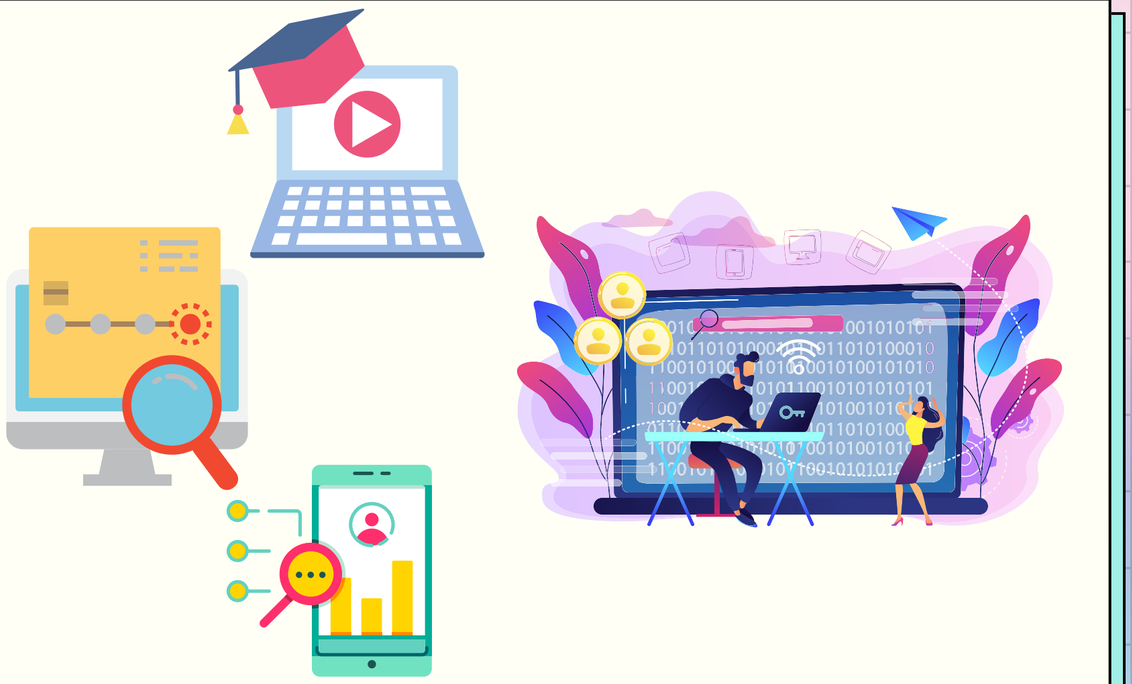
Digitale Selbst-bestimmung

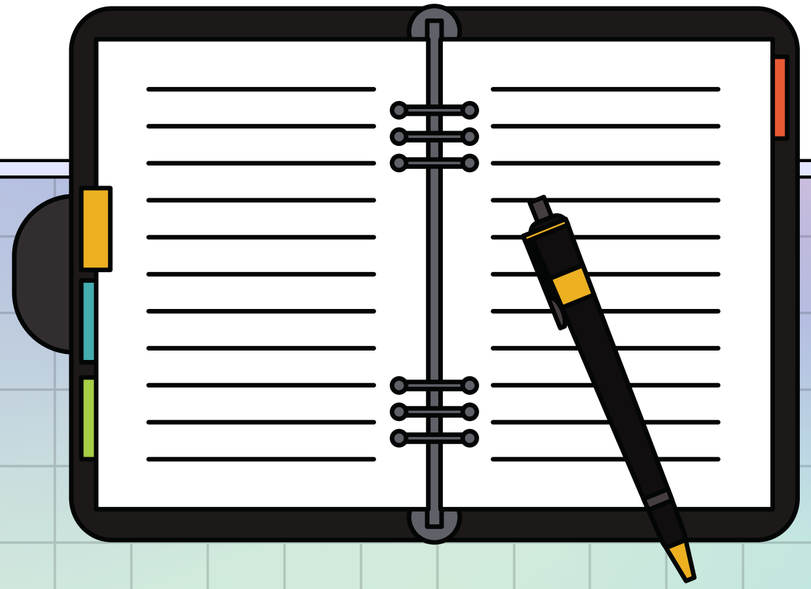
Luise Görlach www.luisegoerlach.de hallo@luisegoerlach.de

Luise Görlach

Referentin für Digitale Selbstbestimmung,
Netzaktivistin, Beratung von Fachkräften
zu Digitalisierung



Heutige Agenda



1. **Was heißt eigentlich digital?!**
2. **Datensparsamkeit**
   - Analoge Tipps & Grundregeln
   - Technische/ digitale Tipps
3. **Gute Anbieter erkennen & nutzen**
   - Freie Software für mobile Geräte
   - Freie Software für den Arbeits/ Uni-Alltag
4. **1x1 der Datensicherheit**
5. **Tipps zur Prävention von Cyberstalting**

Was sind Daten?

Daten sind ableitbare Informationen.

1 Datum = 1 Information

Beispiele:

- **Name**
- **Adresse**
- **Klick auf einen Link**
- **Auto-Kennzeichen**
- **Uhrzeit**
- **Gerätenummer**
- **Koordinaten**
- **Suchwort in einer Suchmaschine...**

Was heißt digital?

