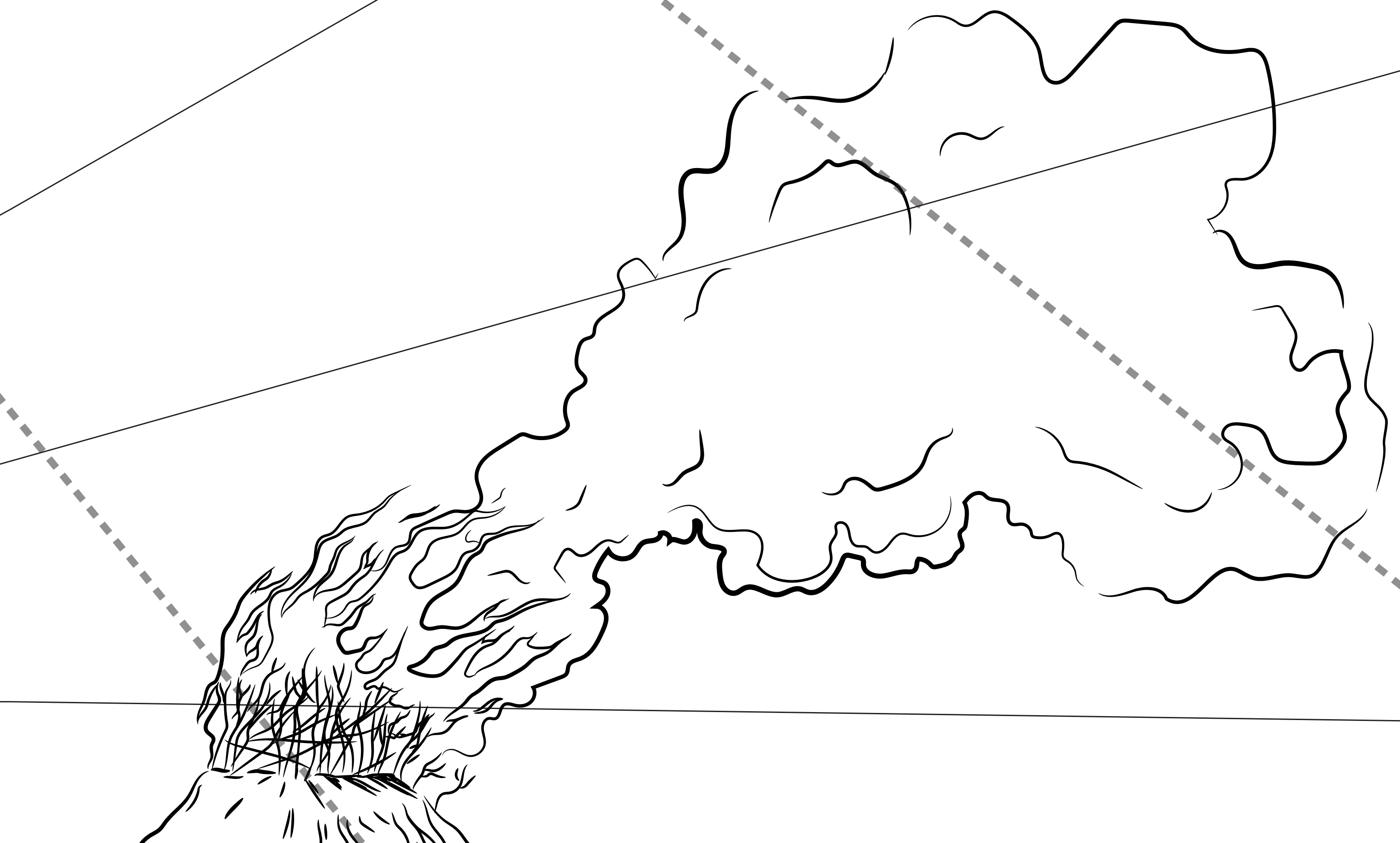
THE COLLECTIVE CARE ZINE

& / DIGITAL SELF-DEFENSE



US AND THEM

Co-funded by the European Union

maghweb

crisis

[EdIPo]
Equipo de Investigación Política

feel free to adapt this information and the parts that are useful to your own context. Take what you need from this information and share the rest.

