Security Essentials

Last updated on **July 18, 2026** Takes about **45 minutes**

ACTIVIST CHECKLIST

The steps that protect activists most: use Signal for messaging, turn off location sharing for apps that do not need it, switch to a privacy-focused browser like Brave and search engine like DuckDuckGo, and set a strong phone passcode. These cover the biggest risks. The rest of the checklist is for people ready to go further.

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

Easier with a crew. Most people mean to get around to these steps and never do. Consider working through this list with friends at a security party: 90 minutes, some snacks, and actual progress that helps make your whole community safer.

Get started

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

These four steps take under 30 minutes and give you the biggest privacy gains immediately. Start here before anything else.

Disable Advertising ID (which can let cops track your location)

Law enforcement uses tools that rely on your advertising ID to track you

We know that ICE and other law enforcement agencies are using location tracking tools that partially rely on the "advertising ID" that your phone provides. These tools are often using these to repress social movements.

Advertising IDs have also been used to pick targets for spyware that gets delivered through ads.

iPhones have this feature disabled by default. On Android, it is on by default and needs to be disabled.

HOW TO DISABLE ADVERTISING ID

IPHONE

Settings → **Privacy & Security** → **Tracking** → **Disable app tracking**

By default, iPhones already have this setting disabled. But you can double-check to make sure.

ANDROID

Settings → Click the search icon and search for "ads" or "advertising" → Tap **Delete advertising ID**

This setting is different on different phones, so searching is easiest.

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

DO: Turn off location tracking for most apps

DO NOT: Let every app know where you are

HOW TO REVIEW LOCATION PERMISSIONS ON IPHONE

1. Go to **Settings** → **Privacy & Security** → **Location Services**
2. Review each app and set to one of these options:
   - **Never: Best choice for most apps**
   - Ask Next Time Or When I Share: Good for apps you rarely need location for
   - While Using the App: Only for essential navigation apps
   - Always: Almost no app should have this permission
3. Make sure to set the **Camera** app to "**Never**" so you don't risk revealing your location when you share or upload photos.
4. Go to the app labeled **System Services** → **Disable Significant Locations**

HOW TO REVIEW LOCATION PERMISSIONS ON ANDROID

1. Go to **Settings** → **Privacy** → **Permission manager** → **Location**
2. Review each app and set to one of these options:
   - **Don't allow: Best choice for most apps**
   - Ask every time: Good for apps you rarely need location for
   - Allow only while using the app: Only for essential navigation apps
   - Allow all the time: Almost no app should have this permission

It is especially important to disable location tracking for your camera/photos app

These apps might genuinely need location while in use:

- Navigation (Apple Maps, Magic Earth, CoMaps)
- Ride-sharing (but only while actively using)

Some apps might need temporary permission:

- Food delivery apps only need location when you're actually ordering

Apps that definitely do NOT need location access:

- Photo apps
- Social media apps
- Games
- Most shopping apps
- Banking apps
- News apps
- Most productivity apps

Remember: Every app with location access is a potential privacy leak. When in doubt, disable location and only re-enable if you find you actually need it.

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

DO: Use Signal	DO NOT: Use Facebook Messenger, Telegram, regular texts, etc. (Avoid WhatsApp if possible)

Most normal texts and calls can be observed by your cell phone provider and the government. Telegram is incredibly insecure. (See below for our thoughts on WhatsApp.)

Signal is the best option to keep your messages secure and to keep who you are talking to private.

HOW TO SET UP SIGNAL

1. Install Signal on your phone.
2. You can now message your existing contacts using their phone number (they must have Signal installed as well). If you're messaging someone new who you don't yet have trust with, you should exchange usernames instead of phone numbers when possible.
3. To start a new message: Press the "Create" icon in the top right of Signal, then type in either the person's phone number or username
4. Enable disappearing messages by default: Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Disappearing Messages** → set to your desired time.
5. Follow the Signal Security Checklist to make sure you have the most security and privacy

When to use Signal

Some examples of when you would especially want to use Signal

- Discussing a protest/action that is not public
- Organizing a protest/action that is public, but the organizers want to protect their privacy
- Criticizing the government or other power-holders

Keep speaking out publicly! Moving some conversations to Signal for security isn't about going silent—it's about organizing safely while still voicing criticism of power holders openly. Do not obey in advance.