Digital beschreibt eine elektronische Technologie, die Daten erzeugt, speichert und verarbeitet, und die eine Datenübertragung durch elektrische oder elektromagnetische Signale übermittelt.

Daten sind Informationen in einem digitalen System: brauchen Systeme, um zu existieren & übertragen zu werden

Was sind diese Systeme?
z.B. Anbieter digitaler Dienste (jeder Anbieter stellt ein System zu einem bestimmten Zweck zur Verfügung)

Was heißt digital?

- Daten bewegen sich in festgelegten Systemen und lassen sich speichern, reproduzieren, übertragen…
- heißt auch: Wer das System bereitstellt, weiß meist auch um die Daten innerhalb des Systems (um den Dienst bereit-zustellen)
- “wissen” heißt auch: verarbeiten, nutzen, verkaufen …

Was heißt digital?

Beispiel WhatsApp:

- **System zur Kommunikation bereitgestellt**
- **Ihre Datenspuren:** Kontakte, Kontaktverhalten, Tastenanschlag, Metadaten von gesendeten Dokumenten u.v.m.
- **Was WhatsApp ableitet:** Interessen, Peergroup, Charakter, Stimmung u.v.m.

Welche digitalen Systeme nutzen Sie?

alle Finger ausstrecken,
pro zutreffender
Aussage geht ein Finger
nach unten

Datenspuren

und wo wir sie überall hinterlassen: Beispiele

Digitaler Raum

- soziale Medien
- Suchmaschinen
- Online-Shopping
- Surfen (Cookies)
- Apps
- Cloud
- Smartphone/ Tablet etc.
- E-Book-Reader

Vernetzte Umwelt/ Internet der Dinge

- Smart Home
- Self-Tracking-Devices (z.B. Fitness-Uhr)
- vernetztes Auto
- smarte Kleidung

Analoger Raum

- Verbindungsdaten (Telefon, SMS)
- Staatliche Stellen
- Ausweis-papiere
- Kundenkarte
- Navigations-geräte
- Gesund heits-karte
- Mautstationen
- Video-Über-wachung
- Flugdaten

Datenkraken

Die beliebtesten Anbieter sind leider auch die datenhungrigsten. “Kostenlose” Dienste bezahlen wir also mit unseren Daten.

Server-Standort: außerhalb der EU

Bis zu 3.000 einzelne Eigenschaften von etwa 700 Millionen Menschen

Beispiele aus dem Consumer Data Products Catalog von *Acxiom*, der hunderte der Eigenschaften auflistet, die das US-Unternehmen anbietet

Mittlerweile gibt es nahezu unendlich viele Kategorien zu allen Lebensbereichen, die in Ihr Profil einfließen. Profile werden von Werbefirmen wie Google und Meta (Facebook) an Werbetreibende verkauft. Leider wissen wir oft nicht, welche Daten von uns gesammelt wurden, wer sie hat und zu welchen Kategorien sie geführt haben.

Ganze Studie: https://crackedlabs.org/studie-kommerzielle-ueberwachung

Konsequenzen auf Datenbasis

Personal-entscheidungen

personalisierte Werbung (Ausnutzen von Schwächen, politische Manipulation siehe TargetLeaks)

Krankheits- und Risikoprognosen

behördliche Überwachung

Diskrimi-nierung

Stalking/ Identitäts-diebstahl

informationelle Einschränkung/ Filterblasen

Kredit-würdigkeit

personalisierte Preise

Das können Sie konkret tun:

Datensparsamkeit

sparsam mit den eigenen Informationen umgehen

Datensicherheit

verantwortungsvoll mit den erhobenen Daten umgehen, die eigenen Daten ausreichend schützen

gute Anbieter wählen

- Systeme wählen, die verantwortungsvoll mit erhobenen Daten umgehen
- sie nicht verkaufen
- gut vor Angreifenden schützen
- DSGVO-konform sind

eigene Geräte sicher einstellen

Datensparsamkeit!

Heißt: Die eigenen Datenspuren kennen und wo es möglich ist reduzieren.

Analoge Tipps

Bleiben Sie analog.

1. auf Kundenkarten/ Payback-Karte/ Deutschlandcard verzichten
2. lieber bar als mit Karte zahlen
3. lieber per Rechnung zahlen bei Bestellungen
4. nicht an Gewinnspielen teilnehmen, wo Sie sensible Daten angeben müssen
5. aus Telefonbuch löschen lassen

Grundregeln

Sparsam mit allen Daten umgehen, die Sie NICHT durch einen vollen Bus rufen würden.

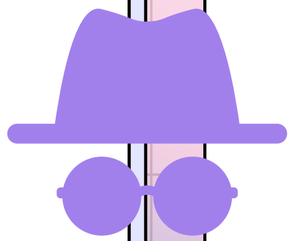
1. Überlegen Sie: Werden ALLE Daten gebraucht? (muss ein Onlineshop Ihre Telefonnummer haben?) –-> Sie müssen nicht immer alles ausfüllen

2. Werden ECHTE Daten gebraucht? Geben Sie falsche Daten an (bei Telefonnummer oder Adresse), wenn diese für den Zweck nicht benötigt werden (z.B. Anmeldung zu einem Online-Workshop)

Technische Tipps

Schwindeln...

