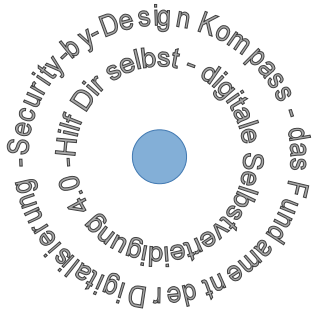
Digitalisierung und Du!
- Macht den Schulen -

- Daten sind das Gold des digitalen Zeitalters! - Wenn Du Dich im Internet bewegst, hinterlässt Du bei jedem Klick Spuren! - Daten sind ruckzuck verbreitet und es gibt viele Goldgräber mit verschiedensten Absichten! - Das Internet ist schnell, Daten sind leicht zu finden und auszuwerten! Löschen ist fast unmöglich! - Trotz Verschlüsselung gibt es viele Möglichkeiten, Dich zu erkennen und deine Aktivitäten auszuspionieren!	Das Problem
- Wie Du anderen Goldgräbern das Handwerk legst! - In zehn Schritten zur Sicherung des Daten-Goldes! - Beuge dem Eigenleben Deiner Daten und dem Datenklau vor!	Das Ziel



Die ***digitale Selbstverteidigung*** ist die Fähigkeit, die Herausforderungen durch die komplexe Medienlandschaft konstruktiv zu bewältigen.

Die angegebenen Maßnahmen sollen Schülerinnen, Schüler und Lehrerschaft in die Lage versetzen, den Mediengebrauch verantwortungsvoll und angemessen zu gestalten.
Damit werden die Chancen der Digitalisierung bei gleichzeitiger Risikominimierung zur Wahrung der persönlichen Gestaltungsfreiheit genutzt.

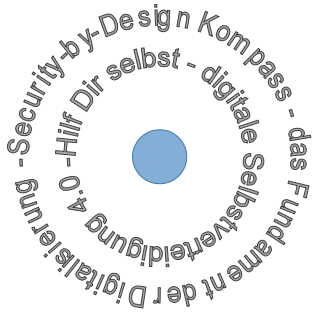
Hundertprozentige Sicherheit *gibt es leider nicht, aber wer durchblickt, dem eröffnen sich neue Chancen! Achte auf Hinweis unter (8)!*

Dieser Kompass entstand datensparsam unter Verwendung von Linux/DarwinOS und Libreoffice. Die Recherche erfolgte mittels datensparsam konfigurierten Firefox-Browser mit den AddOns „NoScript", „httpsEverywhere" und „PrivacyBadger". Die Abstimmung der Inhalte erfolgte mittels gpg-verschlüsselter E-Mail.

(1) Betriebssysteme

Betriebssysteme kennen Dein Gerät und alles, was sich darauf befindet.

allgemeine Tipps:
https://digitalcourage.de/digitale-selbstverteidigung/
https://ssd.eff.org/ (Jan19)
- *Nutze* datensparsame Betriebssysteme!
- *Konfiguriere* sie so, dass:
- kein Mikrofon/Kamera aktiv ist (Anschalten im Bedarfsfall für eine Anwendung, Ausschalten nicht vergessen!)
- keine Telemetriedaten erhoben und versendet werden
- keine Clouddienste verwendet werden
- keine externe Sprach- und Sprechererkennung erfolgt
- *Verwende* Anti-Virus-Programme
- *Sichere* Deine Daten auf nur kurzzeitig angeschlossenen Systemen, sichere am Besten auf DVD (Schutz vor Ransomware)