What about WhatsApp? (Avoid it if you can, use it if you must)

WhatsApp messages are secured with the encryption method developed by Signal, so the contents of your messages are secure. However, Meta harvests a lot of information about who you are talking to, how often, and what groups you're in. In 2024 alone, they turned over data for 78% of government requests. Your messages are safe, but who you are communicating with is not. It is an option to consider if the community you're working with is unlikely to move to Signal. It is safer than normal texts, Telegram, etc. If you do use WhatsApp, follow our WhatsApp security checklist to turn on Strict Account Settings and lock down your privacy settings.

- [ ] Important **Change your default settings so all new Signal threads have disappearing messages enabled**

  This keeps everyone safer if someone's phone is ever confiscated or breached.

The best upgrade everyone can make to their use of Signal is to make sure that disappearing messages are enabled ***by default***. Most activists we talk to haven't enabled this by default. (And most people forget to enable it manually for each new thread.)

This keeps you safe and other people safe. We don't know who's phone will be seized by law enforcement. Even if we believe we're talking about perfectly legal things, the government can find ways to twist our words to attempt to make a case against us for our dissent

There are two things to track related to disappearing messages:

1. **First, change your default** so any thread you make has this feature enabled.
2. **Second, make sure it is enabled for threads that other people start:** if someone else starts the thread, it may not have disappearing messages enabled. You may need to enable it.

HOW TO ENABLE DISAPPEARING MESSAGES

1. **To change the default:** Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Disappearing Messages** → set to your desired time (longer or shorter depending on your risk tolerance).
2. **(Android-only) Change your message retention limit:** This will delete messages on threads even that don't have disappearing messages turned on. (They will only be deleted on your device.) Open Signal → Tap your profile picture → **Settings** → **Data and storage** → **Manage storage** → **Keep Messages** → set to your desired max timeframe. Go back a screen and enable **Apply limits to linked devices**.
3. **To change existing threads:** Signal → Open the message thread you want to change → Click on the person's name (or group name) at the top of the screen → **Disappearing Messages** → set to your desired time.
4. **Delete old messages/threads:** Disappearing messages does NOT apply retroactively. So you may want to delete old threads on your phone. This will not delete them on other people's phones, unfortunately. So if it is very sensitive, you may need to ask them to also manually delete the thread. (And while you're at it, encourage them to turn on disappearing messages by default!)

Choosing your disappearing message time: How long you set your disappearing times depends on the sensitivity of your messages. A question you might ask yourself is "if someone's device was confiscated or hacked, how important is it that these messages are not accessible?"

- For chatting about low-risk things with friends, you might choose 4 weeks.
- For standard political organizing, you might choose 1 week.
- For a higer-risk actions, you might set it to 1 day or 1 hour or 5 minutes, so the messages are gone before the action starts.

Note: Messages only disappear after the message has been read. So if the recipient doesn't read it for 2 weeks, and you have disappearing messages set to 4 weeks, it will actually disappear 6 weeks after you sent it.

Use privacy-focused browser for everyday browsing (instead of Chrome)

Minimize tracking, so there's less of a digital trail.

DO: Use **Brave Browser** (easiest) or **Firefox** (more setup required)

DO NOT: Use Google Chrome, Microsoft Edge, etc.

We recommend **Brave** because it offers the most privacy without any additional configuration, which is our goal on this site.

Bonus Brave configuration tips:

- Install Privacy Badger for some added protection.
- You can install the iPhone or Android Brave app as well.

Other browser options:

HOW TO SET UP BRAVE BROWSER

Brave is a privacy-focused browser that allows you to install Google Chrome extensions.

1. **Install Brave** on your computer (or phone).
2. Follow the steps after you launch to import your configuration from Chrome or another browser. (See warning below about how plugins make you more identifiable.)
3. **Configure privacy settings:** On the desktop browser, go to Brave → **Settings** → **Shields** then select the following: (The mobile app will not have all these settings)
   - Select **Aggressive** under "Trackers & ads blocking"
   - Select **Strict** under "Upgrade connections to HTTPS"
   - Uncheck everything under **Social media blocking**
   - (Optional) Enable **Forget me when I close this site.** (On the mobile app, the settings is called "Shred Site Data") The site won't be able to store anything about you after you reset your browser.

