The time to get ready is now!

When the situation escalates, there is no time or emotional space left to prepare, so start today! Poland is slowly falling down in the rankings for freedom and democracy,[1] as well as for independence of media.[2] The question is not "if" but "when" the internet will start getting shut down[3] and the devices getting confiscated. That is why we need safe communication channels, we need to mask web traffic and build a community around free services.

there is no such thing as total security

Security is not a ready-made solution, but a process of minimizing risks based on cautiousness and improving your habits.

foundations of the Security Culture

I may seem like you have nothing to hide, but remember that materials obtained by secret services and the police can be manipulated, changed and presented in such a way that even completely harmless things could be used to misrepresent the actual story.[4]

- assume that everything ends up in internet (and mobile network) can become public
- you don't need to know everything, so don't ask - it's safer for you and for others
- if you know something, don't spread the word. You may not be the target, but you may be providing information about others who are
- anonymize your contributions, do not use nicknames / names / last names
- delete sensitive data as soon as you no longer need it

The Anarchist Black Cross writes more on this topic in the zine "*What is the Culture of Security all about?*"[5]

where do the agencies obtain data from?

In Poland, there are 9 institutions authorized to conduct the so-called operational and reconnaissance activities, including the Internal Security Agency (ABW) and the police. We know that telecommunications operators store (purely for the needs of the state security agencies) information about where we were, who we called and what we browsed online in the last 12 months. The agencies use this data over a million times a year, because it's there and available immediately to them, without any special orders or permits.

Besides those two, most of the activities of the agencies are secret: they check on us in government registers, they view videos from monitoring systems (including cameras who record license plates on highways or address recording in postal distribution centers), they can put a tail on somebody. They can collect information about thousands of people at once, for example by checking the identity of the owners of all phones

[1] https://freedomhouse.org/report/freedom-world
[2] https://www.press.pl/tresc/65629,polska-coraz-nizej-w-rankingu-wolnosci-mediow
[3] https://rys.io/wypierdalac/netoobrona.md
[4] https://podsluchjaksiepatrzy.org/#inwigilacja
[5] https://pl.anarchistlibraries.net/library/crimethinc-o-co-chodzi-z-kultura-bezpieczenstwa

that were in a protest, or by carefully monitoring selected people e.g. by installing Pegasus spy software on their phones (although it is quite an expensive solution). The head of the Internal Security Agency has been granted the option of wiretapping without the need to obtain a court approval, if he suspects someone of terrorism.

If the police want to wiretap you, they must ask for permission from the court, but this is only a formality - 99% of applications are approved. Annually, the Polish police conduct 8-10 thousand wiretaps, which is 25 a day. The other agencies intercepted 1,267 people in 2019 alone. Permission to wiretap is the only time a police officer has to ask for permission.[6]

Polish agencies and services ask Facebook for data, in 2019 alone they did that 10 thousand times, which is a 100% increase from the year before, and in 50% of the cases they get the requested data.[7] Facebook has its own algorithms to detect undesired behaviors and they report to the police as well (eg. drug trades in the USA).

the key role of human information sources

Impossible? And yet! It is still easier for services to get information from people than to break the security of equipment and devices. 76.21% of the surveyed policemen[8] most frequently use the help of informants (the so-called moles / snitches). We even know of cases of agents steering social movements. The agencies can also obtain information from interrogations and operations (all what happens in the time after the detention) using extensive methods of manipulation.[9]

how far can the agencies go?

[TW: violence]

> *A certain Mark Stone, for many years involved in the radical wing of the movement, organizer of demonstrations, occupations and pickets (including against the G8 summit in Scotland), turned out to be a police informant. The suspicion arose when an activist friend, during their vacation, saw in his passport the name Kennedy instead of Stone. Mark Kennedy lived a double life. He entered into romantic relations with activists. (...) Subsequent investigations revealed a series of ethically questionable actions by British services. There were more spies. With the knowledge of their superiors, while working, they sexually exploited unaware activists. They fathered their children. At times, after completing the "mission" they disappeared from their lives. The fact that police spies co-organized and provoked some of the activities of the environmental justice movement considered against the law led to the withdrawal of charges against those involved in the unsuccessful shutdown of the Ratcliffe-on-Soar coal-fired power plant in Nottinghamshire.* [10]