REFLECTING ON OUR VIRTUAL HABITS AND CONNECTIONS

what virtual lands do we cross and interrelate with?

what traces do we leave behind as we make these crossings?

magic wands don’t exist.
thinking carefully and actively about our everyday habits in the virtual
world and taking on an attentive, open outlook based on reciprocal care
so that we can create new habits, plan and execute preventative action

take time and space

but is not a solitary journey
it is a shared process of continuous learning:
its success depends on our capacity to make it located and collective

paralysed by impotence? Let’s open questions and interrogate our habits while we exchange experiences in the search for tools.

~~SECURITY~~ CARE

~~STATE~~ PROCESS

~~INDIVIDUAL~~ COLLECTIVE

The business model lurking behind our daily interactions cannot be ignored.
We live inside a system that extracts data, that subjects information
to evaluation, speculation, manipulation.

RESISTANCE STRATEGIES

REDUCE_TRACES & IDENTIFICATIONS

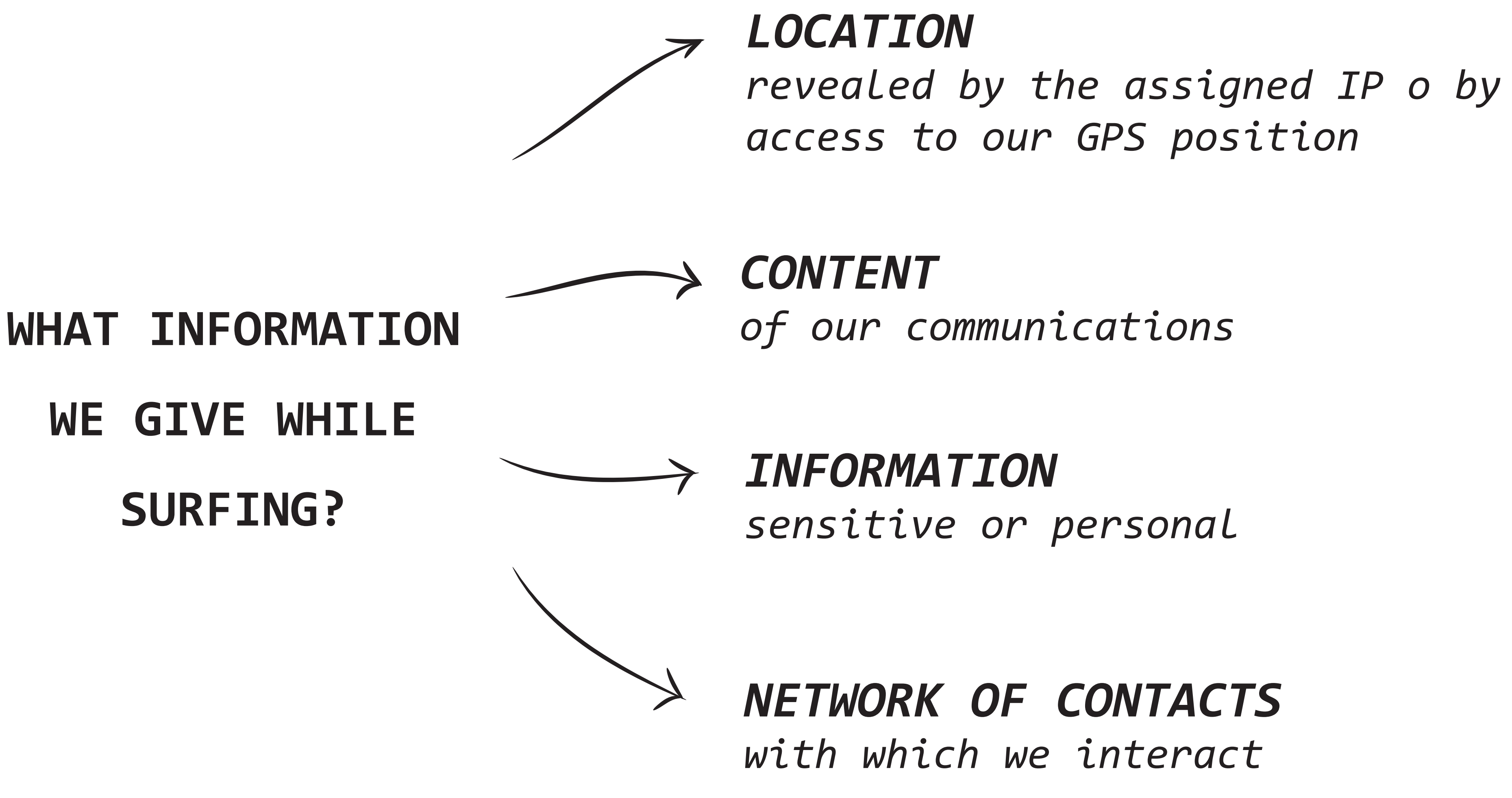
OBSCURE_CONFUSE AND MULTIPLY ONLINE IDENTITIES

