Image not found or type unknown

Planning mobile communications for actions/organising [tactical activity]

tactical_activ_circular_200px-withte

Image not found or type unknown

The following are guiding considerations for groups who are organizing and participating in actions and relying on Messaging Apps. Using this guide, you can facilitate discussions to support groups in considering the kinds of communications they are having and to design group management, message and device protocols that meet the safety needs for that communication.

This activity has 3 stages:

- Mapping communications & Assessing risks
- Planning: Design groups and settings
- Installing Apps (optional)
- Implementing (optional)

If groups have not yet chosen the messaging app they want to use, you may want to do the activity Discussion, input + hands-on: Choosing mobile apps

Learning objectives this activity responds to

- 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. If participants include individuals who will be group admins for messaging groups, plan to implement the designs in the workshop.

Time required

This activity will require about **60 minutes** to map and design and up to **3 hours** if you will be installing messaging apps, mapping and designing, and implementing.

Resources needed for this activity

- Paper for people to draw and complete the Mapping chart

Mechanics

Mapping communications and assessing risk

Consideration: Privacy

Consider that you may have different types of messages to communicate via signal and that some messages can be more public than others. Map the kinds of communications you have and design groups to match your privacy considerations.

What kinds of communication are you doing and what considerations do you have around who has access to communication? Suggest that participants consider these different groups. Ask them if they have more types of information -- for example, is there information that only 2 people should

know, that only one person should know and document and not share?

WHO	EXAMPLE COMMUNICATIONS
1 needs to be kept among a very small circle of people who know each other	*location of lead organizers*

2 is vital for volunteers to know or for small groups to coordinate around	*changes in crowd location*
3 can be shared openly	*rally start time, groups who endorse this action publicly*

PLAN: Design groups and settings

Work with participants to design groups to correspond with the different types of communication.

Guiding suggestions around group design: We suggest starting from these design questions. We have included example suggestions for group management and settings for some common types of

groups. Ask the participants what about this will work and what will not, facilitate the group in modifying the designs to respond to parts that do not work.

Membership

- WHO - Who can join this group?
- HOW - How do people join this group? What is the procedure? Do they need to be vetted, introduced, do they opt-in or sign up?
- ACKNOWLEDGEMENT - How does the group acknowledge when a person joins? Why would you want the group to do this or not?
- COMPLIANCE - What do you do if someone joins without following procedure?
- PERSONAL INFORMATION - with the messaging service you are using, can members of a group can see numbers of other members of a group? If so, for anyone who needs their number to not be known as part of the organizing, they should not join any large groups where the other people don't already know their number and that they do this work.

VERIFICATION: Know who you are talking with

For a type of communication, how will you verify who you are talking to?

- FACE-TO-FACE - will you require that any group member meets the rest of the group face to face in order to join? can a person just be added and vouched for by a member of the group
- SAFETY #s - VERIFY that your Messages are reaching the correct devices. If you are using Signal or Whatsapp, VERIFY SAFETY NUMBERS
- SAFETY WORDS - VERIFY that your calls are reaching the correct devices. If you are using Signal for calls, SPEAK THE SAFETY WORDS to one another. If you are using another calling application, do you want to have a way to check in at the start of a call to verify that a person is who you intended and speaking freely?

Message security - settings

Discuss, based on the sensitivity of the information you are communicating, what agreements do you want to make about how people are using message settings?

- DELETE Messages - How long should group members keep chat logs on their devices?

- DISAPPEAR Messages - In a Signal chat, you can set how long messages will remain before being automatically deleted. Do you want to use this feature? How and why?
- HIDE Messages on your home screen - Set Messaging apps to not preview on your home screen so that if you lose control of your device, people cannot just look at your home screen to see message content
- CODES - For extremely sensitive information, we suggest establishing code words before planning and action. For example, you might substitute words "We're ready for the tea party" instead of "Ready for the protest!"

Common group design templates

1. Small very strictly verified groups for sensitive information

Consideration/Risk: That people will join groups who you don't know and don't want to have access to information that is not okay going public.

- If you have sensitive information that needs to be shared only between a set of known people,
- Very small group, 8 or less, everyone knows each other and has met face to face;
- Only add people when you are face to face;
- VERIFY Identity (on Signal, verify Safety Numbers) in person;
- If anyone's safety numbers change, re-verify in person.
- Don't say more than you need to, don't take unnecessary risks
- DELETE

2. Pods - small groups

Consideration/Risk: That people will join the group and send information that is not useful or intentionally incorrect.

- This manages for the risk of individuals spamming the large group and making it unusable and too noisy;
- 2-20 people, whatever it takes to keep chatter down and have a manageable number of Signal Pods;

- A large group may have multiple pods to keep communication manageable and relevant;
- Pods are connected to one another so that information can flow between. You might consider having one point-person in each pod so they can push information that everyone needs to have;

3. Open group, public Information

Consider information on this channel to be public information in real-time. While information from any of the other groups could be leaked or shared outside of the group, this is a group that you automatically consider to be public.

- If you have any information to share that can be made public, use this!

Device security

If your device is taken, prevent others from pretending to be you and reading your information like signal messages, contact book, email etc. For more detailed facilitation guidance around device security, see the activity: Back it up! Lock it! Delete it! a.k.a. Someone took my mobile: Border crossings, arrests, seizure, theft

- Set your lock to immediate/trigger with any button
- Set a strong password
- Encrypt your phone
- Encrypt your SIM card

Power and service

What if people can't use SIGNAL or your chosen App, Phones, Internet, for any reason - power, busy network, shutdown etc. Do you have backup or redundant internet access - a portable wifi hotspot for instance (if it uses cellular data that would also go down)? Is there an offline plan? Will your hub have a power-charging station for volunteers?

Additional resources

- About how to Verify Safety #s and Safety Words - https://theintercept.com/2016/07/02/security-tips-every-signal-user-should-know/

image-1605452256072.png
Image not found or type unknown

Revision #6

Created 16 April 2023 04:08:39 by Kira

Updated 28 July 2023 14:51:35 by Kira