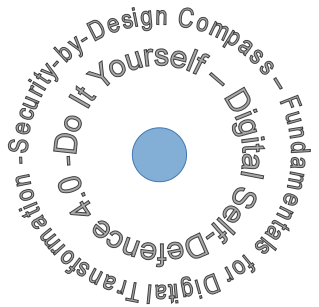
Digital Transformation and You! - Empowering Schools and Students-

- 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.	The Problem
- 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 Goal



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 (8)!*

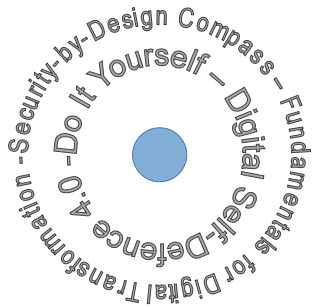
This compass was created using Linux/DarwinOS and LibreOffice. The research was done through the Firefox browser with the add-ons "NoScript", "HTTPS Everywhere" and "Privacy Badger". The content creation was coordinated using gpg-encrypted email.

(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.ncsc.gov.uk/collection/end-user-device-security/platform-specific-guidance/eud-security-guidance-windows-10-1809, https://csrc.nist.gov/publications/detail/sp/800-179/rev-1/draft (Nov19)
- 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)



Special Tips:

- *Do you know* Linux or Quebes? - PC (e.g. DebianEdu) https://www.privacytools.io/operating-systems/, https://www.skolelinux.de/en/, https://www.linuxnewssite.com/ or http://www.linuxmuster.net/de/start/, https://schulnetzkonzept.de (Nov 21)
Mobile (e.g. LineageOS, Ubuntu Touch) https://ubports.com/ (April2019)
- If you *need* to use Windows 10 – configuration required! See for example https://privacyamp.com/knowledge-base/windows-10-5-minute-privacy-configuration/ https://privacyamp.com/knowledge-base/windows-10-privacy-settings/#windows-permissions and https://security.vt.edu/resources/win10privacy.html (April19)
- custom installation
- available data protection options (e.g. advertising ID, typing behaviour, user/app 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: 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:

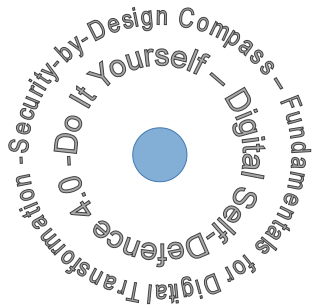
- *When* choosing a browser, *consider* minimal data configuration, expandability, and updatability https://restoreprivacy.com/ *(April19)* and set the startpage and new tabs to a local site or an empty page (about:blank)

Known, in use?

-*Have a look* at suggestions under: https://restoreprivacy.com/secure-browser/ *(April19)*
- *Do you know* e.g. - Firefox https://restoreprivacy.com/firefox-privacy/ (Jan19)
- Waterfox, Pale Moon, Brave https://github.com/brave/brave-browser/issues/3479 (Nov19)

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

Unset/clear the environment variable *SSLKEYLOGFILE* https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/Key_Log_Format (Nov19)



- View videos data-lean and using a proxy: https://redirect.invidious.io/ (May21)
- *Blocking of trackers e.g. with:* Privacy Badger, NoScript, uBlock Origin, uMatrix, Decentraleyes

Known, in use?

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 Spoofer
- *Scan* websites with add-ons e.g. Web-developer or test for third party connections and trackers with *PrivacyScore.org* or *webbkoll.dataskydd.net*
- use strict user.js files https://www.privacy-handbuch.de/download/user.js
-*Test* browsers for SSL security https://www.ssllabs.com/ssltest/viewMyClient.htm (Jan19)

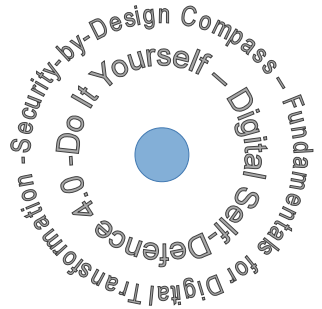
(2b) Internet Browsers

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://restoreprivacy.com/firefox-privacy/, https://restoreprivacy.com/ad-blocker/ (April19)

Tips for special add-ons:

- Panopticlick shows you if you're recognised, Lightbeam shows connections
- Anonymisation services can help disguise your presence: https://restoreprivacy.com/tor/ (April2019)
- *Hint*: Inform yourself about search engines before you use them! Support a data-lean search engine by default! *https://digitalcourage.de/digitale-selbstverteidigung/es-geht-auch-ohne-google-alternative-suchmaschinen (Jan19)*
- *Check out:* Data analysis aiming to create transparency of data usage/processing, e.g. for Facebook *https://labs.rs/en/quantified-lives/ https://labs.rs/wp-content/uploads/2016/08/FacebookFactory-01.gif (Jan19)*



(3) Apps

Apps know all the data they have access rights to.

