Security Culture for Everyone

Accessible security practices that protect your organizing without excluding participants or creating barriers to community involvement.

Security culture isn't about paranoia or exclusion—it's about creating sustainable practices that keep your community safe while remaining open and welcoming. This guide provides practical, implementable security measures that balance protection with accessibility.

⏱ Estimated read time: 25 minutes

What's Covered

Understanding Security Culture

Security culture is a set of practices that help protect activists and their communities from surveillance, infiltration, and repression. Think of it as community self-defense—not just against physical threats, but against information gathering that could be used to disrupt your organizing.

Key Principle

Good security culture makes organizing more effective, not less. If your security practices are preventing people from participating or creating an atmosphere of fear, they need adjustment.

The foundation of security culture rests on three pillars:

- **Need-to-know basis:** Share sensitive information only with those who need it for their role
- **Verification:** Build trust over time and verify new contacts through existing relationships
- **Proportional response:** Match your security measures to actual, not hypothetical, threats

Basic Digital Security

Digital security doesn't require technical expertise. These fundamental practices significantly improve your security posture while remaining accessible to everyone in your community.

Essential Tools and Practices

Signal for Sensitive Conversations

What it is: Free encrypted messaging app available for phones and computers

Why use it: Messages are end-to-end encrypted, meaning only you and the recipient can read them

Quick setup:

1. Download from signal.org or your app store
2. Register with your phone number
3. Enable disappearing messages for sensitive chats
4. Verify safety numbers with important contacts

Pro tip: Create group chats for working groups, but keep them focused and limit membership to active participants.

Password Managers

Recommended options: Bitwarden (free), 1Password, or KeePassXC

Why essential: Unique, strong passwords for every account prevent cascade breaches

Implementation steps:

1. Choose a strong master password (use a passphrase like "correct-horse-battery-staple")
2. Start with your most important accounts (email, banking, social media)
3. Generate 16+ character passwords for each account
4. Enable two-factor authentication wherever possible

Security Practice	Basic Implementation	Advanced Options
Encrypted Communication	Signal for messages	PGP email, encrypted voice calls
Two-Factor	SMS codes (better than	Authenticator apps, hardware keys

Authentication	nothing)	
Secure Browsing	Use HTTPS sites, private browsing	VPN, Tor browser for research
Social Media	Review privacy settings quarterly	Separate activist accounts, pseudonyms

Digital Security Red Flags

- Requests to move sensitive conversations to unencrypted platforms
- Pressure to share passwords or account access
- Links from unknown sources asking for login credentials
- Unexpected requests for personal information via email

Community Security Practices

Strong communities are built on trust, and trust is built through consistent, transparent practices. These guidelines help create security without sacrificing the openness that makes organizing possible.

Building Trust Gradually

New people should be welcomed warmly while being gradually integrated into more sensitive aspects of organizing. Think of it like any relationship—trust develops over time through shared experiences.

> **Welcoming Script for New Members:**
>
> *"We're so glad you're here! For the first few meetings, we'd love for you to observe and ask*

> *questions. As you get to know everyone and find your role, you'll naturally become more involved in planning and decision-making."*

Information Compartmentalization

Not everyone needs to know everything. This isn't about hierarchy or secrecy—it's about protecting people and ensuring operational security.

Practical Compartmentalization

- **Public info:** Event times, locations, general goals
- **Working group info:** Specific plans, logistics, contact lists
- **Need-to-know info:** Legal strategies, vulnerable participants' details, funding sources

Meeting Security

Create meeting environments that balance openness with appropriate caution:

- Choose accessible, comfortable venues that don't require documentation to enter
- Rotate meeting locations for sensitive planning
- Establish phone-free zones for certain discussions
- Use meeting roles (facilitator, note-taker, stack-keeper) to maintain focus

Legal and Physical Safety

Understanding your rights and planning for various scenarios helps everyone feel more confident and secure in their activism.

Know Your Rights

Legal rights vary by location, but some principles remain consistent. Connect with local legal observers or movement lawyers who understand your area's specific laws.

Related Resource

See our Know Your Rights guide for detailed information about protests, police interactions, and legal support.

