Discussion, input + hands-on: Choosing mobile apps [tactical activity]

tactical_activ_circular_200px-withte

Image not found or type unknown

This is discussion and input activity that will focus on enabling the participants to choose mobile apps for themselves, especially after the workshop.

This activity has 3 stages:

- Discussion: What are you using and why?
- Input: Best practices for choosing apps
- Hands-on Activity: Assessing Messaging Apps **OR** Hands-on Activity: Assessing Popular Apps

Learning objective 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;
- 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 session may apply to anyone who has ever used a mobile phone, and wants to have a better handle on how to choose apps.

Intersectionality flag: this activity is designed as practice with assessing safety of mobile apps, specifically messaging apps. Other types of apps that may be more relevant for your participants might include the following:

- menstrual/fertility apps and the data they collect and birth control solutions they might offer
- dating apps
- messaging apps, and immediate erasure /flash apps
- safety apps, esp. for women and what they reveal, what can be turned on and off, if there is remote access,
- gaming or other apps with interactive component
- performative apps like tiktok

Time required

This requires about **60 minutes.**

Resources needed for this activity

- paper for small groups to write notes
- White board or large paper for recording shared notes
- some mobile phones with data and app store capability

Mechanics

Discussion: What are you using and why? - 10 minutes

In plenary, ask: What are 5 apps you use the most? What do you use them for? Get everyone to contribute to the discussion.

- list down the apps as participants mention them, ask who else uses the apps and mark down the # of users of the app in the room
- list down their reason for using the app

Then ask: How did you choose them?

- write down the responses to how they choose the apps and

To synthesise, summarise the reasons and go into the input.

Input: Best practices for choosing apps - 5 minutes

- Research! Learn about options, learn about which is a trustworthy app. Ask participants to share their methods of research – you could read about it somewhere online/offlline, ask a friend who you know likes to research. Read positive and negative comments in the download center.
- How do you begin to make sure that it´s a secure app? Who develops it? What is their privacy policy? Is it open source? Has there been incidents of the app being used to get access to systems?
- Understanding the permissions that apps require. For example, why might a game app need access to your camera or contacts?
- What makes you feel more secure/confident using the app – can you control the permissions? Do you know where it stores information about you or that you generate with the app? / Do you know where stuff goes?
- If this is a social app, how do you want to engage with people on this app? What can you choose about who you are visible to, what is visible to people, how people can interact with you and you can interact with them? What are the default settings, what do they reveal about yourself, who do they connect you to? Do you know of any safety issues on this tool? Are there reporting mechanisms that you can use? That could be used against you?

Hands-on activity: Assessing popular apps - 15 minutes

Go into the app store and try to find an app that does something common in the context. In an urban setting, maybe a taxi-hailing app, subway system map etc.

How do you choose? Look into (1) what permissions does it ask for (2) who is distributing the app and who manages and owns the service. There are a lot of apps out there that are copies of popular apps, made to look like something you want like a game or a subway map and they are actually designed to do other things like send your location to someone else. The developer or company that is distributing the app will be named in the app store. Share what you know about who owns the app/runs the service and research to assess ways in which the values may be similar and different from yours and how that may impact your privacy and safety while using the app. If you are choosing between multiple apps that appear the same, look elsewhere online for more information about the app and who is the developer or company distributing it and double check that you are downloading this one.

Activity: Assessing messaging apps - 30 minutes

Break into small groups. In small groups:

- Identify 2-3 apps that your small group are using for messaging
- Answer the guiding questions

In plenary: Share back, each group share one app until you have shared all of them.

Guiding questions:

- Who, among participants, uses it? Is it easy to use?
- Who owns it? Who runs the service?
- Where are your messages stored?
- Is it encrypted? What other safety and security settings does it have? What other ways do you keep your communication safe when using this app?
- When is it good to use?
- When is it not good to use?

List of messaging apps and considerations

SMS

- Everyone uses SMS
- Mobile company. Particularly risky if there is history of collusion between telco and government, or it´s a government-owned telco or if the company is corrupt.
- Stored by the mobile company -- different retention policies. Messages transmitted to towers between you and the person you are sending the messages through. (to?)
- No encryption.
- Good for communication of topics that are not risky.
- Frequently a cost per message.

Calls

- Everyone uses it
- Mobile company has control over it.
- Stored in mobile company -- metadata, for sure.
- Example of insecurity: Hello, Garcie! Incident in the Philippines where a phone call between the ex-president, Arroyo, and the head of the Commission on Elections, was intercepted, witnessing the president telling the COMELEC head how much lead she wants in the next elections.
- Good for communications that are not risky.
- Frequently a cost per call.

Facebook Messenger

- Anyone with a FB account can use it.
- Comes with its own app
- Encryption promised but not verified
- Facebook owns it
- Instead of using the FB app, use Chat Secure instead. You can use your FB credentials to chat with other FB users. But for encryption to work, the people you are chatting with also need to be using Chat Secure and communicating with you via Chat Secure.
- Frequently free, otherwise requires an internet or paid data connection.

GoogleTalk

- Anyone with a Google account
- Comes with its own app
- Encryption promised, not verified
- Google owns it
- You can use Chat Secure for this as well.

Signal (recommended app)

- Run by tech activists
- End-to-end encryption
- No cloud storage. You store messages on your phone or on your computer, Signal does not store messages after they have been delivered.
- Also has encrypted calls
- Used for sensitive communications

Telegram

- Popular messaging app
- End-to-end encryption only for secret chats

WhatsApp

- Lots of users
- Facebook owns WhatsApp although the WhatsApp developers promise to safeguard users´ privacy in their Privacy Policy
- Only stores undelivered messages. (what only stores undelivered messages, the whatsapp server?)
- End-to-end encryption, but if messages are backed up to your associated email, they are stored unencrypted.
- Good for communicating with a lot of people
- Still some concern about FB ownership

Wire

- End-to-end encryption promised, in the process of verification
- Developed by former Skype developers -- of note because Skype once had backdoors for the Chinese government that they built in collusion with that government
- Has encrypted voice calls

Additional resources

- What is encryption - https://myshadow.org/alternative-chat-apps#end-to-end-encryption-amp-perfect-forward-secrecy
- MyShadow - Alternative Chat apps: https://myshadow.org/alternative-chat-apps
- Why Signal and not Whatsapp
- EFF's Tips, Tools and How-tos for Safer Online Communications - https://ssd.eff.org/en
- It's also a good idea to do a web search about the latest security issues with the apps that you plan on training in. Key words to use are: name of app + security review + year, or name of app + known security issues + year. Depending on what you find, you might want to remove an app with known and un-solved security issues from your training.

image_1605451879726.png
Image not found or type unknown

Revision #3
Created 16 April 2023 04:18:12 by Kira
Updated 27 June 2023 13:21:28 by Kira