Stone/Kennedy was in Poland for an info-tour of G8 in Rostok. He, another policewoman and an activist were responsible for logistics for activists for G8 in Scotland and they infiltrated many groups. Various

[6] https://podsluchjaksiepatrzy.org/#inwigilacja
[7] https://panoptykon.org/jak-bezpiecznie-protestowac
[8] K. Horosiewicz, Współpraca policjantów z osobowymi źródłami informacji, Warszawa 2015
[9] http://szkolenia.policja.waw.pl/wdz/informacje/psychologia/27370,Zasady-przesluchania-metoda-FBI.html
[10] https://krytykapolityczna.pl/kraj/pegasus-inwigilacja-ruchow-ekologicznych/

agencies and services spy not only on groups deemed dangerous by them, one agent has infiltrated CIRA – a group of clowns!

resistance - where to start?

This guide is not intended to create a paralyzing fear in you, but rather an action-motivating concern. By reading the text below, you will learn about specific tools that can help you increase the privacy and the level of security, both for yourself and your communities.

set a password on your phone

First of all, turn off the unlock option by fingerprint or face scan, which can be easily obtained by force when your equipment is confiscated. The best is to lock it with a screen lock pattern (connecting dots), because such lock has many combinations. Pin is also okay, but it should have at least 10 digits, and preferably 13. The 4-digit code can be easily cracked by testing the configurations one by one - with help of a computer.[11]

encrypt messages and calls

Signal[12] and Element[13] (formerly Riot) are tested, simple, relatively safe and therefore recommendable messengers. There are two major differences - Signal requires from you and shares your phone number with the people you are talking to, while Element only needs your email. On the other hand, Signal, unlike Element, also encrypts group communications. Remember that even an encrypted messenger will not protect you if, for example, your keyboard movement are being tracked or if your phone is hacked (pegasus).

Less visually attractive but useful for demonstrations (if you take your phone there) is Briar, which allows you to communicate using Bluetooth (so even when there are problems with the mobile network). The disadvantage is that Briar is that it does not work with iPhone.

Nearly all other messengers are designed mainly to collect data about us, data then sold to anyone who pays. That's especially true about Messenger, Telegram, Viber, Discord or Skype. These solutions should be avoided, especially when we are talking about sensitive topics, although in such case electronic devices should be avoided altogether.

Signal is an instant messaging app that can replace the default messaging (SMS) application on your smartphone and additionally it has a desktop version. It sends SMS to your contacts. To fellow Signal users it sends highly encrypted messages in a way that increases the anonymity of communication. It supports sending images, files, voice messages, locations, and group communication can be created. Its interesting features include disappearing messages and possibility of masking faces on photograps. It is successfully used by some groups as a platform for instant messaging, although with mass demonstrations it is worth remembering that the GSM network can simply be overloaded and not always reliable. Signal is open source, so everyone has the opportunity to thoroughly analyze the security and actively participate in improving the program. In itself, however, Signal is not a guarantee of security or anonymity. But, it is a simple first step in the right direction. The familiar-looking interface and user friendliness makes it suitable for anyone. The more people use it, the less information about us the network operators

[11] https://panoptykon.org/jak-bezpiecznie-protestowac
[12] https://signal.org/pl/download/
[13] https://element.io/

and others are able to gather. Telecom operators are required by law to keep every message sent for a period of a year.[14]

do not keep much data on your phone

Typically, a cellphone is a mine of knowledge about the person who is using it. Many people are non-stop with their mobiles, which increases the risks even further through possible loss. It is better to have as little data as possible on your device. To minimize the risk of sensitive information being taken over by others:

- wipe your phone's content frequently
- enable *disappearing messages* (Signal function) - the messages self-destruct after a chosen time
- remember that external memory cards are **not** encrypted by default!
- check what information each application collects about you, maybe it's time to change its permissions or look for alternatives?

update the system and applications regularly

By doing so you will ensure that the security bugs are fixed and that your phone's content remains encrypted (on IOS and on Android 5 onward update is default and automatic, in earlier versions of Android, encryption must be turned on manually in the settings).

Updating the operating system fixes gaps in security (including for anti-virus and firewall programs which are currently built in in the operating systems).

