Stay Safe, Stay Organized

🔗 **Signal Download:**

https://signal.org/download/

📞 **LUCE MA Hotline:**

617-370-5023 (5am-9pm daily)

📚 **More Security Info:**

https://signal.org/bigbrother/

⚖️ **Legal Support:**

Know your local legal observers and jail support networks

🤝 **SOLIDARITY FOREVER**

Share this zine with your comrades • Print copies for meetings • Organize safely

Based on "Using Signal groups for activism" by Micah Lee • Adapted for distribution

Signal for Activists

A Digital Security Guide for Organizers

🔒 **SECURE •** 📱 **SIMPLE •** 🛡️ **SAFE**

Protect your movement with encrypted communications

Why Signal Matters

🚨 REALITY CHECK

When authorities investigate activists, their primary weapon is **data requests** to tech companies. Google, Meta, Apple, and others regularly hand over user data to law enforcement - over 10,000 times in 2024 for companies like Proton alone.

🛡 Signal's Unique Protection

🔐 **Full Encryption:** Police can't access your conversations even if they demand them from Signal.

👻 **No Metadata Access:** Signal doesn't know what groups you're in or who you message - this data is cryptographically protected.

📞 **Phone Number Privacy:** Your number isn't shared with group members by default.

✊ **Easy to Use:** Critical for mass movements - if it's not simple, people won't use it.

🤷 When Forced to Comply

With government data requests, Signal can only provide: account creation timestamp and last login time. That's literally all they have access to.

Activist Checklist: Signal

This guide helps you take control of your private conversations on Signal. 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.

Security Best Practices

☑ DO:

- Enable disappearing messages
- Use admin approval for new members
- Vet new members through existing trusted contacts
- Have multiple admins
- Use QR codes for in-person recruitment
- Keep group descriptions clear about rules
- Remove inactive or suspicious members

❌ DON'T:

- Share group links publicly online
- Let everyone add new members
- Trust unverified information
- Use real names if not necessary
- Discuss specific illegal activities
- Screenshot sensitive messages
- Forward messages to non-Signal platforms

🕵 Infiltration Reality

Assume bad actors will attempt to join. Vetting processes, admin approval, and the ability to remove members are your main defenses.

⚡ Remember

The goal isn't perfect security (impossible) but **raising the cost** of surveillance high enough that authorities focus their limited resources elsewhere.

Group Links & Permissions

🔗 Group Links

By default, Signal groups are private. But you can create **group links** that allow people to join via a URL or QR code. Groups support up to **1,000 members**.

🌓 **ADMIN APPROVAL:** Always enable "Require Admin Approval" for activist groups. This lets you vet new members before they join.

👥 Permission Settings

Signal groups have two roles: **admins** and **everyone else**. You can control who can:

- **Add Members** - Keep this admin-only for security
- **Edit Group Info** - Usually admin-only
- **Send Messages** - All members for discussion groups, admin-only for announcements

💡 **PRO TIP:** Have multiple admins to share moderation responsibilities and ensure the group continues functioning if one admin is unavailable.

Meeting → Signal Group

Turn any in-person gathering into a secure ongoing communication channel:

Step-by-Step Process:

1. Ask non-Signal users to **install Signal and register** accounts
2. Create a new Signal group and **turn on disappearing messages**
3. Enable **Group Link** in settings
4. Choose **Share → QR Code** to display the group link as a QR code
5. Have everyone **scan the QR code** with their camera app
6. **Enable "Require Admin Approval"** after everyone joins
7. Adjust **permissions** as needed (consider making trusted members admins)

🎯 Result

You now have a secure group that police data requests cannot penetrate. Signal doesn't even know your group exists!

⏰ Disappearing Messages

Always enable this feature. Messages automatically delete after a set time, leaving no permanent record even on devices.

☑ Green Flags:

- Consistent personal narrative
- Verifiable movement involvement
- Strong references from trusted sources
- Authentic social media history
- Patient with vetting process
- Clear commitment to shared values

⚖️ Balance

Vetting protects security while building inclusive movements. The goal is identifying genuine threats, not excluding people based on superficial differences.

Comprehensive Vetting Process

Vetting combines **threat assessment** with **risk management**. Protocols should vary by role - general members need lighter vetting, leadership needs deeper vetting, and staff require the most stringent protocols.

🎯 **Vetting Components (Vision Change Win Framework):**

1. **Standardized Application:** Add security-related questions to existing forms
2. **Background Check:** Verify identity and look for vulnerabilities opponents could exploit
3. **Political Assessment:** Current systems for new members usually suffice
4. **Movement References:** 2-3 references from movement settings (at least one the person doesn't offer themselves)
5. **Social Media Review:** Check individual's online presence and web activity
6. **Flag Assessment:** Look for conflicts or concerning patterns
7. **Interview Process:** Conversation to address any flags or concerns
8. **Final Decision:** Clear approval/denial based on assessment

🚩 **Red Flags to Watch:**

- Inconsistent personal details
- Pressure for quick inclusion
- Excessive questions about security
- No verifiable movement history
- Conflicting social media presence
- Reluctance to provide references

Semi-Public Groups

Create large, secure groups while maintaining safety through vetting:

📋 **Example Rules:**

- "Be cool and be kind, or be kicked out"
- "New members need to be vouched for by an existing member"

Setup Process:

1. **Write a group description** explaining membership rules
2. **Enable Group Link + Require Admin Approval**
3. Set permissions: **Add Members** and **Edit Group Info** to "Only Admins"
4. **Appoint multiple admins** to share moderation duties

🔒 **Privacy Advantage**

Unlike Discord servers or other platforms, Signal groups are completely invisible to authorities. From the server's perspective, it's just encrypted messages - no group data to seize.

Rapid Response Networks

Perfect for **ICE raid alerts**, **protest coordination**, and **emergency communications**:

⚠ Important Note on ICE sightings

Unverified social media posts about ICE sightings spread panic and misinformation. **We are already terrified - please don't make it worse** by posting unverified claims to public chats.

📞 Massachusetts LUCE Hotline

LUCE (Immigrant Justice Network of MA) operates a multilingual hotline at **617-370-5023**, staffed 5am-9pm daily in English, Spanish, Portuguese, French, Mandarin, and Haitian Creole.

🚨 How Professional Verification Works:

- **Hotline:** Community calls/texts reports to monitored number
- **Trained verifiers:** Only qualified volunteers can verify and disseminate reports
- **Firsthand knowledge required:** Verification teams need direct witness accounts
- **Internal alerts first:** Verified info goes to immigrant communities before public posting
- **Coordinated response:** Members use emoji to indicate availability

Setup Announcement-Only Group:

1. **Enable Group Link + Require Admin Approval**
2. Set **Add Members, Edit Group Info, AND Send Messages** to "Only Admins"
3. **Appoint trusted coordinators** as admins

Critical Vetting Principles:

- **Don't post unverified reports** - even well-meaning posts can cause panic
- **Call the hotline first** - let trained verifiers handle assessment
- **Respect the process** - immigration justice groups set up systems for a reason
- **Remember the impact** - false alarms take immigrants out of work and school