# STEP 1:

# TURN OFF YOUR PHONE

THE FRIENDLY NEIGHBORHOOD HACKER'S

## GUIDE TO ACTIVIST DIGITAL SECURITY

TurnOffYourPhone.org

v1.0.1
2025-Oct-08

# What is this?

This is a guide for navigating digital and operational security in our current moment, written by a small group of autonomous organizers who started asking a friendly neighborhood hacker or two for cybersecurity advice after seeing some questionable tips floating around their Signal chats.

There's a quick-start list of easy actionable items for individuals participating in protests to quickly secure their mobile devices, along with more comprehensive steps for individuals who want to ensure their privacy and/or anonymity online and in real life, and protocols for organizers and groups who are planning actions and are at risk of being harassed by opposing groups and law enforcement. This guide has short checklists for people who are not tech savvy, but also has enough information for people who want to learn more about what they're doing and to understand why we're making these specific recommendations.

Other privacy guides have been written to be broad and surface level so that they can be adapted across different technologies and locales, leaving it up to the reader to figure out what exactly they need to do. We started writing this guide specifically with 2024 New Yorkers organizing for Palestine in mind because we want to help our neighbors and comrades defend themselves against a gargantuan police force that has the resources, technology, and training of the most advanced military and intelligence apparatuses in the world. Defending against this adversary is different from hiding your browsing history from advertisers or hiding your location from an abusive partner, and the specific things required are hard to intuit for non-experts. There's a lot of information here, but don't be intimidated: you really do have options in resisting the surveillance state, and that should feel good.

We hope to help you all create safer digital practices while we fight for collective liberation.

Want to contribute your expertise or provide reader feedback on how well this guide works for you? Email us at **toolkit@fightforthefuture.org**



# Table of Contents

# Other guides

These are some of the better guides out there targeted at the same audience. Feel free to consult these as well, but our goal is to go deeper than most of them with 2025 technology in mind.

These are excellent up-to-date supplements to ours:

- Neighborhood Anarchist Collective's Activist Checklists (truly excellent)
- Jonah Aragon, The Protestor's Guide to Smartphone Security
- Equality Labs' Anti-Doxxing Guide for Activists

These EFF guides don't go deep enough on specific steps for activists, but do offer helpful context and definitions if you aren't very familiar with surveillance technology:

- EFF's Field Guide to Police Surveillance (Street Level Surveillance)
- EFF's Surveillance Self Defense Guide

Generally good resources, if less detailed on the topics we cover:

- A Practical Security Handbook for Activists and Campaigns
- Glencora Borradaile's Defend Dissent: Digital Suppression and Cryptographic Defense of Social Movements
- True Leap Press, Security Culture: A Handbook for Activists
- Protection International, Surveillance and Counter-Surveillance: For Human Rights Defenders and Their Organisation

Using Tor Browser is recommended to view these:

- No Trace Project: Digital Best Practices
- Tech Guides for Anarchists
    - Kill the Cop in Your Pocket

# Summary of General Practices

## Individual Practices, Basic (Quickstart Guide)

This a basic checklist of to-dos to maintain digital hygiene on your phone or mobile device.

This section is for people who are participating in an action who want to stay safe from police and protect themselves from surveillance. The steps you need to take depend on what you're doing. These are sufficient for most people, and are a good starting point for everyone. You can get through most of this section in one day. The later sections contain additional information for people who may face higher risks or have extra safety concerns.

You don't have to do anything wrong for law enforcement to investigate or harass you! They could mass arrest people at peaceful protests and try to read all their phones without a warrant, so you should take basic steps to make this harder for them.

### 1. Phone setup

- Have a recent iPhone if possible, iOS 18 or later
    - At least an iPhone 12 (models released 2021 or later)
    - iPhone 13 or newer is even better
    - Latest iOS on recent devices is significantly harder for law enforcement to hack
- For Android, have at least a Pixel 6 or newer if possible.
    - This is the only good choice for Android.
    - Install GrapheneOS if you can.
    - GrapheneOS is very secure and absolutely worth it if your device supports it, but installing a new OS takes some time and comfort with technology.
- **Use a passcode that is 8 or more random digits to unlock your phone**
    - Do not include your address or any dates or numbers significant to you in your passcode
    - Forensic devices will likely try combinations of numbers significant to you first
- **Turn off biometrics** (Face ID, voice recognition, and fingerprint unlocking)
    - On iPhones: *Settings* → *Face ID & Passcode* → under *Use Face ID for*, toggle every setting off
    - On Android: *Settings* → *Security & privacy* → *Device unlock* → *Face & Fingerprint Unlock*
        - Face Unlock (off)
        - Fingerprint Unlock (off)
- **Turn off Siri/Alexa/"Hey Google"**
    - On iPhones: *Settings* → *Siri* → under *Ask Siri*, turn *Listen for* to *Off*
        - *Settings* → *Siri* → *Siri & Dictation History* → *Delete Siri & Dictation History*
        - Additionally, go to the system settings for every app that may have something sensitive (e.g. Signal, maps, social media) and turn off *Siri* → *Learn from this App* and *Suggest App*

    - On Android 15: *Settings* → *Apps* → *Assistant* → *Hey Google & Voice Match* → *Hey Google* (off)
    - On Android 16: *Settings* → *Apps* → *Assistant* → *Digital Assistants from Google* → *You can turn off your digital assistant from Google at any time* (link) → *Turn off*
- **Turn off notification previews on your lock screen**
    - On iPhones: *Settings* → *Notifications* → *Show Previews*: *Never* or *When Unlocked*
    - On Android: *Settings* → *Security & privacy* → *More security & privacy* → *Notifications on lock screen* → *Show sensitive content only when unlocked*
- **Keep your operating system up to date** so known security vulnerabilities are fixed
- **Android: enable Advanced Protection** if your device supports it
    - This is a significant step up in making the phone harder to hack, either remotely or with a Cellebrite
    - *Settings* → *Security & privacy* → *Advanced Protection* → *Device Protection* (on)
- Above all, **turn your phone off when going to an action.**
    - Practice turning it off quickly.
    - Don't just rely on a Faraday bag, you must **turn it off.**
    - Something concerning happening nearby? **Turn it off.**
    - Got some unexpected visitors knocking on your door? **Turn it off.**

## 2. Phone setup, continued

- **Again, set a random 8+ digit passcode**
    - Handy list of estimates on roughly how long it takes to crack a random numeric passcode on iOS depending on length:
        - 4 digits: ~6.5 min average, ~13 min worst case
        - 6 digits: ~11.1 hrs average, ~22.2 hrs worst case
        - 8 digits: ~46 days average, ~92.5 days worst case
        - 10 digits: ~4629 days average, ~9259 days worst case
- **Set up 2-factor authentication (2FA)** if you have that option for any login
    - This involves having to enter a code from a text message, email, or an authenticator app to log in, in addition to a password.
    - This is one of the two most important things you can do to prevent your online accounts being taken over (therefore important for people not being targeted by police, too).
- **Use a password manager**
    - This is the other most important thing people need to do to prevent account compromises
    - FNH recommends Enpass
        - Use it only with local wifi sync between your laptop/phone, not through online services
        - It's safe even if someone gets access to your phone: the password database is encrypted with your main strong password, on top of your phone's storage encryption.
    - See *Preventing Online Account Compromises: Password Managers* below for more details on why/how.
- **Turn on auto factory reset**
    - On Android: *Settings* → *Lock Screen* → *Secure Lock Settings* → *Auto Factory Reset*
        - This will erase your phone data after 10-15 failed attempts at entering your passcode
    - On iPhones: *Settings* → *Face ID & Passcode* → Toggle on *Erase Data*
        - This will erase your phone data after 10 failed attempts at entering your

passcode

- **Make sure your phone locks as soon as you turn the screen off**
  - On iPhones: *Settings* → *Face ID & Passcode* → *Require Passcode*: *Immediately*
- **Audit your Privacy & Security settings**
  - On iPhones: *Settings* → *Privacy & Security*
  - Grant minimum access to apps for: Location Services, Contacts, Photos, Microphone, Camera
  - Make sure you turn off your camera app's access to location services
    - This prevents adding location metadata to photos.
    - On iPhones: *Settings* → *Location Services* → *Camera* → *Allow Location Access: Never*
    - On Android: *Camera* → *Gear icon* → *More Settings* → *Save location* (off)
  - On Android:
    - *Settings* → *Security & privacy* → *Privacy controls* → *Activity Controls* → *Web & App Activity* (off), *Timeline* (off), *Personalized Ads* (off)
    - *Settings* → *Security & privacy* → *More security & privacy* → *Android System Intelligence* → *Customize the experience using your Google Account data* (off)
    - *Settings* → *System* → *Keyboard* → *On-screen keyboard* → *Gboard* → *Privacy*, and uncheck all the sliders
    - *Settings* → *Passwords, passkeys & accounts* → *Google* → *Change* (button) → *None*
      - This will disable your saved logins in Chrome etc, but you should use a real (encrypted) password manager anyway.
    - *Settings* → *Connected devices* → *Connection Preferences* → *Quick Share* → *Who can share with you* → *Visible to nearby devices* (off)
    - This is a non-exhaustive list. Android is a privacy nightmare and you should use an iPhone if you are able. It's Google's business model to collect as much data as they can from Android; that's why it's free to phone makers.
- **Turn off iCloud, Google Backup, or other remote/cloud backup services**
  - For Apple devices, specifically turn off anything that auto uploads to iCloud, like iCloud Photos.
  - On iPhones: under *Settings* → (your name) → *iCloud* → *Saved to iCloud* , turn off any apps with sensitive data, or ideally everything
    - If you need to keep iCloud on for any apps, **turn on Advanced Data Protection** to encrypt most of your data (see *iCloud* section below)
    - *Settings* → (your name) → *iCloud* → *Advanced Data Protection* → *Turn on Advanced Data Protection*
  - On Android: *Settings* → *System* → *Backup*, and uncheck all the boxes
    - Android can encrypt your cloud backups, but it can be confusing what is included, so we don't recommend counting on it.
    - Disabling this will prevent you from storing every photo you take in the cloud, but there is no way to do this safely with Google Photos.
- **Turn off AI features**
  - iOS: *Settings* → *Apple Intelligence & Siri* and toggle off *Apple Intelligence*
  - Android: turn off and uninstall Gemini if your phone has the app

## 3. Basic Signal setup

- Read: EFF SSD: How to Use Signal

- PIN setup: Set a PIN on your Signal app so no one else can register with your phone number
    - They prompt you to do it automatically, but if you haven't, within the Signal app: *Settings* → *Account* → *Change your PIN*
- Username: Set a random username
    - Do not use your legal name or previously known handles.
    - Do not use dates or numbers that have personal significance to you.
    - Your username will allow people to search for and add you without knowing your phone number.
    - Unless you provide it, users will not be able to see your username, only your display name.
    - You can change your username whenever you need if you don't want new people contacting you with the existing one (e.g. someone posts it online for trolls).
- Display name: **Do not use your legal name!** Use initials, emojis, or other words if you can.
    - Your display name is what gets shown to your Signal contacts and groups.
    - Note: If you change your display name, **everyone in every group and DM you're in will be able to see that you changed it**, and those changes do not disappear unless the chat is deleted.
- Profile picture: If you have a short display name, you can add a profile picture for people to tell it apart.
    - Don't use a personal photo/image that can be traced back to your other online identities.
- Messages: **Set disappearing messages for all your chats as default**
    - *Settings* → *Privacy* → *Disappearing Messages*
    - Recommended: 1 week or less
    - Note: **The timer for any message doesn't start for a user until they read the message.**
    - **If you want to be sure that your message has disappeared, you have 24 hours from posting it to manually delete it for everyone in the chat.**
- **Hide your Signal call history from your call logs**
    - *Settings* → *Privacy* → *Calling* → *Show Calls in Recents* (off)
    - Otherwise your phone will show Signal names in your phone call history
- **Hide your phone number from Signal contacts**
    - *Settings* → *Privacy* → *Phone Number* → *Who Can See My Number* (Nobody)
    - You can keep *Who can find me by number* set to *Everybody* – if someone DMs you a chat request, they won't be able to see your display name or other info unless you accept the request.