Tips:

- *Check* app accesses and connections before use e.g. exodus-privacy.eu.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/ (Jan19)
- *Block* access to location data (WLAN, IP, GPS)
- *Do you know* about open app downloads like those through F-Droid? https://edri.org/files/defenders_v_intruders_de_web.pdf (Jan19)

Known, in use?

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

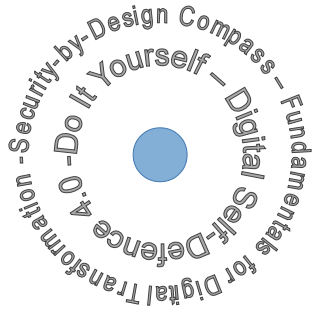
take a look at https://restoreprivacy.com/, https://restoreprivacy.com/private-search-engine/ (April19)

- With search queries and active 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 (Jan2019)
- qwantjunior.com (Mai2019)

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:

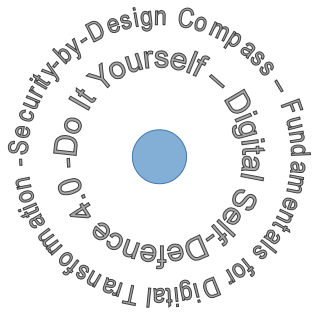
- Interested in secure email providers? Find information e.g. here: https://restoreprivacy.com/, https://restoreprivacy.com/secure-email/ (April2019)
- *Do you know* about extra email programs with encryption (e.g. Thunderbird with Enigmail)? see in https://edri.org/files/defenders_v_intruders_de_web.pdf (Jan19)
- *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
https://www.theregister.co.uk/2018/05/25/ schrems_is_back_facebook_google_get_served_gdpr_complaint/ (Jan19)
- *Avoid* web fonts, analytics
- Configure login areas only with https
- *Use* Captcha scripts local to the server
- *Use* videos only from the used server or saved locally
- *Test* your website at *PrivacyScore.org webbkoll.dataskydd.net, ssllabs.com/ssltest* Known, in use?



- *Do you know* about open data **map and navigation services?** e.g. OpenStreetMap see in https://www.schulportal-thueringen.de/tip/resources/medien/38205?dateiname=Joeran-Muuss-Merholz-Freie-Unterrichtsmaterialien-Beltz-2018.pdf (Jan10) Known, in use?
- *Check* web building blocks for integrated connections to third parties and disable them
- *Learn* about data-lean schedulers e.g. https://www.fdm.uni-hamburg.de/service/werkzeuge.html (Jan2019)
- *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

Caution:
The basic data protection regulation calls for special protection of children regarding advertising purposes, the creation of personal or user profiles, and the use of services offered directly to children.

Social Networks, Chat, Messenger, Navigation Services (7)

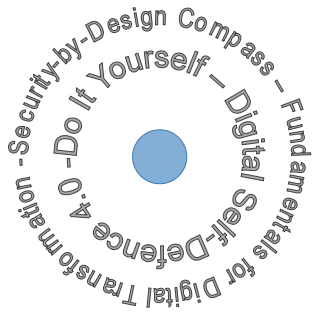
Social networks know you, your friends and contacts. Navigation services know your location and destinations. They want your data.

Tips:

- *Do you know about* decentralised, open source based **social networks?** e.g. from the Fediverse https://www.privacytools.io/services/ (April2019) Known, in use?

- *Recognise and block* access and tracking techniques e.g. by web fonts and APIs, use tools such as (2a), (2b) and (4) like e.g. Privacy Badger, *webbkoll.dataskydd.net* for recognition and Blokada for prevention.

