notified about incoming Signal calls.

If you use Signal Desktop, make sure to disable notifications there as well.

FYI: If you want to clear the notification log that iOS has already stored, the only way to do that is to factory reset your phone and restore it as a new device — not from a backup, as backups include the notification history.

Enable "Screen Lock" and "Hide in App Switcher"

If you hand your phone to someone, Screen Lock is an extra layer of security.

- **Screen Lock:** If you hand your phone to someone while unlocked, this ensures they must provide the face/fingerprint/PIN unlock again before opening Signal.
- **Hide in App Switcher:** This will hide your messages when switching between apps.

HOW TO HIDE SCREEN IN APP SWITCHER

IPHONE

Open Signal → Tap your profile picture → **Settings** → **Privacy** → Enable **Screen Lock** then enable **Hide Screen in App Switcher**

ANDROID

Open Signal → Tap your profile picture to open **Settings** → **Privacy** → Enable **Screen lock** then enable **Screen Security**

Disable "Show Calls in Recents" (iPhone-only)

This prevents the cops from seeing your Signal call history if they confiscate your phone.

HOW TO DISABLE "SHOW CALLS IN RECENTS"

This setting only exists on iPhones: Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Calling** → Disable **Show Calls in Recents**

Leave Signal groups that might put others at risk

This helps protect your network if your phone is confiscated.

If your phone is confiscated by law enforcement, one of the biggest risks is exposing your entire network. Even if people aren't using their real name on their Signal account, there is still a unique ID behind every Signal username. And the cops can use this to correlate someone's identity across many seized devices.

You need to both leave AND delete the group:

- If you only leave the group, old messages stay on your phone as well as the history of who was in the group.
- If you only delete the group, new messages will still come through and the thread re-appears.

HOW TO LEAVE AND DELETE A SIGNAL GROUP

1. **Make a plan to re-join afterwards:** When headed into a situation with possible arrest, make a list on paper at home or somewhere safe of all the groups and who you need to message who can re-add you after the action or border-crossing is complete.
2. **To leave the group:** Signal → [Group] → Tap the group icon at the top → **Leave group**
   - If you're the only admin, you have to either remove all members or assign another admin.
3. **To delete the group from your phone:** Signal → Main screen → Swipe left on the thread → **Delete**
   - This won't delete it for anyone else.

Security hygiene tips:

- Set a recurring reminder to clean up your Signal thread every 3 months.
- Make sure you take note of which groups you are leaving and who you can ask to re-add you after the action.

Note: If you find this process very annoying and cumbersome (because it is!), that's another good reason to use a secondary phone[12] for actions. That phone would only ever be in the one or two groups needed to pull off the action that day.

Enable Signal PIN and Registration lock

Protects you from advanced attacks where someone "steals" your phone number and registers it on Signal

If a highly-motivated attacker is able to find out your phone number, they can attempt to take it over through something called "SIM Swapping" or by calling your service provider and initiating a phone number "port" to a new provider. They could then use your phone number to register a Signal account and start receiving messages meant for you.

These are advanced attacks that don't happen to most folks. Still, it is easy to protect your Signal account.

You can protect yourself by enabling **registration lock** on Signal. It prevents someone from hijacking your account even if they steal your phone number. No one will be able to register a new Signal account on your number until your account has been inactive for 7 days.

If you forget your PIN, you will have to wait 7 days before you can create a new account (and your contacts will not be recovered). More on PINs & registration lock[13].

HOW TO ENABLE SIGNAL PIN AND REGISTRATION LOCK

Enable registration lock: Open Signal → Tap your profile picture → **Settings** → **Account** → Enable **Registration Lock**

Upgrade your PIN: You had to set a Signal PIN during setup. If you don't remember it or want to use a stronger PIN, here's how you can do that:

1. **Generate a strong PIN:** For maximum security, use a PIN that is 8 or 10 digits and make sure it is computer-generated. Here's a random PIN generator[14] you can use.
2. **Set a Signal PIN:** Open Signal → Tap your profile picture → **Settings** → **Account** → **Create/Change PIN** (If you don't already know what your PIN is).
3. **Save your PIN or enable PIN reminders:** If you have a password manager[15] you use reliably, save your PIN there. If you think you might forget where you saved your PIN, leave "PIN reminders" enabled.

☐ Enable a private keyboard for Signal (Android-only)

On Android, the default keyboard can log what you type.