- www.frankgehtran.de // 01631737743 oder 052116391643
- Wegwerf-Mailadresse (3 Tage gültig): www.muellmail.com
- alternative Mail-Adressen über die App SimpleLogin
- KI-generierte Profilbilder: https://thispersondoesnotexist.com/



Einstellungen...

- ungenutzte Apps löschen
- Schnelleinstellungen: Flugmodus aktivieren, GPS/Bluetooth/WLAN bei Nicht-Nutzung deaktivieren
- App-Berechtigungen in den Einstellungen einschränken (besonders Zugriff auf Mikrofon, Kamera, Kontakte/ Telefon, Kalender)
- iOS: Apps nicht erlauben, Sie zu tracken
- Google-Einstellungen: Standortverlauf und personalisierte Werbung deaktivieren

Anleitungen hier

Einstellungen

Standortzugriff

- **Android**: Einstellungen –> Standortzugriff deaktivieren
- **iOS**: Einstellungen –> Privatsphäre & Sicherheit –> Standortzugriff ausschalten
- **Kamera-App** öffnen → Einstellungen → Standortmarkierung bzw. Standortstempel deaktivieren

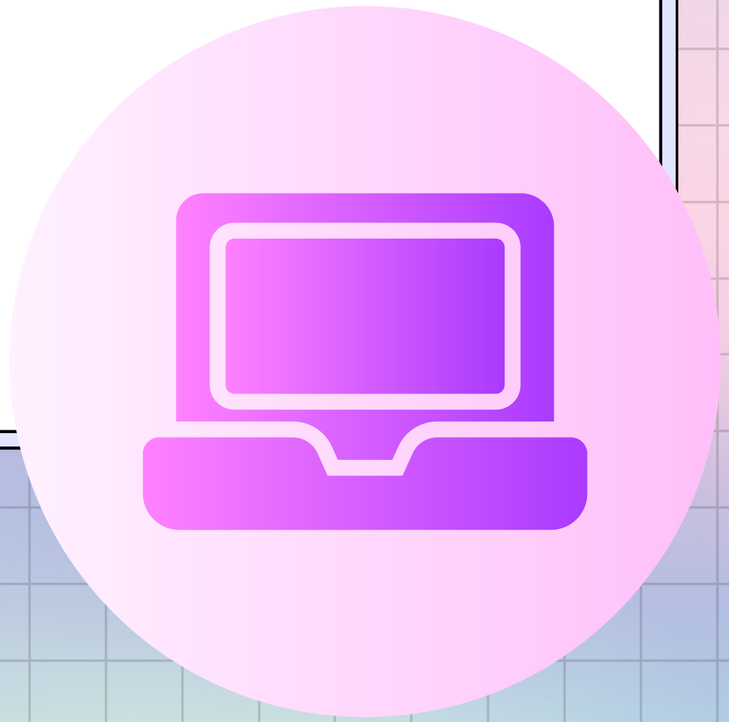
Apps & Berechtigungen

- Einstellungen –> Berechtigungsverwaltung –> Zugriffe der Apps auf Standort, Kamera, Mikrofon einschränken
- Einstellungen –> Apps –> Aktionen nicht speichern
- iOS: Einstellungen → Datenschutz → Tracking → ‚Apps erlauben, Tracking anzufordern“ deaktivieren

Datenschutz-Einstellungen

- Datenschutz → Werbung und Datenschutz → Personalisierte Werbung deaktivieren
- UND Werbe-ID zurücksetzen/ deaktivieren
- Datenschutz → Werbung und Datenschutz → Weitere Informationen → Intelligente Werbung deaktivieren UND Erfassung von Werbe-ID-Statistiken deaktivieren
- Datenschutz → Autofill-Service von Google deaktivieren UND Google-Standortverlauf deaktivieren UND Nutzung und Diagnose AUS
- in den Google-Einstellungen: Web- & App-Aktivitäten prüfen PAUSIEREN
- Google-Werbe-ID deaktivieren: (GAID)
- Einstellungen → Google → unter Dienste auf Anzeigen klicken → Werbe-ID löschen
- **iOS**: Einstellungen → Datenschutz → Apple-Werbung → "Personalisierte Werbung“ deaktivieren

Laptop



1 Datenschutz-Einstellungen:

- Allgemein: alles deaktivieren
- Spracherkennung: aus
- App-Berechtigungen: alle deaktivieren (und bei Bedarf aktivieren)