Legal Observer Training

Legal observers document police and protester actions to support potential legal cases. Key practices include:

- Wear visible identification (green hats, vests marked "LEGAL OBSERVER")
- Document everything: times, badge numbers, actions taken
- Never interfere with arrests—observe and record only
- Have lawyers' numbers written on your body in permanent marker

De-escalation Techniques

De-escalation keeps everyone safer. These techniques work in various contexts, from heated meetings to street confrontations:

> **De-escalation Phrases:**
>
> - *"I hear that you're frustrated. Can you help me understand what's happening?"*
> - *"Let's take a breath and step back for a moment."*
> - *"We're all here for the same reason. How can we work together?"*
> - *"Your safety is important to us. What do you need right now?"*

Threat Modeling Basics

Threat modeling helps you make informed decisions about security by understanding what you're protecting, who might want to access it, and what resources they have. It's not about paranoia—it's about proportional responses to real risks.

The Five Questions Framework

Question	What to Consider	Example Answers
What do I want to protect?	Information, people, resources, plans	Member contact list, meeting locations, funding sources
Who do I want to protect it from?	Specific adversaries with capabilities	Local police, opposition groups, data brokers
How likely is it I need to protect it?	Based on past incidents and current context	High for public events, low for internal planning
How bad are the consequences if I fail?	Impact on individuals and movement	Minor inconvenience to serious legal consequences
How much trouble am I willing to go through?	Balance security with accessibility	Extra steps for sensitive data, basic measures for public info

Scenario: Planning a Protest

Assets to protect: Organizer identities, tactical plans, participant safety

Likely adversaries: Local police (monitoring social media), counter-protesters (disruption)

Proportional measures:

- Use Signal for tactical discussions
- Public promotion focuses on goals, not tactics
- Designate roles for safety, legal observers, and media
- Have contingency plans but don't over-share them

Creating Security Agreements

Security agreements are collective commitments that groups make to protect each other. They should be created democratically and revisited regularly.

Sample Security Agreement Template

Our Group Security Agreement

We agree to:

- Use Signal for any discussion of tactics, logistics, or sensitive planning
- Ask before taking photos at meetings and events
- Not share personal information about other members without consent
- Verify new members through existing trusted relationships
- Report security concerns to designated security point-people

We understand that:

- Perfect security doesn't exist—we do our best with the tools we have
- These agreements protect everyone and build trust
- Violations will be addressed through our conflict resolution process

Review date: [Every 3 months or after significant events]

Making Agreements Stick

- Involve everyone in creating the agreement
- Make it living document that can be updated
- Regular gentle reminders, not harsh enforcement
- Model the behavior you want to see

Scenario Planning Exercises

Practice makes prepared. Regular scenario planning helps groups respond calmly to challenging situations.

Exercise 1: The Disruptive Meeting Attendee

Scenario Setup

A new person arrives at your public meeting and begins asking detailed questions about members' full names, employers, and specific tactical plans. They're recording on their phone.

Discussion questions:

- How do you redirect without creating confrontation?

- What information is OK to share publicly?
- Who takes the lead in this situation?

Practice responses: Role-play with calm redirection, setting boundaries, and post-meeting debriefs.

Exercise 2: Digital Security Breach

Scenario Setup

A member's email is compromised, and opposition groups now have access to your mailing list and some planning documents.

Immediate response checklist:

- Alert all affected members within 2 hours
- Change all shared passwords
- Move sensitive conversations to secure channels
- Document what was compromised
- Support the affected member (no blame)

Long-term fixes: Implement two-factor authentication requirement, regular security trainings, and better compartmentalization.

Exercise 3: Police Surveillance at Events

Scenario Setup

You notice obvious police surveillance at your public event—marked cars, photographers, and potential undercovers.

Prepared responses:

- Legal observers document all surveillance
- Designated people engage with media (if present)
- Continue with planned program—don't let surveillance shut you down
- Brief participants on their rights
- Have lawyers' numbers visible and available

Next Steps

Security culture is a practice, not a destination. Start with the basics and build based on your actual needs and capacity.

This Week

- Download Signal and get 5 key organizers using it
- Set up two-factor authentication on your email
- Have a brief security discussion at your next meeting

This Month

- Conduct a basic threat modeling session with your core group
- Create or update your group's security agreement
- Run through one scenario planning exercise
- Connect with local legal support organizations

Ongoing

- Regular security check-ins and agreement reviews
- Build relationships with movement lawyers and legal observers
- Stay updated on local surveillance technologies and laws
- Share knowledge and resources with allied groups

Remember

The best security culture is one that your community will actually practice. Start where you are, use what you have, do what you can. Perfect security that no one follows is worse than good-enough security that everyone uses.

Related Resources

Continue Learning

- Know Your Rights - Legal information for activists
- Sustainable Organizing Practices - Build security into long-term organizing
- Coalition Building Guide - Security considerations for multi-group work