HOLISTIC SECURITY IN ACTIVIST GROUPS

WHAT YOU WILL FIND IN THIS RESOURCE

INTRO

Security is crucial in our political activism. In order to understand it as much as possible, with its nuances and layers, we prefer to adopt the holistic approach. It emphasizes the intersection and mutual relation of three processes: psycho-social well-being, organisational security and digital security. Each of them can function separately, but only the holistic perspective allows us to see the interconnections, impacts of one on another without prioritizing any. We refuse the competition between them and we believe that taking care of all the aspects at the same time is not only possible, but inevitable to strengthen the whole system of individual, group and societal security.

We recognise that this topic is huge and that is why we want to offer you an accessible way in. This handout is mostly aimed at people from new groups, starting collectives, dipping toes in activism who wish to explore how to do it in a more safe way. At the same time it can provide a structured way to continue expanding the practices and knowledge in long existing groups or perhaps a small push towards creating a reflection space on the topic. We want to emphasise that this handout does not provide exhaustive knowledge and is not sufficient for people engaging in direct action (you might need to explore the area of physical safety more as well as the digital one).

Security is a process of continuous learning, adapting and improvement. When developing a security plan, always first analyse the risk you and your group are facing. The level of security should always match your activism - too many unnecessary security demands for the group members can deter them from participating, too little security can pose a serious threat of repression!

We want to thank all the co-authors who contributed to the resource.

KNOW YOURSELF SO OTHERS CAN KNOW YOU AS WELL

As an individual you probably have some understanding of holistic security for yourself, regardless of the terminology - In which situation do you feel safe, comfortable? What stresses you out? What is your strategy to deal with anxiety or fear, yours or your best friend's? What seems too dangerous for you, when you don't understand the language spoken around you? There are a dozen questions you can ask yourself in order to create a map (a mental one or even a page of words or drawings) of what safety means to you.

When every person in a group, collective or organisation can share with others not only their understanding of safety, but also their boundaries and preferences, strategies and solutions towards it, collective knowledge can be created. This can be a starting point of the first discussion on the topic, part of a care protocol or a security plan your group wants to have. The idea is not to remember everything about everyone, but rather draw the baseline, get to know each other better, include unpopular standpoints or needs and share the vulnerabilities in order to build a strong and resilient group. This is knowledge that needs to be refreshed, nothing is set in stone as people change and grow.

There are many theoretical concepts and models, which can help you to reflect on personal feelings of safety and security, stressors and responses to them and also practices you can implement to increase your psycho-somatic capacity to deal with threats.

Here we are offering two of them:

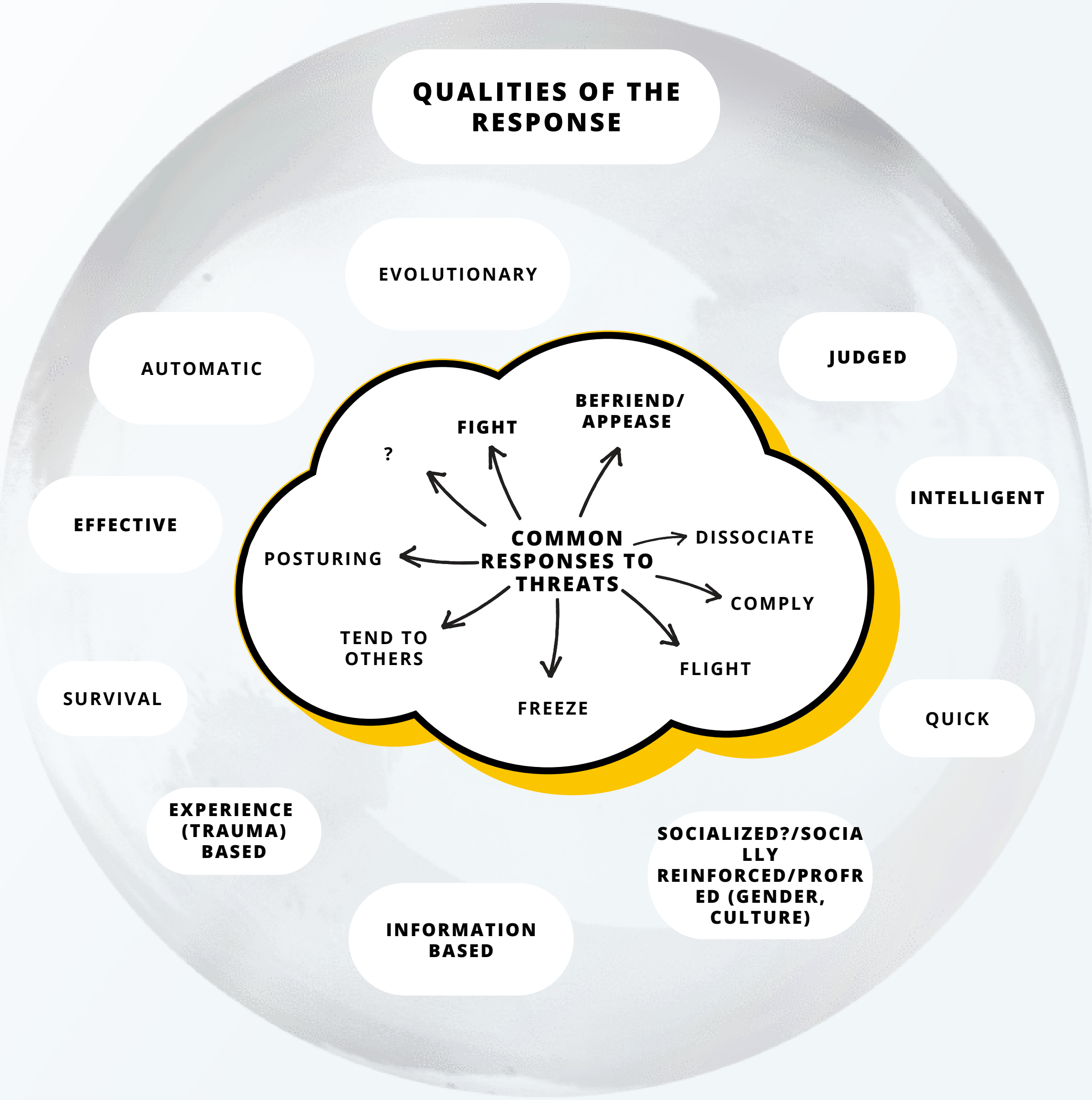
COMMON RESPONSES TO THREATS

Besides the best known fight-flight modes there are many more responses to threat and stress that are embodied in people. Learning about them is the right way to understand what happens in your body on a psycho-somatic level and to appreciate the surviving mechanisms we already have.

WINDOW OF TOLERANCE

Window of Tolerance is a model introduced by a psychiatrist Dan Siegel that identifies 3 states in which we function: arousal, hyperarousal and hypoarousal. Each is characterized by different emotions and sensations, in each we act differently and have other needs.

COMMON RESPONSES TO THREATS



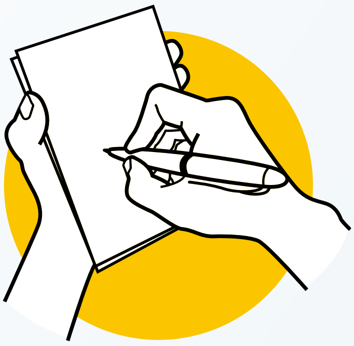
How to work with this model?

Think about your strategies in various stressful situations:

- What comes easy to you?
- What feels familiar?
- When can some particular reaction be helpful?

There is no better or worse strategy – they work, which means they allow us to survive and save our resources. Rather than judging, try to acknowledge them and learn about yourself.

COMMON RESPONSES TO THREATS



In the process of exploring you can focus on two elements:

1. In which situations do I have space to choose my strategy? What has to happen then?

Example: your default and common reaction to stressful situations is fight mode, you act confrontational and defensive.