DIVIDE_EVERYTHING IN ITS PLACE/ SEPARATE PROFILES

REINFORCE_PROTECTIVE BARRIERS

DEFENCE LINE ONE

There is no technical tools that replace analogue practices: *AVOID OVERSHARING* and only provide the minimum personals sensitive information.
When possible, use different accounts or data.



WHAT INFORMATION WE GIVE WHILE SURFING?

LOCATION
revealed by the assigned IP o by access to our GPS position

CONTENT
of our communications

INFORMATION
sensitive or personal

NETWORK OF CONTACTS
with which we interact

MODEL TO (DIS)ASSEMBLE

A pause in the maelstrom to think together where we stand.

THE GUIDING QUESTIONS TO CARRY OUT A RISK ASSESSMENT

Examples
Collective channels of communication; members' personal data; data belonging to the community following us or participating in our events.

WHAT do we want to protect?

What ***THREATS*** it face?

Examples
Password theft through phishing; bullying and harassment; unauthorised access to devices; identity theft on social media; government monitoring or surveillance; interception of communication

Examples
From an ex partner;
General, ad hoc attacks;
Advertising companies;
Servers and providers that keep all non-encrypted navigation data

Where do they could come from?

How likely is it to happen and how bad is it if it happens?

What resources can we use to defend ourselves?

We're not asking you to be constantly on guard, we're asking you to nurture concrete, conscientious virtual behaviour that reduces damage, based on our risks, capacities, needs and priorities

Identifying threats and ordering them according to their likelihood and damage allows us to assess risk mitigation action more effectively.

THREAT	PROBABILITY 1- very slow 5- very high	DAMAGE 1- light 5- very severe	MITIGATION What can we do?	OBSTACLES
Password theft thro phishing -virtual trickery through false links-	*3*	*5*	*Integrate authentication factors; use an app to manage our passwords; be careful of the links we receive*	*Time and availability needed to reinforce password security and access*