HOW TO MAKE SURE YOU HAVE A PRIVATE KEYBOARD ON ANDROID

Note: This is for Android phones only. iPhones keyboards are already private unless you installed a custom keyboard.

OPTION 1 (easier) - Enable an incognito keyboard
Open Signal → Tap your profile picture → **Settings** → **Privacy** → **App security** → Enable **Incognito keyboard**

OPTION 2 (more private) - Replace the built-in keyboard system-wide

- The option above simply "asks" the keyboard provider (Google) to not log your keystrokes. There is no guarantee it is abiding. The more secure move is to install a custom keyboard.
- FlorisBoard[16] is one good option. You must install F-Droid[17] first, which is a more-private app store.

☐ Disable AI notification summaries

Google and Apple haven't made it clear when their AI tools are sending our private information (like Signal messages) off of our device onto their services. If they are sent to their servers, they are at risk of being accessed via a government court order.

Our understanding is that these AI features ***currently*** only summarize notifications. But with the way things are going, they might try to be more invasive.

Read our article on Is Apple Intelligence reading my Signal messages?[18]

OPTION A: HOW TO DISABLE AI NOTIFICATIONS SUMMARIES JUST FOR SIGNAL

Option A: Disable AI notifications summaries just for Signal

IPHONE

Open the **Settings** app → **Notifications** → **Summarize Notifications** → Toggle off **Signal**

ANDROID

Settings → **Notifications** → **Notification summaries** → **Manage apps** (under **Don't include these apps**) → Toggle off **Signal**

HOW TO ENTIRELY DISABLE AI NOTIFICATION SUMMARIES

Option B: Entirely Disable AI notification summaries

IPHONE

Open the **Settings** app → **Apple Intelligence & Siri** → Toggle off **Apple Intelligence**

ANDROID

Open **Settings** → **Notifications** → Toggle off **Use notification summaries** (or **Notification summaries**)

MAC

> **System Settings** → **Apple Intelligence & Siri** → Toggle off **Apple Intelligence** → **Confirm**

(Mac requires an Apple computer with an M1 processor or newer.)

Be alert for fake messages from "Signal Support" trying to get your Signal PIN or verification code

Protect your account by being attentive not to turn over your verification code or PIN

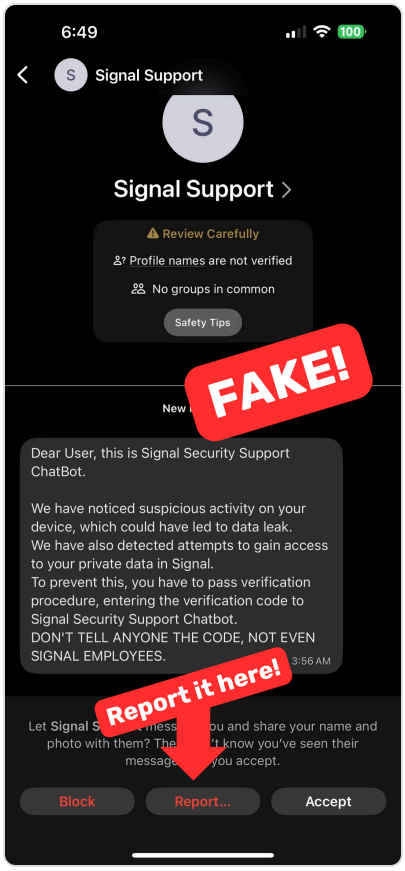
There have been an increasing number of fake messages from "Signal Support"[19] that are attempting to hijack your account.

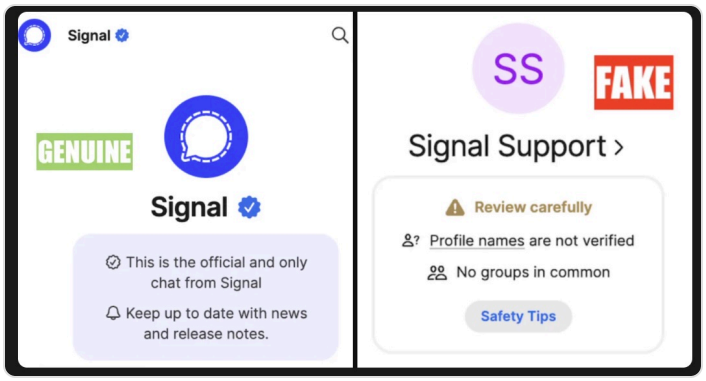
Use these examples below to keep an eye out for fake signal messages.

