How To INFOSEC & OPSEC;

a 50501 Movement Handbook for Protesters and Organizers

Version 1.6.3, Updated 16 Febuary, 2025

Welcome to the Movement!

Whether you're showing up to a protest or helping to organize, it's important to think about how you protect your personal information and keep your communications secure. This handbook will give you the lowdown on how to practice good OPSEC (Operational Security) and INFOSEC (Information Security). Let's be clear: while 50501 strives to remain a peaceful and legal Movement, we are protecting ourselves from *anyone* who might want to take advantage of us, scam us, or cause harm, not just law enforcement. There have already been several identified violent threats against the movement, and safety should always be your top priotity. **Please remember, this is not a complete guide, nor should it be approached as an all-or-nothing task:** Do what you can *now*, learn more and do more later. Check out the list of external resources at the bottom.

What is Op/Info/Cyber Security?

OpSec (Operational Security): This is a *way of thinking* about information security through tools like threat modeling. By identifying and analyzing specific vunerabilities, threats, and risks, you can make informed decisions about what information you make available and what countermeasures you take. Think: analyzing threats and making a plan.

InfoSec (Information Security): This is a the pratice of choosing *what* information to protect by mitigating risks. This is about keeping your information— and there for you— safe everywhere; including digitally, socially, and physically. Think: combatting doxxing, social engineering, and implementing good cyber security.

CyberSec (Cyber Security): This is *how* you go about implementing specific measures to keep your electronic data (aka, information) safe. Think: using encryption, strong passwords, VPNs, etc.

Key Terms You Should Know:

- **Personally Identifiable Information (PII):**
  Anything that can be used to identify you, like your name, address, phone number, social media accounts, or even where you hang out. Keep it as private as possible!
    - *Pro Tip:* The more info you share, the easier it is for others to track or target you, even if it seems innocous.
- **Virtual Private Network (VPN):**
  A VPN hides your IP address by routing your internet traffic through a secure server, making your online activity harder to track. Think of it like a cloak for your internet.
    - *Pro Tip:* Always use a VPN when browsing or messaging, this is your first line of defense. But remember, a VPN does not ensure the security of the website you're visiting, it secures your connection, not the site itself.
- **Doxxing:**
  This is when someone intentionally posts your personal info (like your address or workplace) online to harm or harass you. You don't want to be an easy target.
    - *Pro Tip:* Keep personal info as hidden as possible. It's better to be safe than sorry!
- **End-to-End Encryption (E2EE):**
  This ensures that no one but you and the person you're talking to can read your messages or listen to your calls. Even if someone tries to intercept it, they won't be able to crack it.
    - *Pro Tip:* Always choose platforms with E2EE for anything that matters, Signal is a solid option.
- **Signal:**
  A secure messaging app that uses E2EE to protect your conversations. If you're serious about keeping things private, this is the go-to.
    - **Pro Tip:** Don't use platforms like regular text messages or Facebook Messenger, they're not secure.
- **Discord:**
  This is a popular chat app for activists and interest groups. While it's convenient, it doesn't offer encryption, so it's not the best for private or sensitive conversations.
    - **Pro Tip:** Discord's fine for casual chats and making connections, but use something like Signal for anything private.

- **Trust But Verify:**

  Check your sources! Use fact checking, your trusted social network, and vetting pratices to confirm that people and things are what they appear to be. Use multiple sources.

- **"Least Privlidge Access":**

  When sharing any information or access permissions, always ask what material *needs* to be shared with somone else or yourself. What would happen is a bad actor got their hands on it? Can the goal be achieved with less risk by limiting access permissions or self-censoring non-relevent information? Balancing the need for transparency and communication against security and safety is difficult, but necessary.

- **Threat Model:**

  A tool for thinking and planning to assist in risk assessment. What are we working on? What can go wrong? What are we going to do about it? Did we do a good enough job?