## 4. Social media best practices

- Don't use your legal name on public social media.
- Do not publicly share photos and videos of the action that have identifying features – faces, tattoos, jewelry, etc. – especially if you do not have the subjects' consent.
- If you share a link from social media, **remove identifier codes from the link.**
    - These are identifiers that tell Meta what account and/or button the link was shared from.
    - e.g. Instagram links should look like this: https://www.instagram.com/reel/C7PoMC1OjhV/ and Youtube links should look something like this: https://youtu.be/2XID_W4neJo
    - If a link has something that looks like `?igshid=asldfkjsd29hf` or `?utm_source=ig_web_button_share_sheet` or `?si=ahdfjkakjc234yabsdjfbas` after following the link format above, **remove the**

**question mark and everything after it**
    - If the IG link contains `/share/`, like https://www.instagram.com/share/BADxwBrKds, the identifier is already embedded in the link; if you copy and paste that into Tor Browser, you can get one formatted as above, and remove the tracking code that way
- More detailed social media practices below

## 5. Securing your phone before and at an action

- The safest way to prevent your phone's data from being copied by cops is to **keep your phone at home** or stashed with someone else so you don't have it if you get arrested.
- The second safest way is to **keep it powered off unless you need to use it briefly**, and keep cellular data, wifi, location, and Bluetooth off unless you need to use them. Turning it off makes it much harder to crack your passcode with Cellebrite/Graykey.
- The third not-so-safe way: If you get arrested, **throw your phone away from you and to someone friendly** (and hope whoever catches it doesn't also get arrested).
- If you're going to any action with your phone:
    - Turn off biometrics and use an 8+ digit passcode to unlock your phone (**see #1 and #2**)
    - **Leave and delete any sensitive Signal chats from your phone**.
        - You can rejoin chats later if you're the one who left them.
        - If you need to retain messages and are at low risk of having your home or office searched, you can keep a copy of Signal on your computer.
        - You can also screenshot messages or copy and paste them into a text file and encrypt that file (see: *Storing/archiving sensitive files locally*).
    - **Turn off data, wifi, location and Bluetooth unless necessary.**
        - Check each time, as it may be reenabled after an OS update
    - **Keep your phone powered off.**
    - Disable Bluetooth low energy location tracking when the phone is off.
        - On iPhones: *Settings* → (your name) → *Find My* → *Find My iPhone* → *Find My network* (off)
            - Or turn off *Find My iPhone* entirely
        - On Android: *Settings* → *Security & Privacy* → *Device Finders* → *Find Hub* → *Find your offline devices* (off)
            - You should probably just entirely turn off *Allow device to be located*
    - You can buy a Faraday bag to keep your phone in.
        - This prevents low-power chips from transmitting data to other devices while your phone is off. (e.g. Find My Phone does this if you allow it, it works the same way as AirTags.)
        - This is only for extra peace of mind. You can already disable Bluetooth tracking as above.
        - Do not make your own bag, it probably won't work.
    - You can also buy tamper-evident stickers to place over the USB port of your phone.
        - If you're arrested and the tamper-evident seal is broken when your phone is returned to you, law enforcement may have attempted to plug in a device to access your phone. (Please see #6.)

## 6. What to do if you're arrested

- If you have your phone, **turn it off** if possible.
    - On iPhones: Hold both buttons down → *Slide to power off*

    - On Android: Hold down the power button
- If you use a passcode to unlock your phone (please do, see #1 and #2):
    - **Do not give your passcode to the cops** even if they ask for it
    - **Do not unlock your phone**, even to show ID, even to call your lawyer! Ask for a phone to be provided to you.
    - If they force you to give up your passcode, tell your lawyer because this might be illegal.
    - Do not unlock your phone in front of cops or in police-surveilled areas with cameras that can see you.
- If the cops get your phone:
    - There is a chance that they copied all of your phone data using a forensic device like Cellebrite or Graykey.
        - You may not know that they did this or even got a warrant to do this unless they use any evidence they found through it against you in court.
        - If they do not give you your phone back immediately upon your release, it is very likely that they have tried to do this, though they may not succeed if you have a good passcode and a good phone.
        - See #15 What You Can Assume... for more on this
    - Reset your phone (or get a new one if you're fancy).
    - Change your phone passcode.
    - You may want to change your most important passwords and log out of any active sessions (e.g. email, Apple ID, Google, CryptPad, Proton Mail)
        - Hopefully you already set up a password manager which makes this easier.
        - Changing online passwords and logging out is not the highest priority, but it is an extra precaution against anyone accessing those accounts.

# Individual Practices, Extended

This section contains additional steps that individuals can take, which are less urgent than the previous section of Basic Practices. These can be longer term changes you make to your habits, not necessarily the things you must do before going to an action.

## 7. Browser setup

- For maximum anonymity and/or searching sensitive information, **use Tor, preferably on desktop**:
    - Desktop: Tor Browser
    - iOS: Onion Browser
    - Android: Orbot
    - Routing traffic through Tor is slower, but it hides your IP address from the websites you're accessing; Tor is basically the best VPN, the only one that actually offers anonymity.
    - Logging into a site with an account that you use outside of Tor negates Tor's effectiveness, so avoid doing that.
    - Using Tor Browser is effectively the only way to be anonymous online.
    - See Tor section below
- The following recommendations are helpful for minimizing your tracking footprint to advertisers (some of whom sell their data to law enforcement):
- For general browsing **use Firefox, and install privacy extensions**
    - FNH recommends Firefox with the following extensions:
        - uBlock Origin
        - Privacy Badger
        - Adblocker Ultimate
        - Disconnect
        - Cookie AutoDelete
        - Firefox multi-account containers
        - Consent-O-Matic
    - Brave has similarly useful settings and extensions but is based on Chrome.
- General browsing settings, in order of increasing difficulty:
    - Use private windows to prevent the saving of browsing history for specific tasks
        - Note: **Your IP address is still visible in private windows**! That's why we prefer Tor.
    - Turn on **Strict** Enhanced Tracking Protection in Firefox.
        - *Preferences* → *Privacy & Security* → *Enhanced Tracking Protection* → Strict
    - Set your search engine to DuckDuckGo, only use Google as a fallback.
    - Turn off browser history entirely and set Firefox to delete cookies on exit.
    - Turn off Javascript (most secure, but most sites become hard to use)

## 8. Advanced Signal practices

- Disappearing messages
    - The more sensitive the info in the message, the shorter the time should be.

        - Use 3 days to 1 week as default
        - 1-3 days for more sensitive messages
        - 30 seconds or 5 minutes for extra sensitive
        - Again: The timer for any message doesn't start for a user until they read the message.
            - **If you want to be sure that your message has disappeared, you have 24 hours from posting it to manually delete it for everyone in the chat.**
- Message editing
    - **The safest way to edit a message is to delete it for everyone and post a new one.**
    - If you edit a message, the edit history is viewable if you tap on the word "Edited".
- Groups
    - Groups big enough that you can't mentally keep track of who's who are not considered private for sensitive information.
    - **Don't use any sensitive information in group names, avatars, or descriptions**. This can be visible even when the chat is not open, and do not disappear.
    - If you need to change your display name, do it before joining any large groups.
    - Once an action is over, **leave and delete any groups or DMs** specific to that action.
    - If you're the group admin: before removing members from the group remind them to delete the group chat once they're removed, then remove all members from the group, and then delete it from your own chats.
    - **Make sure to regularly leave and delete old and inactive chats.**

## 9. Social media privacy practices, by platform

- **Venmo**: Venmo was originally a social network, so review your personal Venmo's privacy settings, especially if you're going to use it for mutual aid.
    - Default privacy settings: Set to "Friends" or "Private"
    - Friends List: Set to "Friends" or "Private", turn off "Appear in other users' friends lists"
    - Past Transactions: "Change to Friends" or "Change All to Private"
    - Note: The above settings don't affect payment usability. And you will still be publicly searchable by your username, so choose one that isn't linked to your legal name or your private identities.
    - **If you've been doxed** and you are being harassed on Venmo, you have the option to close your Venmo account: *Settings* → *Account* → *Close Venmo Account*
- Facebook:
    - Review all of your *Audience & Visibility* settings.
    - Limit visibility on your past posts.
    - Prevent random people from sending you friend requests under *How people find and contact you*.
    - Hide your public profile info under *Followers and public content*
    - **If you've been doxed**, you can delete or temporarily deactivate your account
- Instagram
    - Profile page → hamburger menu (three lines)
        - Under *Who can see your content*:
            - **If you've been doxed**, you can go to *Account privacy* and toggle on *Private account*
            - *Crossposting* → toggle off *Recommend reels on Facebook*
        - Under *How others can interact with you*:

        - *Messages and story replies*:
            - Set *Message requests* so that only your followers can send you message requests (or so you don't receive them at all), and only people you follow can add you to group chats
            - Set *Story replies* so that only people you follow can send you story replies, or don't allow them
        - *Comments*: If you've been doxed, you can set *Allow comments from* to *Your followers*
        - *Tags and mentions*: If you've been doxed, you can toggle all of these settings off
        - *Sharing and remixes*: If you've been doxed, you can toggle all of these settings off
    - Under *Your app and media*:
        - *Device permissions*: Allow only the minimum viable permissions for you to use the app.
            - *Photos*: *Allow selected photos* instead of allowing Instagram to access all your photos, so that you can control which items in your Camera Roll Instagram is allowed to see.
            - *Contacts*: *Not allowed*
        - *Archiving and downloading*: Turn off automatically saving copies of your posts and live videos to your Camera Roll if you are sharing sensitive information.
- Likes are public; use bookmarks for saving things you don't want public.
    - Social media surveillance companies can access likes and you can't prevent this.
    - Bookmarking posts will signal that content like this should still show up in your feed, and possibly your friends' feeds, without publicly showing your interest.
- If you've been doxed in a post, you can report it for an Instagram violation:
    - Click on the horizontal shish kebab dots on the post → *Report*
        - Under *Why are you reporting this post?* you can select *Bullying or harassment* for *Me* or *Someone I know*
        - If the post is an outright threat, you can select *Violence or dangerous organizations* → *Credible threat to safety*

- Tiktok:
    - Review all of your privacy settings: Profile page → *Settings & privacy* → *Privacy*
        - Under *Discoverability*:
            - **If you've been doxed**, you can toggle on *Private account*
            - Turn off everything in *Suggest your account to others* and *Sync contacts and Facebook friends*
        - Under *Interactions*:
            - Make sure your settings are set to *Friends*, *Only you*, or *No one*
            - Focus on: Direct messages, Following list, and Liked videos
- Twitter/X:
    - **If you've been doxed**, you can deactivate your account: Left menu bar → *More* → *Settings and privacy* → *Your account* → *Download an archive of your data* and then *Deactivate your account*
    - Review all of your privacy settings: Left menu bar → *More* → *Settings and privacy*

