QUICK ACTIONABLE TIPS FOR PERSONAL SECURITY FOR ACTIVISTS 2024

This guide is for those going to protests or do direct action for causes important to you. It is to help you protect yourself IRL and digitally.

SECURE YOUR IDENTITY: MASKS

There is nothing wrong with standing up for what you believe in with your face - but lots of people, organizations and authority institutions don't play fair and will seek to use facial recognition systems or photos to identify you.

This can have ramifications like upsetting your livelihood , having your family harassed , or upset your immigration status. To prevent this, wear a mask.

A surgical mask is highly recommended at the minimum which is justifiable by avoiding spreading germs and is non threatening. There are advanced makeup and specific facial recognition defeating masks you can use for true facial recognition defeat, but a surgical mask , headwear and eyewear are a good place to start to defeat most systems.

You should also cover any identifying tattoos and check clothes for identifying marks to organizations or institutions you belong to. Strongly consider wearing clothes you don't normally wear to throw off identification.

SECURE YOUR PHONE

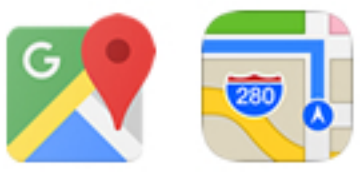
Cell phone security, for end-to-end encryption in communications we currently recommend Signal. You can send messages, images, and voice and video calls and even group messages with true disappearing messages.

Signal

We recommend setting your phone to using a PIN rather than face or fingerprint recognition, as you can forget a PIN, but be compelled legally to use your face or fingerprint or a copy of your face or fingerprint can be used to open your phone.

When doing direct action and protesting - if you can turn off WiFi and Bluetooth, as authorities use devices like Stingray that ping the location of all phones in the area, or counter-activist could use devices like Flipper to catch your identity via Bluetooth or hijack listening in.

You should also consider logging into Google Maps/Apple Maps and turn off location tracking. If there is an option on your phone to turn off GPS/location you should toggle that off as well.



For true blocking of tracking - consider getting a Faraday pouch / bag and wallet to keep your phone and cards in during protests or direct action, no data will get in or out whether you are on a call or not. It blocks all radio signals: WIFI, Bluetooth, NFC, RFID etc.

Another highly recommended practice is to get a burner phone. A separate cell phone that doesn't have your personal data on you only use during protests or direct action. If you can get a pay as go top off card without giving identificaton to activate it that is the best. You can still have a device to document things and contact people but if you lose it or it is stolen or you are compelled to give it by force it wont have identifying information on it.

SECURE YOUR DIGITAL IDENTITY

Always consider what you post to social media about direct action and protests. While it is important to get the word out, things that seem cool and are just can also be used against people to upset their lives or worse. Also, lock down your social media with 2fa to help delay or foil potential hackers.

TikTok Meta

Consider generating a new separate email address for protests and direct action. Never use your work email for your for protest and direct action communications or updates. Consider not using your personal email either, in case it is compromised. This precaution also goes for any work tools - from Slack to Asana - don't use these for protest or communications.

This technique also applies to social media, for protests and direct action it may be a good idea to make burner social media accounts for your activities and make your voice heard without exposing yourself to risk from doxxers.

Turn off location in social media apps and for posts. You should also check the options for turning off the location data in the camera apps so your GPS coordinates don't wind up embedded in your photos.

When organizing or have comms on Zoom, consider enabling end-to l-end encryption on it and, even better, consider trying WIRE for more privacy

zoom

SECURE YOUR NAME

On site during a protest or direct action - consider using nicknames and code names when addressing each other in public to avoid being doxxed. If you do get a burner email or phone number - give those when signing up for things. Also consider rotating your nicknames in case one nickname becomes too known.

Weigh your personal situation on whether to carry ID or not in case counter protestors gain access to your bag or pockets.

SECURE YOUR FISCAL TRAIL

Consider getting prepaid gift cards and/or cash to operate with during direct action and protests , authorities can track your purchases in a local area to determine your participation.

Please Distribute to whoever you need to for any cause you are standing up for. Good Luck. See you out there