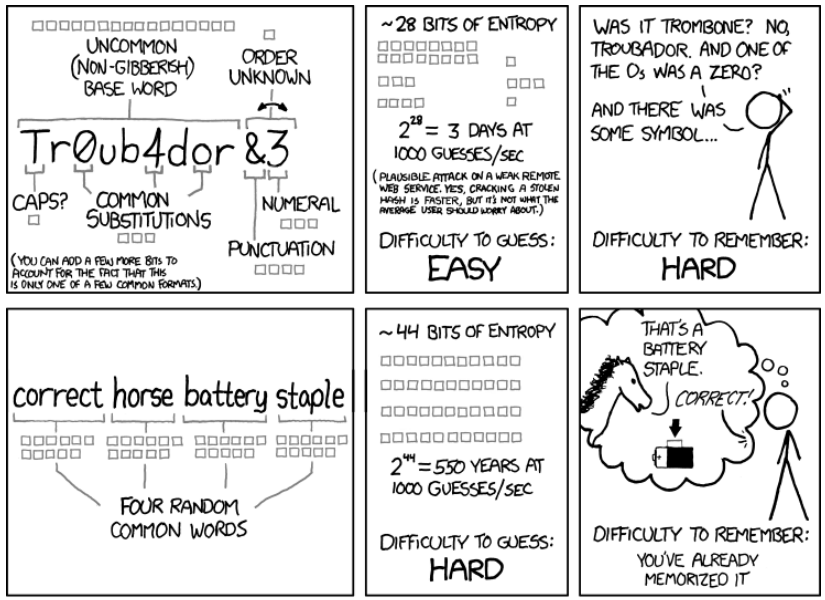
passwords

Imagine a data leak from some site where you created a forgettable account 5 years ago, to only used it once. If you happened to use the same password as to your email, someone could take control of virtually all your accounts by using the "forgot password" option. Therefore, do not repeat the same passwords in different places. Using a modification of the same password is also not a solution, learning about one modification makes guessing the next easy.

How to avoid such situation? Create 4 sentences containing capital letters and punctuation, each of 4-5 words. You don't need to remember anything else! No complicated sequences of characters are required, and your level of protection will be higher.

- The first sentence will be your system's password (for logging into your computer).
- The second sentence will be the password to decrypt the disk (more info below).
- The third sentence will be the password to the e-mail.
- And the fourth sentence to the password manager (more info below).

[14] https://szmer.info/post/3437



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

A password manager is a program / application that creates an encrypted database with information about your passwords at different sites. With the help of a password manager you can generate complex passwords, consisting of all available alphabets, special characters and numbers - practically impossible to break.

We recommend **KeePassXC**, because e.g.:

- Mozilla and Chromium plugin are available and automatically link passwords to accounts
- it works offline
- it works on Windows, Linux and Mac
- it works with Android and iOS
- it can synchronize data between devices
- it offers strong encryption algorithms
- is an open source application (so we will avoid suspicions of interference in the code)
- it's free[15]

Remember: do not save passwords in the browser!

use two-factor authentication

Use two-factor authentication on websites that offer this option. It is an additional level of security for online accounts, next to logins and passwords. Use FreeOTP to have all the tokens in one place. It's a free, open-source phone app that generates one-time expiring tokens/codes for two-factor online account authentication. Tokens can be added either by scanning the QR code or manually. The generated tokens are unique and only valid for a short time, so they very hard to hack. They are generated even if the phone is in airplane mode.

do not click on unknown links

It's easier to gain access to your equipment through social engineering than by cracking their security. You may receive seemingly not suspicious messages (e-mails / text messages), even phone calls. With an element of surprise and a little manipulation, they can persuade a person to enter a password. Commonly, they capitalizes on distraction and moment of negligence - you just click on a dangerous link and lose control over the equipment and data.

[15] https://niebezpiecznik.pl/post/keepass-jak-zaczac-swoja-przygode-z-managerem-hasel/

encrypt your computer disk

Disk encryption is a solution that protects the information on your computer's disk. Encryption is nothing more than changing the contents of the disk into an incomprehensible code that can only be decoded by entering a password. This means that without entering a password its content is useless. Disk encryption tools may depend on the operating system, but VeraCrypt is a universal solution (recommended for IOS and Windows).