TOOLS for Self-Defense

They are not definitive resolutions

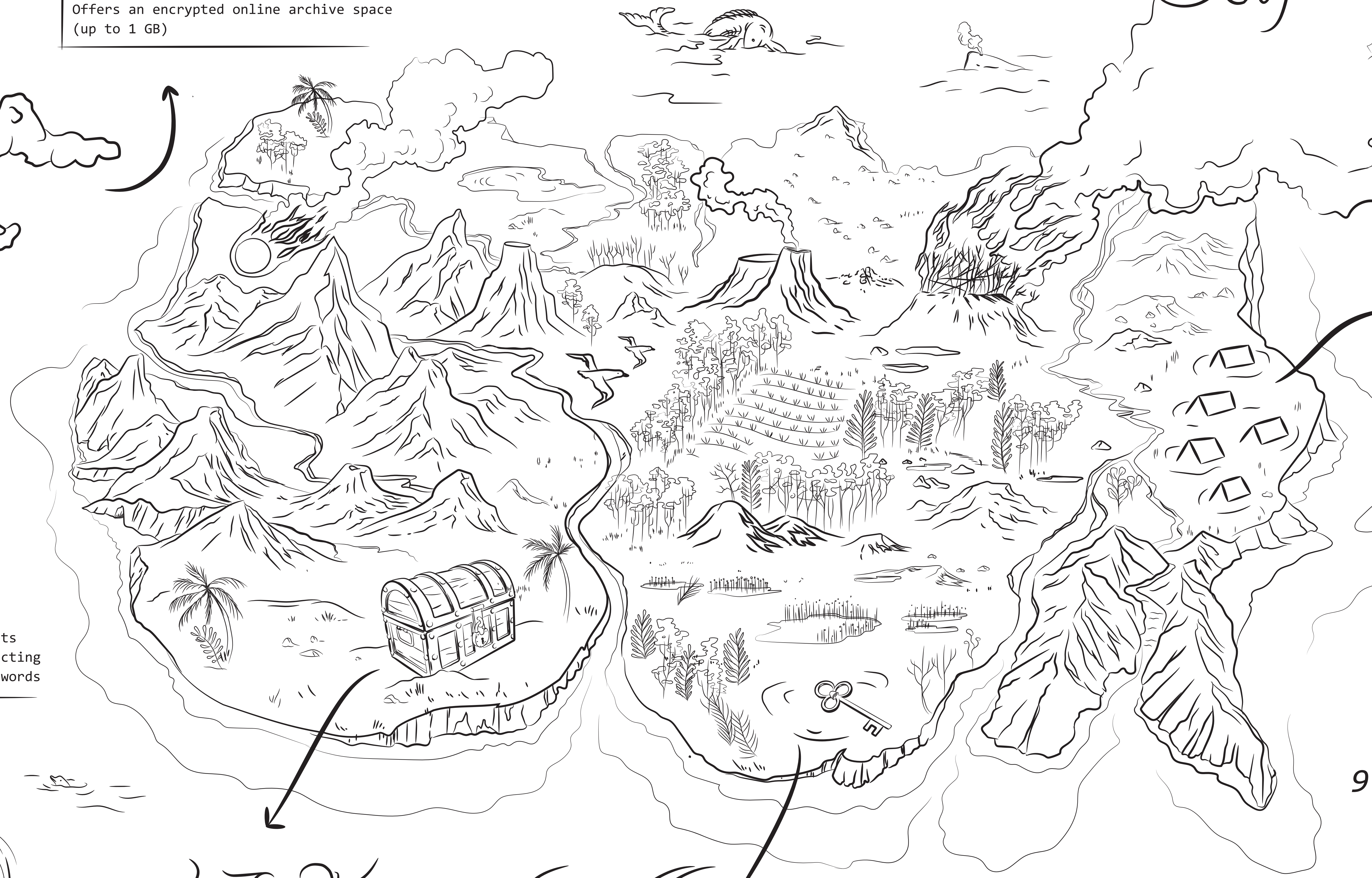
✓ open source ✓ free

Protondrive

8 Encrypted online archiving services (maximum 1GB per account)

CryptPad

4 Online collaboration space that allows you to work on spreadsheets, textual documents, kanban, forms and slides. Offers an encrypted online archive space (up to 1 GB)



Tails

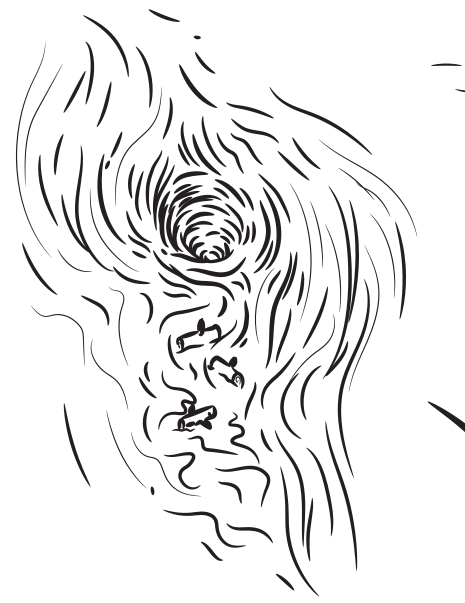
Parallel operating system nature laptop anonymous and amnesiac. Offers a selection of tools for work with information sensitive and communication safe.