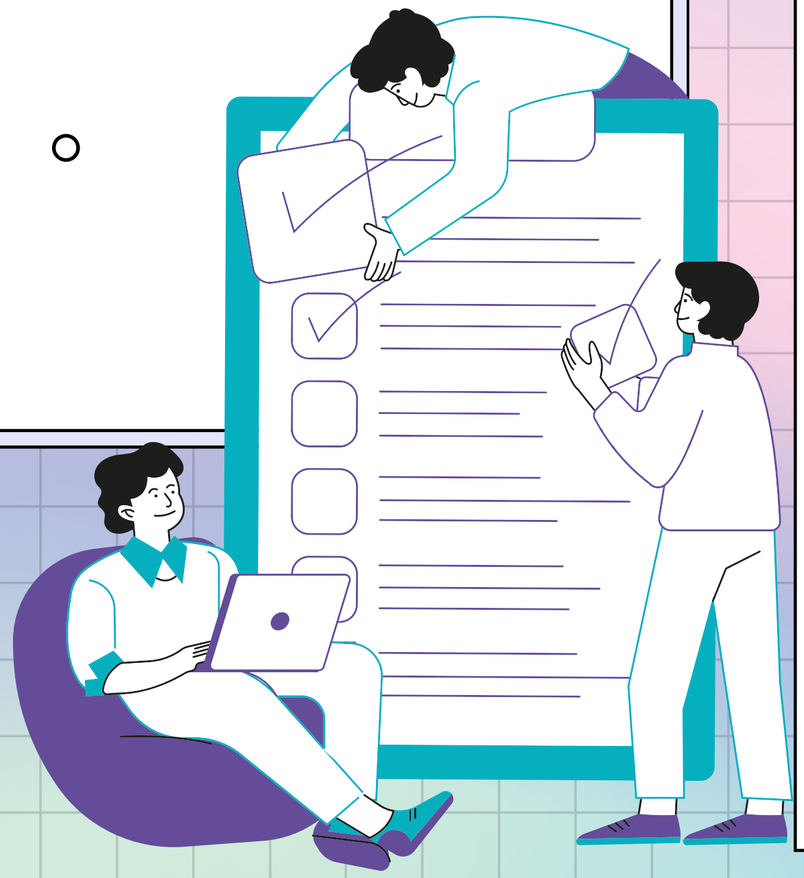
2 Systemsteuerung

- Eigenschaften von Internet --> Datenschutz --> Popupblocker einschalten
- Eigenschaften von Internet --> Datenschutz --> Erweitert --> Cookies von Drittanbietern --> Blocken

3 Einstellungen am Mac

- https://www.konsumentenschutz.ch/online-ratgeber/privatsphaere-mac-schutz/

Gute Anbieter nutzen



1. datensparsam: erfasst nur nötigsten Daten
2. funktioniert in Browser (kein App-Download nötig)
3. keine Registrierung erforderlich
4. freie Software
5. Firmenhauptsitz UND Serverstandort in der EU

Apps prüfen:
https://reports.exodus-privacy.eu.org/de/
oder
https://appcheck.mobilsicher.de/

offener Quellcode

darf frei genutzt, verbreitet, verbessert & angepasst werden

Freie Software

ermöglicht Unabhängigkeit von Datenkraken

unabhängige Prüfung

F-Droid

https://f-droid.org/

Installationsanleitung

App-Empfehlungen für jeden Anlass

- = alternative App-Quelle für Android-Apps (mehr dazu hier)
- betrieben von Ehrenamtlichen & auf Spendenbasis
- bietet ausschließlich freie Software an, die nach strengen Regeln geprüft wird: müssen quelloffen, werbefrei, trackerfrei und kostenlos sein
- dadurch Apps, die datenschutzfreundlicher, nicht kommerziell und ohne Kostenfalle sind
- dadurch auch besonders geeignet für Kinder

Privatsphäre

aus dem F-Droid Store

AdAway (Werbe- & Tracking-blocker)

Tracker Control (Überwachung von einzelnen Trackern)

Blokada (Werbe- und Tracking-blocker)

Exodus (prüft Tracker & Berechti-gungen)

Orbot (VPN über Tor Netzwerk)

UntrackMe (leitet auf datensparsame Alternative zu sozialen Netzwerken um)

Installationsanleitung: https://mobilsicher.de/ratgeber/so-installieren-sie-den-app-store-f-droid

Sicherheit

aus dem F-Droid Store

Aegis (2-Faktor-Authenti-fizierung via TOTP)

KeePassDX (Passwort-Manager)

NetGuard (Firewall mit VPN-Funktion)

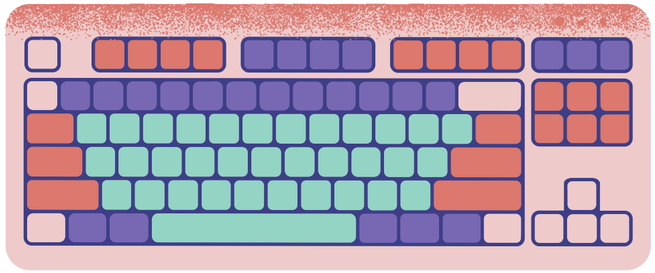
Karma Firewall (Firewall für einzelne Apps)

Weitere tolle Apps & Infos zum F-Droid:
https://digitalcourage.de/digitale-selbstverteidigung/f-droid-appstore oder hier

Installationsanleitung: https://mobilsicher.de/ratgeber/so-installieren-sie-den-app-store-f-droid

Tastatur

vorinstallierte Tastatur (meist Microsoft SwiftKey oder Google Gboard) lesen mit & erfordern viele Berechtigungen (auf Kalender, Standort etc.) & Internetzugriff



OPTION 1:

In den Einstellungen der Tastatur-App die Berechtigungen entziehen & die Netzwerkverbindung (in den Einstellungen bei den Apps “Datennutzung” deaktivieren (geht auch über die App TrackerControl)

OPTION 2:

Eine alternative Tastatur (z.B. “Schlichte Tastatur” oder “OpenBoard”) herunterladen, öffnen und als Standard-Tastatur einstellen)

Empfohlene Office- Tools

- Alternative zur Microsoft Office Suite: LibreOffice (Text, Tabelle, Präsi)
- Termine finden/Umfragen: nuudel von Digitalcourage
- VeraCrypt: verschlüsselt Dateien & Ordner
- Cryptpad: kollaborativ Texte, Tabellen, Präsis erstellen, Umfragen, geteilte Ordner/ Dateien
- Signal: Messenger
- Videokonferenzen: Meetzi (Jitsi) & Senfcall (BigBlueButton)
- schicks.digital: anonym große Dateien versenden

Freie Software . . . .