Linux typically comes with disk encryption already built in, which is open source like the system itself. iOS has a FileVault option that encrypts the drive but automatically syncs the decryption password with the system password. Windows provides the disk encryption option only in professional versions, only after logging into your Microsoft account, and your decryption key is kept on Microsoft's servers (which is absolutely not secure).

make a safe backup

Keep encrypted files on an external drive or in a secure cloud. Remember to update the contents of the backup frequently. That way in the event of hardware loss you will lose only a small part of your data.

emergency situations

If you need to quickly protect your device in case of for example visit of law enforcement agents, you have two options:

- Turn off the power in your computer. It will prevent others from entering it but may also cause damage.
- Block the screen with keyboard shortcuts. This solution creates no potential damage to the devise. If you plan to use the shortcut, write it down in a visible place (from the perspective of the person sitting at the computer):
  - ✓ for Windows: Windows + L
  - ✓ for Mac: Option + Shift + Command + Q
  - ✓ for Linux: CTRL + ALT + L or Windows + L

Under stress otherwise simple activities may become complicated.

use open source alternatives

Open source software - software with source code available to everyone, so it can be changed, improved and disseminated. The programs are therefore quickly developed.

Why should the source code of the programs / tools be open source? Because only then is it verifiable by allowing experts to carry out tests and verify that the program really is what it claims to be.

The importance of open source can be demonstrated on the example of ANoM - a phone that was sold as secure, developed on a modified version of Android with a built-in communication encryption application. Sounds great? As it turned out, these devices were not on Android but their own

system, they were introduced to the market by the FBI and then distributed through an inmate who "recommended" them in exchange for a reduction of their sentence. The system and application code were not verified and the strategy resulted in criminals communicating through channels prepared for them by the American services.[16]

Open source programs and apps:

Linux[17] is a family of operating systems; probably the most suitable version for the user is ubuntu. There is a comprehensive guide in Polish on how to install it.[18]

Tails and CubesOS are more focused on security, and suitable for those rather more technically advanced.

Mozilla Firefox is an accessible browser that works on any system (including mobile devices). It has many extensions that will help you make browsing the Internet more comfortable and secure.

Which plugins should you add?

- uBlock Origin[19] - blocks ads (including audio) and has many additional filters for the Polish Internet [20]
- https everywhere[21] - makes sure that your connection with the website is encrypted
- Privacy Badger[22] - blocks elements that track your internet activity
- KeePassXC Browser[23] - automatically retrieves passwords from the manager when the database of passwords in open

Office programs such as Microsoft Office can be replaced by Libre[24] or Calligra[25], which offer even more possibilities than the corporate package. You can use ThunderBird[26] if you need an email client. Video conferencing applications such as zoom or skype can be replaced by jitsi[27] (available in the browser, without registration, both for iOS and Android) or Signal (for phone and desktop). F-droid is an alternative to the Play store, with only open-source apps, made available for free.

software / programs

corporate	open source
windows, macOS	linux (np. ubuntu)
chrome, chromium, safari	mozilla firefox, librewolf, falkon
office	libre, calligra
outlook	thunderbird
zoom, skype	jitsi, signal

[16] https://szmer.info/post/5767, http://blogotech.eu/index.php/11728-anom-spreparowany-telefon-dla-przestepcow
[17] https://www.linux.org/pages/download/
[18] http://ubuntu.pl/dokumenty/Przewodnik_Ubuntu_14.04_LTS_Trusty_Tahr.pdf
[19] https://addons.mozilla.org/pl/firefox/addon/ublock-origin/
[20] https://majkiit.github.io/polish-ads-filter/
[21] https://www.eff.org/https-everywhere
[22] https://www.eff.org/pages/privacy-badger
[23] https://addons.mozilla.org/pl/firefox/addon/keepassxc-browser/
[24] https://www.libreoffice.org/download/download/
[25] https://calligra.org/download/
[26] https://www.thunderbird.net/pl/
[27] https://meet.jit.si/

services

corporate	open source
gmail, hotmail, wp poczta, onet poczta, interia, o2	disroot, protonmail,
facebook	friendica, pleroma
facebook event	radar squat net, mobilizon
instagram	pixelfed
twitter	mastodon
youtube	peertube
reddit, wykop	szmer, lemmy
google	searX, qwant
google maps	open street maps
google driver / google suit	nextcloud, riseup, disroot

Some of the services[28] listed in the table above form a so called Fediversum (fediverse - federated universe) - a network of independently functioning social networks that communicate with each other.[29] Unlike the profit-making spying algorithms on the corporate platforms, the open source services show you the accounts you decided to follow.

Platforms to organize, share and mobilize:

- disroot.org - mail, chat, cloud, forums, pads, spreadsheets, etc.
- riseup.net - mail, forums, workgroups, to-do lists, etc.