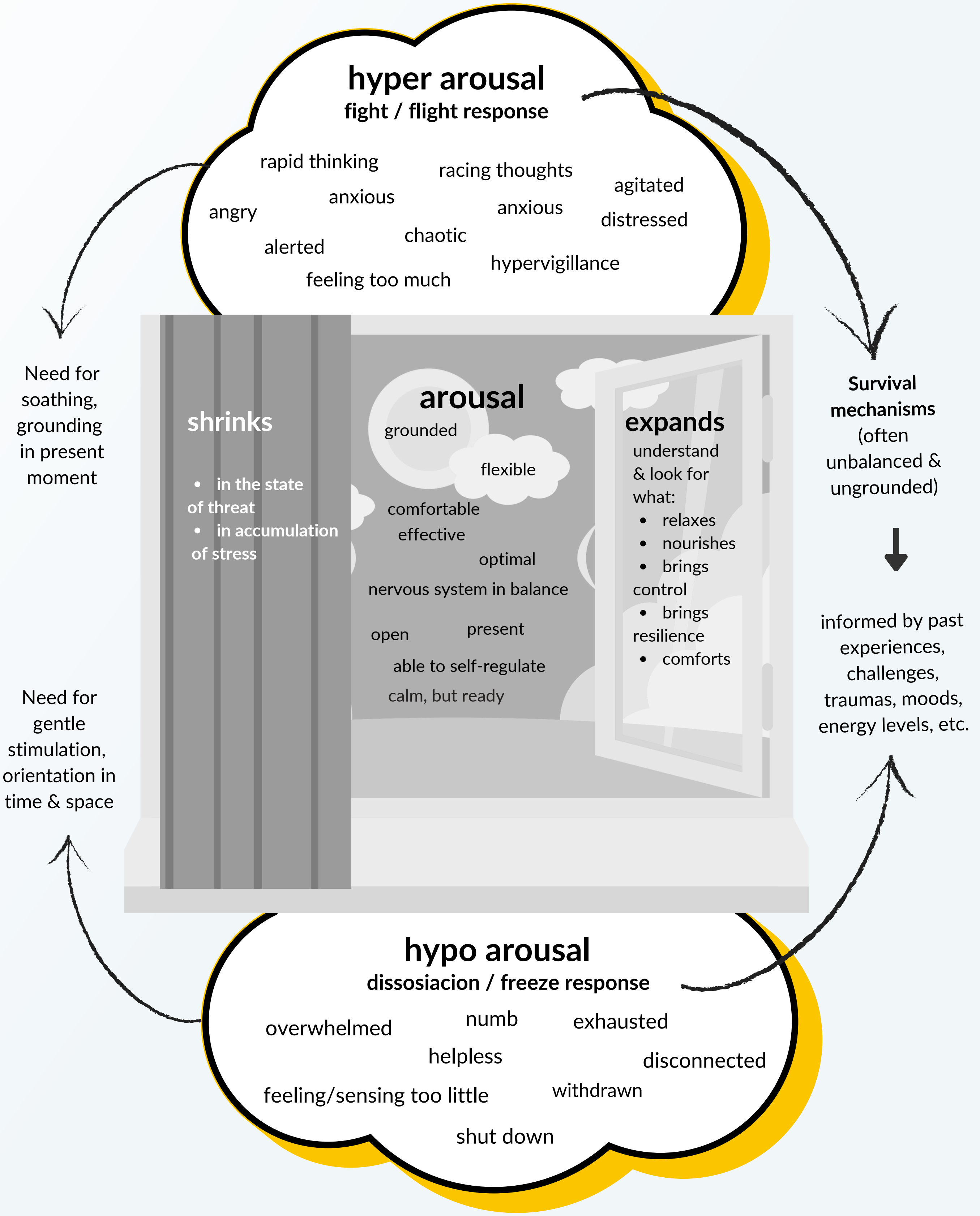
- Is this the strategy you would like to use in the tense moment of group talk, while being criticized or would you rather try other responses?
- If you want to try new responses, what skills do you need to learn?
- What practices to implement?

2. How to use the model on a collective level? Can different strategies be combined? How can we work on group responses to threats and stress? Which seems to be more useful as the collective body reaction?