     This will make it harder for sites to track you across the internet. It's good for privacy, but you'll want to manually override this for specific sites. Visit the site → Click the Brave (lion) logo in the URL bar → **Advanced controls** → **Disable Forget me when I close this site**

Optional:

1. Disable the annoying new tab page: Brave → **Settings** → **Get started** → **New Tab Page** → Select **Blank page** from the dropdown
2. Disable toolbar items: Brave → **Settings** → **Appearance** → **Toolbar** → Disable all the toolbar buttons that you don't want (Brave Rewards, VPN, Wallet, Leo AI, etc)

Plugins warning: Every plugin you install makes your browser stand out from "the crowd" and makes you more identifiable, reducing the effectiveness of the privacy features built-in to Brave.

- **Firefox** can offer even more privacy if you take the time to install the right plugins and configure it properly.
- Use **Tor Browser** for highly sensitive browsing that is truly anonymous

Ditch Google Search and use a search engine like Brave Search instead

Your search history tells a lot about your interests and political leanings.

DO: Use a privacy-respecting search engine like **Brave Search** or **DuckDuckGo**.

DO NOT: Use Google Search, Bing, Yahoo, etc.

- **Brave Search** tends to have better results and we trust them, but some folks don't align with their business model
- **DuckDuckGo** results aren't as reliable but it has a slightly stronger privacy record.

HOW TO SET UP PRIVATE SEARCH

- **Brave Search:** If you're using Brave browser, it's the default. If you're using another browser, you can follow these instructions.
- **DuckDuckGo:** Follow these instructions to make DuckDuckGo your default search engine.

Use a privacy-focused map/navigation app (Apple Maps or Magic Earth)

Protect yourself from Google turning over your data to law enforcement

DO: Use **Apple Maps** (iPhone-only) or **Magic Earth** (free)

DO NOT: Use Google Maps

Your location history reveals a lot about your interests, friends, and political activity. It can also be used against you in court.

Your phone is always revealing your approximate location to your cell provider because it knows what cell tower you are connected to. But any app you give your exact GPS location to has much more detail.

You can protect yourself by using a mapping app that is more privacy-preserving.

Apple Maps (iPhone only) offers privacy protections that are stronger than you might expect and is much more private than Google. However, as a big tech company, it's best for everyday use rather than sensitive organizing. We recommend it because it provides live traffic and public transportation features that privacy-focused alternatives lack.

HOW TO SET UP APPLE MAPS (IPHONE ONLY)

1. Apple Maps is installed by default (you can re-install it if you removed it).
2. Go to **Settings** → **Privacy & Security** → **Location Services** → **System Services**, then disable **iPhone Analytics**, **Routing & Traffic**, and **Improve Maps**.

Magic Earth (iPhone or Android; free) offers strong privacy. It is much easier to use than our other cross-platform suggestion (CoMaps). Some features are only available in the paid version, though.

HOW TO SET UP MAGIC EARTH (IPHONE OR ANDROID)

1. Install Magic Earth (free; paid for live traffic)
2. It functions mostly like Google Maps or Apple Maps!

CoMaps (iPhone or Android; free) is less user-friendly than Magic Earth or Apple Maps, but has the strongest privacy promises. You can operate it entirely offline, which is especially helpful for activists doing sensitive work. That said, it doesn't have live traffic data or public transit routes, which makes it hard to use as your main navigation app.

Baseline protections

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

Keep your phone (and laptop) updated to the latest operating system version

Protects you from hackers, spyware, and the phone hacking tools the cops use.

DO: Install updates as soon as you're prompted

DO NOT: Keep pushing the "update later" button

Every time a new operating system update comes out, it is fixing security holes. Each update you haven't installed represents a longer list of ways the cops can hack into your device. Think of it as a big building with more and more doors left unlocked.

If your operating system is not up-to-date, many of the other recommendations in this guide will not protect your data.