→ *Privacy and safety*
    - *Audience, media and tagging*: Make your account private by checking *Protect your posts* and toggle *Photo tagging* off
    - *Your posts*: Make sure *Add location information to your posts* is unchecked
    - If you've been doxed, you can also use *Remove all location information attached to your posts*
    - *Direct Messages*: If you've been doxed, you can set *Allow message requests from* to *No one* (but people you follow will always be able to message you)
    - *Spaces*: You can toggle this off
    - *Discoverability and contacts*: You can uncheck all of these settings if you don't want to be found, and *Remove all contacts*
    - *Data sharing and personalization*: Uncheck everything, these settings allow Twitter to serve you personalized ads based on who and where they think you are
- **If you have been doxed in a tweet**, you can report it for a privacy violation
    - Click on the horizontal shish kebab dots on the upper right-hand corner of the tweet → *Report post*
- If you want to correct a tweet with misinformation, you can:
    - Report it for misinformation, or
    - Ask people who are active on Twitter and have the ability to add community notes to add a note that corrects the tweet

## 10. Doxing protection

- At an action:
    - **An action is only over when everyone is home.** Even at jail support and on the way home, keep your face and tattoos covered, and don't display any identifying marks or jewelry.
    - **Don't speak anyone's legal name out loud.** Whenever possible, only share legal names and personal info with a known/vetted jail support intake person in a disappearing Signal DM.
- Pre-dox
    - Review and lock down your social media privacy settings (see #9).
    - Remove your contact information from data gathering sites (listed in decreasing order of effectiveness:
        - Manually: Big Ass Data-Broker Opt-Out List
        - Optery Ultimate (paid service, expensive)
        - **EasyOptOuts** (paid service, very cost effective, recommended)
            - a few important sites aren't covered and you have to do them manually
        - Mozilla Monitor (has paid tier)
        - DeleteMe (not recommended, less effective, much more expensive)
    - If you must have public social media accounts, keep any real life social media tied to your legal name private and let your activism social media be public/anonymous.
    - Use a Google Voice number to sign up for anything requiring your phone number.
    - Read the gold standard anti-doxing guide: Equality Labs Anti-Doxing Guide for Activists
    - Another good anti-doxing guide for activists

- Post-dox
    - Again, review and lock down your social media privacy settings (see #9)

# For Organizers

This section contains further information for people who handle and communicate sensitive information. These practices are extra helpful at preventing information leaks and keeping your identify safe for those especially concerned about their privacy and their data. There are additional recommendations for Signal, meetings, and how to safely store and share important files.

Please make sure you follow **both of the** Individual Practices sections above first before continuing.

Note: The No Trace Project has a more detailed guide specifically for anarchists being targeted on their page Digital Best Practices (you may want to use Tor Browser to access this site).

## 11. Secure Signal chats

- Make sure your username, display name, and profile picture do not have any identifying information about you, your loved ones, or any other online personas you have.
- Types of group chats:
    - Public chats: no vouch
        - Random people can join just by using the link or being added by an existing member.
        - Do not say anything in the chat that you would not be comfortable getting read back to you in court.
        - Signal chats with over 150 members may begin to experience message delays.
    - Semi-vetted chats: one vouch
        - Only people who have been vouched for by at least one existing member are admitted.
        - Big-picture conversations and connections to smaller working groups often happen here.
        - Can be large, but the larger a chat is, the more likely it will have a mole.
        - Rule of thumb: Treat chat opps like Covid in December 2020 – If there are 20 or more people in a room, the likelihood of at least one person being infectious might be over 50%.
    - Action/affinity/autonomous group (AG) chats: two or more vouches
        - These chats are for planning/preparing for actions and communicating while on the ground with trusted comrades.
        - Do not create AGs of more than 10-15 trusted people per group.
        - Double/triple-vet each member before admitting by asking others who know them in person and have organized with them to vouch for them.
- Disappearing message timer
    - Make sure you, a team lead, or a remote admin can plan to adjust the disappearing message time accordingly for all action-based groups, but especially for high-risk (red/dark red) teams.
    - For planning non-sensitive details, set disappearing message time to 3-4 days.
    - For planning sensitive details, make sure the other parties are currently active on signal and set disappearing message time to 5m or 30s.
    - For the day of, set disappearing message time to 1-3 hours or fewer.
    - If you're on the ground and there is police activity, set disappearing message time to 1

hour or as short as possible.
    - Again: **The timer for any message doesn't start for a user until they read the message.**
        - **If you want to be sure that your message has disappeared, you have 24 hours from posting it to manually delete it for everyone in the chat.**

## 12. Secure meetings

- The most secure meetings are fewer than ten vetted people, in person, with
    - no devices present, or
    - devices turned off and stored in Faraday bags before arriving to the meeting location, which should have ideally been scouted for surveillance equipment in advance.
- If you can't do that, here are some safer practices for virtual meetings:
    - Separate action members into small teams of 10-15 max in your Signal chats if you haven't already.
        - Sort them by what part of the action they're participating in and by the level of risk they're willing to take on
        - e.g. green for jail support, yellow for protestors, red & dark red for most sensitive parts of action
        - Note: The traffic light system is at best a guess – **any role can escalate into a red role at any time**
    - Make sure they know who their team leader is, but they don't need to know other organizers' info
    - If necessary, brief them group by group in a conference call (preferably Signal, but if you must, use Wire or a trusted server running Jitsi Desktop instead of Zoom) with all participants' cameras turned off by default
    - See Online Meetings section below for comparison of call/video services
- Brief each team only on what they need to know for the action
    - e.g. green teams should not know about red team-specific plans, etc.

## 13. Storing/archiving sensitive files locally or online

### Locally

Mac

- Enable FileVault to encrypt the entire drive
    - Use a login password at least 12 characters long, not made of dictionary words
- If using Time Machine, enable encrypted backups
    - 16+ character password, ideally random; store it in your password manager
    - You won't have to enter it very often
- External drives
    - Format the drive using Disk Utility
    - Use the APFS (Encrypted) filesystem with a unique password from your password manager
- Especially sensitive files can be stored with additional encryption with a different unique password (16+ characters).
    - DMG file (disk image): most convenient, only usable on Mac
        - Use Disk Utility to create an encrypted DMG file

                - Size: big enough for the files you want to store
                - Format: APFS
                - Encryption: 256-bit AES
            - Open the disk image, enter the password, put files into the disk, unmount when done.
            - Delete the unencrypted file when you're sure you've saved it in the disk image safely and stored the password.
            - You can save files directly into the mounted disk to never store an unencrypted copy.
        - Zip file: less convenient, but shareable to Windows/Linux
            - Free way: via the Terminal
                - `zip -er <output filename> <input directory/file path>`
            - $5.99 way: Keka app
            - Can't save directly to the archive, you have to put existing files into it.
            - Can't edit the files inside the archive, you have to make a new archive.
            - Note: the file names you put in the archive are still visible without the password.

Windows

- Enable Device Encryption
    - Use a password at least 12 characters long, not made of dictionary words.
- External drives
    - Enable BitLocker if your version of Windows has it.
    - Use VeraCrypt or zip files if not.
- Especially sensitive files can be stored with additional encryption with a different unique password.
    - Zip file: most widely supported
        - Use 7-zip to create an encrypted zip file.
        - Choose Zip format, not 7z, for best compatibility when sharing.
        - Delete the unencrypted file when you're sure you've saved it in the zip file safely and stored the password.
        - 7-zip lets you add/replace files to existing archives, but you can't edit a file directly without decrypting first.
        - Note: the file names you put in the archive are still visible without the password.
    - VeraCrypt: convenient when it works, harder to share
        - Can save directly into the disk image, never storing an unencrypted copy
        - Recipients need to install the software
        - Current Mac support unclear
        - Potential for bugs, breakage during Windows updates

Android

- Use EDS or EDS Lite to create a VeraCrypt container
- Use a unique password (from your password manager) to add an additional layer of

encryption over what the phone already has
- Many Android phones are easy to hack, so this would help for sensitive files
- You can share the .hc disk image to desktop for use there after installing VeraCrypt (method and support varies widely by platform)

iOS

- Use Disk Decipher to create a VeraCrypt container
- Use a unique password (from your password manager) to add an additional layer of encryption over what the phone already has
- iOS encryption is already good, but potentially irrelevant if the phone is seized when it's on
- You can share the .hc disk image to desktop for use there after installing VeraCrypt (method and support varies widely by platform)

### Online

**Never store unencrypted sensitive files in common cloud services like Dropbox, Google Drive, etc**. Even if you encrypt them yourself following the procedure above, the service can see the filename of the zip archive, which you probably are not going to randomize. Putting your files into the hands of a service like this raises the risk if you use a bad password or get careless.

CryptDrive/Cryptpad Drive or Proton Drive are reasonable options for encrypted cloud storage. The services cannot read the content of your files or the file names, assuming you have a good password on your account. For very sensitive files, additionally encrypt them yourself locally before uploading (see above).

Letting the files leave your machine is **usually** a higher risk than storing them all locally. Your machine could be seized, but you have some control over this. You can store your laptop somewhere safe, and you probably don't always carry it around. A search warrant for cloud storage is easier and faster to execute than one for your apartment.

Remote storage could be better if you have the discipline to successfully do it anonymously. Always logging in to Cryptpad over Tor makes it hard to trace back to you. If you have a Cryptpad account that truly can't be linked to your identity, storing encrypted files there would make them harder to find in the first place.

### Files that you expect to use in court

- Give a copy to your lawyer
- Advise them to store it safely, as above
- Keep an encrypted copy yourself in case theirs is lost or damaged

## 14. Sharing sensitive data

Before sending any photos or videos you've taken to anyone via a method other than Signal, **you should remove as much metadata as possible**. Your phone embeds timestamps, camera model, camera settings, and more, which most apps other than Signal do not remove. You can disable location tagging, but not the rest.

Image/video metadata removal on different platforms:

- iOS: Exif Metadata app
- Android: Photo Exif Editor
- Windows 11: via Windows Explorer
- Windows 10: ExifTool
- Mac: ExifTool

PDFs and office documents usually contain metadata about who created them. This is more difficult to remove completely. ExifTool is a good start against casual snoopers, but doesn't actually delete the data in a PDF, it basically hides it. You can have greater confidence that it will work better on other formats like images. You can use the `--linearize` option with `qpdf` to go further, but it still might not be guaranteed. mat2 is probably the best option for PDFs, but none of these have a GUI. There are various GUI tools but we have not evaluated them.

You can also take a screenshot of an image or document, which will likely remove the authorship, but may still indicate the kind of computer or phone it was taken on. Sending an image or video to yourself via Signal will definitely remove the metadata, but can decrease the quality.