Remember: Signal will never ask you to send them your PIN or verification code. It will only be asked of you when you are installing the app for the first time on a device.

Read more about Signal scams/phishing.[20]

Here are some examples of scam messages:





Secure your phone

Signal is only as secure as the phone it's on. If your device is confiscated or hacked, police have forensic tools that can crack weak passcodes and pull messages straight off your device. These steps protect your Signal messages at the device level.

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

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[14] 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[14]. (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[14].

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

iPhone

1. **Verify your device is still supported:** Check if your iPhone is still supported[21]
2. **Operating System:** Settings → General → Software Update
3. **Apps** are set to update automatically by default. To check, go to **Settings** → **Apps** → **App Store** and make sure **App Updates** is on.

Mac

1. **Verify your device is still supported:** Check if your Mac is still supported[21]
2. **Operating System:** Apple menu → System Settings → General → Software Update
3. **Apps installed via the Mac App Store:** These apps are set to update automatically by default. To check, open the **App Store**, go to App Store → **Settings**, and make sure **Automatic Updates** is on.
4. **Other apps:** Check for updates by going to top menu bar → Click on the app name → Click either **Check for updates** or **About [APP NAME]**, or look inside **Settings...**. If you don't see an option to update, it may be set to automatically update in the background.

Android

1. **Verify your device is still supported:** Check if your Android is still supported[21]
2. **Operating System:** Settings → System → System Update (may vary by manufacturer)
3. **Apps** from the Google Play Store are set to update automatically by default. To check, open the **Play Store**, tap your profile icon, then go to **Settings** → **Network preferences** → **Auto-update apps**.

Windows

1. **Update your system:** Start → Settings → Update & Security → Windows Update
2. **Verify your device is still supported:** Check if your Windows machine is still supported[21]
3. **Microsoft Store apps:** Make sure you enable automatic updates[22] (on by default).
4. **Other apps:** Look for updates in menu bar → **Help** → **Check for Updates**, or search for **Updates** or **About** in the app's settings.

Disable face/fingerprint unlock (biometric)

You have stronger legal standing[23] 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**.

Higher protection

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.

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**[24] and on Android, it's called **Advanced Protection Program**[25]. (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[26]. 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.

- [ ] **Verify safety numbers with important contacts**

  Confirms no one is secretly intercepting your messages in between you and the other person

Signal encrypts your messages so only you and the other person can read them. But in theory, a sophisticated attacker could position themselves in between you and your contact, intercepting messages before passing them along. This is called a "man-in-the-middle" attack. **Safety numbers** let you confirm that your encrypted connection goes directly to your contact with no one sitting in the middle.

Most people don't need to do this. If you're chatting with friends about everyday organizing, Signal's encryption is already doing its job. But if you're communicating about something high-risk (direct actions, sensitive legal matters, jouranlist talking with a source), verifying safety numbers is worth the extra step.

Think of it like a wax seal on an envelope. Encryption is the seal, but a sophisticated attacker could break it, read the contents, and reseal it with their own wax. Verifying safety numbers is how you confirm no one swapped the seal.

HOW TO VERIFY SAFETY NUMBERS

1. **Open the conversation** with the person you want to verify → **Tap their name** at the top → **View Safety Number**.
2. **Compare numbers with your contact:**
   - **In person (best):** Tap "Scan Code" and scan their QR code. If it matches, you'll see a success message.
   - **Not in person:** Read the numbers to each other over a call or video chat where you're confident you're talking to the right person. Don't verify over Signal itself.
3. **Mark as verified:** If the numbers match, tap the checkmark.

You only need to do this once per contact unless their safety numbers change (for example, if they get a new phone). If that happens, Signal will notify you. Verify again before sharing anything sensitive.

Has Signal been hacked? Is it safe? Is it secure?

Every few months, we see posts circulate claiming that Signal isn't secure or has been hacked.

Has Signal been hacked? Almost certainly not[27].

For a fuller explanation on Signal's security, including nonprofit ownership, encryption, open source, funding rumors, and device risks, read our article: Is Signal secure?[28].

There are risks to using Signal, but they are usually related to using it securely, rather than the technology itself.

For example, if someone infiltrates a private Signal group, they could screenshot all of the messages and post them online.

It's also possible that the cops can confiscate your phone and break into it if you have a weak passcode. That's not a failing of Signal, though. All your messages are available if anyone if they have physical access to your phone and can unlock it. That's why we recommend having a strong passcode[15] and always updating your device operating system[15].