Spezielle Tipps:
- *Kennst* Du Linux? – PC (z.B. DebianEdu)
https://www.teckids.org/de/freie-software-fur-die-bildung/skolelinux/, https://digitalcourage.de/digitale-selbstverteidigung/gnulinux-now (Jan19),
Mobile (z.B. LineageOS, Ubuntu Touch)
ttps://de.wikipedia.org/wiki/Fairphone_2 oder https://digitalcourage.de/digitale-selbstverteidigung/befreien-sie-ihr-smartphone (Jan2019)
- *Falls* Du Windows 10 benutzen musst - erheblicher Konfigurationsbedarf! Siehe https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf und https://www.dfn.de/fileadmin/3Beratung/Recht/handlungsempfehlungen/Datenschutzrechtliche_Probleme_bei_der_Einfuehrung_neuer_Betriebssysteme.pdf (Jan19)
- benutzerdefinierte Installation
- bereitgestellte Datenschutzoptionen (u.a. zu WerbeID, Schreibverhalten, Nutzer-/App Protokollierung)
- lokale Konten (kein Microsoft-Konto)
- Apps Dritter (z.B. Browser, E-Mail)
- niedrigstes Telemetrieniveau (basic, trotzdem keine vollständige Sperrung)
- *Beachte* Deaktivierungshinweise zu Cortana, Spracherkennung, Verbindungs- und Fehlerberichterstattung, Clouddienste als Datenspeicher
- *Überprüfe* Konfiguration nach Update!

(2a) Internetbrowser

Browser wissen viel über Dich und sind die „Tür zum Internet".

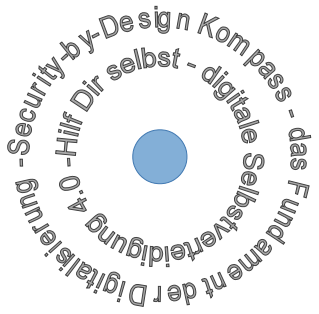
Tipps zur Grundsicherung:
- *Achte* bei Browserwahl auf datenarme Konfigurierbarkeit, Erweiterbarkeit und Updatefähigkeit
https://digitalcourage.de/digitale-selbstverteidigung/ https://www.youngdata.de/digitale-selbstverteidigung/allgemeines/browsersicherheit/ https://restoreprivacy.com/secure-browser/ https://www.youngdata.de/digitale-selbstverteidigung/allgemeines/browsersicherheit/ (Jan19)

Bekannt, genutzt?

-*Schau* mal bei den Anregungen unter https://restoreprivacy.com/secure-browser/ oder *https://www.kuketz-blog.de/umgang-mit-daten-im-privatleben-datensouveraenitaet-teil3/ (Jan19)*
- *Kennst* Du z.B. - Firefox
https://restoreprivacy.com/firefox-privacy/ (Jan19)
- Waterfox, Pale Moon, Brave

Achtung Konfigurationsbedarf und achte auf Aktualisierungen, Prüfe Korrektheit der Einstellungen nach Update

-*Teste* Browser auf SSL-Sicherheit
https://www.ssllabs.com/ssltest/viewMyClient.htm (Jan19)



- *Konfiguriere, aktualisiere und nutze* Browser AddOns für: https://privacy-handbuch.de/download/privacy-handbuch.pdf (Jan19)

Bekannt, genutzt?

- *Blocken von Trackern z. B. mit:* Privacy Badger, NoScript, Ghostery, uBlock Origin, uMatrix, Decentraleyes

Achtung: Alle Programme müssen konfiguriert werden! Ein Kompass für Konfiguration ist in Vorbereitung!

- *Anzeige von Verbindungen zu Servern und Erzwingen von Verschlüsselung z.B.*: HTTPS Everywhere
- *Cookie Management z.B.:* Cookie Autodelete, Clear Flash Cookie
- *Verstecken von Nutzern z.B.:* User Agent Platform Spoofer

Bekannt, genutzt?