Start with your phone. If you're doing something higher risk, make sure to update all your devices.

HOW TO RUN UPDATES

Because security updates are so important, **we designed a tool to walk you through the process**.

Check your phone and computer updates →

HOW TO RUN UPDATES MANUALLY

If you prefer to run updates manually, here is how to do it for each device:

Click to show the manual steps

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.

"People search" sites collect and publish profiles on all of us including our name, addresses, phone numbers, profile photos, email addresses, and social media accounts. The checklist linked below shows you how to remove yourself

Doxxing is an increasingly common tactic used against activists where a bad actor posts your email/phone/address/etc with an intent to get others to harass you online and sometimes in-person.

HOW TO PROTECT YOURSELF AGAINST DOXXING

1. Start by completing the **first three items** on our Doxxing Defense checklist.

   Doxxing Defense Checklist →

2. After that, start working through the rest of that checklist.

Use a password manager with unique 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.

DO: We recommend 1Password ($3/month) or Bitwarden (free)

DO NOT: Re-use passwords or use passwords generated by AI. We don't recommend using LastPass.

If you have the time, using a password manager is the best option because it will automatically help you generate strong, random, unique passwords for each site/app/account.

If you have to choose between strong passwords (long, random) and unique passwords (not re-using the same password between sites), it's better to choose unique passwords. This will help prevent a stolen password on one site from effecting all your other sites.

Our tool recommendations are:

- **1Password**: Very user-friendly. Slightly more secure. Costs $3/month.
- **Bitwarden**: Free. Still quite secure.

HOW TO SET UP 1PASSWORD

1. **Download:** Download and install 1Password ($3/month)
2. **Master password:** Create a strong, random "master password" using a passphrase generator. It should be memorable, but not a password you use anywhere else. Write your master password down on paper rather than storing it digitally. Set a reminder to destroy the paper in a few weeks once you have it memorized.
3. **Import:** Import your existing passwords from your computer or browser
4. **Apps:** Install the browser extension and mobile app (iPhone, Android) to help you save and autofill passwords
5. **Change passwords:** If you had been re-using similar passwords, update your most important ones using the random password generator built-in to 1Password.

See 1Password's getting started guide for a video of these steps.

Bonus: Here's a good introduction on how to get the most out of 1Password.

Alternative options:

- Proton Pass: has a free option
- KeePassXC: Open-source and allows you to store passwords only on your machine instead of the cloud, but the user interface is very clunky.

☐ 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.

DO: Enable two-factor authentication for important sites

DO NOT: Use only a password

After entering your password, you'll need to enter a code from your phone to prove it's really you. Think of it like having both a key and an alarm code to get into your house—someone needs both to get in.

Your email is the most important account to protect with two-factor authentication. If an attacker gets access to your email, they can reset all your other passwords.

HOW TO SET UP

Install an authenticator app:

1. **Option 1: 1Password:** If you're using 1Password, it has an "authenticator" feature built-in (details here).
2. **Option 2: Ente Auth:** Install Ente Auth (iPhone, Android)
   - Optional: You can create an account. Your data is end-to-end encrypted. Or you can not have an account, but you may lose your one time passwords if your phone is not backed up.

To set up two-factor authentication:

1. Go to Security/Privacy settings
2. Look for "2FA" or "two-factor authentication" or "multi-factor authentication"
3. If an “authenticator app” option is available, select that! (Remember to save the backup codes somewhere secure, like your password manager.)
4. If “text/SMS verification” is the only option, select that and follow the instructions.
5. Links to set up 2FA on common sites:
   - Google
   - Apple ID
   - Facebook
   - Twitter / X
   - Instagram
   - Or look up whether a website/service/app has 2FA on the 2FA Directory.

Note: When a service allows you to choose between an **authenticator app** and **SMS text message verification codes,** opting for the authenticator app is always best. It’s possible for an attacker to intercept your SMS texts.

☐ 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.

DO: Use a **random passcode generator** to create an 8 to 10-digit code

DO NOT: Use any passcode you thought of yourself (dates, patterns on the keyboard, etc.). Do not use 6-digit passcodes if possible.