Different kinds of data are best shared in different ways:

- Editable documents or any other files with trusted parties: Cryptpad/CryptDrive
    - use an instance on a server run by a trusted comrade in another country if possible
        - If not, cryptpad.fr
    - CryptPad does not require an email to register, can be used over Tor
    - Grant access to your contact's account rather than sending a link
    - Links cannot be revoked, the file must be deleted
- Files shared publicly or with less trusted parties: Proton Drive
    - Links can be disabled and changed as needed.
    - By default, anyone with the link can download the file.
    - You can disable this by setting a password for the link, which can be changed without changing the link.
    - It is not easy for the receiver to identify you based on the link, but Proton can identify the account that owns a link.
- Messaging and photos under 25MB or videos under 100MB: Signal
- Videos over 100MB: CryptDrive or Proton Drive
- Video/audio calls: Signal
- Email: Use Signal instead – why does it need to be an email?
    - If you absolutely must: For sending/receiving anonymous emails, make a free Tuta account through Tor Browser (preferably on desktop) per each new correspondant or group
    - It may take a few tries to register from different circuits/IPs
    - **Always** use Tor when you log into that account
    - Do not email yourself or any additional people else using that account
    - ProtonMail is only a useful option if you want privacy of the message body but do not need anonymity; it is almost impossible to register anonymously. Even then, content privacy is only increased if you email other Proton users or people who use

PGP/GPG.

- Sending story tips to journalists: SecureDrop if their publication offers it
    - Use Signal if not. Make sure your Signal settings do not show your phone number to people who don't already know it. Refer back to Signal setup instructions above when messaging people you don't know.

## 15. What you can assume has been done to your device if you've been arrested or targeted

- Refer to #6 What to do if you're arrested
- If you're arrested and cops hold your phone for more than a few hours:
    - Depending on the phone, it could be completely compromised. If you don't have a recent iPhone or Pixel, you may want to consider getting a new one if you would be stressed about this.
    - If your phone is on and unlocked:
        - Graykey/Cellebrite/etc can easily be used to copy the contents of your entire phone for later examination.
    - If your phone is on, even if it's locked:
        - Graykey or Cellebrite may be able to hack the phone and copy all the data on it, if you have a model that is vulnerable.
    - If your phone is off
        - iPhone 12 or Pixel 6 or newer:
            - As far as we know as of Summer 2024, iPhone 12 or newer and Pixel 6 should be safe if you have a long enough passcode and have enabled the guess limit.
        - Any other Android phone or older iPhone:
            - They can more easily try every possible passcode and can still get all the data off the phone if the passcode is not long enough, and in some cases regardless of the passcode.
            - Graykey spyware could be installed on a vulnerable phone to capture your passcode the next time you type it in. So the next time you are arrested, cops may be able to use that to extract all of your phone data. You may want to reset the phone.
    - You may not know that they got a warrant to do any of this unless they use any evidence they found on it against you in court. They may do it without a warrant and never use it in court.
- If you try to factory reset your phone and it causes errors, this may be because of spyware.
    - Contact the EFF, Citizen Lab, or Access Now because they may be interested in examining your phone.
    - This is uncommon, so you should not stress out about it excessively, but in the event it happens it is worth looking into.

# How to think about security and privacy

## Threat Modeling

Now that you've carefully followed all those instructions (right?), it's time to understand more about why we recommend these things. This will let you make up your own mind about what is most important to you in the future as you get into new situations, consider using new tools, and meet new people who might have different practices.

The most important security and privacy question to ask yourself is "What am I trying to protect, and from whom?" Then you can ask: How motivated and capable are they to find it out? What would happen if they get it? What am I willing to do to prevent that?

This is called **threat modeling**. Not every type of information carries the same risk, and not everyone who you want privacy from has the same capabilities. These people are all after different things and have wildly different abilities to get them:

- **Random people on the internet**: they can find your personal information from public sources and send trolls to harass you online or in person.
- **Your local law enforcement**: (depends where you are, but in general) they can monitor protests, use facial recognition on surveillance footage, request a lot of data from tech companies/cell carriers, use Cellebrite/Graykey/etc to hack many types of phones if they have the phone physically in hand.
- **The most sophisticated law enforcement**: the FBI has a lab in Virginia that can hack or physically access some locked phones that are not possible by podunk cops using off-the-shelf vendors, and (very) occasionally also hack some things remotely, but the FBI rarely gets involved in minor local matters.
- **The NSA and CIA**: they have the most sophisticated hackers in the world, so there is not much you personally could do to 100% stop them. But their targets are almost exclusively outside the United States and even then usually high-value. You are probably not an officer of the Russian military or an Iranian nuclear scientist. They actually don't care about what you're doing.

Examples of information you might want to protect:

- Your home or work address
- Your family members' names
- Search terms you use
- The contents of your documents and photos
- Your contacts and who you are messaging
- The fact that you are the one running a particular social media account
- The fact that you are the one posting to a blog or website
- Where you have been, where you are going to be
- What you are buying

Almost all of that can be kept secret from random people on the internet. Most of it can be kept secret from local police, but it's harder, so you have to be careful and change more habits. Similarly

for the FBI, but again it gets even harder. When you decide which things you care most about, you can focus on which of your practices you need to change.

## Security vs privacy vs anonymity

If you aren't experienced with cybersecurity, these might seem the same, but it's important to distinguish them when thinking about what you're trying to protect and from whom.

- Security: does a device or service work the way it's supposed to? Can someone who's not supposed to access it find a bug and exploit it to break in?
    - You can have a service that's secure but not private or anonymous. If it's not even secure, privacy and anonymity may be impossible.
- Privacy: what are you talking or writing about? Can the content be known to anyone besides the person you want to share it with?
    - We now have very usable tools that keep your content private.
- Anonymity: who are you, and who are you talking to?
    - This is distinct from what you are talking/writing about, and is much harder to protect consistently.

Recent iPhones and Pixels are quite secure. Most apps on them are neither private nor anonymous.

Signal has excellent privacy, and a limited amount of anonymity if you use it correctly. WhatsApp has decent privacy, but no anonymity; Meta knows who is talking to whom and is very interested in this. VPNs can offer some privacy from your cell carrier or ISP, but don't really hide your identity if law enforcement can get customer logs from them. No website is anonymous if you don't use Tor Browser, and not even then if you give the site any identifiying info, or sometimes log in without Tor.

Separating these concepts will help you think through what you are really after when you want more "privacy", and which things that people are trying to sell you will actually help.

## Technologies and techniques to defend against

Well-resourced US law enforcement have a lot of tools at their disposal to identify people they're after. We have written these recommendations with the most common ones in mind. If you want to think more deeply about what you're doing and why, you need to understand how they work. There are other technologies that you may see mentioned elsewhere, such as Stingrays/IMSI catchers, gait recognition, cell exploits, mercenary spyware, tracking phones that are off, etc. that we don't have good reason to believe are actually being widely used in the United States. These are the techniques that will be often used against you, so these are the ones to understand:

- Seizing and searching your phone
    - Forensic devices: Cellebrite UEFD, GrayKey, Axiom, Salvation Data AFA9500, etc
    - If your phone is on, even if it's encrypted with a passcode, these devices can hack many of them; there is more attack surface to exploit when it's fully booted, and the storage encryption keys stay in memory until it is turned off.
    - If your phone is off, they will have to try to brute force the passcode before it can decrypt itself.

    - Only recent iPhones and Pixels are at all resistant to this brute-force passcode search.
    - If your passcode is short, trying every possible passcode is possible in a short time.
- Requests to online services
    - Most online services keep detailed logs of your activity forever.
    - Some of them insist on seeing a warrant to give up your data (for data that would require a warrant), and some don't.
    - Requesting stored content, like your email, messages, call recordings, or photos, should require a warrant that indicates probable cause to believe you have committed a crime, if the provider insists on seeing the warrant.
    - Requesting metadata, like who you messaged, who you follow, when you logged in and from what IP, only requires a subpoena, which has a much lower standard. Services more often have to comply with this. This is usually enough to identify you.
    - You should use services that use end-to-end encryption for your content, so the provider can't give it up, like Signal, Cryptpad, and iCloud Advanced Data Protection.
    - Hide your IP from the service provider using Tor; VPNs only move this problem around, because they can know the real IP you connected from, and likely your identity from your payment. **Logging in to an account even once from your real IP is enough to identify you**.
    - See the blogging section below for how to create an email account to register for and use (some) services anonymously.
- Requests to your ISP/cell carrier
    - Your carrier/ISP knows which IP is assigned to your device/home at all times.
    - Online activity from services that log your IP can be traced back to you via your carrier.
    - There is no way to hide a phone's physical location from the cell network when it is turned on and connected. The carriers store historical logs of this.
        - Rather than using a Faraday bag, just turn the phone off to hide its location.
    - Changing the SIM card in your phone is not enough to anonymize it from the cell network. The phone itself contains an ID (IMEI) that can be linked to any other SIM cards you may use.
- Facial recognition
    - This has gotten very good recently.
    - Cameras are everywhere in public. NYPD, for example, has their own, and law enforcement usually has no trouble requesting footage from stores and doorbell cameras.
    - Even part of your face, such as your nose or eyebrows, combined with the shape of your head, might be enough to identify you in a good image, or link images from different places together.
- Requests to merchants and banks
    - ATM transactions and credit card purchases are strongly linked to your identity.
    - Transit card swipes can be linked to you if you pay for that card with a bank card.
- Automated license plate readers, or footage of a license plate
    - Cars are basically impossible to make anonymous legally.

# In-Depth (Advanced) Topics

This section contains more detailed information on how to do specific things online more safely. Once you've locked down your phone with all the instructions above, you're ready to actually get back to work, which will likely require some changes in your habits if you want to expose less information to fewer people. But the good news is that in the year 2025 we now have a lot of safer options that work, and you actually can dramatically increase your privacy and anonymity for the most important information if you do it right.

What you're doing and what you're most interested in protecting will determine which of the following sections are most relevant to you. So think about which parts of your work you are most worried about keeping private (and from whom!) and focus your energy there.

Don't be intimidated by "advanced", this is stuff that a lot of organizers need to do! But at this point we need to get a little more into the weeds of the how and why, because strong anonymity and the best security you can reasonably achieve both require more than just changing a few settings.

## How to ensure maximum privacy & anonymity for web browsing: use Tor

Tor is the only VPN-like service that actually provides strong anonymity. Your traffic is routed through constantly-changing groups of thousands of volunteer computers around the world. It's encrypted such that none of relay computers can simultaneously know your IP address **and** which site you are connecting to, and you don't need to trust anyone involved in running it. Real-world cases of law enforcement or intelligence agencies being able to identify someone who uses Tor correctly all the time are extremely rare. If you have taken some computer science courses, the original paper describing how it works is surprisingly readable.

If you've never used Tor, be aware that it can be slow, and some sites don't allow you to use it. You may get frustrated trying to watch a lot of HD videos. People do use it for normal everyday browsing activities all the time so it's totally doable, but you have to accept a little friction here and there.

**Use Tor Browser on desktop.**

**Use Onion Browser on iOS.**

**Use Tor Browser on Android.**

These are browsers you can use like Firefox or Chrome. Very straightforward. Do your web browsing through them and it will go through Tor. Only the activities you're doing in the browser will use Tor, not other apps. On mobile, make sure you're using one of the apps above; there are a bunch of knock-offs of dubious quality with similar names.

**Additional mobile option: Orbot for iOS or Android**

Orbot is better than Tor Browser in some ways, and worse in others. From the perspective of the operating system, Orbot appears to be a VPN, so essentially all apps on the phone will route their traffic through Tor. This is great when you want to use Tor, but some sites or apps won't allow it, so you have to disconnect Orbot to use them. Before disconnecting, you should close any app or site

you used Tor with, so you don't accidentally connect to it from your real IP. It's best to also use the appropriate Tor browser in combination with Orbot to avoid that when possible. If you are ever not sure whether you're currently using Tor, visit https://check.torproject.org in your browser and it will tell you.