Example: your group runs a campaign concerning the protection of local bodies of water from being polluted. One of the celebrities made a comment on social media (together with a photo, yes) and triggered a storm of comments, mostly from people who don't understand the topic nor live in the area. Some people from the group want to immediately engage in the media discussion, others have no time even to read the comments.

- Can 'to freeze' response, so pausing, doing nothing for some time be the right chosen strategy for you?
- How else can you allocate the resources saved by choosing this response?

WINDOW OF TOLERANCE



hyper arousal

fight / flight response

rapid thinking

racing thoughts

agitated

anxious

angry

anxious

distressed

chaotic

alerted

hypervigillance

feeling too much

Need for soathing, grounding in present moment

Need for gentle stimulation, orientation in time & space

shrinks

- in the state of threat
- in accumulation of stress

arousal

grounded

flexible

comfortable

effective

optimal

nervous system in balance

open

present

able to self-regulate

calm, but ready

expands

understand & look for what:

- relaxes
- nourishes
- brings control
- brings resilience
- comforts

Survival mechanisms (often unbalanced & ungrounded)

↓

informed by past experiences, challenges, traumas, moods, energy levels, etc.

hypo arousal

dissosiacion / freeze response

overwhelmed

numb

exhausted

helpless

disconnected

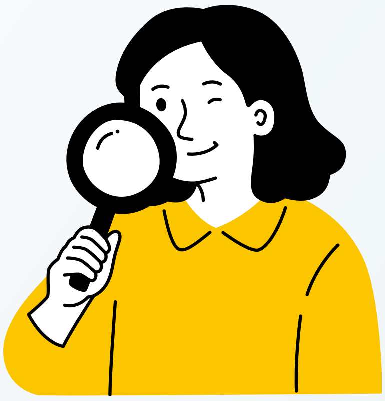
feeling/sensing too little

withdrawn

shut down

WINDOW OF TOLERANCE

How to work with this model?



Thinking about your imbalanced moments and periods of life, as well as the time you felt good, grounded and in control can help you identify the needs you might then have. When you understand what situations are within your window of tolerance, you can go a step further and try to expand it. The bigger your window is the better you can navigate life challenges and reach well-being.

In the following step you can create and plan the routines, on both individual and collective level, which are useful to keep the window wide open.

Example: In the hypoarousal phase you feel overwhelmed and disconnected, you start avoiding people and don't come to the meetings. In that moment reaching out for help is especially difficult. Make a plan with a person or two from your collective, in which you ask them to check with you when you disappear and decide together what is the best way to do it.

LEARNING TOGETHER AND FROM EACH OTHER

Holistic Security is a big concept but what exactly does it mean for you and your comrades, in your context, your language, your experiences? You and the others from your group should fill this term together – with practices, ideas, emotions, scripts, plans, tools and more.

First, bring the topic of Holistic Security on the agenda and educate yourselves. How?

- You can take part in a training, workshop, webinar and share the know-how.
- You can read materials together and discuss them, adjust, change, criticize, localize. Regardless of the result, just engaging in the topic is already a big step!
- You can invite an external facilitator, trainer or expert, who can help your group to understand the idea and develop a security plan.
- You can dedicate 20 minutes of each meeting, in-person or online, to sharing one good tip for increasing the security in your group.
- You can form a working group, which first explores the topic and next includes the rest of the collective with proposals and suggestions.

When educating yourself and within your group on holistic security, keep in mind two important aspects:

HOLISTICY – HOW VARIOUS SECURITY PROTOCOLS ARE INTERTWINED AND FEEDING EACH OTHER.

Example: a person who is not doing well, for instance overworked, burn-out or struggling with personal obstacles is less likely to remember all the rules your collective has established for cyber security.

COLLECTIVITY – THE WHOLE GROUP IS RESPONSIBLE FOR THE SAFETY OF ITS MEMBERS.

Example: the group meetings dominated by male speakers, where the patriarchal patterns are not addressed, can result in overseeing the needs of queer and non-binary participants of the action and, in consequence, expose certain people to systemic violence.

COLLECTIVE CARE, COLLECTIVE RESPONSIBILITY

When we look closer at the collective sense of insecurity, these are things that usually appear - conflict, lack of trust, poor communication, divisions in the movement, scarcity of resources.