- *Durchleuchte* Webseiten mit Add-on z.B. Webdeveloper oder teste auf Tracker mit PrivacyScore.org

(2b) Internetbrowser

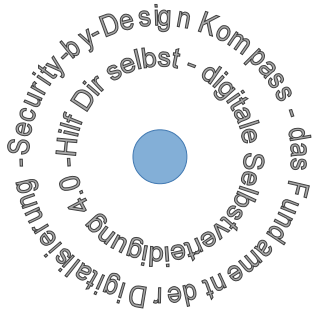
Browser-URLs sind Postkarten (http) bzw. Briefe (https) - der Absender, der Empfänger und die Form des Briefumschlags sind immer erkennbar

Tipps zu speziellen AddOns:
- Panopticlick zeigt Dir, ob man Dich erkennt, Lightbeam zeigt Verbindungen

- Anonymisierungsdienste können die eigene Präsenz verschleiern helfen:
https://anon.inf.tu-dresden.de/help/jap_help/de/help/jondonym.html

- *Anregung*: informiere Dich über Suchmaschinen bevor Du sie nutzt! Trage dir eine datensparsame Suchmaschine als Default ein!
https://digitalcourage.de/digitale-selbstverteidigung/es-geht-auch-ohne-google-alternative-suchmaschinen (Jan19)

- *Schau mal unter:* Datenanalyse zur Schaffung von Transparenz von Datennutzung und -verwertung am Beispiel von Facebook
https://labs.rs/en/quantified-lives/, https://labs.rs/wp-content/uploads/2016/08/FacebookFactory-01.gif (Jan19)



(3) Apps

Die Apps kennen alle Daten, auf die sie Zugriff haben.

Tipps:
- *Überprüfe* App Zugriffe und Verbindungen vor dem Einsatz z.B. exodus-privacy.eu.org
- *Konfiguriere* Apps datensparsam
https://digitalcourage.de/digitale-selbstverteidigung/mobil (Jan19)
- *Blockiere* Zugriffe durch App Einstellungen auf dem Telefon (z.B. auf Mikrofon, Kamera, Speicher)
- *Verwende z.B.* BLOKADA zur Sperrung von Trackern https://www.kuketz-blog.de/blokada-tracking-und-werbung-unter-android-unterbinden/ (Jan19)
- *Blockiere* Zugriffe zu Positionsdaten (WLAN, IP, GPS)
- *Kennst* du offene App-Downloads wie F-Droid? https://edri.org/files/defenders_v_intruders_de_web.pdf 01/19
Achtung! Vermeide unbedingt Apps mit ständig aktivierten Mikrofon und Kamera im Unterricht, sie zeichnen Dich und die Umgebung auf, stören mit akustische Meldungen oder geben persönliche Nachrichten preis!

(4) Suchmaschine

Die meisten Suchmaschinen (durch-)suchen auch Dich.

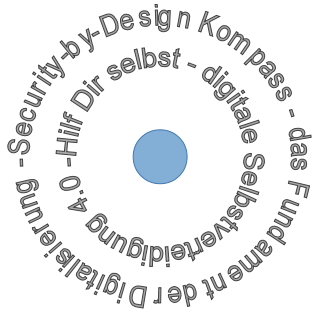
Tipps:
Kennst Du die Suchmaschinen?

- lite.qwant.de
- MetaGer.de
- YaCy.net
schau doch mal unter https://digitalcourage.de/digitale-selbstverteidigung/es-geht-auch-ohne-google-alternative-suchmaschinen (Jan19)

Kennst Du die Kindersuchmaschine
- blinde-kuh.de ? – Analytics-frei für den besonderen Schutz für Kinder (Jan2019)

Wichtig: Empfohlen ist die direkte Suche, bei Drittanbietern gibt es oftmals personalisierte Ergebnisse.

Auf Aktualisierungen achten!



(5) E-Mail

E-Mails sind elektronische Postkarten, die von jedermann gelesen werden können, wenn Du nichts dagegen unternimmst.

