On this page

Security Essentials

Last reviewed on **January 29, 2026** Takes about **45 minutes**

Every click, message, and location ping creates a digital trail that can be used against activists and organizers. Law enforcement regularly demands data from tech companies to identify and surveil people working for social change.

This guide helps you minimize your digital trail. These steps won't make you invisible, but they'll make it substantially harder for authorities to:

- Track your location and movement patterns
- Monitor your communications and political discussions
- Map your relationships and networks
- Build profiles of your activities and associations

Baseline protections

Expand all

EVERYONE This section is for anyone doing activism or advocacy work.

- [ ] **Use Signal for encrypted texts and calls, especially your activism and political conversations**
  Normal calls and texts are not private and can be easily surveilled and turned over to law enforcement
- [ ] Important **Change your default settings so all new Signal threads have disappearing messaged enabled**
  This keeps everyone safer if someone's phone is ever confiscated or breached.
- [ ] **Use privacy-focused browser for everyday browsing (instead of Chrome)**
  Minimize tracking, so there's less of a digital trail.
- [ ] **Install the latest software updates for your laptop, phone, and apps**
  The latest updates for your computer, phone, and apps all contain security fixes that help keep your system safe from attackers.
- [ ] **Ditch Google Search and use a search engine like Brave Search instead**
  Your search history tells a lot about your interests and political leanings.
- [ ] **Use a privacy-focused map/navigation app (Apple Maps or Magic Earth)**
  Protect yourself from Google turning over your data to law enforcement
- [ ] **Revoke location permissions from individual apps that don't need it (which is most of them)**
  Protect yourself from apps with location access giving the government or data brokers a detailed log of your movements
- [ ] **Protect yourself from doxxing (online harassment) by removing yourself from "people search" sites**
  Your home address and phone number are very likely already exposed on dozens of websites.
- [ ] **Use a password manager with strong passwords**
  When you use the same password on multiple sites and one site gets hacked, a hacker can gain access to many other accounts. If you use a weak password, the cops will have an easier time targeting you.
- [ ] **Enable two-factor authentication**
  If someone steals your password, two-factor authentication keeps them from being able to get in unless they have your phone too.
- [ ] **Set your phone passcode to 8 to 10 random digits**
  It takes years for cops to crack an 8-digit random passcode. They can probably guess your current passcode in less than 5 minutes with automated tools.
- [ ] **Use Proton Docs and Mail for activism instead of Google Docs and Gmail**
  Protect yourself and your community from government data demands that you don't know about.
- [ ] **Enable encryption on your laptop**
  Ensure your laptop is encrypted and secured with sufficiently strong password.

Enhanced protections

Expand all

MEDIUM-THREAT This section is for you if you are in a leadership role or you are doing activism that is more likely be targetted by the state or your opposition.

- [ ] **Disable Advertising ID (which can let cops track your location)**
  Law enforcement uses tools rely on your advertising ID to track you
- [ ] **Install a trusted VPN with ad-blocking to make it harder for cops to do warantless surviillance**
  A VPN makes it harder for websites to track you and prevents your internet provider from logging your traffic.
- [ ] **Enable Lockdown Mode (iPhone) or Advanced Protection (Google & Android)**
- [ ] **Remove smart home speakers from your home (Alexa, Google Home, etc)**
- [ ] **Follow our phone security checklist**
- [ ] **Leave Signal groups that might put others at risk**
  This helps protect your network if your phone is confiscated.
- [ ] **Don't click suspicious links**
  You can protect yourself against spyware by being cautious about what you click on
- [ ] **Avoid using “Sign in with [Google, Facebook, etc]”**

Keep learning with these related guides

Prepare for a protest
Digital security for anyone attending a protest.
View checklist →

Signal security
Secure your Signal messaging app for safer communications.
View checklist →

Have Questions?

Let us know if you have questions or feedback so we can make these guides as useful as possible.

Type your question... Send