You don't need an invitation to create an email at disroot (unlike at riseup.net).

[28] https://fediverse.pl/poznaj-alternatywy/

More open source programs and apps can be found here:

- https://switching.software/
- https://alternativeto.net/
- https://osalt.com/

TOR browser (The Onion Routing)

The Tor Browser provides online anonymity by hiding users' IP address, circumvents online censorship by enabling users to access blocked websites and/or webpages, does not include default online tracking features, and does not make money out of users' data. Tor prevents tracking which websites you visit and it prevents the sites you visit from learning your physical location. It is a distributed and decentralized network which makes it difficult to shut down.

The information sent is public, unlike its source, which is why it is so important not to send data about yourself while using the browser, such as last name, address, date of birth or credit card number. If you wish to stay completely anonymous, you should not log into any sites that require personal data.

Tor:

- blocks trackers – Tor Browser isolates each website you visit so third-party trackers and ads can't follow you. Any cookies and browsing history clear automatically when you're done browsing. Trackers collect information about which websites you've visited, as well as information about your devices.
- defends against surveillance – Tor Browser prevents someone who is monitoring your connection from knowing what websites you visit. However, they are able to see that you're using Tor.

- resists fingerprinting – Tor Browser aims to make all users look the same making it difficult to fingerprint you based on your browser and device information. Fingerprint in the digital world is a group of information about your browser and devices that can be used to identify you (or not). Those fingerprints can be unique, but it's better if they are not. You can check it here: https://coveryourtracks.eff.org/
- gives multi-layered encryption – Your traffic is relayed and encrypted three times as it passes over the Tor network.

Your network operator can see that you are using ToR, if they actively check for this information. Otherwise they see that there is an encrypted connection.
Don't use plugins or add-ons - The Tor Browser package already includes several add-ons such as HTTPS Everywhere and NoScript, all of which are safe to use and increase your anonymity. Leave them as are, and do not add others.

VPN (Virtual Private Network)

When you are connected to a VPN, all the data you send (such as requests to servers while browsing the web), appear to the website's or service's operators to be coming from a VPN server, instead of your Internet Service Provider (ISP). Your IP address is masked, which normally in combination with information about your ISP, point to your exact location.

A VPN protects your internet traffic from public network surveillance, but it doesn't protect your data from the private network you use. If you use a corporate VPN, whoever manages the corporate network will see your traffic. If you use a commercial VPN, whoever manages the service will be able to see your traffic.

You can use Riseup's VPN[30] at a free price, but it would be advisable not to use it to watching funny cats video ☺

Unlike most VPN providers, Riseup doesn't log your IP address. It's super easy to use. You just install it and run it - no setup, no account registration.

Or you can build your own VPN using relatively simple solutions like yunoHost.

support (in Polish)

It certainly has not been possible to exhaust the topic in this resource. Plus technologies are constantly changing and education is a long process. You are encouraged to explore further, for example on the website of Foundation Panoptykon[31], and community pages such as *cyberbezpieczeństwo,*[32] *wolny internet,*[33] or *hakt*[34] you will also find a list of practical technical tips. [35] You can find more about agencies and law enforcement in the dedicated communities.[36] There are also industry portals such as niebezpiecznik and sekurak, but they push their own training courses in quite an intrusive manner.

[30] https://riseup.net/pl/vpn
[31] https://panoptykon.org/wiedza
[32] https://szmer.info/c/cyberbezpieczenstwo
[33] https://szmer.info/c/wolnyinternet
[34] https://szmer.info/c/hakt
[35] https://szmer.info/post/2890
[36] https://szmer.info/c/policja

For many, however, this all can be an awful lot of information, enough to make you feel lost or anxious. If you have any doubts, run into installation issues etc, you may ask the collective knowledge of nerds and geeks from the *zapytaj Szmer*[37]community (without whom this very resource would not have come into existence!).

Thanks for your interest and commitment to build free internet.

support (in English)

- Data detox[38]
- Holistic security[39]
- Frontline defenders[40]
- Security box[41]

notes

[37] https://szmer.info/c/zapytajszmer
[38] https://datadetoxkit.org/en/home
[39] https://holistic-security.tacticaltech.org/
[40] https://www.frontlinedefenders.org/en/workbook-security
[41] https://securityinabox.org/en/