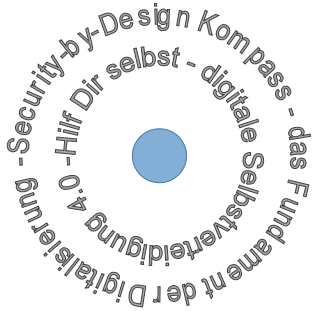
Tipps:
- *Interesse* an sicheren E-Mail Anbietern? Dann findest Du Infos hier:
https://www.privacy-handbuch.de/handbuch_31.htm (Jan2019)
- *Kennst* Du extra E-Mail Programme mit Verschlüsselung (z.B. Thunderbird mit Enigmail)? siehe in https://edri.org/files/defenders_v_intruders_de_web.pdf oder https://www.kuketz-blog.de/umgang-mit-daten-im-privatleben-datensouveraenitaet-teil3/ https://www.privacy-handbuch.de/handbuch_31a0.htm https://digitalcourage.de/digitale-selbstverteidigung/pc (Jan19)
- *Lasse* Dir immer den langen E-Mail Briefkopf (Header) anzeigen und überprüfe die Email-Adressen
- Verwende Virenscanner!
- *Empfohlen:* kein automatisches Nachladen von Bildern und Öffnen von Links im Webbrowser, keine html Mails

Schulwebauftritt (6)

Mit Deinem Webauftritt übernimmst Du Verantwortung für IT-Sicherheit und Datenschutz für Dich und Deine Nutzer.

Tipps:

- *Nutze* lokale Schriftarten, Übersetzungs-, Vorlesedienste
- *Gib* Löschfristen für gespeicherte Daten an und halte sie ein
- *Prüfe* auf voreingestellte, ungewollte Analytics-Funktionen der Software
- *Verwende* Opt-In anstelle von Opt-Out
- *Verwende* IP-Adressanonymisierung auf Metaebene
  https://www.theregister.co.uk/2018/05/25/ schrems_is_back_facebook_google_get_served_gdpr_complaint/ (Jan19)
- *Vermeide* Webfonts, Analytics
- *Teste* Deinen Webauftritt unter PrivacyScore.org Bekannt, genutzt?
- *Nutze* Videos nur vom genutzten Server bzw. lokal gespeichert
- *Nutze* Server-lokale Captcha Skripte



- *Kennst* Du Open Data **Karten- und Navigationsdienste?** Bsp. Openstreetmap siehe in https://www.schulportal-thueringen.de/tip/resources/medien/38205?dateiname=Joeran-Muuss-Merholz-Freie-Unterrichtsmaterialien-Beltz-2018.pdf (Jan10) Bekannt, genutzt?
- *Prüfe* bei Webbaukästen auf integrierte Verbindungsaufbauten an Dritte und deaktiviere sie
- *Informiere* dich zu datensparsamen Terminplanern z.B. unter https://www.fdm.uni-hamburg.de/service/werkzeuge.html (Jan2019)
- *Binde* Vorlesediensten, Clouddienste, Übersetzungen lokal ein
- *Vermeide* eine Kombination von Drittanbietern bei Verwendung von anonymisierten Diensten z.B. anonymisierte Analytics und Webfonts

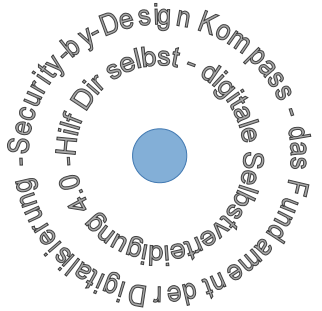
Achtung:
Die Datenschutzgrundverordnung fordert den besonderen Schutz für Kinder für Werbezwecke, für die Erstellung von Persönlichkeits- oder Nutzerprofilen und bei der Nutzung von Diensten, die Kindern direkt angeboten werden.

Soziale Netzwerke, Chat, Messenger, Navigationsdienste (7)

Soziale Netzwerke kennen Dich und Deine Freunde und Kontakte. Navigationsdienste kennen Deinen Standort und Reiseziele. Sie wollen Deine Daten.