To take care of them together we should work on all the fields ongoingly, include them in our protocols in the same way we approach cybersecurity, personal safety or first aid in the actions. While there is no one easy exercise to build the trust in a collective, we can definitely work on our communication skills, conflict transformation procedures and opportunities to build alliances, share resources and grow as a movement. If we can cover the aforementioned pieces, the trust level increases.

We suggest starting with these three tools for creating healthy group processes:

- Facilitation on the meetings
- Giving and receiving feedback
- Mediation

FACILITATION ON MEETINGS

You can find multiple hand-outs and tips online, even books about good facilitation (some of them in the section of Resources). How is it connected to the framework of safety? Here are some examples:

- It feels safer for people to participate in meetings when somebody - a facilitator - holds the space – checks time, gives voices, follows the plan. The role can be rotated to redistribute the power and responsibilities and grow capacities.

- Facilitators can spot and address unhealthy dynamics such as discrimination, microaggression and oppressive behaviour faster. This is crucial because systems of oppression, which we unwillingly copy in our circles, are the key contributor to conflicts, splits and harms in groups. And while facilitation doesn’t solve them, it can add to the group feeling of safety.

- Having an agenda, timeframe, plan, notes and visuals supports people with different needs in participation and opens the space for them to engage. Inclusivity is a strength, and a strong group is less vulnerable to external danger.

MEDIATION

The activist world offers some options; you can hire an external mediator, start the accountability process or learn basic skills yourself. When there is a conflict in your group, but also a will to work on the differences, finding someone who can open the space for an honest talk can change a lot.

Some aspects to keep in mind:

- bringing every issue to the whole group does not have to always be the best way. Ask people directly engaged in the conflicting situation if talking on a side would work. Provide the basic structure – facilitator or witness (someone who measures the time, listens actively, helps rephrasing, summarises)
- read about activist mediation and initiate a small self-educated working group, which can try their skills on some not-too-heavy situations,
- consider regular supervision. With the external person experienced in supervision your group can discuss problems in a safer manner, address the tensions, evaluate the work or deliver feedback

GIVING AND RECEIVING FEEDBACK

Feedback is often a matter of practice, as it requires many skills we are not taught in regular educational institutions. Do some exercises in your group or use the evaluation after an action or campaign to practice. Decide you want to dedicate the time to it - it will improve your group's cooperation in the long run.

In a heated discussion it is not very likely you will go point by point, but when you want to write an email addressing someone's behaviour, why not? Or when you can make time to prepare the constructive critique? It does not hurt to try.

DIGITAL SECURITY BASICS

For everyone in 10 easy steps!

★ Can you recall a full day during which you have not touched your phone?
★ Can your group organize an action without using any online services?
★ If the Internet was down, could you reach your comrades?

Digital means of communication have completely taken over how we organize and work together, therefore we need to put some care into how we use all the cyber tools available to us.

Exploring the ten steps below will give you a basic overview of how to improve security – your own, in your group as well as the people you are in contact with. Whether you want to protect your data and conversations from national states, big-tech corporations or simply online criminals, you need to think about the digital traces you leave behind every day. You should cover your online presence and actions, because sharing some of them (such as your personal data, credit card number or action plans) can cost you money, cause trouble or even persecution!

1 EVERY PHONE IS A TRACKING DEVICE!

Be aware that just the fact of having your phone with you (without even making calls or transferring data) leaves identifying traces of your presence. Many apps can access your phone's location and contacts. You can review the permissions and disable them. Consider going for a walk without your phone sometimes.

2 ACCESS TO YOUR DEVICES

Make sure your smartphone’s lock is a long code (minimum 6 characters). Refrain from using fingerprint or face unlock. Prevent your phone from displaying incoming messages and notifications on a locked screen. Check if your laptop is password protected as well. It's best to use a combination of upper and lower case, numbers, and special characters, minimum of 16 characters.

3 ENCRYPTION FOR EVERYDAY MESSAGING

Encryption is a process of converting readable data into unreadable data that is safe to store on your devices or transmit through the Internet. Use an encrypted messaging app like Signal for everyday conversations. By the way, calls over cellular networks as well as SMS messages are not safe.