Other resources

- Is Signal secure?[28] — how Signal works, what data it can share, and common myths about its security.
- Here's a great guide on how to use Signal groups for activism[29].
- Locking down Signal[30] — Freedom of the Press Foundation

Frequently asked questions

Is Signal actually secure?

Yes. Signal is the most secure mainstream messenger available. Messages and calls are end-to-end encrypted, the code is open source, and Signal is run by a nonprofit that does not store message contents. The biggest risks are usually how Signal gets used, not the technology itself: a weak phone passcode, a group with an infiltrator, or someone taking screenshots.

Can police read my Signal messages?

It depends. They can't get your data from Signal's servers. Your messages are end-to-end encrypted, so if police subpoena Signal, the company can only turn over basic account info, like when you signed up and when you last used the app. However, if the cops confiscate your phone, they can force your face or fingerprint to unlock it, or use forensic tools to crack a weak passcode. Once they're in, they can read every message still on the phone. The same goes for anyone you've been chatting with, which is why we recommend a strong passcode, turning off face/fingerprint unlock, and disappearing messages for everyone.

Is Signal safer than WhatsApp?

For activist use, yes. WhatsApp uses the same encryption protocol Signal invented, but it is owned by Meta, collects detailed metadata about who talks to whom and when, and shares that with Facebook. In response to law enforcement requests, Meta turns over significantly more data than Signal.

Do I need to verify safety numbers?

For your closest organizing contacts and anyone you discuss sensitive plans with, yes. Verifying once tells Signal you have confirmed this contact is who they say they are. Without verification, a sophisticated attacker who controls the phone network could in theory swap a key. With verification, you would be alerted if that happened.

Should I use my real phone number on Signal?

If you can use a username instead of your number, that is the more private option. Signal now lets you set a username and hide your number from people who do not already have it in their contacts. Activists who want extra distance can register Signal with a secondary number from MySudo, Google Voice, or a prepaid SIM.

What is the registration PIN for?

The PIN lets you recover your Signal profile, contacts, and group memberships if you lose your phone or set up Signal on a new device. It also protects against someone who steals your SIM from being able to register Signal as you on their phone. Pick a long PIN, save it in your password manager.

Keep learning with these related guides

Security essentials
Core security practices every activist should follow.

Prepare for a protest
Digital security for anyone attending a protest.

Travel & flight security
Digital security practices for activists traveling.

Spyware protection
Protect yourself from spyware and surveillance software.

VPNs for activists 14 min read 9 · Security update checker 21 · How to use Proton safely 15 min read 31
Remove link tracking 3 min read 32 · Is Apple Intelligence reading my Signal messages? 5 min read 18

Links

1. signal.org
2. ssd.eff.org/module/how-to-use-signal
3. activistchecklist.org/party/
4. nitter.net/camhigby/status/2015093531526729789
5. theguardian.com/us-news/2025/nov/21/fbi-signal-group-chat-immigration
6. activistchecklist.org/doxxing/
7. signal.org/blog/phone-number-privacy-usernames/
8. gist.github.com/hackermondev/45a3cdfa52246f1d1201c1e8cdef6117
9. activistchecklist.org/vpn/
10. support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages
11. bsky.app/profile/activistchecklist.org/post/3mityctmsfc2v
12. activistchecklist.org/secondary/
13. support.signal.org/hc/en-us/articles/360007059792-Signal-PIN
14. strongphrase.net/passcode
15. activistchecklist.org/essentials/
16. florisboard.org
17. f-droid.org/en/
18. activistchecklist.org/signal-ai/
19. netzpolitik.org/2026/phishing-attack-numerous-journalists-targeted-in-attack-via-signal-messenger/
20. support.signal.org/hc/en-us/articles/9932566320410-Staying-Safe-from-Phishing-Scams-and-Impersonation
21. activistchecklist.org/updates/
22. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
23. ssd.eff.org/module/attending-protest
24. support.apple.com/en-us/105120
25. landing.google.com/intl/en_us/advancedprotection/
26. activistchecklist.org/lockdown/
27. hassignalbeenhacked.info
28. activistchecklist.org/signal-secure/
29. micahflee.com/using-signal-groups-for-activism/
30. freedom.press/digisec/blog/locking-down-signal/
31. activistchecklist.org/proton/
32. activistchecklist.org/links/