Tipps:

- *Kennst* Du dezentrale, Open Source basierte **soziale Netzwerke?** z.B. aus dem Fediverse Bekannt, genutzt?
  https://digitalcourage.de/blog/2018/kommt-mit-uns-ins-fediverse
  https://www.heise.de/download/specials/Die-besten-Facebook-Alternativen-4039433 (Jan2019)
- *Erkenne und blockiere* Tracking-techniken z.B. über Webfonts und APIs, nutze die Hilfsmittel aus (2a) und (2b) wie z.B. Privacy Badger zur Erkennung und BLOKADA zur Unterbindung
- *Kennst* Du zum Beispiel datensparsame **Messenger** (z.B. Jabber/XMPP oder Wire) oder IRC Klienten (z.B. Xchat)? siehe in https://privacy-handbuch.de/download/privacy-handbuch.pdf oder https://digitalcourage.de/digitale-selbstverteidigung/alternativen-zu-whatsapp-und-threema-instant-messenger (Jan19)



- *Aktiviere* Ende-zu-Ende-Verschlüsselung (OMEMO)

- *Kennst Du alternative* **Navigationsdienste?** wie z.B. https://www.openstreetmap.org/ https://map.project-osrm.org/ Bekannt, genutzt?
  https://digitalcourage.de/digitale-selbstverteidigung/wege-finden-ohne-google-maps-openstreetmap

- *Vermeide* datenreiche Messenger (u.a.) WhatsApp
  zu WhatsApp in der Schule siehe inhttps://www.gew-thueringen.de/index.php?eID=dumpFile&t=f&f=71477&token=aac68cf7661509eb1cb976fedbc4946107001 1b5&download=&n=Datenschutz_in_der_Schule_Vortrag_des_Thueringer_Datenschutzbeauftragten_auf_der_LVV_der_GEW_Thueringen_21092018.pdf S.14 (Jan19)

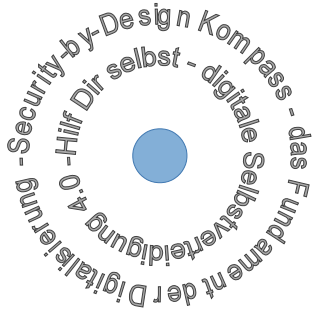
- *Abmelden?* Bsp. Whatsapp, Facebook:
  (Android) https://faq.whatsapp.com/en/android/21119703/?lang=de
  (IOS) https://faq.whatsapp.com/de/iphone/21325453/?category=5245246
  https://de-de.facebook.com/help/359046244166395/

Internet-Gateway/Firewall (8)

Das Gateway ist das Tor zum Internet und die letzte Verteidigungslinie für die Systeme des Nutzers.

Tipps:

- über DNS kannst Du unerwünschte Dienste ausblenden, deshalb *konfiguriere und betreibe* eigene DNS Server oder den des Providers, keine Drittanbieter
- *Konfiguriere und verwende* Firewalls zur Filterung des Netzwerkverkehrs
- *Konfiguriere und betreibe* Intrusion Prevention Systeme zum Schutz vor Schadcode
- *Prüfe und konfiguriere* App-Zugriffe z.B. bei exodus-privacy.eu.org (u.a. Zugriffe auf Smartphone-Dienste) Bekannt, genutzt?
  https://exodus-privacy.eu.org/en/page/ (Jan19)



- *Teste* ssl-Sicherheit für eigene Server (z.B. Webauftritt) mit ssl-Labs Bekannt, genutzt?
  https://www.ssllabs.com/ssltest/ (Jan19)
- *Kennst* Du eigene, lokale Server für Messengerdienste? Achte auf die Absicherung!
  https://digitalcourage.de/digitale-selbstverteidigung/alternativen-zu-whatsapp-und-threema-instant-messenger (Jan19)

Wichtig:

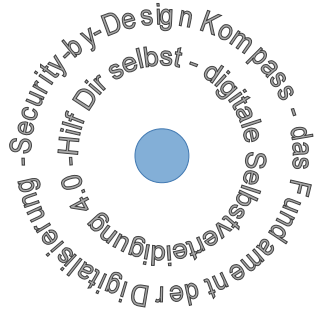
Die Informationen und Referenzen stellen einen ersten Einstieg zum Thema dar. Die Inhalte sind vor dem Hintergrund der Informatik erstellt und mit größter Sorgfalt recherchiert. Es kann dennoch keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der bereit gestellten Informationen übernommen werden. Die Informationen sind insbesondere auch allgemeiner Art und stellen keine Rechtsberatung im Einzelfall dar. Bei Benutzung der Werkzeuge kann keine Haftung für Schäden erfolgen und und die Nutzung erfolgt ausschließlich auf eigenes Risiko.

