Back it up! Lock it! Delete it! a.k.a. Someone took my mobile: Border crossings, arrests, seizure, theft [tactical activity]

tactical_activ_circular_200px-withte

Image not found or type unknown

In this activity, we plan and prepare for situations where participants and their phones may be at physical risk. Scenarios may include:

- Safety when participating in protests
- Safety at border crossings
- Safety when there is threat of arrest and seizure
- Safety when there is risk of theft and harassment

This activity has 4 stages with optional hands-on activities with installing and preparing devices. The stages include:

- Current practices in caring for ourselves
- Planning and preparing our devices
- Inputs – Optional

Optionally, follow this activity with hands-on exercises to practice the strategies and tactics.

Learning objectives this activity responds to

- an understanding of mobile communication safety from the perspective that mobile phones are our tools for both personal, private and public, movement communications;
- an understanding of basic concepts of how mobile communications work in order to better understand the risks of mobile communications;
- shared and practiced strategies and tactics for mobile safety to manage the impacts of our mobile communications on ourselves, our colleagues, our movements;

Who is this activity for?

This activity is for participants with varied levels of experience in using mobile phones to practice tactical safety with a focus on care and mobile phones.

Time required

This activity will require about **80 minutes**.

Resources needed for this activity

- flip chart paper + markers to document group discussion

Mechanics

This exercise is designed to support activists who are planning to engage in risky situations with their mobile phones. In the end, they will have a map of tools and tactics they can use.

Current practices in caring for ourselves – 20 minutes

> ***Care note**: This activity is a tactical activity to plan and prepare for using mobile phones in situations where people and their devices are at risk. Begin by acknowledging that to prepare for a risky situation, we need to consider first how we care for ourselves before, during and after.*

Begin with grounding and discussion about how people care for themselves in high risk situations.

Ask each individual to begin by working on their own. Hand out paper and ask them to consider these questions and to write their answers:

- What situations do you engage in where you will need to consider the physical safety of yourself and your mobile phone?
- What are you already doing to care for yourself – before, during and after these experiences?

Ask participants to divide their paper in 3 sections: before, during and after. Their paper will look something like this:

Participants' Paper Example		
BEFORE	**DURING**	**AFTER**

As a full group, invite participants to share their practices. Write these on a white board or piece of paper visible to the full group. Leave this up in a place that is visible. Ask people to share practices they do as individuals and with others.

Participants will continue to use this simple method for organizing practices in the next part of the workshop.

Planning and preparing our devices - 45 minutes

If you are working with participants to prepare for a specific event, it is best to work with the actual event. The following are scenarios that you might use in case workshop participants are not preparing for a specific event or your group needs more grounding for any reason. These are examples and we invite you to take these and make them your own.

Scenario 1: Safety when participating in protests

You are about to attend a mass protest. You need to be able to keep the data in your phone safe and to keep yourself from being tracked in the protest, but also be able to use your phone to contact allies for emergency purposes. You are also thinking of using your phone to document the protest and any possible human rights violations that will happen there.

Scenario 2: Safety at (unsafe) border crossings

You are in transit, and are about to cross a border into an unsafe location. You want to be able to use your phone to keep contact with your allies, but not as a personal tracking device. Ask people

what their strategies are when they know someone else may have access to their phone. Examples of situations might include border crossings, flight boarding, going to a street protest.

Scenario 3: Safety when there is threat of arrest or seizure

You have heard from a reliable contact that you are being targeted by the state for arrest and seizure of devices because of your activism.

Scenario 4: Safety when there is risk of theft and harassment

You are concerned that someone may steal your phone and use the content to harass you.

Ask participants to document their discussions on paper and to divide their paper in 3 sections: before, during and after. Their paper will look something like this:

Participants' Paper Example		
BEFORE	**DURING**	**AFTER**

In small groups, facilitate participants to work through the following sets of questions.

How are people impacted: In this scenario/the event or experience you are preparing for, what are the risks? Who is impacted by this? Consider yourself, people who are on your phone in some way, your organizing/the issue you are working on (if applicable).

You can use the following questions as guiding questions for groups to consider how to reduce the impacts on people from a tactical perspective.

Before: Think about what you will do to prepare your mobile phone for this scenario.

- What files will you delete from your phone? Why?
- What applications will you install? Why?
- Who will you inform about your plans? Do you want to set up a check in system for before and after the experience, is that possible?
- What secure communications set-up will you have with others?
- What other strategies will you and your allies have in place to keep yourselves safe during this experience?
- Location services: Is it safer for you to have location and tracking on or off? Do you want other trusted people to be able to follow your location?

- Remote wipe: Do you want to activate remote deletion in case you lose access to your device?

During: Think about how you will use your phone during the scenario.

- Power: Is power a concern? How will you ensure that people's mobile phones have charge?
- Service: Is service a concern? What will you do if people cannot use their mobile service, apps, or data? Is there an offline plan?
- Who do you want to communicate with during this scenario? How will you communicate with them?
- Are you documenting the protest? If so, are you using any special app for it?
- Who will be able to contact you through your mobile phone?
- Who will you be contacting through your mobile phone?
- If you will need to use a SIM card different from your regular SIM card, how will you choose your carrier? Is there one that is safer than others for your communication? Who will be able to contact you? Who will you contact?