HOW TO CHANGE YOUR PASSCODE

1. Generate a random 8 to 10-digit passcode using this random passcode generator. (Don't make one up yourself—humans are bad at choosing randomly!)
2. Change your passcode:

   IPHONE

   Settings → **Face ID & Passcode** → **Change Passcode** → **Passcode Options** → **Custom Numeric Code**

   ANDROID

   Settings → **Security** → **Screen Lock** → Enter Current Lock → **PIN/Password** → Enter a Passcode
3. **Practice the new passcode** at least 10 times in a row right now so you are more likely to remember it. (Disabling biometrics will force a passcode request every time you lock the phone.)
4. Write your new passcode on paper and keep it somewhere safe at home until you've memorized it. Then destroy it after 2–3 weeks. Setting a reminder on your phone can help.

How long does it take to crack a passcode?

TYPE	TIME IT TAKES TO CRACK (AVERAGE)	EXAMPLE
6-digit *easy-to-guess* pattern	**Less than 24 hours** to crack	*333666 (common pattern)* or *110585 (date pattern for Nov 5, 1982)*
6-digit *random* code	**200 days** to crack	*238253*
8-digit *random* code	**40+ years** to crack	*34780026*

Note: These times only apply to phones. Computers can be cracked much more quickly, and need much stronger passwords.

Sources: The estimates in the table above assume real-world observed attempts/second from police forensic hacking tools. If you need more security, use a 10-digit passcode, which will protect you even under the highest-possible cracking scenarios. See the sources linked in the passcode FAQ here.

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.

DO: Use **Proton Docs** and **Proton Mail**

DO NOT: Use Google Docs and Gmail for activism communications

Tech companies (like Google) often receive government demands to turn over all the account data for an activist. This often includes a "gag order" which means the company can't tell the user until months or years later.

Encrypted cloud tools like Proton Mail, Drive, Docs, and Sheets ensure the company doesn't hold readable copies of your data to hand over. If the government wants it, they'd need to demand it from you—giving you notice and the opportunity to challenge it with legal support.

Limitations of encrypted email: Proton encrypts everything on their servers. But encryption only protects both ends if the recipient also uses encrypted email. If you email a Gmail user, Google has a copy they can hand over.

For sensitive communication, always use Signal with disappearing messages enabled.

HOW TO SET UP AND USE PROTON DOCS AND PROTON MAIL

Create a Proton account

> **Suggestion:** Choose a random username and random display name. so you have the option of not revealing you share this email address.

1. **Sign up** for a free Proton account.
2. **Verify:** When asked to verify if you are a human, choose the “CAPTCHA” option rather than the “email” option, so you don't link your true identity.
3. When asked to set your phone number / email as a recovery method, choose **Maybe later.**

Use Proton Drive/Docs/Sheets

- **Create and edit** documents collaboratively much like Google Docs. Someone must have a Proton account to be shared directly.
- **Share securely:** Only use "share by link" when necessary, set a document password, set the "public link" to have an expiration date.

Use Proton Mail

- **Use Proton Mail for:** website accounts, newsletters, public-facing communications needing anonymity, and non-sensitive organizing work.
- **Don't use any email for:** truly sensitive communications that might put someone at legal risk.
- **What gets encrypted vs not:** Messages between Proton Mail users are automatically end-to-end encrypted. Messages to people using a different email provider will not be encrypted, but you can send a password-protected email.

CryptPad is another popular encrypted doc option, but it is very difficult to use. If it has features you need, it accomplishes the same result.

> **Using Proton safely:** Proton is a big upgrade over Gmail/Google Docs, but it has real limitations you should know about. See our guide to using Proton safely for what's encrypted, what's not, and how to avoid common pitfalls.

Enhanced protections

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

Enable encryption on your laptop

Ensure your laptop is encrypted and secured with a sufficiently strong password.

If you have a strong password, disable face/fingerprint unlock, and enable disk encryption, your laptop and other devices will be very hard to access. **Encryption** is an essential part of these defenses. Without it, your password and other steps are basically meaningless if the state seizes your device.