4 ENCRYPT YOUR PHONE

Newer Android versions are encrypted by default. Same with iPhones (as long as the phone is protected by a code). Double check on the Internet if your operating system provides encryption by default (or ask your local nerd).

5 ENCRYPT YOUR COMPUTER

Many popular Linux operating systems, newer Windows versions and macOS allow you to encrypt your disk. That means if someone gets physical access to your computer and does not know the password, they will not be able to see the contents of the disk. Check if your operating system allows encryption and consider changing it if that is not the case.

6 STAY UP TO DATE

Make sure automatic software updates are switched on on your computers and smartphones. Newer software means safer software as vulnerabilities are being discovered (and patched) all the time.

7 DELETE, REMOVE, CLEAN!

Get rid of files and emails that you don’t need anymore, same goes for old apps that you don’t use anymore. Enable the option to automatically delete old messages in your messaging app (eg. set up disappearing messages in Signal).

8 E-MAILS

In many countries email providers do not protect the content of your emails if the authorities ask them. Consider using a provider that makes it a priority to keep your data secure (for example riseup.net or tutanota.com).

9 WEB BROWSING

Unfortunately, passwords we use for online services get leaked quite often. Never reuse passwords for different accounts and forget about using the “Save password” option in the websites – instead use a password manager like Bitwarden which remembers all your passwords in an encrypted form (and therefore you don’t need to memorize them all). Also, a friendly reminder to not write your passwords or other sensitive information on paper.

10 PASSWORD MANAGERS

Usually the web browser that is on your device by default is not the most secure choice. Some recommended options are Firefox or Chromium, for extra privacy choose Tor. Add-ons such as Privacy Badger or uBlock Origin can increase your privacy and save you from being overexposed to advertisements. To make your online presence even safer, you can use a VPN like Mullvad or ProtonVPN. If you are using an unknown network (like in a café or in public transport) remember that the information you share could be accessible and monitored.

★ Paranoia is not security ★

Get informed, not scared – find out as much as you need to feel at least some confidence around the digital tools you use, but don’t allow the complexity of the topic discourage you from actually doing things in real life!

★ Security is a process of continuous improvement ★

It is not enough to read one guide and set up your devices once – the technologies, threats and the Internet changes literally every day. Keep bringing up the topic of digital security from time to time both in your organizing and in the context of your everyday life.

RESOURCES AND FURTHER READING

ON HOLISTIC SECURITY

- About the Holistic security concept (many manuals to download): Link
- Ulex training (also trainings focused on collaboration, collective care, dealing with conflicts): Link
- In two parts of the podcast How to Survive the End of the World you can learn more about the Window of Tolerance concept: Link
- A manual you can download to explore the topic of security and inclusivity in an NGO sector working with youth (american context). You can find there self and collective care good practices: Link
- Tools for facilitation and more: Link
- Manual on facilitation: Link
- Resources on conflict navigation and mediation: Link
- Resources for grassroots collectives from the UK based groups Seeds for Change and Navigate
- Conflict is inevitable: Link

ON DIGITAL SECURITY SPECIFICALLY

- Guides on surveillance self-defence: Link
- More guides on security: Link
- Anonymous web browsing: Link
- Password manager Bitwarden: Link
- Clean your data step by step: Link

Non-corporate online service providers:
In case you want to stop using Google for your documents, cloud, e-mail - there are many groups that host these services for free and safely!

- Systemli (Nextcloud, e-mail, Mastodon, polls, hosting): Link
- Nolog (file sharing, documents, pads, polls): Link
- Riseup (e-mail, mailing lists, pads, file sharing): Link
- Cryptpad (collaboration suite including shared files, polls, surveys, forms, slides): Link
- Proton: cloud storage, email and more: Link

THE MOVEMENT HUB

The Movement Hub empowers anyone fighting for that is livable and just for all – by providing a platform for learning and sharing stories, tools and techniques. Whether you’re an activist who fought injustice or climate breakdown for decades, a young member of a grassroots group, or even a changemaker working alone – we have something to offer you.

www.themovementhub.org