Werkzeuge zur Medienproduktion/ –bearbeitung:

- Tonspuren aufnehmen & Bearbeiten mit Audacity
- Videos schneiden/ bearbeiten mit Avidemux oder Shotcut
- Videos aufzeichnen & streamen mit OBS oder SimpleScreenRecorder
- Bildbearbeitung mit GIMP
- Mindmaps erstellen mit Freeplane oder Freemind
- Diagramme & Zeichnungen erstellen mit Dia
- Lernkarten mit Anki erstellen & über verschiedene Geräte synchronisieren
- PDFs bearbeiten mit Master PDF Editor
- übersichtliches Durchsuchen und Verwalten von Mediatheken der ÖR mit MediathekView

Einladung zum Netzwerk Freie Schulsoftware

Unsere Ziele

- Schulen befinden sich in Bezug auf Schulsoftware in einem **Dilemma**: Funktionalität, Wirtschaftlichkeit, Ethik, Technik, Politik und Behördenauflagen wollen vereinbart werden. Wir möchten bei der **Orientierung** helfen.
- Wer **Freie Software an Schulen** einsetzt, tut etwas für den **Schutz von Daten und Grundrechten** der Schüler.innen und Lehrkräfte. Wir möchten u.a. über den Zusammenhang aufklären und den Einsatz dieser Software fördern.
- Überall im Land versteckt sich wertvolles **Experten- und Erfahrungswissen** zum Einsatz freier Schulsoftware. Wir möchten Sie **mit Gleichgesinnten und Hilfesuchenden vernetzen.**

https://digitalcourage.de/netzwerk-freie-schulsoftware

Zusammen-fassung Datensparsamkeit

Am besten geschützt sind die Daten, die gar nicht erst entstehen!

Eine gute Orientierung bieten die Angebote Ihrer Hochschule

1. **Browser-basierte Dienste statt Apps** (z.B. Bahn, Shopping, ViKo...)

2. **Datensparsame Apps/ Software :**
   - statt Chrome lieber Firefox & Tor Browser
   - statt Google Suche lieber MetaGer/ Startpage/ DuckDuckGo
   - statt WhatsApp lieber Signal
   - statt MS Teams lieber Rocket.Chat
   - statt Zoom/ Webex lieber BigBlueButton/ Jitsi
   - statt WeTransfer lieber Cryptpad (große Dateien versenden)
   - statt MS Office lieber LibreOffice
   - statt Cloud lieber externe Festplatte (verschlüsseln mit VeraCrypt/ Cryptomator)

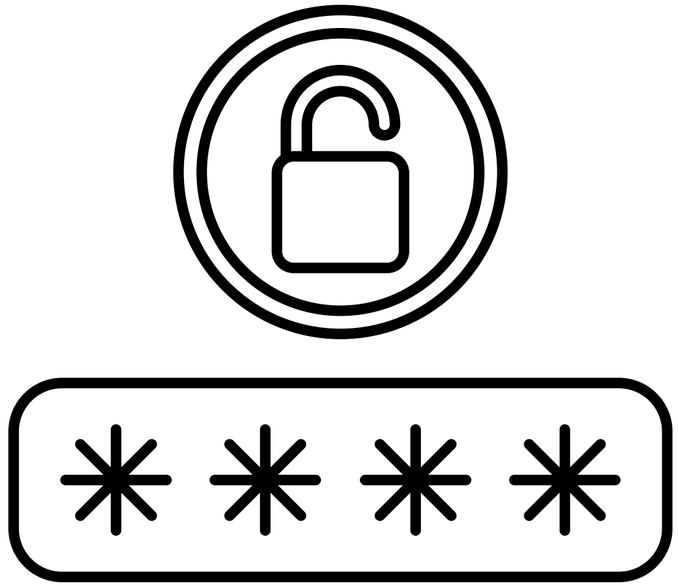
1 Punkt pro zutreffender Aussage

Mein Passwort hat etwas mit meinem Privatleben zu tun.	Ich habe eine einzige E-Mail-Adresse. die ich für alles nutze.	Mein*e Partner*in kennt viele meiner Passwörter.
Was sind nochmal Backups?	Meine Passwörter stehen auf dem Zettel unter der Tastatur.	Updates mache ich nicht. Die dauern doch ewig!
Ich speichere meine Passwörter im Browser.	Ich bin wenig skeptisch bei Mails und klicke schnell auf Links/ Anhänge.	Ich habe überall dasselbe Passwort.

Datensicherheit

Wie verantwortungsvoll gehen Sie mit Daten um?