In our experience, Orbot doesn't work very well on some older iOS devices. You can try it and see if works for you. If so, we recommend you use it along with the browsers, but the using one of browsers by itself is a very good start.

If you want to go an extra level on desktop, you can download a special OS called Tails, install it on a USB stick, and boot your computer from the USB. When using Tails, everything you do on that computer will go through Tor, not just your browser. This is for people who need top-level anonymity, if you use lots of online applications outside the browser. You'll need to be comfortable with a little technical setup and usage (it's based on Linux). If you are just getting started, don't start with this, just use Tor Browser. Nothing you download or install will be saved when you reboot, which makes it a little hard to use for daily life.

### Should you use a VPN while downloading Tor Browser/Onion Browser/Orbot?

For just downloading the apps, it's not necessary to hide it. Tor is mostly used by regular people who just want more privacy. If you have a VPN, feel free to turn it on when downloading the browser. But on a mobile device, Apple or Google will still know that you installed it from the app store anyway.

### Should you use a VPN in addition to Tor?

When using Tor, we do not recommend using a VPN at the same time. In the best case, it's mostly unnecessary and will make browsing even slower. The only benefit you get from also using a VPN is that your ISP/cell carrier will see you using a VPN instead of seeing that you are using Tor, but using Tor on its own is not suspicious in most situations where you are doing something legal. There's nothing the ISP can do about it. The VPN provider would still know that you're using Tor. In the worst case scenario, if you're doing something nonstandard like setting up your own server or configuring VPNs manually on Linux, doing things in the wrong order can negate the benefit of using Tor. If you decide to use them together, make sure to check that it's working correctly at https://check.torproject.org/.

### Do I need to use Tor bridges?

No, and you probably won't even see any reference to this when things work correctly. If you are asked if you want to use bridges, it's likely not necessary, there may just be some hiccup in your internet connection. This is usually only necessary in countries that block Tor. ISPs in the United States generally do not. If you want, you *can* use bridges to make it less obvious you're using Tor, but this is not usually something to worry about.

## iCloud: use Advanced Data Protection

TL;DR if you use iCloud, you must turn on Advanced Data Protection ASAP, no exceptions.

iCloud is obviously useful for backing things up on your iPhone like photos, notes, etc. If you have

some other method of storing copies of these yourself in an encrypted way, and you are confident in that method, that's great, use that. But most people don't, which means you are probably either using iCloud or nothing at all.

You can choose not to use iCloud (or other cloud services) if you don't want sensitive things leaving your device. Go to *Settings* → *Apple ID* → *iCloud* and uncheck every box. You will then want to manually back everything up to your computer regularly. You should set up local encryption for that computer – FileVault or Encrypted APFS Filesystem on Mac, Device Encryption/BitLocker on Windows. This is more of a pain than just automatically using the cloud, but it's doable. The biggest tradeoff is that you can't access all of your files if you have too many photos/videos to fit on the phone and can only store them on the computer. In case the computer's drive dies, you should have more than one copy of things you don't want to lose, which means you should also have a complete encrypted backup of the computer (e.g. encrypted Time Machine on Mac).

If you do want to use iCloud, there is some good news. Within the last couple of years, Apple has introduced a feature called Advanced Data Protection that allows you to encrypt most of your iCloud storage end-to-end. Only devices signed in to your account can read the files, Apple cannot, and Apple therefore cannot give them to anyone else either. Prior to this, most data stored in iCloud was visible to Apple. Most of it still is, because most people don't turn this on. 4,300 people had their iCloud content disclosed to US law enforcement in response to a search warrant in the first half of 2023. Cops absolutely love this. Cloud backups are their preferred tool for getting around encrypted devices. If you care about the data on your phone and you use iCloud, you must turn on Advanced Data Protection.

### Setting up iCloud Advanced Data Protection

ADP is a setting you have to specifically enable, and Apple makes you jump through a couple of necessary hoops to make sure you don't accidentally lose all your data. That's a real risk, which is why they don't enable this for everyone by default. If you are currently using iCloud, go ahead and turn this feature on right now. Yes, now! I'm serious, do it now. Or at least do it once you are done reading this section, but do not move on to anything else before enabling it, because you will forget, and you really need to do this if you are the kind of person reading this guide.

### What is encrypted by ADP?

- Photos
- Device backup (including iMessage)
- Notes
- Safari bookmarks
- Voice memos
- Most other Apple app data
- Data from some third-party apps if the developer enables it

### What is not encrypted by ADP?

- Contacts
- Calendars
- iCloud Mail (<your-email>@icloud.com)
- Metadata (like file size, creation, and access times), even of files whose content is encrypted

- Data stored by third-party apps if the developer has not enabled ADP

### Recovery Method

When enabling Advanced Data Protection, you have to set up some kind of recovery method. The whole point of ADP is that Apple can't access your data, so if you forget your device password or lose all your linked devices you have to be able to recover the data yourself. There are two recovery methods:

- Recovery key
    - This is ideal if you trust yourself to store the key safely. You should store it in your password manager (see section on password managers). You should not store it in plaintext (unencrypted) on any device that might get searched, or in some cleartext cloud storage like a Google Doc, or on a piece of paper in your apartment that anyone who can enter there could read.
- Recovery contact
    - You can also designate someone else's iCloud account as your recovery method. Basically their devices get copies of your keys. This is OK if you totally trust this person and also trust that their devices will not be compromised. They should also be following the advice in this guide!
- Both key and contact
    - This could give you more peace of mind that you won't lose access to the data, but this comes with both the risk that the other person's device is compromised, and the risk that the piece of paper that we told you not to use gets discovered.

### Is this really secure???

It's understandable if you still don't trust Apple in this case and want to keep everything off of their servers; go ahead and use local backups and open-source products. But Apple is pretty good at this kind of thing. We can't examine the source code of their servers to know exactly how it works and that they have done everything 100% perfectly, but no one has yet found anything lacking in how they say it is supposed to work, and a very notable cryptographer seems basically satisfied. They have gone to some lengths to use hardware security modules to prevent themselves from accessing your keys without your password. We can't know how well that hardware works, but most consumer cloud services do not even pretend to claim anything like this.

Apple does have a lot of their reputation riding on this; they make a big deal about privacy in their marketing. In the world of security and privacy, as in most things, trust is more easily lost than gained. If it turns out that this whole thing does not at all do what they say, they are probably going to end up losing a lot of money. Take that for what you will. If you need to use iCloud, it's mostly safe if you turn on Advanced Data Protection.

## Preventing Online Account Compromises: Password Managers

(i.e. How to keep your account from getting "hacked")

**Why use a password manager?**

Using unique passwords, i.e. a different one for every site, is one of the top three things that everybody needs to do to improve their personal cybersecurity. It is also one of the least likely things that people will actually do. Though protestors and organizers face special risks, they *also* face all the same risks as everybody else. Getting scammed out of your money or having your Instagram account taken over by spammers is no more helpful for activists than for anybody else. So, in addition to not clicking on phishing links where you end up telling the attacker your password, and after you have set up 2FA everywhere possible, you need to start using better passwords. A password manager makes this easy.

The end goal is not so much to use "good" passwords like `bjF7sNkaw*aF@8KE` or `goof-weasel-bout-boar-hardpan` for their own sake, but to use *different* passwords on every site. Using `bjF7sNkaw*aF@8KE` on every site is no help. Various sites' password databases get hacked all the time. If you want to find out how many times your online passwords have been leaked by hackers, enter your email here: https://haveibeenpwned.com (this is a reputable site). Once someone compromises a service, they can probably figure out a bunch of the passwords in the database. A lot of those people likely used the same email and password somewhere else, too. And that's how the attackers figure out your password to other sites even if you don't click on a phishing link. One of the authors of this guide has had more than 10 of their passwords compromised over the last few years this way, and those are just the ones they know about. Password managers also help in any other situation where someone learns your password – logging in to a phishing link, using a compromised public computer, etc. Using unique passwords limits the damage to one site.

Remembering different passwords for every site is hard. You probably have hundreds, maybe even 1000 online accounts. When you sign up for random sites to buy tickets, to order food, to get discounts, to apply for jobs, etc, you probably sometimes use similar passwords on a lot of them. Maybe your cat's name is Muffin and your birthday is July 20; you probably have a few passwords that are variations of `Muffin720!`, `muffinCAT7/20`, `muffin_123_WTF`. Once someone figures out one of those, it's easier to figure out the rest, and even easier if you reuse the exact same variation (say, `Muff1nTheC@t` that most sites will accept). So when some random shopping website that you bought a bulk order of hair ties from 10 years ago gets hacked, now someone is going to take over your Instagram and start sending cryptocurrency scams to all your friends. Womp womp. Password managers prevent that scenario because they help you use truly different passwords everywhere.

There are a lot of password managers out there, like Enpass, 1Password, KeePass, Bitwarden, Proton Pass, iCloud Keychain, etc. Anything is better than nothing, as long as you stop using `Muff1nTheC@t`. When choosing one of these password manager, it's best to avoid any that store your passwords remotely in the cloud, like LastPass. If you must use iCloud at all, you may as well use it for passwords too, but see the iCloud section, in general we recommend avoiding iCloud if you can manage it.

It's ideal to sync passwords between your mobile device and computer via your local wifi network, not through a cloud service. In the past, this meant 1Password, Enpass, one of the variants of KeePass, or just a few others. Unfortunately, it is becoming harder to find a password manager that doesn't use the cloud; even 1Password now makes you sync through their servers. To be clear, this is still better than continuing to use `Muff1nTheC@t` on every site, but it's not ideal for people at higher risk if you can avoid it. 1Password is still an OK choice, as the remote copy of your password file is end-to-end encrypted. But you should avoid the cloud if possible, so Enpass is the best choice.

### How to get started with a password manager

Enpass and KeePassXC are some of the few remaining options that let you sync without the public internet. KeePassXC is free; it doesn't have its own mobile apps, but if you're up for it, you can try manually syncing it using third party apps. Enpass is a paid service, but it's the most user-friendly option, maybe 90% as easy as 1Password. If you don't like Enpass for any reason, 1Password, iCloud, and BitWarden are reasonable choices (especially. if you have family members who want to share accounts via 1Password, for example).

You still very much do need to avoid any services that can decrypt your database without your primary password, i.e. "recover" your account just with your email or the like. If the service can decrypt your password file without your main password, so can anybody who hacks them or forces them to turn it over. Stick to those we've recommended, and stay far away from LastPass or Dashlane. KeePassXC is free and open source, which means it's got more rough edges, which isn't lovely when dealing with something as frequent as logins. Enpass is $24/year to get unlimited use on mobile, but as with many things these days, quality is worth paying for if you can.

Once you have selected your password manager, you need do a number of things. It's an adjustment, but it's worth it.

