THE

FRIENDLY NEIGHBORHOOD HACKER'S

(QUICK!) GUIDE

TO DIGITAL SECURITY

Full version at turnoffyourphone.org

Individual Practices, Basic (Quick-start Guide)

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

It assumes that you are a participant in an action that is not intentionally exposing yourself to arrest. It also assumes that you are not being specifically targeted as part of an investigation by law enforcement.

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.

The safest way to prevent your phone from being copied or bugged by cops is to **keep your phone at home** or stashed with someone else so you don’t have it if you get arrested. If you’re unable to do that, here are the basic safety procedures we recommend.

1. Phone setup

- 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, as law enforcement will 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

- **Turn off Siri/Alexa/"Hey Google"**

  - On iPhones: "Settings" --> "Siri & Search" --> under "Ask Siri", turn "Listen for" to "Off"

- **Turn off notification previews on your lock screen**

  - On iPhones: "Settings" --> "Notifications" --> "Show Previews": "Never" or "When Unlocked"

- **Keep your operating system up to date so known security vulnerabilities are fixed**

- **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.

2. Basic Signal setup

- Read: EFF SSD, How to Use Signal: https://ssd.eff.org/module/how-to-use-signal

- **Set a PIN on your Signal app for extra security**
    - They prompt you to do it automatically, but: Settings --> Account --> Change your PIN

- **Username: Set a random username**
    - Do not use your legal name or previously known handles, dates, or numbers that have personal signifcance 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

- **Display name: Do not use your legal name! Use initials & emojis 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.

- **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.** (Recommended: 1 week or less)
    - 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.

- **Turn off "Show calls in recents"**

3. Social Media Safety

- **Don't use your legal name on public social media**

- **Do not publicly share photos and videos of the action,** especially ones 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 identifer codes from the link

  ○ e.g. Instagram links should look like this:

  https://www.instagram.com/reel/C7PoMC1OjhV/

  Youtube links should look something like this:

  h*ttps://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*"

  following the link format above, remove the question mark and everything after it. Those are identifers that tell Meta what account and/or button the link was shared from.

4. Securing your phone before and at an action

- When bringing your phone to an action, the safest way to secure it is to **keep it powered off** unless you need to use it, and keep cellular data, wifi, location, and Bluetooth off unless you need to use them.

- 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 laptop or desktop computer.

    - You can buy or make a Faraday bag to keep your phone in. This prevents low-power chips from transmitting data to other devices while your phone is off.

    - You can also buy tamper-evident stickers to place over the charge/data port of your phone.

        - If the seal is broken when your phone is returned to you, law enforcement may have attempted to plug in a device to access your phone.

- **Use a password manager**
    - use it only with local wif sync between your laptop/ phone, never through their online service
- **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
    - 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"
- **Turn on auto factory reset**
    - On Androids: Settings --> Lock Screen --> Secure Lock Settings --> Auto Factory Reset
    - On iPhones: Face ID & Passcode --> Toggle on "Erase Data"
- **Turn off iCloud, Google Backup, or other remote/cloud backup services**
    - At the very least, you **must** enable iCloud Advanced Data Protection if you need to keep using iCloud

5. What to do if you're arrested

- **If you have your phone and can't throw it to a safe person, turn off your phone if possible**
  - On iPhones: Hold both buttons down --> Slide to power off
- **If you use a passcode to unlock your phone :**
  - 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 Cellebrite device.
    - 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.
  - **Reset your phone** (or get a new one if you're fancy)
  - **Change your phone passcode, and the password on your main password manager, if you have one.**