Riseup Pad

5 Allows for the creation of collaborative online documents and the possibility of protecting these documents through passwords

Protonmail

9 E-mail with end-to-end cryptography



VeraCrypt

7 Tool that encrypts discs and folders on computers and pendrives.

KeePass

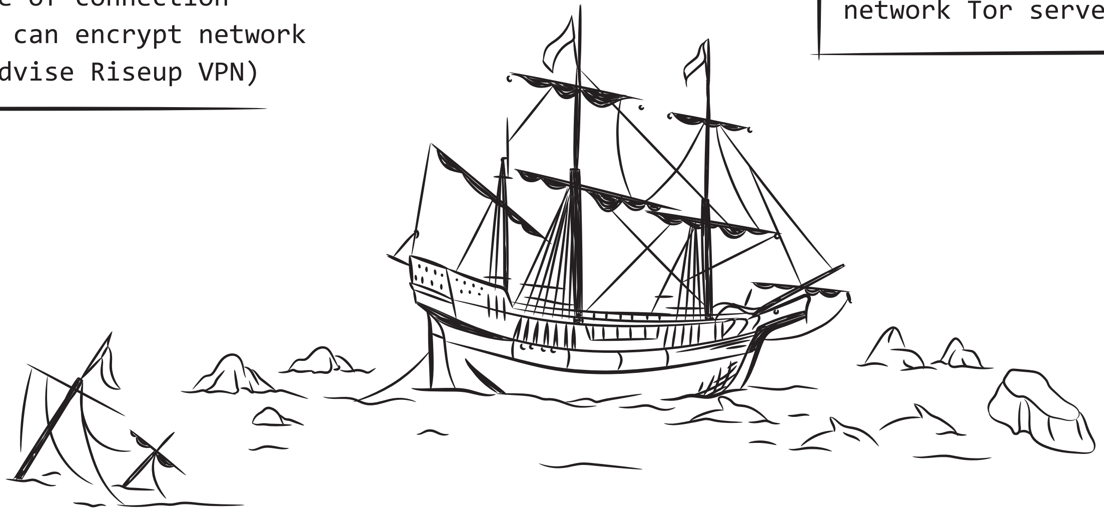
6 Tool that securely manages different passwords with a unique master password

V.P.N.

1 Makes the site of connection anonymous and can encrypt network traffic (we advise Riseup VPN)

Tor

2 Can encrypt the network traffic three times and redirect it through random network Tor servers to hide its origin



Wormhole

3 Allows for the sharing of files (up to 10GB) with end-to-end cryptography through an automatically expiring link

None of these tools are useful if they are not updated

There is no infallible tool, there is no tool that guarantees 100% anonymity on the Internet. However, different tools provide different levels of protection. Tools change just like risks; it's important to always keep ourselves updated and informed. Regularly updating operative systems and software is advised and so is updating our own means of assessment and strategies.

NAVIGATION

1- VPN: https://riseup.net/en/vpn

It makes the site of connection anonymous and can encrypt network traffic. It circumvents censoring and prevents tracing that's used for surveillance or advertising. How? An encrypted connection is like a tunnel, channelling your data through its secure servers into the public internet space.

2- TOR: https://www.torproject.org/download

It can encrypt network traffic three times and redirect it through random Tor network servers to hide the traffic's origin and the destination. It blocks data tracing and makes third party navigation content invisible. Tor can encrypt our data traffic, make it anonymous, sifting it through three levels—servers managed by different people and organisations across the whole world. Tor stops intruders from seeing your internet connection and knowing what your online activities are. Weak spots have emerged in some of Tor's exit ways so adding another level of protection by combining Tor use with a VPN is advised.

COLLABORATION

3- WORMHOLE: https://wormhole.app/

End-to-end cryptography and automatically expiring links file sending (files up to 10GB). The cloud stays online for 24 hours maximum, then autodestructs.

4- CRYPTPAD: https://cryptpad.fr/

Online collaboration space with end-to-end cryptography, allows you to work on spreadsheets, textual documents, kanban, codes, forms, blackboards and slides (up to 1GB maximum). Be careful! Forgotten passwords are impossible to retrieve.

5- PAD RISE UP: https://pad.riseup.net/

Allows for the creation of online collaborative documents on safe servers, the possibility of protecting them with a password and programming their autodestruction. An alternative for virtual chatting that doesn't require other apps.

SAFEGUARDING INFORMATION

6- KeePass: https://keepassxc.org/

Tool to securely manage all passwords so that you don't have to remember them but can access them with a unique master password. Also generates safe passwords.

7- VERACRYPT: https://www.veracrypt.fr/

Can encrypt harddisks and folders that are at rest to avoid third party intrusion.

COMMUNICATION

8- PROTONDRIVE: https://proton.me/es/drive

Makes 1 GB of encrypted archiving space available in an online cloud.