After: Think about what you will do after the scenario.

- Media: If applicable, what will you do with the footage, pictures, audio and other media that you gathered?
- Metadata and records that your mobile makes: What considerations do you need to take about the data your phone is creating during this scenario, consider metadata, records of communication, location of your device.
- In case of seizure: How will you know if you have a spy-ware free phone?
- In case of theft or seizure: What will you do to regain the integrity and safety of your mobile phone?

Give the groups a minimum of 30 minutes to a maximum of 45 minutes to come up with plans, strategies and tactics.

At the end of the group discussion, ask the groups to talk about their plans, strategies and tactics.

Use the results of the report-back to plan your hands-on for mobile safety.

Input (optional) - 15 minutes

> **Notes for trainer/facilitator** Depending on your style and your participants, you may want to deepen and add inputs as groups debrief or as a planned input section. The following are notes that we believe may be useful as you plan this.

Before

- Let people know you will be in a situation where you are concerned about yourself and your personal belongings. Make plans to check in with your trusted friend as you enter and exit this situation. Choose a frequency of checking in that fits the risks you are facing.
- For a very high risk situation: We recommend planning to be in touch as frequently as every 10 minutes. For example, if you are going to be at a high-risk protest or doing a particularly risky border crossing. Plan to communicate every 10 minutes on your approach, while you wait (if possible), and upon crossing.
- For less risky situations: For example you are in a town working with a group of sex workers. You are traveling to and from meetings throughout the day. Make a plan to check in with your trusted partner when you are on your way and when you arrive at each meeting. Check in when you are going to bed, a simple “going to bed” and when you wake up “starting the day.”
- Clean it: What is on your device that you may want to keep private?
- Log out: Log out of any services that you don't need to be logged into. Don't stay logged into services you don't have to be logged into. If someone takes your phone, they will be able to access your accounts, see your activity, act as you on the service if you are logged in.
- Lock and encrypt: You can encrypt your phone, SD card, and SIM card, locking each with its own PIN will mean that if someone else has it, they won't be able to access the information on it or use it on the network without your PIN. *If you are in a situation where you are being threatened for your access information, you may not be able to keep the PINs and passwords private. Discuss with others and consider this as you make your safety plans.*
- Device Copying: Many law enforcement agencies have access to equipment to copy digital devices including mobile phones, laptops, hard drives. If your phone is copied and is encrypted, the person who copied it will need your password to decrypt it. If your phone is not encrypted, the person who copied your phone can access all content via the copy of the phone.
- Be quiet: turn off notification sounds and graphics, keep it on mute
- Remote wipe: You may or may not want to enable remote wipe. In some situations, you may want to prepare for remote wipe and ensure that you and a trusted colleague have the ability to remotely delete the content of your phone if someone has taken it or you have lost it.
- SIM cards and devices: Our mobile phones are devices that create and broadcast a lot of information, from messages and calls that we make and send, to data sent to apps, to location and time stamps communicated frequently with mobile phone carriers. Assess if you want to carry your personal device into a risky situation. If you do, this device may be linked to you by opponents and tracked ongoing. You may instead, choose to leave your device at home or to use a “burner” device, a device that you intend to use only for this action or event, that you expect will be linked to your activity during the action or event, and that you can and will discard afterwards. Note, you will need to have both a phone and SIM card in order for this to work. Both your phone and the SIM have an ID. If you use your regular phone and a burner SIM, and replace your regular SIM after the action, you will still be known by the ID of your phone. *This is an expensive option and keeping a phone and SIM from being tracked to you will take a lot of planning and the ability to stop using and destroy the device. If you are unable to discard the device, you might still think*

of carrying an alternative phone into risky situations, but the more you use it, the more easily it will be linked to you.

- Removing SIM cards: If you find yourself entering a risky situation without having planned, you may want to remove sensitive parts of your phone like your SIM card and memory card (if possible). *Note: in some situations this may be used as an excuse by aggressors to escalate harm.*

During

- Remote wipe
- PixelKnot for encrypted messaging
- Firechat for protests and network shutdowns

After your phone has been out of your control

- Clean it or get a new device: Our best recommendation is to factory reinstall. If you can afford it, replace the device; do not reset your first device, instead send it to someone who can analyze it.
- Your services: Reset passwords to all of your services.
- Let people know: If your phone has been out of your control, let your contacts and people you had active communications with know and what the implications may be for them.

Additional resources

- EFF Surveillance Self Defense - Encrypt your iPhone - https://ssd.eff.org/en/module/how-encrypt-your-iphone
- EFF Surveillance Self Defense - Using Signal on an iPhone - https://ssd.eff.org/en/module/how-use-signal-ios
- EFF Surveillance Self Defense - Using Signal on an Android - https://ssd.eff.org/en/module/how-use-signal-android
- EFF Surveillance Self Defense - Using Whatsapp on an iPhone - https://ssd.eff.org/en/module/how-use-whatsapp-ios
- EFF Surveillance Self Defense - Using Whatsapp on an Android - https://ssd.eff.org/en/module/how-use-whatsapp-android

image-1605451259399.png
Image not found or type unknown

Revision #4
Created 16 April 2023 04:15:34 by Kira
Updated 27 June 2023 13:20:33 by Kira