Image not found or type unknown

Alternative tools for networking and communications [tactical activity]

tactical_activ_circular_200px-withte

Image not found or type unknown

This learning activity is mostly guided hands-on for individuals and groups to start using alternative tools to "free" proprietary services.

This activity is most effective when the participants are part of the network so they are able to start developing new ways of communicating among each other.

This activity will focus on three communication tools that are commonly used: Email, chat apps, and alternatives to Google docs.

Learning objectives this activity responds to

- Come up with some strategies to create safe online spaces for themselves and their networks.

Who is this activity for?

This can be run with participants with varying skill levels in using online tools.

Time required

To complete this, you will probably need at least 5 hours.

Resources needed for this activity

- Internet connection
- Laptops
- Mobile phones
- Projector

Mechanics

The point of this activity is to encourage your participants to be less reliant on commercial services that breach users privacy and security.

Protonmail hands-on

Why Protonmail?

- Non-commercial
- Hosted in Switzerland with strong data protection
- Has strong privacy policies about user data
- Offers end-to-end encryption by default (depending on the experience of the group, you might need to do explain this). By default, they employ encryption at-rest. Emails are stored encrypted on their servers – which means the people who own Protonmail will not be able to read your emails (different from the Google model where they focus on encryption in-transit only – messages are encrypted while it is being sent, but once it gets to their servers, they have the means to ¨un-lock¨ your emails). This might need some differentiation between HTTPS and GPG to explain.

- Will allow users to send password-protected emails between different email services (i.e., a Proton user can send password-protect emails to a Gmail user, and the using that same message send a password-protect email back)
- You can opt to have self-destructing messages – for your most sensitive communications.
- Has GPG built in, so if you are looking to extend the training to GPG encryption, this is a good tool to start with

Protonmail limitations

- For free accounts, only 500 MB of space. For 5GB space and more, users need to pay. https://protonmail.com/pricing

To sign up for a Protonmail account: https://protonmail.com/

Notes: If you all using the same internet connection (as we do in training workshops), Protonmail might not allow multiple sign-ups on the same IP address. This might cause delay in the activity. Having multiple access points (with different IP addresses) will mitigate this issue.

> **Jargon Watch:** This has a lot of jargon. Please make sure that you have established a way for the participants to pause and clarify concepts they don´t understand as you do your training. It could be as simple as reminding them that they can raise their hands any time when they don´t understand something, and you asking them directly if they don´t understand a technical term.

Signal hands-on

Why Signal?

- Independently-owned and run by tech activists
- Offers end-to-end encryption
- The encryption protocol that WhatsApp uses is based on the Signal back-end. The difference is that Facebook does not own Signal – so communications and users are more secure.
- Messages in Signal are stored only on their servers until it received by a device (mobile or computer). Once it received, the message is only stored in the device that sent the

message and the device that received it.

Signal limitations

- Can be slow
- The interface is basic
- Requires a mobile number to use – so for contexts where there is registration of mobile phone numbers, this can be an issue.
- There is no message syncing on Signal. So even if you can use Signal on your mobile phone and your laptop with the same account, the messages will only be stored in the device that receives the message first. This is part of what makes Signal secure.

Signal can be downloaded on the Google Play Store and on App Store.

Tasks for the Signal hands-on

- Download the app
- Set up an account. This requires the mobile number being used to be accessible to the user during set up.
- Sync contacts.
- You can opt to use Signal to manage even your SMS messages – it means it will store those messages on your phone encrypted. It will NOT encrypt your SMS messages as they are sent.
- Password protecting your Signal app. Privacy >> Screen lock
- Block screenshots in the app. Privacy >> Screen security
- Verify identities. Have everyone share with each other their Signal numbers. Once they have added people others to their Address Book, click on a contact then scroll down to look for View Safety Number, then click on Verify. This will have two users to scan each others QR codes to verify identity.
    - What this means is that if ever that contact changes phones you will have to re-verify their identity on Signal. This is an extra layer of security to ensure that you are know who you are talking to, and if that person is no longer verified, you should probably take steps to be more careful with your messaging with that person.
- If needed, create a group chat on Signal.

Riseup Pad / Ethercalc hands-on

Why?

- You don´t need to sign-up for an account to use these services
- Simple, light-weight interface for communities with slow connections
- Offers anonymity
- You can control how long the pads / calcs can be retained

Limitations

- Simple formatting
- Pads can´t have tables
- Ethercalc editing is not like Excel

Set up a pad: https://pad.riseup.net/

Set up a spreadsheet: https://ethercalc.org

Safety considerations in using pads

- Check to make sure that your pads are updated as some of them expire and are deleted automatically, if not updated for a long time.
- You can password protect a pad to limit access to it
- Be sure to send pad links (and passwords, if you´re using that option) using secure communications channels

Jit.si hands-on

Why Jitsi?

- Allows you to make temporary chat rooms that don´t need log-ins
- Much harder to find a live jitsi chat room (as it is temporary)
- No applications needed (for computers) – just a web browser
- Promised end-to-end encryption

Limitations

- For more than 10 people in the room the connection becomes unreliable

Tasks for Jitsi hands-on

- Set up a chat room at https://meet.jit.si/.
- Share the link with the participants.
- For those who want to use the mobile app, download the app and enter the room name.
- Test voice, video and other functionalities in the app

Trainers notes: Before you begin, practice setting up the services/tools just in case how to do tasks have changed.

Additional resources

Alternative To is a website crowd-sources lists and ratings for alternative tools (platforms, software, apps). They have notes / tags that mention security functionalities of the listed tools. This is a good resource to find alternatives to popular tools.

After finding an alternative tool, confirm its security and privacy features by doing a search with the following terms:

- Name of software + security issues
- Name of software + privacy policy
- Name of software + security review

image-1605452256072.png
Image not found or type unknown

Revision #2
Created 16 April 2023 03:30:25 by Kira
Updated 27 June 2023 13:05:06 by Kira