Digital Security Toolkit

Operational Defense Against Surveillance, Doxxing, and Digital Repression

TRANS ARMY

Last update: 2025-05-06

Digital Security Toolkit

Operational Defense Against Surveillance, Doxxing, and Digital Repression
Version 1.3 – April 2025

Digital repression is a frontline weapon in the state's war on trans liberation. Our phones are surveillance devices. Our clouds are subpoenas waiting to happen. Our metadata can lead cops straight to our organizers.

This toolkit is your digital armor.

Built for trans-led movements, this guide teaches the tools, habits, and setups that keep your comms safe, your files protected, and your identity secured, even under the eyes of the algorithm and the badge.

Inside, you'll find:

- How to secure your phone and computer against seizure
- Best messaging apps and how to configure them right
- VPNs, Tor, and anonymizing techniques to evade surveillance
- File encryption, metadata stripping, and cloud safety protocols
- Burner phone tactics and protest-specific digital prep
- Trusted tools list: Bitwarden, VeraCrypt, Signal, ProtonVPN, and more

This isn't about paranoia.
It's about refusing to be easy prey.

This toolkit equips trans activists with critical tools and strategies to protect their digital security, safeguard sensitive information, and mitigate surveillance while organizing and protesting in the U.S.

I. Secure Your Devices - Prevent Unauthorized Access

1. Use Strong Passwords:

- Create passwords that are at least 12-16 characters long and include a mix of upper and lowercase letters, numbers, and symbols.
- Avoid using easily guessable information like names or birthdays.
- Consider using a **password manager** such as Bitwarden or LastPass to generate and store strong passwords.

2. Enable Device Encryption:

- **Encrypt Your Phone and Computer:** Full-disk encryption protects your data even if your device is confiscated or stolen.
- On iOS: Enabled by default when a passcode is set.
- On Android: Enable in Settings > Security > Encryption.
- On Windows: Use BitLocker.
- On macOS: Use FileVault.

3. Set Strong Screen Lock:

- Use PINs or strong passwords rather than fingerprint or facial recognition, which can be forcibly unlocked.
- Set devices to lock after 30 seconds of inactivity.

II. Protect Your Communications - Secure Messaging

1. Use Encrypted Messaging Apps:

- **Signal:** Gold standard for encrypted communications. Supports disappearing messages, secure voice/video calls, and group chats.
- **Session:** Decentralized, anonymous messaging alternative.

2. Avoid SMS for Sensitive Conversations:

- SMS are easily intercepted and vulnerable to surveillance.

3. Turn Off Cloud Backups:

- Disable cloud backups for Signal and other messaging apps to prevent copies from being stored on insecure servers.

III. **Protect Your Online Identity - Anonymize Your Online Presence**

1. Use a VPN:

- A Virtual Private Network (VPN) encrypts your internet traffic, hides your IP address, and protects you from surveillance.
- Recommended VPNs: **Mullvad**, **ProtonVPN**, **IVPN**.

2. Use Tor for Anonymous Browsing:

- Tor Browser anonymizes your online activity by routing it through multiple nodes.
- Avoid logging into personal accounts while using Tor.

3. Limit Social Media Footprint:

- Set profiles to **private** and remove identifying information.
- Use pseudonyms or burner accounts when organizing.
- Avoid posting live updates from protest locations to prevent doxxing or surveillance.

IV. **Protect Sensitive Data - Secure File Storage and Sharing**

1. Encrypt Files Before Uploading:

- Use tools like **VeraCrypt** or **Cryptomator** to encrypt sensitive files.

2. Secure Cloud Storage:

- Choose privacy-focused services such as **Tresorit**, **Proton Drive**, or **Sync.com**.

3. Avoid Google Drive for Sensitive Info:

- Google may comply with subpoenas or government requests.

V. **Lock Down Social Media - Privacy and Anonymity**

1. Set Social Media Accounts to Private:

- Restrict posts and limit visibility to trusted contacts.
- Disable location tagging.

2. Remove Metadata from Photos:

- Use tools like **ExifCleaner** to strip metadata that may reveal your location.

3. Avoid Geotagging:

- Turn off location services while posting or attending protests.

VI. Avoid Government and Law Enforcement Tracking - Location Privacy

1. Turn Off Location Services:

- Disable GPS and geolocation on your phone when attending protests or engaging in sensitive activities.

2. Use Airplane Mode During Protests:

- Prevent your phone from transmitting location data.

3. Burner Phones for Protests:

- Consider using a prepaid or burner phone without personal information for high-risk actions.

VII. Emergency Digital Security Checklist

1. Before Protests:

- Enable full-disk encryption.
- Backup critical data offline.
- Install secure apps (Signal, VPN, Tor).
- Disable biometric unlock.

2. During Protests:

- Use Airplane Mode or burner phones.
- Avoid logging into personal accounts.
- Record police interactions securely.

3. After Protests:

- Clear metadata from photos.
- Delete sensitive messages and contacts.
- Wipe devices if necessary.

VIII. Trusted Digital Security Tools

- **Signal:** Encrypted messaging.
- **Tor Browser:** Anonymous internet browsing.
- **ProtonVPN:** Privacy-focused VPN.
- **Bitwarden:** Password manager.
- **VeraCrypt:** Encrypt sensitive files.
- **ExifCleaner:** Remove metadata from images.

Conclusion

We live in an era where digital footprints are tracked, conversations are intercepted, and resistance is algorithmically profiled before it even hits the streets. Governments, corporations, and third-party actors, many of them openly hostile to trans lives and liberation movements, are tightening the noose of surveillance under the guise of "safety," "anti-terrorism," or "national security." But we know what they're really after: control, compliance, and silence.

In these conditions, protecting your digital privacy isn't just a personal choice, it's a tactical necessity. Every unencrypted message, every GPS ping, every unguarded login is a potential threat vector. Not just to you, but to your comrades, your network, and your collective future. This is why we encrypt. This is why we compartmentalize. This is why we never assume digital innocence in a weaponized network.

Digital hygiene is political armor. Use end-to-end encryption (Signal, ProtonMail, Session). Turn off location tracking. Scrub metadata. Use burner devices. Build threat models. Normalize anonymity. Never use your real name where your enemies can see it. Keep your opsec as sharp as your politics.

But don't stop there. Train others. Spread tools. Share guides. If only a few of us are protected, none of us truly are. Make your encryption a community ritual. Make your resistance collective.

Let them surveil blank screens. Let their panopticon choke on our silence, our codewords, our firewalls. We are not data to be mined, we are chaos systems in motion.

Stay vigilant, because they are watching.
Stay encrypted, because they are listening.
Resist with confidence, because we are winning.

Legal Disclaimer
This document is provided for educational and harm-reduction purposes only. It does not endorse or instruct illegal activity. All tactics are drawn from publicly available digital rights resources and community safety guidelines. Users are encouraged to adapt tools within their legal context.