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! Delete 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 present and prevent data theft!

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/DarwinOS 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.

Special Tips:
- Do you know Linux or Quebes? - PC
  (e.g. Debian/Edu) https://www.proxycache.org/pasting-system.html.
  https://svn.debian.org/svn/debian-cache-cache/.
  https://www.debianproject.org/.
  https://www.debian组织/.
  
  Mobile (e.g. LineageOS, Ubuntu Touch)
  https://androidengineering.com/.
  https://www.debianproject.org/.
  
  If you need to use Windows 10 – configuration required! See for example:
  https://www.helper.org/home/windows-10-home-windows-10-desktop-drivers-for-linux
  https://www.helper.org/home/windows-10-home-desktop-driver
  https://www.helper.org/home/windows-10-desktop-drivers-for-and
  https://www.helper.org/home/windows-10-desktop-drivers-for-and-
  
  - Maven 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)
  - lowest level of telemetry (basic, but cannot be completely disabled)
  - Consider deactivation guides for:
    - Content speech recognition, connection and error reporting, cloud services for data storage
    - Check configuration after updates!

- Configure, update and use browser add-ons for:
  - https://addons.mozilla.org/ga/
  - https://addons.mozilla.org/au/
  
  Mobile (e.g. LineageOS, Ubuntu Touch)
  https://androidengineering.com/.
  https://www.debianproject.org/.
  
  - Install blocking of trackers e.g. with:
    - Privacy Badger
    - NoScript
    - uBlock Origin
    - uMatrix
    - Decentraleyes

Warning: All programs must be configured! A compass for configuration is a work in progress!

- Display of connections to servers and enforcement of encryption e.g. HTTPS Everywhere
  - Cookie management e.g. Cookie AutoDelete, Clear Flash Cookies
  - Hiding of users e.g. User Agent Platform Spoof
  - Search websites with add-ons e.g. Webdeveloper or test for third party connections and trackers with
    - PrivacyScore on or webtoolkit.datasets.ytd.net
    - use strict user files
    - Check website for SSL security

Digital Transformation and You! - Empowering Schools and Students

(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
  (switch on if necessary for an application, but do not forget to switch off!) see e.g. https://www.pcside.de/aktuelles/der-secure-duck/ftp/ftp-open-sourced-secure-duck-update-x-1-0-10-36380/.
- no telemetry data is collected and sent
- no cloud services are used
- no external speech and speaker recognition occurs
- Use data-lean anti-virus programs
- Back your data up only on hardware connected to the system temporarily for the back-up task, back-up best on DVD (for protection against ransomware)

(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
- Do you know what you’re looking at?
  - set the startpage and new tabs to a local site or an empty page (about_blank)
- Have a websites with add-ons e.g. Webdeveloper or test for third party connections and trackers with
  - PrivacyScore on or webtoolkit.datasets.ytd.net
  - use strict user files
  
(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

Tips for special add-ons:
- Panoplight shows you if you’re recognised, Lightbeam shows connections
- Anonymisation services can help disguise your presence:
  - https://httpbin.org
  - https://websiteapi.com/website/identity
  - https://webanalytic.com/
- Hint: Inform yourself about search engines before you use them! Support a data-lean search engine by default
  - https://duckduckgo.com
  - https://alexa.com

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

Unset all the environment variable SSLKEYLOGFILE
https://developer.mozilla.org/
https://www.bittorrent.org/ssl-keylog-format

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

Tips:
- Check app accesses and connections before use e.g. mediaplug.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/
  https://blokada.org/
- Block access to location data (WLAN, IP, GPS)
- Do you know about open app downloads like those through F-Droid?
  https://f-droid.org/
  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 at https://metaexpansy.com/
- https://searchengine.com
- Important: Searching directly is recommended, through third-parties there are often personalised results.

Pay attention to updates!

(5) Email
Emails are electronic postcards, which can be read by anyone, unless you do something about it.

Tips:
- Interested in secure email providers? Find information e.g. here:
  https://www.debian.org/.
  https://www.debian.org/.
  https://www.debian.org/.
- Do you know about extra email programs with encryption (e.g. Thunderbird with Enigmail)?
  https://www.debian.org/.
  https://www.debian.org/.
- Always display the long email header and check the email addresses
- Use a data-lean virus scanner
- Use only official email for official purposes, no relaying, check incoming mail
  - Recommended: No automatic loading of images and opening of links in the web browser, no HTML emails.
School Website (6)
With your website you assume responsibility for IT security and data protection for yourself and your users.
**Tips:**
- Use native fonts, translation and reading services.
- Specify and adhere to deletion periods for stored data.
- Check for present, unwanted analytical functions of software.
- Use opt-in rather than opt-out.
- Use IP address anonymisation at the meta level.