1. First, **choose a good primary password**. It needs to be a truly new one, not something related to Muffin that has been leaked. This is pretty much the only password you will ever need to memorize from now on. Use at least 16 characters, and not just three words that you like strung together. Yes, this sucks, but every other password signup is going to suck less from now on.
2. Next, **get the mobile app and make sure you are comfortable syncing** between desktop and mobile. You want to make sure you have multiple copies of your password database and that you can still access your accounts on every device. If using Enpass, make sure to use local wifi sync, not a cloud service like Dropbox.
3. **Install the desktop browser extensions** so that the manager can automatically fill passwords into web forms for you without having to copy and paste.
4. Now start using it. Every time you log in to a service, enter your account in the password manager. You could start by saving your existing passwords, but what you should really do is change each one the first time you log in. Over time you will get to most or all of them. Change them to random ones generated by the password manager.
5. You should **change a few important passwords sooner rather than later** even if you aren't forced to log in right away. Social media accounts that you care about are high priority. Banks, Venmo, Cashapp, money, enough said. Any online file storage where you have placed sensitive documents or photos should be changed soon so that Muffin can't read them.
6. You may want to hold off briefly on changing your main email password until you are comfortable with the whole system. Your email is usually the main way to recover your accounts if you forget the password or screw up during the password change process. That email is probably your single most important account, so for this reason you can consider using a (unique) password on it that you actually do remember, rather than a totally random one from the password manager in case anything ever goes wrong, like your phone and laptop are both in the same bag that falls off a boat. But if you do this, make sure it's actually a good one, nothing to do with `Muff1nTheC@t`, nothing used anywhere else at all.
7. **Create a copy of your main password and put it somewhere safe** that someone you trust can access if anything happens to you. You could write it down and have a family member you don't live with keep it with their birth certificate, have your best friend store it in their own password manager, or put it in a safe deposit box in Switzerland if you are James Bond.

8. If using an app where syncing and storage are under your control, like Enpass, KeePassXC, or the old 1Password, you should **back up a copy of the encrypted database** somewhere else regularly. Maybe a flash drive with a friend, that safe deposit box, whatever. At the very least, put a copy on an external drive you keep at home. Store a backup under the assumption that your laptop could fall into a river.
9. When you change passwords and create new accounts, make sure to sync over your local wifi if it's not happening automatically.

You also might want to change some settings to make things easier, for example extending the timeout for the app to lock itself when inactive. The whole concept is a big adjustment, but once you get used it and set it up the way you like, it becomes second nature, and actually much easier than trying to remember whether you used `Muffin720!` or `Muff1n720$` on each site.

## Privacy and safety for online meetings

Conducting private real-time meetings or calls online requires some compromises. There are a few common options that differ in the level of privacy, reliability, and ease of use. In general, most online meetings people commonly use are not end-to-end encrypted, meaning the server operator can record calls if they want, or if they are compelled to by a wiretap warrant. Unless they make a big deal out of it not being the case, you can assume that a service will allow the server operator to wiretap the call. Even participating in a call fully anonymously is difficult.

The following options are presented in decreasing order of recommendation. We explain why below.

1. Signal
2. Wire
3. Jitsi Desktop with Linphone
4. Jitsi web via meet.jit.si
5. WhatsApp
6. Zoom or anything else

### Signal

Signal is recognized to offer the best encryption for messages. It is open source and well studied. Signal calls are encrypted in a similar way. The content of the call is not visible to the service operator. This is the best option when possible, but there is a limit of 50 people per call, and you may still encounter problems with fewer people. Reliability of audio/video probably depends on your cell carrier/ISP. Try disabling video and just use audio if you run into problems with call quality. Signal is not entirely anonymous; you need to have some contact information for the people you communicate with, though they do not require you to share your phone number with contacts anymore. The server has some information about your contacts, but it's not easy for them to access this, and the membership of groups is never known to the server.

*Pros:*

- Best encryption, always on
- Group/call membership is not known to the server, cannot be disclosed
- Most private choice
- Service operator is relatively trustworthy
- Recently added call links so you don't have to create a chat group for each call or know all

the contacts previously

*Cons:*

- Limited to 50 people per call (maybe fewer in practice)
- Can't schedule meetings to start at a specific time

### Wire

Wire is another end-to-end encrypted messenger similar to Signal, which also supports encrypted audio/video calls. It's produced by a for-profit company in Switzerland. Its encryption is probably fine, and some of it is also open source. Being based in Switzerland, it is not subject to the same requirements for information disclosure to US law enforcement as US companies. This is relevant as the service does not make any effort to avoid learning your contacts and may store other metadata. It is not clear if they store data on the participants of calls, but in general they make less effort to hide such data from themselves.

This lower degree of anonymity is somewhat offset by the difficulty of getting the information due to Swiss privacy laws, which make it harder for US agencies to request data. US agencies can still request data, but international law enforcement cooperation is such a hassle that's usually only worth it for serious cases. Registration only requires an email, which you can sign up for anonymously (see section on blogging), so you can more easily easily use multiple accounts on one device. Wire is mainly targeted at businesses, but they offer a free account for personal use. Calls are limited to 25 people, but being targeted at businesses, they are probably decent quality. Overall it is not necessarily better or worse than Signal, but an acceptable alternative if you prefer it. It has different tradeoffs. It is not clear if you can schedule meetings ahead of time with the free personal plan.

*Pros:*

- Likely good encryption, always on
- Based in Switzerland, good privacy laws
- Register with an email instead of phone number

*Cons:*

- Most people don't already have it installed
- Contacts are stored by the service
- Metadata in general may be more visible to the server

### Jitsi Desktop or Linphone with VOIP server

Note: this is *NOT* the most common way to use Jitsi. If you have joined Jitsi meetings via a web browser, this is not what you used. That service is very different.

Jitsi used to be an open-source app but hasn't had substantial updates in years. Some volunteers are doing minor maintenance, but it might not work on some devices or might run into bugs in the future. But we recommended this because old version does not rely on the server run by meet.jit.si, meaning you can connect it to any VOIP server or run your own. It does support end-to-end encryption with ZRTP/SRTP, which are older methods than those developed by Signal or Wire, but

better than nothing. Because it's open source and you can use it with your own server or any server you trust, you can have some confidence that the encryption is working if you enable it, and that the metadata won't be stored. Metadata and call record storage does depend on the VOIP server, so you need to pick a good server. Unfortunately the old Jitsi client only supports desktop, not mobile, which is a pretty big drawback.

One VOIP server you can use is run by Linphone. We can't vouch for their metadata storage policies, but you can try it out to see if Jitsi will work for you. Some configuration is definitely required. Linphone also offers their own apps now, including both desktop and mobile. They are also open source, but it's hard to say how much scrutiny they have received. They are more up to date, so they might be easier to use than Jitsi Desktop, but configuration will still be required.

If you know how to run any kind of server, tt is not particularly hard to run your own open-source SIP/RTP server. That offers the best assurance regarding metadata/call logs, but you'll need a ton of bandwidth for video calls. Audio calls don't need as much bandwidth, but you'll still need a good server with a decent amount of bandwidth and CPUs; e.g. the AWS free tier is not big enough. You'll need to make sure encryption support is enabled both on the server and the client. The combination of these open-source options is by far the hardest to use of the services we recommend, but if you're comfortable trying out some new apps and finding a good server or running one, this is a good choice.

*Pros:*

- You can host your own server
- You can choose any other server
- End-to-end encryption is supported

*Cons:*

- Harder to set up
- You need to make sure encryption is enabled
- You have to choose a server and get an account, which could cost money

### Jitsi web via meet.jit.si

This is the default way to use Jitsi, and it is not as good as using the older desktop app. It is now run by a for-profit company that no longer updates the open-source version. They offer a setting to enable end-to-end encryption per meeting, which you should definitely turn on. This requires you to share the password with other participants. You should use a unique password per call. The web client is delivered to your browser every time you load the page, which means there's basically no practical way to verify what it's doing. Its encryption might not even be enabled when it says it is. This is better than Zoom, the nearest direct comparison, which doesn't even pretend to offer call encryption, but it's not very trustworthy. If other options higher on the list work for your use case, they are more trustworthy. It's hard to know if the official Jitsi server keeps metadata or call logs, so you may assume that it can.

*Pros:*

- Good reputation for reliability/call quality
- Supports many call participants

- Easy to join via web for public meetings
- Offers end-to-end encryption, if you enable it

*Cons:*

- Encryption is hard to verify
- Encryption is not on by default
- Service may store contacts or metadata

### WhatsApp

WhatsApp uses encryption based on Signal's (the creators of Signal helped them implement it), so of all the common chat apps, it offers more content privacy by default. If you need to call someone on WhatsApp, the call content will not be visible to the server. But WhatsApp is owned by Meta/Facebook, which is obviously a privacy nightmare. It is not anonymous at all. Meta/Facebook make their money on surveillance, and the only data they can really get from WhatsApp is your contacts and other metadata like who you call and when, so you can bet that they save this forever.

*Pros:*

- Likely good encryption, always on
- Many people already have it installed

*Cons:*

- The opposite of anonymous; Facebook probably stores call records forever
- Limited to 32 people per call
- Can't schedule meetings ahead of time or provide a call link
- Must create a group to start a call with those contacts

### Zoom

Zoom is common and works well with very large meetings, which is why it's the most common choice. But it is not private at all, never mind anonymous. It is not end-to-end encrypted. The service can record the call. It does have the benefit of people being able to join meetings without an account or being already connected to you, but Zoom probably stores metadata about who joined calls (account if they used one, their IP, what kind of device, etc). Zoom should only be used for topics that you already consider basically open to the public. If you do use it for public meetings, you should enable some meeting options that give you control over who joins and what they can do, and lets you kick them out if necessary.

*Pros:*

- Everyone already has Zoom
- Good quality calls

*Cons:*

- Not at all private or anonymous

### Google Meet, Facebook Messenger, whatever else

These options do not provide end-to-end encryption. The service operator can record the call. They are just presented here for completeness because people use them.

*Pros:*

- People may already use them
- Some offer good call quality

*Cons:*

- Not at all private or anonymous

## Running a public blog anonymously

This takes some time. Anonymity is hard to get right, so you have to follow the steps and be patient. Tor, especially over .onion links, can be slow. You must always use Tor for every step. Never, even *once*, log in to your blog from a normal browser or the Tumblr app. Always use Tor Browser. If you ever log in to your account outside of Tor Browser, Tumblr will learn your IP and all of this will be for nothing.

### Create burner email

#### Email option 1: a true burner email

This is temporary, you won't be able to log in to this email later to recover the Tumblr account/change password etc.

1. Using Tor Browser, get a temporary email at https://mail.tm
2. Leave that window open so you can see the email that gets sent to it

#### Email option 2: Tuta

This is usable after 48 hours, and thereafter. You can log into it indefinitely once it is activated, if you need to change the Tumblr password later. You must log in every 6 months to keep it active. Probably the better option, and more likely to work. Be aware that Tuta may sometimes flag and deactivate accounts created over Tor, so this is not 100% guaranteed to work over time, but it has worked. You can wait longer to make sure the account isn't deleted immediately if you want to be able to access it later.

1. Using Tor Browser, sign up at https://tuta.com/
    1. If they deny registration from that IP, try a new circuit, it should work eventually
2. Don't select an email address that has anything to do with you, e.g. use random words from https://randomtextgenerator.com/
3. Wait 48 hours until they unlock your account
4. Never use this for anything else. Don't email yourself or anyone you know.