- *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/, https://xmpp.org/software/clients.html, https://restoreprivacy.com/(April19)
or email server networks (chat over email) see e.g. https://delta.chat.de (May 19)
- *Activate* end-to-end encryption (E2EE)



- *Do you know alternative* **navigation services?** e.g.
https://www.openstreetmap.org/
https://map.project-osrm.org/
https://maps.metager.de/map Known, in use?
https://digitalcourage.de/digitale-selbstverteidigung/wege-finden-ohne-google-maps-openstreetmap

- *Avoid* data-rich messengers e.g. WhatsApp https://www.theguardian.com/technology/2018/feb/05/whatsapp-deleting-year-what-i-learned (April19)

- *Deregister?* For example: WhatsApp, Facebook (Android) https://faq.whatsapp.com/en/android/21119703/?lang=de (IOS) https://faq.whatsapp.com/de/iphone/21325453/?category=5245246 https://de-de.facebook.com/help/359046244166395/

Read up on safe and data protecting **conference system** solutions!
https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf

https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/

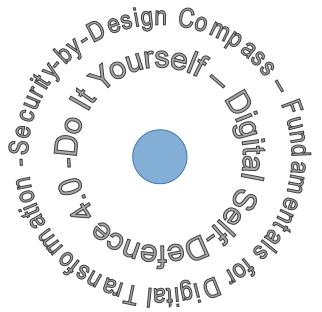
Selessa/Moodle: https://lisa.sachsen-anhalt.de/unterricht/digitale-bildung/e-

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)
- *Suppress* telemetry (e.g. Windows) https://github.com/crazy-max/WindowsSpyBlocker/blob/master/data/hosts/spy.txt (Oct19)
- *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://exodus-privacy.eu.org/en/page/ (Jan19) Known, in use?



- *Block* unwanted DNS e.g. https://www.reddit.com/r/pihole/comments/930g2z/psa_google_services_including_ads_and_others_try/ (Oct 19)
- *Test* SSL security for your own server (e.g. website) with SSL Labs https://www.ssllabs.com/ssltest/ (Jan19) Known, in use?
- *Do you know* about private, local servers for messenger services? Pay attention to security! https://www.jabber.org/ (Jan19)
- *Check* connections, e.g. using Wireshark

Important:

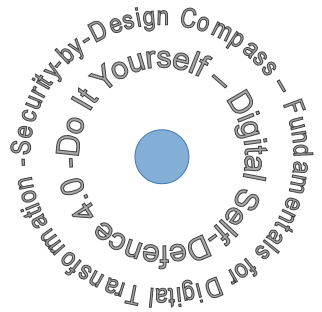
The information and references represent a first introduction to the topic. The contents have been created with the background of computer science and were researched with the greatest care. Nonetheless, no liability can be accepted for the correctness, completeness, and present day validity of the information 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.

Password (9)

Passwords are an important measure to secure 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: "***I**n **S**pain **i**n **2**018, **J**ane **h**ad **a** **b**lue **s**wimsuit **w**ith **1**7 **s**tripes **a**nd **8** **s**pots!"*
Isi2Jhabsw1sa8s!
- *Cannot remember passwords at all?*: *Use* **local** password generators and **local** open source password managers



Office Applications (10)

Office applications know all the data they process.

Tips:

- *Do you know* any locally installed open source applications? e.g. see in https://en.wikipedia.org/wiki/List_of_free_and_open-source_software_packages (Jan19)
- LibreOffice
- GIMP
- *Use* local native spelling and translation support Known, in use?

Check privacy conditions of cloud-based applications with subscription models (e.g. Office 365) and Microsoft Office
https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office/DPIA+Microsoft+Office+2016+and+365+-+20191105.pdf (Jan19)

Note

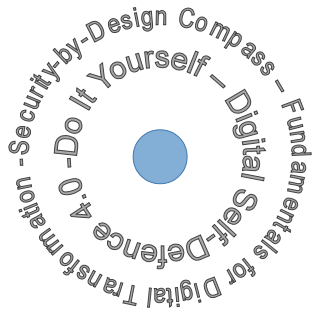
The links given are deliberately printed in small print and should be looked up digitally.

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: https://www.ic3.gov/media/2018/180913.aspx

Already in use: Influencing your sovereignty, e.g. not to go to voting
https://qz.com/916801/americans-dont-know-their-neighbors-anymore and-thats-bad-for-the-future-of-democracy/ (Sep19)
dynamic, personalised pricing:
- profiling
- Neuromarketing
- behaviour-based 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.abida.de/sites/default/files/Gutachten_Handel_Bezahlsysteme.pdf – E5 - Seite 77 (Jan19)



"When you shop, your data may be the most valuable thing for sale."
https://irlpodcast.org/season4/episode1/ (Jan19)
"The regulatory authorities may 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.abida.de/sites/default/files/Gutachten_Handel_Bezahlsysteme.pdf E5 – Seite 78 und E6 – Seite 81 (Jan19)
If the customer is not satisfied, the offer can be withdrawn (disguised, for example, as a disconnection).
https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf Seite 32 (Jan19)