[www.tiegelkieler.de/2015/05/20/schule/studien/ http://www.de/species.html] (web)

Internet Gateway/Firewall (8)
The gateway is the door to the internet and the last line of defence for the user's systems.
**Tips:**
- DNS (Mirax) and run your own DNS server or one from a provider, no third-party providers.
- Do not change your DNS (DNS over HTTPS).
- Configure and use firewalls to filter network traffic.
- Configure and run intrusion prevention systems to help protect against malicious code.
- Check and configure app accesses e.g. at exodus-privacy.eu.org (accesses to smartphone services).

[https://book-privacy.org.uk/pages/1019/] (web)

Password (9)
Passwords are an important measure to secure the digital identity.
**Tips:**
- Use long passwords (at least 10 characters) which include special characters/names and avoid common words.
- Use each password for one service/accound 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.'
- Is2Jhabs1waAs1!
- 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.
- Already in use: Influencing your sovereignty, e.g. not to go to voting [https://www.bbc.com/ (web)] (web)
- Dynamic, personalised pricing.
- Profiling.
- Neuromarketing.
- Behavioural Marketing.
- Algorithmic decision-making.
- People's creditworthiness.
- Personalised pricing.
- Best suited are all the products where the buyer has no idea about a reasonable price.

[https://www.de/species.html] (web)

Office Applications (10)
Office applications know all the data they process.
**Tips:**
- Do you know any locally installed open source applications? e.g. [https://en.wikipedia.org/wiki/Free_officeソフトウェア](web)
- LibreOffice.
- GIMP.
- Use local native spelling and translation support.

[https://www.de/species.html] (web)

Important:
The information and references represent a first introduction to the topic. The contents have been created with the background of computer science and were researched with the greatest care. Nonetheless, no liability can be accepted for the correctness, completeness, and present day validity of the information provided. In particular, the information is of a general nature and does not constitute legal advice in individual cases. When using the tools, no liability can be accepted for damages and such use is exclusively at the user's own risk.

Note:
The links given are deliberately printed in small print and should be looked up digitally.

"When you shop, your data may be the most valuable thing for sale." [https://blog.mozilla.org/security/files/Gutierrez/Habits_andSystems.pdf] (pdf - 3/2 - 77 pdf)

"The regulatory authorities may not well intervene. The question is how to prove the application of personalised prices. I believe it will be very difficult to uncover the evidence of this. But even if it is proven, the regulatory authorities would have to be able to react swiftly. And now consider the sheer volume of transactions in the market." (…)"My sister always gets ten times the number of points, so why don't I?… If it is a simple coupon that the customer only receives once, I typically don’t get complaints…” (…)

[https://www.de/species.html] (web)

"Do you know examples for data-lean messengers (e.g. Jabber/XMPP, see e.g. Conversions) or IRC clients (e.g. XChat)? See in [https://www.jabber.org/](web)
- Embed reading services, cloud services, translations local.
- Avoid a combination of third-party providers when using anonymous services e.g. anonymous analytics and web fonts.

[https://www.de/species.html] (web)

Block unwanted DNs e.g.

[https://www.de/species.html] (web)

Do you know examples for data-lean messengers (e.g. Jabber/XMPP, see e.g. Conversions) or IRC clients (e.g. XChat)? See in [https://www.jabber.org/](web)
- Embed reading services, cloud services, translations local.
- Avoid a combination of third-party providers when using anonymous services e.g. anonymous analytics and web fonts.

[https://www.de/species.html] (web)

Block unwanted DNs e.g.

[https://www.de/species.html] (web)

Do you know examples for data-lean messengers (e.g. Jabber/XMPP, see e.g. Conversions) or IRC clients (e.g. XChat)? See in [https://www.jabber.org/](web)
- Embed reading services, cloud services, translations local.
- Avoid a combination of third-party providers when using anonymous services e.g. anonymous analytics and web fonts.

[https://www.de/species.html] (web)

 jokeday.

[https://www.de/species.html] (web)

Internet Gateway/Firewall (8)
The gateway is the door to the internet and the last line of defence for the user's systems.
**Tips:**
- DNS (Mirax) and run your own DNS server or one from a provider, no third-party providers.
- Do not change your DNS (DNS over HTTPS).
- Configure and use firewalls to filter network traffic.
- Configure and run intrusion prevention systems to help protect against malicious code.
- Check and configure app accesses e.g. at exodus-privacy.eu.org (accesses to smartphone services).

[https://book-privacy.org.uk/pages/1019/] (web)

Password (9)
Passwords are an important measure to secure the digital identity.
**Tips:**
- Use long passwords (at least 10 characters) which include special characters/names and avoid common words.
- Use each password for one service/accound 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.'
- Is2Jhabs1waAs1!
- 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.
- Already in use: Influencing your sovereignty, e.g. not to go to voting [https://www.bbc.com/ (web)] (web)
- Dynamic, personalised pricing.
- Profiling.
- Neuromarketing.
- Behavioural Marketing.
- Algorithmic decision-making.
- People's creditworthiness.
- Personalised pricing.
- Best suited are all the products where the buyer has no idea about a reasonable price.