HOW TO ENABLE ENCRYPTION ON YOUR LAPTOP (AND BACKUPS)

Encryption may need to be enabled on your laptop:

MACOS

System Settings → **Privacy & Security** [scroll to bottom] → **FileVault** → Click **Turn on...**

Save the **Recovery Key** in your password manager or somewhere secure. For maximum security, do not enable recovery using iCloud (but you will be required to remember your password and never lose it!)

WINDOWS

Settings → **Privacy & Security** → **Device encryption** → **Enable**

Also, make sure you have encryption turned on for your **external hard drives** and any backups you create.

Phone encryption: iPhones and modern Android phones are already encrypted by default.

Enable Lockdown Mode (iPhone) or Advanced Protection (Google & Android)

Spyware is an advanced type of attack, exploiting sophisticated vulnerabilities on our devices. In response, Apple and Google have introduced an advanced security mode that offers enhanced protection against spyware.

On iPhones, it's called **Lockdown Mode** and on Android, it's called **Advanced Protection Program**. (You can also enable Advanced Protection Program on just your Google Account even if you don't have an Android phone.)

We have **no reports** of anyone getting infected with spyware who had Apple's Lockdown Mode enabled. Android's Advanced Protection is more recent and its effectiveness has yet to be tested.

Usability trade-offs: Both features come with some functionality sacrifices. See the full list of trade-offs. If you encounter issues that don't work for your needs, you can always disable the feature later.

HOW TO ENABLE LOCKDOWN MODE FOR IPHONES

IPHONE

Settings → **Privacy & Security** → **Lockdown Mode** → **Enable**

This feature is available for iOS version 16 and above.

HOW TO ENABLE ADVANCED PROTECTION ON ANDROID

ANDROID

Settings → **Security & Privacy** → under **Other Settings** tap **Advanced Protection**

Note: The location of this setting may vary between Android devices, so we recommend searching for 'Advanced Protection' in the Settings search bar.

This feature is available for Android 16 and above.

Remove smart home speakers from your home (Alexa, Google Home, etc)

If you're in a higher risk category, you should be conscious anytime you're talking about political activity around a microphone. This includes laptops, phones, smart watches, and **smart speakers**.

Risks: These devices have microphones that are always listening.

Protecting yourself: Removing smart speakers from your home is one easy step to take to reduce the likelihood of surveillance.

Most of us are not being actively surveilled most of the time, but it is safer to get into the habit of assuming you might be. Once you're used to it, it doesn't take much work.

HOW TO REMOVE SMART SPEAKERS

1. Just get rid of the **smart speakers** and anything that **has a microphone and is internet-connected**. Look for phrases like "voice control," "works with Alexa/Google Assistant," or "built-in assistant". This includes:
   - Amazon Alexa (Echo, Dot, etc)
   - Google Nest Speaker, Google Home
   - Sonos and other home speakers
   - Smart thermostats (some newer models have microphones and voice assistants built-in)
   - Smart TVs or streaming devices (Look into whether yours has a microphone built-in or not. If so, try to replace it.)
2. If you need a speaker for music, search for something that doesn't include a microphone at all. Or a simple bluetooth portable speaker that might have a microphone, but isn't internet connected (and gets turned off when not in use).

If you're replacing a product, try to buy used to reduce e-waste and resource extraction.

Background:

- In 2017 we learned of the CIA developing a hack for some smart TV to be always listening even when they appeared to be off.
- Amazon also frequently receives legal requests for smart speaker recordings from law enforcement.

☐ Complete our guide to secure your phone

As an organizer of an action, you're much more likely to be the target of state surveillance, so it's important to take more precautions.

HOW TO

Do everything in the Prepare for a Protest checklist (including the "enhanced security" section)

☐ Leave Signal groups that might put others at risk

This helps protect your network if your phone is confiscated.

If your phone is confiscated by law enforcement, one of the biggest risks is exposing your entire network. Even if people aren't using their real name on their Signal account, there is still a unique ID behind every Signal username. And the cops can use this to correlate someone's identity across many seized devices.

You need to both leave AND delete the group:

- If you only leave the group, old messages stay on your phone as well as the history of who was in the group.
- If you only delete the group, new messages will still come through and the thread re-appears.