Passwörter



Top Ten deutscher Passwörter 2021

123456

passwort

12345

hallo

123456789

qwertz

schatz

basteln

berlin

12345678

Gute Passwörter

Passwortmanager

Download: https://keepassxc.org/

- legen sämtliche Passwörter in einer verschlüsselten Datenbank auf der Festplatte ab (regelmäßig aktualisieren & mit allen Geräten synchronisieren, Anleitung verlinkt)
- schützen sie durch ein einziges Passwort, das Hauptpasswort
- generieren eigene Passwörter

Merkmale guter Passwörter

–nur einmalig nutzen, mit niemandem teilen

–mindestens 15 Zeichen

–Kombi aus Groß– und Kleinbuchstaben, Zahlen und Sonderzeichen

–keine echten Wörter(außer aufgereiht, mit Sonderzeichen & Zahlen dazwischen)

–echte Wörter teilweise chiffrieren:
A zu ^, E zu 3, S zu $, T zu +

– Merksätze nutzen, um komplexe Passwörter zu erinnern

Sichere Passwörter

Bei Verdacht auf Stalking sollten Sie umgehend ALLE Passwörter (insbesondere zu Google, Amazon, Mails etc.) ändern
–-> neue Passwörter lieber analog in einem Passwort–Heftchen notieren als digital speichern

1.Beispielsatz überlegen

Ich trinke meinen Kaffee immer mit zwei Stückchen Zucker und Milch.

2. Anfangsbuchstaben der Wörter notieren und wenn möglich durch Zahlen und Symbole ersetzen

Ich trinke meinen Kaffee immer mit 2 Stückchen Zucker & Milch.

ItmKim2SZ&M.

2-Faktor-Authentifizierung

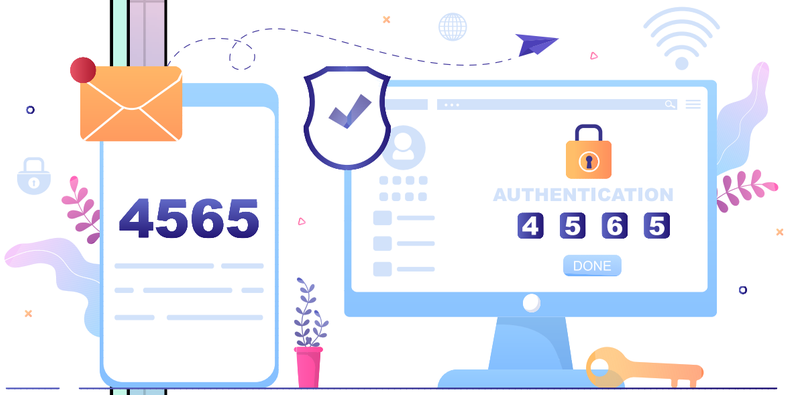
Wissenswertes

- bieten viele Dienste an (in den Sicherheitseinstellungen kann die Option manuell aktiviert werden)
- verschiedene Arten: App (meist mit App des jeweiligen Dienstes verknüpft), SMS (Code per SMS erhalten), Hardwaretoken (z.B. Tan-Generator vieler Banken), biometrische Verfahren (Fingerabdruck, Gesichtsscan)

Selbst per App

Für Android: Aegis

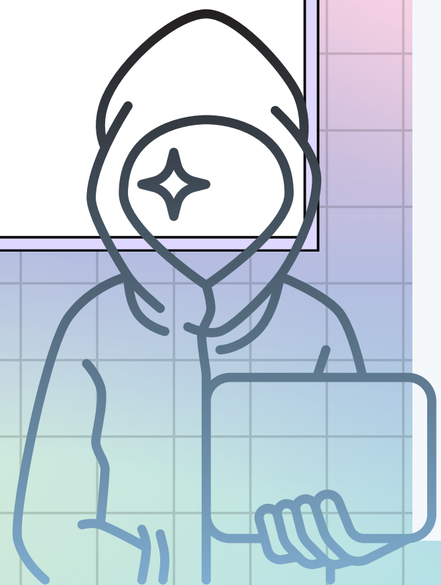
Für iOS: Raido OTP



Viel wahrscheinlicher als ein Einbruch ist, dass Sie Teil

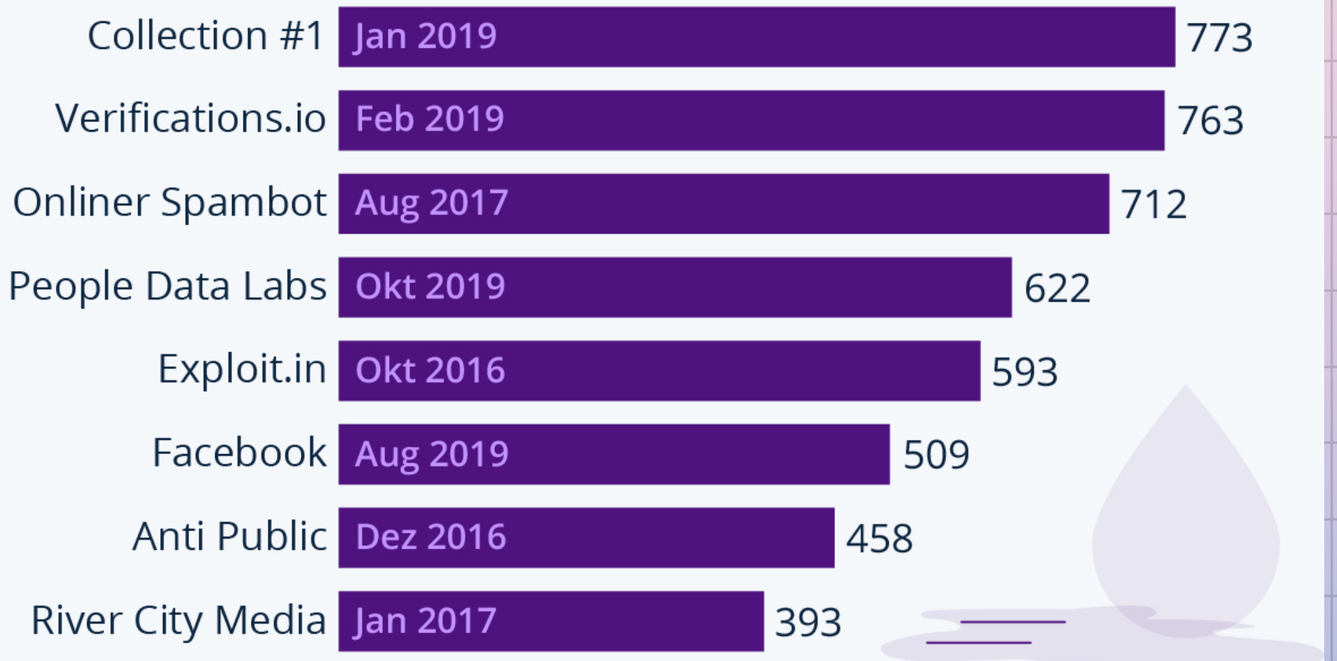
- eines Datenlecks (Daten “liegen ungeschützt im Internet rum”) oder
- eines Datendiebstahls (Hacker dringen in Systeme ein und “stehlen” sensible Daten, die sie dann weiterverkaufen oder Menschen damit erpressen)