Why OPSEC Matters

OPSEC isn't just about protecting yourself from law enforcement; it's about protecting yourself from **anyone** who might try to take advantage of you. Bad actors could be anyone: scammers, doxxers, or other people with malicious intentions. Strong OPSEC is all about reducing risk. The less information people have on you, the harder it is for them to do anything harmful.

Digital OPSEC Tips for Protesters

1. Control Your PII (Personally Identifiable Information)

- **Use Fake Names When Possible:** Don't give out your real name unless it's absolutely necessary. Use a pseudonym for online activism.
- **Limit Social Media:** Go ahead and delete or lock down your social media. We're talking about making your profiles private, or better yet, just deleting them if you can.
- **Don't Overshare:** Don't share personal info in public chats or with strangers. Share only with trusted individuals in trusted spaces.

- **Use a VPN:** Seriously, always use a VPN. You don't want your internet activity being traced back to you.
    - *Pro Tip:* Check out why VPNs are important here.
- **Remove Metadata from EVERYTHING:** Before sharing any images, files, or links online, strip the metadata (location, device info, etc.) from them.
    - *Pro Tip:* ExifCleaner is one of several free and open-source tools for scrubbing file exif data.
    - *Pro Tip:* Use LinkCleaner to remove any tracking codes from links before sharing them.
- **Keep Devices Up to Date:** Regularly update your devices to patch security vulnerabilities. Restart your devices from time to time to ensure they function optimally.
- **Turn Off Biometrics:** Biometrics are generally considered secure, but in the US, they are not protected by the 5th Amendment or current law. It's safer to disable your biometric logins and use strong passwords instead.
- **Photos:** Keep yourself and others by not sharing un-censored photos in aggregated ways or high-risk spaces such as in Discord and Reddit, or posting links to large photo dumps of protests. Each platform has it's own unique degree of and associated factors, this is not a one-size-fits-all guideline. Ultimately it is your own responsibility to keep your own identity safe, and we strongly encourage you to cover your face at protests. We encourage you to only share photos of protests with your own community by sharing 1-2 images with blurred features or taken from an angle that does not expose people without their consent.
    - *Pro Tip:* Read this [Wired Article](Protest Photography Safety Tips: Dos and Don'ts, How to Blur Faces, Essential Gear | WIRED) if you are interested in taking photographs at a protest

---

2. Secure Your Communications

- **Use Encrypted Apps:**
    - **Signal** is the gold standard. Use it for private messages and calls.
    - *Pro Tip:* Check out this guide to get started with Signal.
- **Keep It Private:** Only share sensitive information in secure, private groups. If you're unsure, don't say it.

- **Don’t Trust Insecure Platforms:** Discord is cool, but it’s not secure for private convos. Stick to platforms that prioritize your security.
- **Trust But Verify:** *Any* time you make new contact with a stranger, make sure that you vet that person before sharing information. Are they a good actor?
    - The simpliest way to do this is with a **Trust Network**: check in about them with 2-3 mutual contacts whom you already implicitly trust who can vouch for them.
    - Use Open Source Intelligence gathering to learn more about them through communication channels you are in.

---

3. Watch Out for Sketchy Links & Files

- **Don’t Click Random Links:** Never click on links that come from people you don’t know or sources you don’t trust.
    - *Pro Tip:* Use VirusTotal URL scanner or a similair service to scan links before clicking on them.
    - *Pro Tip:* Use LinkCleaner to remove any tracking codes from links before sharing them.
- **Scan Files for Malware:** Always scan files before opening them. It only takes a few seconds and could save you from getting hacked.
    - *Pro Tip:* Upload any suspicious files to VirusTotal to see if they’re safe.