### Use the new email address to create a Tumblr

1. Using Tor Browser, sign up for a new blog at tumblr.com
2. Use your burner email address to sign up
3. Select some random suggested interests
4. Follow some random suggested blogs
5. Do not enter your real birthdate
6. When choosing your username/display name, do not use anything that would violate Tumblr's terms of service or identify you. You can use one of their suggested names or random words.
7. Verify your burner email using the link they send you
8. Never log in without Tor Browser; never use another browser or their app
9. Start posting

### Or, use the new email address to create a Wordpress blog

1. Using Tor Browser, sign up for a new blog at wordpress.com
2. Use your burner email address to sign up
3. Choose a subdomain of wordpress.com that can't identify you or your group
    1. Don't buy a domain or sign up for any paid plan
4. Go to your profile and change your display name
5. Verify your burner email using the link they send you
6. Never log in without Tor Browser; never use another browser or an app
7. Start posting

Tumblr, Wordpress, or really most commercial services, are not ideal for extremely spicy content. Anything illegal can be flagged and get you banned. It is never recommended to post anything illegal, and you will be subject to all their terms of service. You might get shut down if you cross the line.

People viewing the blog will only be anonymous if they use Tor Browser. Users signed in to the Tumblr app can be logged by Tumblr.

### Temporary note posting options: pastebin-like sites

For posting plain text content at non-memorable URLs, you can use sites like https://pastebin.com via Tor Browser. If you post over Tor, the author will be anonymous. It is not a long-term blog, they may be deleted at any time. This might be useful for quickly sharing simple notes that you don't mind anyone on the internet being able to read or potentially delete.

### Running a public website

This is a very advanced blogging option requiring significant technical experience. You can use hosting sites based outside the US, such as in the EU. European privacy laws are stronger than in the US, and getting information from these hosts is a hassle for US law enforcement. If you understand the following information and think you can manage this, this is ideal.

You can rent a server with, for example, Hetzner.

Hetzner requires payment methods that are strongly linked to your identity, but they are otherwise a good host based in Europe. Many Tor relays are hosted on Hetzner. Payment is a big weak link. If

you know someone outside the US who can pay for you, they may be less concerned about their identity being known to the host, depending what you plan on posting on the blog.

Some cloud server hosts accept cryptocurrency. If you know how to use cryptocurrency anonymously, you may be able to register a server that is not strongly linked to your identity. Contrary to popular belief, most cryptocurrencies are not very anonymous. Attempting to use cryptocurrency anonymously is outside the scope of this guide. Selecting a server host that accepts cryptocurrency and does not require other identity verification is also out of scope. They may exist, some of them may be reputable, but YMMV. Registration should obviously be done only through Tor Browser.

Once you have a server in the EU, you must administer it over Tor. How to route your ssh connection over Tor is OS-dependent. Briefly, you use the non-browser Tor binary to set up a local SOCKS proxy, and configure your ssh client to use the proxy. Try first using curl over the SOCKS proxy to make sure it's working; it will probably look something like this:

```
$ curl --socks5 127.0.0.1:9050 https://check.torproject.org/
```

Once you know Tor is creating the local proxy, use it with ssh, maybe something like this.

Once you are able to ssh to your server over Tor, you can install blogging software like Ghost or Wordpress. Be very diligent keeping your software (esp. Wordpress) up to date! People using a web UI to write posts should log in via Tor Browser. Everything about securely administering servers and blog software still applies: use unique passwords for users who post, keep your software up to date, use ssh keys instead of passwords, don't run unnecessary services or leave ports open, etc. This is all an exercise to the reader because running your own servers is a substantial undertaking, so you need to already know what you are doing.

## How to attempt to use a burner phone

We don't really recommend using a burner phone domestically, because it will probably fail. It can't hurt, but it is so complicated to do completely correctly that it's probably not practical to expect it to achieve what most people are after: untraceability, anonymity, etc. This is something that law enforcement is now extremely good at seeing through. Correlating multiple, changing phones owned by the same person was the original advertised use case for Palantir, so this is not a cutting edge capability.

Basically everything else in this guide, including securing your regular phone, reducing your usage of unencrypted cloud services, and using Tor, are much higher priority. If you've already done all of that, then you can think about buying more phones. If you do any of this wrong, there's a good chance it won't work the way you want.

### What are you trying to protect?

Using multiple phones might be intended to obscure several things:

- Where you go
- Who you are talking to

- Which accounts (e.g. social media) are tied to you

Some of these are easier than others. None work if the phone is eventually tied to your identity, for example if it is seized while you have it, or if you use it from your home. The phones of people you're talking to could also be seized and your identity learned from theirs (e.g. if you texted your new number to them, or if they told someone else). Which of these things you're trying to protect will influence which steps you need to be most careful about. Location is among the hardest things to hide, but you can try to avoid connecting the location of the new phone with the location of your main one.

Using social media accounts not tied to your main phone is much more achievable. A separate phone for traveling abroad is a good idea. Hiding domestic location and your ownership of the device are the really hard parts.

If your goal for a separate phone is simply to not carry around your main phone with all its sensitive data in case it gets seized, you can certainly do this, but you can't use the second phone for any of your normal activities or talk to any of your normal contacts on it. It really must be only for checking maps or subway times or the like. Once you start accumulating data, accounts, and messages on it, you've defeated the point.

### What phone to get

If you can afford it, a recent iPhone (12 or newer) or Pixel (6 or newer, ideally with GrapheneOS) is your best bet. This is obviously not your typical corner store Tracfone, but it's the only way you can be very confident that it'll resist cracking by Cellebrite or GrayKey with a long passcode. You get what you pay for.

If obscuring your location is what you're most worried about, for example attendance at a protest, and you're less worried about protecting the contents of the phone, you can try buying a cheap Android device. This will require changing a lot of settings to disable as much tracking as possible. Try to avoid linking a Google account to it at all, disable any kind of backup or cloud services, disable location services, disable analytics or data sharing, set a good passcode, and enable the lock screen. We bought a cheap Android device recently to test it out, and it is barely functional, much worse than an even cheaper one from 7 years ago, go figure. Maybe some are better than that model, but these phones are by and large not good. You can be almost positive that a no-name $50 or $100 Android phone is crackable by Cellebrite, especially when it's on.

### How to buy the phone

- Use cash
- Don't bring your regular phone with you
- Don't use your existing Metrocard, OMNY card, or bank card to take the subway there
- Buy it from a store with no cameras (good luck)
- Get a SIM from a prepaid carrier that you can refill or pay the bill with cash
- Take it somewhere like a park to set it up; don't ever use it at home
- Turn it off once you're done setting it up

Most of that is not possible for a used iPhone or Pixel. If you're going to buy those from someone on Craigslist, make sure Craigslist and the seller can't identify you by your email, phone, or home IP (see other sections on Tor and anonymous email).

**How (not) to use it**

- Don't connect it to any wifi networks you use with your main phone
- Don't have it and your main phone both powered on in the same location
- Don't use SMS or regular phone calls
- Don't contact any phone numbers or Signal users that you communicate with on your main phone
- Don't log into any of your existing accounts on it
- Don't log in on any other device to any accounts you create from it
- Don't do any activities on it that are tied to your home address (e.g. buying things)
- Don't message your main phone or personal accounts with it, even to send files/photos/URLs
- Don't keep using it if anything happens that could leak its connection to you
- Don't bring your main phone with you or be on camera when paying the bill each month

If you really want to do everything to keep the phone from being traced back to you, you can't mess any of that up. One slip-up could be enough for a determined adversary who has access to data from the carrier, online services, stores, the MTA, etc. The phone will still be on the cell network, so anywhere you take it while it's on can be correlated with all the cameras there. None of this is a sure bet. If you're just casually trying to reduce your data footprint and make things harder for the many parties tracking you daily, go for it, but make sure you do all the other stuff in this guide first.

# Q & A with FNH

This section starts to get off into the technical weeds. You only need to consult the remainder of this guide if you happen to have any of these specific questions. Some of them do tend to come up, so you may find other people wondering about them, or accidentally spreading misinformation related to them, so they could be useful to share in that case.

## Should I use XYZ brand of VPN that I see advertised on YouTube and the subway?

The problem with VPNs is that the provider sees your true IP. It is a very weak form of anonymity. It's better than nothing. It hides your IP from the site, but it may still be found out from the VPN provider, and then your identity can be acquired from your cell carrier/ISP. It comes down to risk and trust. You can decide if you're comfortable with, for example, Proton's audit of their logs. Proton is easy to use and fast, and their politics are fairly privacy-forward. Proton does log the IP you used to register. They're in Switzerland, which has better privacy laws than the US, but it might still be unwise to trust a private company to keep you out of jail when there are other options.

For casual everyday purposes, hiding the IP from the site is enough anonymity. You may as well use a VPN if it is reputable; your ISP is probably worse. But if your threat model includes law enforcement, they can force many companies to give them the information they need to link your activity to your identity. No single party has everything, but law enforcement can make each of them give up enough dots to connect. It's an extra hurdle, and maybe they don't do it for every single investigation. It depends on your risk.

Random free VPNs can actually be worse than nothing; some sell access to your device to turn it into a VPN for organized crime botnets. How do you think they make money if it's free for you?

If you want good anonymity, you need to use Tor.

## Is CryptPad safe? How should we use it safely?

A full audit of their code by JavaScript programmers and serious cryptographers would be helpful, but their documentation does give a good idea how it works. It's a reasonable design and a good tool to use. The design is not quite perfect, but the problem they're trying to solve is pretty hard. There is not much else that is this well thought out and easy to use for collaboratively writing documents online that the server can't read.

There are a few things you should know about CryptPad:

1. It's not designed to be anonymous, exactly. If the server wanted to, it could store the IP of people viewing and editing specific documents.
2. You have to trust the server to send your browser the correct code every time you load a page. A malicious server could send your browser some code that sends the plaintext contents of your documents, or your encryption key, to the server or somewhere else.
3. There is no way to revoke a shared link.

The implications of these are:

1. You should use it over Tor if you are concerned about someone compelling the server operator to keep a log of which IPs access which files.
2. It would be ideal to use an instance of CryptPad run on a server by someone you trust who knows what they're doing, located in a country where it's unlikely they would be compelled by law enforcement to serve you malware.
3. You should share documents to specific people's CryptPad accounts, not via links, when possible.

Some people we know are using the main instance at https://cryptpad.fr, which is run by the developers of CryptPad and hosted in France. It's good that they're in France, not in the US. You can decide if that's trustworthy enough for you, if you think those people will never be co-opted into sending your browser the wrong code.

An aside on browser-based apps: doing privacy-sensitive cryptography in the client's browser in this way would suffer the same risk from any app, any provider, like Proton Drive or the like. Some cryptographers are uncomfortable with this concept, that every time you load the site it could be doing the wrong thing. This is unlike the Signal app on your phone, which you only download from the App Store and is cryptographically signed by the developer. In the browser you can't know this, it's possible for the server to send you a malicious page each time. But the tradeoff is that until recently no one made anything like this! It's basically Google Docs, but the server has extremely little knowledge of what any of the data is. It's pretty cool.

It would be better if they had a desktop/mobile app, but the world is not perfect. So hopefully the operators of cryptpad.fr don't get co-opted into distributing malware, and you can assure yourself this won't happen by operating your own instance or having a knowledgable tech friend do it. There are also other public instances operated by net-freedom collectives and the like in various countries.

Regardless of your confidence in cryptpad.fr, if you want anonymity, you should use Tor Browser to access CryptPad.