HOW TO LEAVE AND DELETE A SIGNAL GROUP

1. **Make a plan to re-join afterwards:** When headed into a situation with possible arrest, make a list on paper at home or somewhere safe of all the groups and who you need to message who can re-add you after the action or border-crossing is complete.
2. **To leave the group:** Signal → [Group] → Tap the group icon at the top → **Leave group**
   - If you're the only admin, you have to either remove all members or assign another admin.
3. **To delete the group from your phone:** Signal → Main screen → Swipe left on the thread → **Delete**
   - This won't delete it for anyone else.

Security hygiene tips:

- Set a recurring reminder to clean up your Signal thread every 3 months.
- Make sure you take note of which groups you are leaving and who you can ask to re-add you after the action.

Note: If you find this process very annoying and cumbersome (because it is!), that's another good reason to use a secondary phone for actions. That phone would only ever be in the one or two groups needed to pull off the action that day.

Don't click suspicious links

You can protect yourself against spyware by being cautious about what you click on

Spyware often arrives through a text or email with a link custom-designed to feel impossible to ignore, specifically for you. These aren't random spam - they're personalized attacks that exploit what matters most to you.

HOW TO CATCH AND RESPOND TO SUSPICIOUS LINKS

When in doubt: *Do not click the link!*

1. Instead, contact the sender (whether a business or a friend) through a different method (call them, use a different app) to verify they actually sent it. Taking 2 minutes to verify is always better than clicking and compromising your device.
2. If it is a shortened URL like bit.ly or tinyurl.com, you can use ExpandURL.net to view the destination page, but this provides no guarantee that the page isn't spyware. It just helps you view the true URL so you can make a better assessment of whether you trust it.
3. To check whether a link has already been flagged as malicious, you can paste it into a phishing and malware database like VirusTotal (owned by Google/Alphabet). Only submit links that are public and non-personal, because VirusTotal is a public repository that anyone can search.

Red flags to watch for:

- **Messages from numbers you don't recognize:** We all get messages from services that aren't in our contact book often, so it can take work to discern whether this is a legitimate message or not. If it's someone not in your contact book, approach it with more caution.
- **Urgency or fear**: "Your account will be locked," "Urgent security alert," "Family emergency"
- **Unfamiliar domain name:** Spyware texts often come from weird domains like `adsmetrics[.]co`
- **Too personal**: References your activism, recent events you attended, or people you know - designed to bypass your critical thinking
- **Unexpected messages**: A contact sends a link with no context, unusual phrasing, or at a strange time (their account may be compromised)
- **Shortened URLs**: `bit.ly`, `tinyurl.com`, or other link shorteners that hide the real destination
- **Slight misspellings in the URL**: `goog1e.com` instead of `google.com`

Spyware messages can be highly targeted. Here are some real-world examples of how Pegasus Spyware has been deployed:

> "Dear Carmen my brother died in an accident, I'm devastated, I send you the information about the funeral, I hope you can come: [spyware link]" (source)

> USEMBASSY.GOV/ WE DETECTED A PROBLEM WITH YOUR VISA PLEASE GO PROMPTLY TO THE EMBASSY. SEE DETAILS [spyware link] (source)

> LX 1955 BCN-ZRH 26Jun2020 - Click on the link to receive your mobile boarding pass [spyware link] (source)

Be aware: Some spyware is deployed using exploits that don't require you clicking a link at all ("zero click exploits"). These might show up as missed calls on WhatsApp, for example.

☐ Avoid using "Sign in with [Google, Facebook, etc]"

DO: Create an actual account with your email address when signing up on a new site

DO NOT: Use "Sign in with [Google, Facebook, etc]"

Every time you use "Sign in with Google" (or similar options) you're letting Google track which services you use and connect them to your real identity. Creating separate accounts with unique passwords (using your password manager) makes it harder for corporations and authorities to build a complete picture of your online activities.

Keep learning with these related guides

Prepare for a protest

Digital security for anyone attending a protest.

Signal security

Secure your Signal messaging app for safer communications.

- VPNs for activists 14 min read
- Security update checker
- How to use Proton safely 15 min read
- Remove link tracking 3 min read
- Is Signal secure? 4 min read
- Is Apple Intelligence reading my Signal messages? 5 min read