werden.



Die größten Daten-diebstähle der Welt

Größte bekannte Datenlecks
nach Anzahl betroffener Accounts (in Mio.)*



* Ohne Duplikate
Quelle: Have I Been Pwned?

statista

E-Mail-Adressen prüfen:

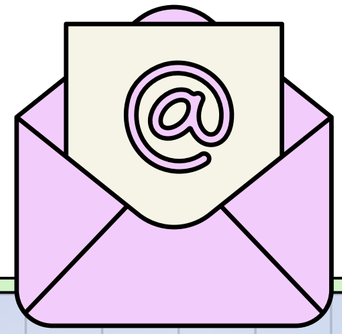
https://haveibeenpwned.com/

https://sec.hpi.uni-potsdam.de/ilc/search?lang=de

E-Mail

- sparsam preisgeben
- mehrere Mail-Adressen für verschiedene Zwecke anlegen (Alias)
- Temporäres Postfach: www.muellmail.com

- gute E-Mail-Anbieter: posteo.de und mailbox.org (bieten automatische Verschlüsselung an, kosten 1 Euro/ Monat)
- keine guten E-Mail-Anbieter: gmail, gmx, web.de, hotmail, freenet, yahoo (durchleuchten Mails nach Schlüsselwörtern & analysieren Metdaten)
- E-Mail-Client für den Laptop: Thunderbird (inklusive Kalender & Kontakte)
- E-Mail-Client für Android: FairEmail, K-9 Mail
- E-Mail-Client für iOS: ProtonMail

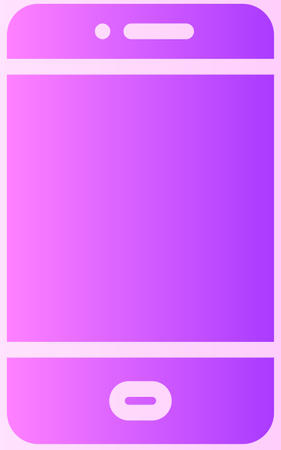


Was tun gegen Phishing?

https://phishingquiz.withgoogle.com/?hl=de

- gesunde Skepsis & Logik
- ungenutzte Accounts löschen
- bei offensichtlicher Spam: Mail nicht öffnen, sondern direkt in Spam-Ordner
- Webseite/ Dienst nicht über Link aufrufen
- Medienbruch: anrufen
- Stolperstein: Rückfrage
- Umfeld sensibilisieren
- mit Cursor Absender & Anhang prüfen (nicht klicken!)

Smart-phone



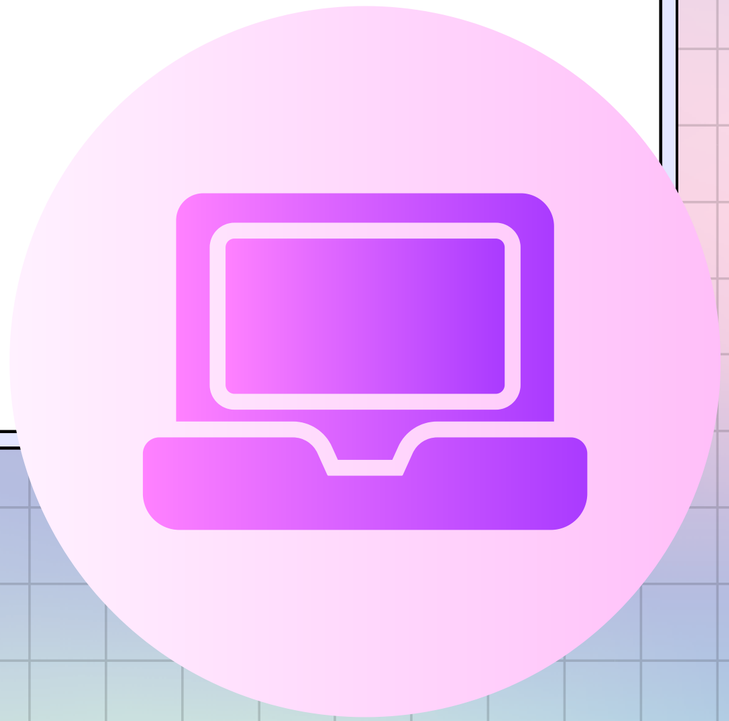
1. Software aktuell halten (automatische Updates aktivieren in den Einstellungen), unnötige Funktionen bei Nicht-Nutzung deaktivieren (GPS, Bluetooth, WLAN)

