OpSec for Trans Organizing Toolkit

Operational Security (OpSec) is essential for protecting trans activists, organizers, and communities from surveillance, infiltration, and repression. This toolkit provides strategies for safeguarding communication, protecting identities, and ensuring that trans organizing efforts remain secure in hostile environments.

1. Understanding OpSec for Trans Activists

- What is OpSec?
 - Operational Security (OpSec): A set of practices used to protect information, identities, and organizational strategies from adversaries.
 - For Trans Organizers: Ensures the safety of trans activists working against state violence, antitrans legislation, and fascist repression.

Core Goals of OpSec:

- Protect sensitive information about members and actions.
- Shield vulnerable communities from doxxing, infiltration, and surveillance.
- Minimize digital and physical footprints during organizing.

2. Securing Communications and Data

Encrypted Communication Channels

Use Encrypted Messaging Apps:

- Signal: End-to-end encrypted messaging, voice, and video calls. Supports disappearing messages.
- **Session:** Decentralized, metadata-free messaging alternative.

Avoid SMS and Unencrypted Platforms:

- SMS, Facebook Messenger, and WhatsApp are vulnerable to interception and tracking.
- Encourage all organizers to migrate to encrypted platforms.

Turn Off Cloud Backups:

Disable backups for Signal and other secure apps to prevent copies from being stored in vulnerable cloud environments.

Protection and Protection

Encrypt Devices:

- Use full-disk encryption on phones, laptops, and tablets.
- For Android: Enable encryption under **Security Settings**.
- For iOS: Encryption is enabled automatically with a strong passcode.

Secure File Storage:

- Use encryption tools like VeraCrypt for sensitive files.
- Store files in secure cloud services like **Tresorit** or **Proton Drive**.
- 3. Protecting Your Digital Identity
- Anonymize Online Activity
- Use VPNs to Mask Your IP:
 - VPNs like Mullvad, ProtonVPN, and IVPN protect your IP address and prevent location tracking.
- Use Tor for Anonymous Browsing:
 - **Tor Browser** anonymizes your internet activity by routing it through multiple nodes.
 - Avoid logging into personal accounts while using Tor.
- Create Burner Accounts:
 - Use pseudonyms or burner accounts for high-risk organizing.
 - Avoid connecting burner accounts to real-world identities.
- Limit Social Media Exposure
- Set Profiles to Private:
 - Restrict visibility of posts and limit friend/follower lists.
 - Regularly audit friend lists to remove unknown or inactive accounts.
- Avoid Posting Protest Locations:
 - Do not share live updates or location data from protests.
 - Use encrypted apps to communicate logistics securely.
- 4. Building Secure Organizing Structures
- Decentralize Leadership and Decision-Making
- Use Distributed Organizing Models:

- Avoid hierarchical structures that can be easily dismantled.
- Empower smaller, autonomous teams with clear objectives.

Limit Access to Sensitive Information:

- Share information on a need-to-know basis.
- Restrict access to organizational documents and sensitive data.

>> Verify and Vet New Members

Screen New Members:

- Require new members to be referred by trusted individuals.
- Conduct security briefings and explain OpSec protocols.

✓ Be Cautious of Infiltrators:

 Watch for signs of suspicious behavior, such as individuals asking excessive questions or attempting to access sensitive information.

1 5. Countering Surveillance and Infiltration

| Identify and Avoid Surveillance Tactics

Recognize State and Non-State Actors:

- Be aware of infiltration efforts by law enforcement and far-right groups.
- Monitor for unusual behavior and document potential infiltration.

Limit Public Disclosure:

- Use codenames and aliases for sensitive organizing work.
- Limit public discussion of protest strategies and direct actions.

✓ Rotate Meeting Locations and Times:

- Prevent surveillance by avoiding predictable patterns.
- Use encrypted channels to share meeting details securely.

O Anti-Doxxing Measures

Remove Personal Information Online:

- Regularly search for and remove identifying information from public databases.
- Use services like **DeleteMe** to scrub your online presence.

Create Pseudonyms for High-Risk Work:

• Use alternate names when engaging in direct action or high-profile organizing.

6. Digital Hygiene and Security Protocols

- Best Practices for Digital Safety
- **✓** Use Strong Passwords and 2FA:
 - Use unique, complex passwords for all accounts.
 - Enable Two-Factor Authentication (2FA) to protect critical accounts.

Regularly Audit Security Practices:

- Conduct periodic security audits to identify vulnerabilities.
- Update software and security settings to stay ahead of threats.

Secure Collaborative Platforms:

- Use secure platforms like **CryptPad** or **Riseup Pad** for collaboration.
- Avoid Google Docs and other mainstream platforms that lack encryption.

7. Physical Security for High-Risk Organizing

- Secure Meeting Spaces
- Use Trusted Locations:
 - Meet in safe, undisclosed locations.
 - Rotate locations to prevent pattern recognition.

Limit Physical Access:

- Restrict entry to verified members.
- Implement check-in procedures for new attendees.

Plan Exit Strategies and Emergency Protocols

Map Out Emergency Exits:

- Identify multiple escape routes from meeting spaces.
- Develop rally points if members need to evacuate.

✓ Have a Legal Observer on Standby:

• Coordinate with the **National Lawyers Guild (NLG)** for legal observers.

8. Emergency Protocols and Crisis Response

♦ Crisis Management Plan

Develop a Crisis Protocol:

- Create contingency plans for emergencies, including police raids or arrests.
- Establish clear communication lines and designated crisis coordinators.

✓ Secure Emergency Contacts:

• Maintain an updated list of emergency contacts and legal aid organizations.

✓ Document and Report Incidents:

• Record details of harassment, infiltration, and police misconduct.

9. Emergency OpSec Checklist

Before High-Risk Actions:

- Update secure communication channels.
- Secure sensitive files and encrypt devices.

During Actions:

- Use encrypted platforms to relay information.
- Monitor for suspicious behavior and document incidents.

After Actions:

- Review security protocols and debrief with trusted allies.
- Identify any vulnerabilities and reinforce OpSec measures.

10. Trusted OpSec Resources for Trans Organizers

- 1. **Electronic Frontier Foundation (EFF):** Digital privacy and security resources.
- 2. **Digital Defense Fund:** Security guidance for activists and organizers.
- 3. National Lawyers Guild (NLG): Legal defense and observer programs.
- 4. **DeleteMe:** Privacy service for removing personal information.

5. **Privacy Badger:** Browser extension to block trackers and protect privacy.

Secure Your Movement and Protect Your People

OpSec is not paranoia—it's survival. Protect your movement, safeguard your identity, and ensure the safety of your community. Stay secure, stay resilient, and resist with confidence.