(1) Operating Systems
Operating systems know your device and everything on it.

General Tips:
- Use operating systems with lean data usage which respects privacy!
- Configure them such that:
  - no microphone or camera is active
  - no telemetry data is collected and sent
  - no cloud services are used
  - use data-lean anti-virus programs
- Back-up your data on local storage in case the system temporarily for the back-up task, back-up best on DVD (for protection against ransomware)

Special Tips:
- Do you know Linux or Quebeck - PC (e.g. Debian/Edu?)
  - https://www.debian.org/education/index.html
  - https://www.ubuntu.com
  - https://www.debian.org/education/index.html
- Mobile (e.g. LineageOS, Ubuntu Touch)
  - https://lineageos.org
  - https://touch-os.org
  - https://www.openpandora.com/
- If you need to use Windows 10 – configuration required! See for example:
  - https://github.com/peterdochsadam/vanillawindows10-16-12
timeout
  - https://github.com/peterdochsadam/vanillawindows10-16-12
- custom installation
  - available data protection options (e.g. advertising ID, typing behaviour, userapp logging)
  - local accounts (no Microsoft account)
  - third party apps (e.g. browser, email)
  - latest set of telemetry (basic, but cannot be completely disabled)
- Consider deactivation guides for:
  - Cortana
  - Speech recognition
  - Connection and error reporting
  - cloud services for data storage
- Check configuration after updates!

(2a) Internet Browsers
Browsers know a lot about you and are the “door to the internet”.

Tips for Basic Security:
- When choosing a browser, consider minimal data configuration, expandability, and updatability
- and set the startpage and new tabs to a local site or an empty page (about:blank)
- - install a firewall
- - do not forget to switch off)

Tips for special add-ons:
- - install add-ons for which you’re recognised
- - Lightbeam shows connections
- - Anonymisation services can help disguise your presence

SSL KEYLOGFILE
https://developers.mozilla.org
Using cookies in Firefox (SSM format)

Watch out! Configure settings as required and be wary of updates, check correctness of settings after an update

Unset the environment variable SSLKEYLOGFILE

(2b) Internet Browsers
Browser URLs are postcards (http) or letters (https) – the sender, the recipient and the shape of the envelope can always be identified
- Configure, update and use browser add-ons for:
  https://metamorphosy.com/firefox-private/
  https://metamorphosy.com/chrome-private/

Tips for special add-ons:
- - install add-ons for which you’re recognised
- - Lightbeam shows connections
- - Anonymisation services can help disguise your presence

Do you know the children’s search engine?
- blinde-kuh.de – Free of analytics for special protection of children
- google-alternative-workshop.de
- Check out!’s data analysis to create transparent usage/processing, e.g. for Facebook

(3) Apps
Apps know all the data they have access rights to.

Tips:
- Check app access and connections before use e.g. mobile.privacy.org
- Configure apps to be data-lean
- Prefer native apps (need-to-know)
- Block access through app settings on phones (e.g. to the microphone, camera, memory
- Use e. g. Blokada to block trackers
  - https://blokada.org/
- Block access to location data (WLAN, IP, GPS)
- Do you know about open app downloads like the ones through F-Droid?
  - https://f-droid.org
- Watch out! Avoid apps with a permanently activated microphone and camera in class, they record you and your surroundings, are disturbed by acoustic noise, or reveal personal messages!

(4) Search Engines
Most search engines also search for you.

Tips:
- Do you know these search engines?
  - lite qwant.de
  - MetaGer.de
  - YaCy.net take a look
  - https://metamorphosy.com/chrome-private/

- Do you see queries and give search suggestions you reveal information about yourself (profiling).
- Do you know the children’s search engine?
  - blinde-kuh.de – Free of analytics for special protection of children
  - google-alternative-workshop.de

- Qwant Junior
- Search directly is recommended, through third-parties there are often personalised results.

Pay attention to updates!

Digital Self-Defence is the ability to constructively overcome the challenges faced in the complex media landscape.

The measures listed are intended to enable pupils, teachers and students to use digital media responsibly and appropriately. In this way, the opportunities offered by digital transformation are harnessed, while at the same time risks are minimised in order to preserve personal freedom.

One-hundred percent security unfortunately doesn’t exist, but with a clear understanding, anyone can open up new opportunities! Note the reference under (6)!

This compass was created using Linux/Darwin/OS and LibreOffice. The research was done through the Firefox browser with the add-ons NoScript, “HTTPS Everywhere” and “Privacy Badger”. The content creation was coordinated using gpg-encrypted email.

Digital Transformation and You!
- Empowering Schools and Students-

- Data is the gold of the digital age!
  - While you are surfing the internet, you leave traces with every click!
  - Data is spread rapidly and there are many gold diggers with various motives!
  - The internet is fast, data is easy to find and analyse! Deletion is near impossible!
  - Even with encryption, there are many ways to identify you and track your activity.

- Learn how to put a stop to other gold diggers!
- Secure your data gold in ten steps!
  - Control your data presence and prevent data theft!

- The Problem

- The Goal

- The compass

- The Task

- The compass

- The success story

- The compass

- Digital Transformation and You!
- Empowering Schools and Students-
Social Networks, Chat, Messenger, Navigation Services (7)

Social networks know you, your friends and contacts. Navigation services know your location and destinations. They want your data.

Tips:
- Do you know about decentralised, open source based social networks e.g. from the Fédéral?world
- Do you know about decentralised, open source based chat services e.g. from the Fédéral?world
- Do you know about decentralized, open source based messaging services e.g. from the Fédéral?world
- Do you know about decentralized, open source based navigation services e.g. from the Fédéral?world

Internet Gateway/Firewall (8)

The gateway is the door to the internet and the last line of defence for the user's systems.

Tips:
- via DNS you can hide unwanted services, therefore configure and run your own DNS server or one from a provider, no third-party providers, encrypt DNS (DNS over HTTPS)
- Block unwanted DNS e.g. from the Fédéral?world
- Test SSL security for your own server (e.g. website) with SSL Labs
- Check for DNS hackability and DNS security

Password (9)

Passwords are an important measure to ensure the digital identity.

Tips:
- Use long passwords (at least 10 characters) which include special characters/numbers and avoid common words
- Use each password for one service/account only
- Create and memorise a secret sentence and build the password from it using e.g. the first letters and numbers, for example: 'In Spain in 2018, Jane had a blue swimsuit with 17 stripes and 8 spots'
- Is/2Jhabs1w1as8!
- Cannot remember passwords at all?
- Use local password generators and local open source password managers

Consequences

Privacy-by-Design actively supports sustainability! Reduce energy costs by blocking and code reduction. If Privacy-by-Design is not implemented, there will be direct and significant consequences.

The FBI warns! visitsite: https://www.fbi.gov(errno)4702/8661

Already in use: Influencing your sovereignty, e.g. not to go to voting
- Neomarketing
- Behaviour-based Marketing
- Algorithmic decision-making
- People's creditworthiness
- Personalised pricing
- Best suited are the products where the buyer has no idea about a reasonable price.