Passwort (9)

Passwörter sind eine wichtige Maßnahme zur Sicherung der digitalen Identität.

Tipps:

- *Verwende* lange Passwörter (mind. 10 Zeichen) mit Sonderzeichen und Zahlen ohne bekannte Wörter
- *Verwende* jedes Passwort nur für einen Dienst/Account
- *Verwende* lokale Passwortgeneratoren und lokale OpenSource Passwortmanager oder:
- *Bilde und merke* Dir einen geheimen Satz und *erzeuge* daraus das Passwort anhand z. B. der Anfangsbuchstaben und Zahlen, Beispiel: „***I**m **U**rlaub **2**018 **h**atte **i**ch **e**inen **b**lauen **B**adeanzug **m**it **1**7 **S**treifen **u**nd **8 P**unkten!"
  IU2hiebBm1Su8P!
- Fülle keine Sicherheitsanfragen aus!



Büroanwendungen (10)

Die Büroanwendungen kennen alle Daten, die sie verarbeiten.

Tipps:

Kennst Du lokal installierte Open Source Anwendungen? z.B. siehe in https://www.kuketz-blog.de/umgang-mit-daten-im-privatleben-datensouveraenitaet-teil3/ (Jan19)
- LibreOffice
- GIMP Bekannt, genutzt?

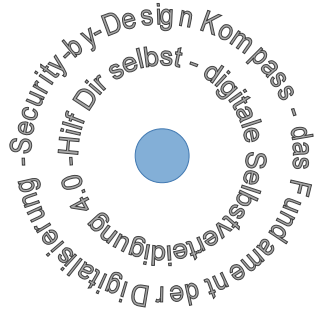
Achte bei Cloud-basierten Anwendungen mit Abo-Modell (u.a. Office 365) und Microsoft Office auf die Datenschutzanalyse
https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office/DPIA+Microsoft+Office+2016+and+365+-+20191105.pdf (Jan19)

Konsequenzen

Wenn Privacy-by-Design nicht umgesetzt wird, ergeben sich ***direkte und spürbare Konsequenzen***!

- Profilbildung
- Neuro Marketing
- verhaltensbasiertes Marketing
- algorithmische Entscheidungsfindung
- Kreditwürdigkeit von Personen
- personenbezogene Preisermittlung

Bereits im Einsatz: dynamische, personalisierte Preisgestaltung:
„Also besonders gut eignen sich all die Produkte, wo der Käufer kein Gefühl dafür hat, was sie kosten. Ich denke, dass nicht nur die absolute Höhe des Preises entscheidend ist, sondern die Preissensibilität eine wichtige Rolle spielt."
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)



„Der Regulierer kann gerne eingreifen. Die Frage ist nur, wie man den Unternehmen die Verwendung von personalisierten Preisen nachweist. Ich glaube, es wird sehr schwierig, entsprechende Nachweise zu finden. Selbst wenn es nachgewiesen wird, müsste der Regulierer schnell eingreifen können. Und das bei der schieren Masse an Transaktionen, die am Markt auftreten." (...)
„Und ein Kunde, den ich als reinen Smart-Shopper identifiziere, als relativ untreuen Kunde, der stark auf Aktionen geht, den möchte ich auch nicht unbedingt aktivieren." (...)
„meine Schwester bekommt immer zehnfach Punkte, wieso bekomme ich das nicht? … Wenn das ein einfacher Coupon ist, den man nur einmal bekommt, gibt es diese Beschwerden eher nicht, …" (...)
https://www.abida.de/sites/default/files/Gutachten_Handel_Bezahlsysteme.pdf E5 – Seite 78 und E6 – Seite 81 (Jan19)
Bei Nichtgefallen des Kunden kann auch das Angebot entzogen werden (getarnt z.B. als Verbindungsabbruch).
https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf Seite 32 (Jan19)