9- PROTONMAIL: https://proton.me/es/mail

E-mail with end-to-end cryptography.

10- JITSI MEET: https://meet.jit.si/

Free software for video conferences, open source and end-to-server/transit cryptography (cryptography from the device to the server, where it is deciphered and newly encrypted before being sent to its destination). Registration not required.

11- CORREOS ELECTRÓNICOS DESCARTABLES:

https://temp-mail.org and **https://www.guerrillamail.com**

Temporary email addresses that not require registration.

SEARCHING INFORMATION

12- DUCKDUCK GO: https://duckduckgo.com/

Research engine that does not register network traffic and does not redirect results that are functional to the user's profile to commercial destinations.

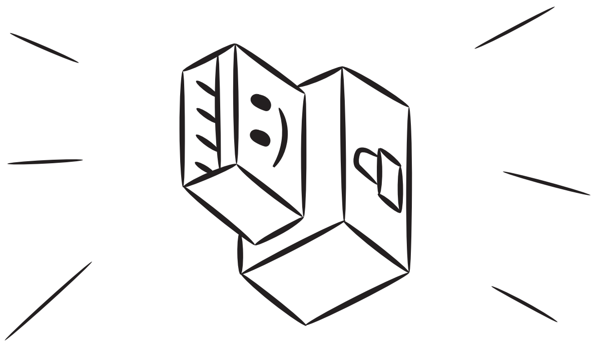
Looking after our virtual safety does not only depend on tools: the weak link is often revealed inside the user's practice, not the user's devices. Even if we do use sophisticated tools, it's always possible for information to leak..

Tails

A portable operating system that protects us from surveillance and censorship.

Independent system that you can load onto a pendrive and use from any computer.

- ✓ **AVOID TRACING**
- ✓ **FREE SOFTWARE**
- ✓ **MAXIMUM FREE SECURITY**



It doesn’t leave any traces on your computer

All you need to activate TAILS is a USB pendrive.

Persistent archive

You can save some file titles in a Persistent Volume

Amnesia

Everything desappears automatically when you stop using TAILS.

Equipment

Has applications with wich you can work on sensitive documents and communicate safely:

- Tor Browser with uBlock, a safe browser with an integrated function for the advertisement block.
- Thunderbird, for encoded emails.
- KeePassXC, to create and keep safe passwords.
- LibreOffice, an app suite from Office.
- OnionShare, to share files through Tor.
- Apps to remove metadata.

https://tails.boum.org

PREPARING EVERYTHING TO SURF WITH PREDEFINED, SAFE CONFIGURATION

To evoid errors:

- *Applications are automatically blocked if they try to connect to the internet without Tor.*
- *All the files in the persistent archive are automatically encoded.*
- *Tails does not inscribe anything onto the hard disk. The whole memory disappears as soon you stop using it.*

recommendations

- Controlling access to and sharing of passwords with Google and other apps: asking ourselves who has access to my passwords, position, photos, connections and contacts?

- Cleaning virtual identity: eliminate accounts and applications that you don’t use, just as you do with photos, messages and emails that you don’t need anymore.

- Interrupt emission of signals (bluetooth, wifi, GPS) and cover webcams when they are not being used. Keep your phone distant to avoid it meddling with sensitive content.

- Don’t trust unexpected links, even if you know the sender. Always check before opening them.

- When it’s possible, activate automatic elimination of messages and choose communication channels that can encrypt information in network traffic (end-to-end).

- Change old passwords, don’t use the same password for more than one account and increase the authentication factors.

It’s important to remember that everything you upload on the internet remains archived even if the user deletes and hides it. Doing a clean to reduce hacker risks is advised but bear in mind that information doesn’t disappears.

SAFE PASSWORD CRITERIA

- Long (one sentence is best)
- Don’t include personal data
- Change it often
- Don’t use it too many times even if you slightly change it each time
- Double authentication factor

IDEAL

Use a password manager that automatically generates passwords, asks you to change passwords and guards encrypted passwords outside of the browser

How safe is my password?

https://www.security.org/how-secure-is-my-password

How do I know if I’ve been attacked by a hacker or if there’s been an information leak?

https://haveibeenpwned.com

US AND THEM

Co-funded by the European Union

maghweb

crisis

[EdIPo]
Equipo de Investigación Política