**Best practices**

- Edit and view documents via Tor
- Use servers hosted outside the US
- When possible, share documents to specific accounts, not by sending links around
    - Links can be accessed by anyone who knows them, not only the person you send it to
    - Access to links cannot be revoked, other than changing the password if present
    - Use "Access Lists" in combination with this to revoke access (not possible if you sent them a link)
- When sharing documents, give the least privilege necessary
    - If someone just needs to read it, don't give them edit access
    - If sharing publicly to the world, use the link that only gives read access
    - Use "View Once and Self Destruct" access/links for anything spicy that someone just needs to see briefly (it gets deleted for everyone)
- Use passwords on sensitive documents to provide extra protection and the ability to revoke access by changing the password
- If you need to revoke access to someone you shared a non-password link to:
    - Copy the contents to a fresh document
    - Destroy the original

- There is no other way
- Be thoughtful who you give either read or write access to in the first place

One nice thing about CryptPad is that their documents and folders are stored the same was as any other files. So you can share any kind of file this way. There are other ways to share files, while not a lot of ways to edit documents, but it can be used for both.

## I've heard that people can set up malicious Tor relays that can intercept your traffic and the whole thing is just a government honeypot

While it is possible to set up malicious nodes, this is blown way out of proportion, usually by people who misunderstand the underlying concept of how Tor works. Every circuit you set up uses at least three relays, more for .onion sites, and your browser/Tor client is frequently changing them. To know which source IP is accessing which site, all three relays in the circuit must be malicious and operated by the same party. There are almost 9,000 relays operated by probably thousands of different people, leading to around 23 billion possible circuit combinations. The network operators monitor for large additions of new ones to try to detect malicious groups of relays trying to join. It is not easy to suddenly add a lot of new malicious nodes without someone noticing, which would be required to have any reasonable chance of controlling all three in many circuits very often.

It has occasionally happened that someone, maybe the Russian government, created some malicious exit nodes, which see the final connection to the site (but not the originating node where the user is actually connected to). This can be useful to them if you access non-encrypted HTTP sites, not HTTPS, because they could see when you log in with a unique username, for example. Basically no popular websites allow logins over HTTP anymore, it's all HTTPS. Remember how browsers used to show that padlock icon for HTTPS? They don't anymore because it's expected that every site should have it. That means a hypothetical malicious Tor exit node couldn't see much of interest anyway these days.

As of 2013, according to the Snowden documents, the NSA could not break Tor, and they were pretty mad about it. Multiple research papers are published every year studying Tor and trying to find any new way to break it. These are useful and lead to improvements, but none since 2013 has fundamentally changed the understanding of how it works.

## I've heard that using Tor makes you stand out and makes it obvious that you're doing something shady

It is true that your ISP, your school, or your employer can easily see that you're using Tor on their network. This is all they can see. In most cases this is not shady at all. It is mostly used by people who want more privacy, which is becoming more common lately.

Whether it is suspicious to be using it very much depends on the situation. If your employer is investigating a security breach, and they suspect Tor was used by the attacker, any employee using it at the time would probably face some questions. There is a case of a student who sent a bomb threat to his university to get out of an exam and was identified despite using Tor. In his case, the university had pretty good reason to believe that the bomb reporter might physically be on campus and therefore using their network, and very few students were using Tor at the time. They knocked on each of those students' doors and asked them about it, and he confessed. These kinds of situations don't apply to cell carriers or residential ISPs, whose customers are doing legal things and just don't want anyone snooping on it.

If you are particularly concerned about this for whatever reason, you can first connect to a VPN, then to Tor. Then your ISP will not even see that you are using Tor, only that you are using a VPN, which is even more common these days. We don't normally recommend using both, but if you do it correctly, it would avoid this problem. Be sure to check https://check.torproject.org to make sure it is working correctly. If this is configured in the wrong order, and your connection first goes over Tor *then* the VPN, this defeats the purpose entirely, which is why we don't usually recommend it.

Another option if you are especially worried about standing out is using Tor bridges, which are relays that are not publicly listed. This makes it less obvious, except to a really serious adversary like the Chinese government (most ISPs likely will not notice). You can set this up in the browser itself, and don't need any other VPN.

## Can sites use JavaScript or some other method to determine your real IP when using Tor?

On most platforms, this is not a concern now that we don't use plugins like Flash anymore. On iOS, there is a limitation on what apps are allowed to do, and that means some media streams (WebRTC) can't go through a Tor connection created within a single app. A malicious site could use this against a browser with Tor built in, such as Onion Browser. This is not something that legitimate sites do, but it is a theoretical concern. The solution to this is to use Orbot when possible. While using Orbot any app, including Onion Browser, would have all its traffic go through Tor. Basically, this is not a huge concern, but you can use Orbot to avoid it in any case, or use Tor Browser on desktop for the best protection.

## What's the point of any of this if cops can buy surveillance data from advertisers and data brokers?

This arose thanks to this article: LAPD Is Using Israeli Surveillance Software That Can Track Your Phone and Social Media

It has always seemed like a risk that companies like Palantir could tie all this commercial data together. That's what Palantir does. The Israeli software in the article specifically gets its input from data brokers like advertisers. For 20 years, there was a danger that someone would figure out how to sell that stuff to cops, and in the last few years they finally have. This is in fact pretty hard to stop completely.

This is one area where iOS is better than Android. It's hard to link device IDs used for ads across apps on recent iOS versions. It seems to work reasonably well, to the point that Facebook has started losing money because of it. Android, of course, is given away for free by Google because it's an ad platform. But it's unlikely that iOS is totally immune to this. There is so much data generated by everything we do online these days. The document shown in that article says they can correlate useful identifiers even from iOS. And it's true that by going through surveillance capitalists law enforcement doesn't have to get a warrant. It's not great.

In a very general way, ad blockers and cookie blockers help with this type of surveillance somewhat, reducing the easiest ways of tracking sites you visit. But there's so much more than that out there, from IP tracking to endless new methods of browser fingerprinting. And browser ad blockers don't work within mobile apps. Mobile app ad blocking usually relies on using special DNS servers, which very few people bother to set up, and probably misses a lot. There's so much commercial surveillance going on, it's hard for any one person to even know about it all.

Using Tor Browser leaves much less of a trail. Good VPNs also might help, somewhat. Mobile apps are still a minefield.

It's easy to get paranoid in the face of things like this. On some level, it's probably not possible to live 100% off the grid anymore if you want to talk to people. But you can reduce your tracking risk. That's the point you want to get to, finding the balance that works for your situation where you can do useful things in the safest way possible.

The harder you make them work to link tidbits together, the fewer people they can do it to. If you do things that reduce risk, you can sleep better than if you don't do those things. Just because you may not be able to avoid every single last method of tracking on a smartphone doesn't mean you shouldn't try to avoid a lot of them.

## Can police use the phone's microphone to record or listen to your in-person conversations and calls, and Signal calls? Or record calls over the air?

In principle, malware on the phone could do this. Commercial spyware exists that is sold to intelligence agencies, foreign governments, and foreign law enforcement agencies. There are no reports of domestic law enforcement agencies using this kind of thing (though as of September 2025, ICE may be getting access to this, stay tuned to see how that develops). A warrant to use this should probably specify it, since it would not be the usual method of doing things like recording calls. If there's any reason to believe it has actually happened to someone inside the United States, they should get a really good lawyer because it will probably be an important case and they should carefully examine the warrant application. This stuff is evolving, and there's still a lot that isn't known about what technology cops have access to, when they use them, and what they tell the judge. As far as anyone knows, this is not being done except in very rare cases. Even intelligence clients of the commercial spyware companies don't like to use it too much; the more often they use it, the sooner it will get found out.

Recording Signal calls or the mic or camera of the phone would require this kind of spyware. Recording normal phone calls does not. Recording calls was possible with analog landlines and continues to be possible by the cell carrier, if the police provide them a wiretap warrant. Normal SMS messages are also stored by the carrier and can be given up with a wiretap warrant. While easy, this is still not extremely common. It would not be typical to do it to dozens or hundreds of people just because they happen to have been arrested at a protest. However, it would be a normal enough tool to use against someone who's the target of a longer-term investigation.

Recording call audio signals from phones over the air was simple 30 years ago, anyone could do it. Currently with modern phones, it requires a device called a Stingray, or IMSI Catcher, that has to be deployed near the person being targeted. It is not known how well these work in 2025. They likely have to trick your phone into thinking that it's talking to a 20-year-old cell tower to record the call. Newer phones have tried to prevent this from working. Many larger police departments have Stingrays, but as with most of their technology, they don't like to use evidence from them in court to avoid giving details on how they work. It may be that IMSI Catchers are now mostly useful for finding or tracking the location of specific phones, or identifying which phones are at a physical location, which is something they probably can still do. If these do still work, and if they are used near you, they would be able to intercept only normal phone calls and SMS. Signal/WhatsApp/Facetime/etc would still be encrypted end-to-end; the carrier (or a fake carrier) can never read the content of those.

## Isn’t it now unconstitutional to search phones of people who get arrested? Can that data be used in court?

It’s admissible with a warrant. If they arrest you and you’re in jail for three hours and they give your phone back, that’s probably not enough time to get a warrant. If they release you and hold on to the phone for two weeks afterwards, it is.

## If a phone has been in custody for a week and is returned, would resetting it remove any spyware? Would a phone backup give any indication of this?

Unfortunately, civilians don't have as much detail as we’d like about how forensic tools work. It’s not hard to get a Cellebrite, but it’s extremely hard to get a law enforcement model that’s up-to-date.

It is theoretically possible for spyware they have put on a phone to persist past a reboot and factory reset. The spyware used by foreign intelligence agencies probably does persist, especially on Android. There are no reports of that grade of malware being used by US domestic police.

There is one type of more limited spyware installed by a forensic device called GrayKey (similar to Cellebrite) when they seize the phone and hold on to it for a while. The GrayKey device will try to crack the passcode by guessing it (with six numbers, there are only 1,000,000 possible passcodes, they can try all of them). If this doesn't work or takes too long, it installs some malware on the device that will record the passcode the next time the owner types it in. Then if the cops get the phone again (maybe they give it back to you temporarily to “let you call your lawyer”), their forensic device can get the passcode from the spyware and then dump the contents. So, *some* limited type of spyware installed while they have seized a phone is a real thing, but we are not aware of any publicly reported examples of this happening, and certainly not anything more than this.

From what we’ve learned, this GrayKey spyware attempts to prevent a factory reset so you can’t delete anything. So if you try to wipe the phone, and it fails…you've now got a one-of-a-kind collector's item, so get that phone to the EFF or Citizen Lab or someone qualified to extract the malware from it and analyze it. It is unlikely that a normal phone backup would contain the malware.

If you reset the phone and it works, that particular spyware was probably not installed. How careful you want to be after this point is a risk calculation on your part. If you are in a position to get a new phone, that is certainly the safest option, but it’s probably not necessary for most people. Again, as far as anyone knows, domestic police installing spyware is not a common practice, and it should require a warrant specifically authorizing it. It depends on how careful you want to be based on what you’re doing, how anxious you would be that we might be wrong about this, and what you can afford.

## Can I jam lint into the charging port of my phone to tell if a Cellebrite was used on it?

You may remember from *1984* that Winston tried to secure his diary with a piece of hair or lint or something placed just so, which the agents who read it then replaced, way back in the 1940s. So you’ll want something better than lint. What you're looking for are called “tamper-evident stickers”. When they're removed, they leave part of themselves behind, so you can't replace them exactly as they were. You would want ones with serial numbers so that they're harder to replace with a similar one. Try placing and removing them to see what it looks like, to be sure you can tell if it was

removed. We haven't heard of anyone using this method yet, but it seems like it should give some peace of mind if the stickers are good quality.