---

4. Use Private Browsing

- **Incognito Mode:** Always browse in a private or incognito window to avoid leaving tracking data behind.
- **VPN Always On:** Don’t surf the web without your VPN. VPNs anonymize you by putting your browing data in the hands of your VPN company, ideally somewhere in Europe. Remember that your VPN company can and will hand over that data to authorities if compelled.
    - **TOR** anonymizes you in a similair way to a VPN by putting your traffic data in the hands of three randomly selected volunteer servers, instead of one single company. Tor also has a suite of antifingerprinting techniques that will prevent you from being

ID'd by malicious websites in ways incognito mode in other browsers won't. Keep in mind that Tor cannot protect you when downloading or torrenting, and only provides moderate privacy against nation-state intelligence.

    - *Which one?* Anything is better than nothing, multiple is better. For Web Browsing, Tor is generally better than [Brand Name VPN company]. The best option, for those who have the resources, is usually a VPN which you set up yourself— such as OpenVPN—which can dirrect your traffic through a Swiss or GDPR protected server overseas for better legal protection.

OPSEC During Protests

1. Know Your Rights

Before you go to a protest, it's important to understand what your rights are, especially in case things go sideways.

- *Pro Tip:* Check out your protester rights with the ACLU here.

2. Secure Your Phone

- **Lock It Up:** Set a strong password or PIN on your phone. DO NOT use Biometrics if you are in the US. Biometrics are not protected information under law and will be used to compel you to unlock your phone for law enforcement.
- **Leave It Behind If You Can:** Don't use your phone unless you have to. Phones are easy to track.
- **Avoid Tracking:** Learn how to protect yourself from surveillance, especially during protests.
    - *Pro Tip:* The ACLU has a great guide here.

3. Stick with Trusted Groups

- **Find Well-Organized Groups:** If you're protesting, make sure you're with a solid, trusted group.
- **Listen to Experienced Organizers:** They know what to do and how to keep things safe for everyone.
- **Follow Safety Guidelines:** Always have an exit plan, and follow any instructions that keep you and others out of danger.

- *Pro Tip:* Check out How to Protest Safely.

OPSEC for Organizers

1. Build your Network

- Movements rely on indivudals to connectting to other indivudals and resources to make things happen. Do this safely by praticing "Trust but Verify" and "Least Privilege Access".

2. Build a Security Culture

- **Know the Threats:** Be aware of potential infiltrators or disorganization within the group. Set up secure systems.
- **Coordinate with Other Groups:** Join forces with other organizations to strengthen your efforts and share security tips.
  - *Pro Tip:* Read more about building a security culture from the Activist Handbook.

3. Know the Law

- Before organizing, understand the legal landscape. Do you need a permit? What are the laws in your area?
  - *Pro Tip:* The Constitutional Protest Guide is a good resource.

4. Protect Your PII

- If you want to stay anonymous, take extra steps to remove your personal info from the internet.
  - *Pro Tip:* Use tools like Cybernews Privacy Tools and IntelTechniques to scrub your data.

More External Resources

- Electronic Frontier Foundation – Security: a digestabable InfoSec guide including everything here and more

- Cyber Peace – Information, Education and Communication: more detailed InfoSec guides, whitepapers, printable entry level handbooks, and more
- Activist Handbook – Introduction: a guide to activist-specific safety
- EFF – Signal Encryption Guide: how to use Signal
- Threat Modeling - OWASP Cheat Sheet Series: an introduction to threat modeling

---

Protect Yourself, Protect the Movement

The more careful we are about protecting our personal information, the stronger and safer the movement becomes. Follow these tips to keep your data safe, communicate securely, and stay one step ahead of those who might try to take advantage of you. Stay safe, stay secure, and keep fighting for what's right!

Licensing and Use

How To INFOSEC & OPSEC; a 50501 Movement Handbook for Protesters and Organizers by the 50501 Movement is marked with CC0 1.0 Universal. To view a copy of this license, visit https://creativecommons.org/publicdomain/zero/1.0/

By marking the work with a CC0 public domain dedication, the creator is giving up their copyright and allowing reusers to distribute, remix, adapt, and build upon the material in any medium or format, even for commercial purposes.

Please share widely. This Document will continue to be itterated upon.