2. Sensible Dateien auf Smartphone mit Passwort schützen (bei Android über Funktion "Private Space" bei iOS über "Geführter Zugriff oder über App "Folder Lock"

3. Hilfreiche Apps (Android):
   - LibreAV (F-Droid Store)
   - KarmaFirewall (F-Droid Store)
   - PilferShush (blockiert Mikrofon, F-Droid Store)
   - K9-Mail (verschlüsseltes E-Mail-Postfach)
   - PrivacyScanner

4. Hilfreiche Apps (iOS):
   - FamilyTime (begrenzt Zugriffe von Apps)
   - Lookout (Maleware-Scanner, allerdings mit Google Tracker!)

Laptop



1 Hardware

- Kameraschieber
- Safe
- sensible Daten/regelmäßige Backups auf externer Festplatte (im Safe!)
- weitere: https://shop.digitalcourage.de/gadgets

2 Einstellungen/ Software

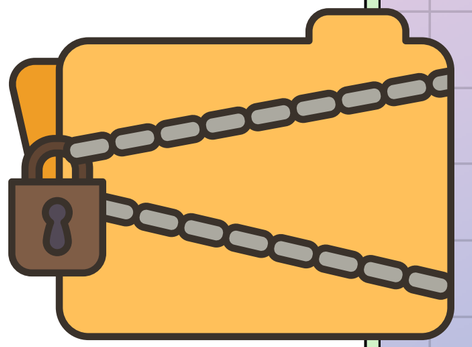
- aktuelle Software (automatische Updates aktivieren)
- nur das Nötigste in Cloud (dann Nextcloud, Links im Cryptpad)
- Verschlüsselung von Ordnern, Dateien und Datenträgern mit VeraCrypt (https://www.veracrypt.fr/)
- Firewall und Virenschutz aktivieren

Daten verschlüsseln

Alternative Verschlüsselungs-Möglichkeiten für Festplatten finden Sie hier

VeraCrypt

- **Warum?** Schutz der Daten vor Angriffen von Außen –-> sind dazu im beruflichen Kontext gesetzlich verpflichtet
- Verschlüsselung ist eine einfache und sehr effektive Maßnahme, um personenbezogene Daten vor unautorisiertem Zugriff zu schützen.



VeraCrypt kann ganze Datenträger oder Container verschlüsseln:

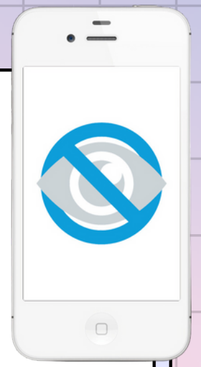
- Software herunterladen: https://www.veracrypt.fr/en/Downloads.html
- entweder verschlüsselten Ordner (=Container) auf dem Laptop erstellen oder das Speichermedium auswählen, das verschlüsselt werden soll
- Detaillierte Anleitung hier

VeraCrypt

Anti-Stalking

Prävention

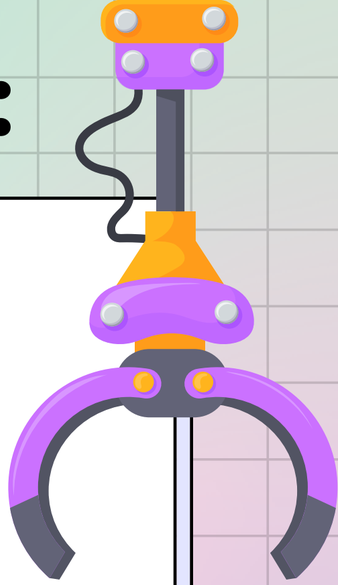
Allgemein:



- gesundes **Misstrauen** bei geschenkten Smartphones
- Geräte **selbst einrichten** (evtl. Kurse dazu besuchen)
- **Passwörter**/ Entsperrungsmuster/ Zugänge **nicht** mit anderen **teilen**
- keine geteilte Cloud (am besten gar **keine Cloud**)
- Dokumentation über NoStalk App (Weisser Ring)

- **Standorterkennung** beim Gerät **deaktivieren** & separat in Apps (z.B. Kamera!)
- **Metadaten** von Dateien **löschen** (z.B. mit Apps wie Scrambled Exif)
- bei Android: **PlayProtect aktivieren**
- **starke Passwörter** (nicht in Browser speichern) & **2-Faktor-Authentifizierung**
- **Incognito/ privater Modus** im Browser nutzen
- nicht auf externen Seiten mit Google/ Facebook/ Amazon Konto anmelden (bei Neu-Registrierung Wegwerf-Adressen ohne Klarnamen nehmen: muellmail.com)
- datensparsame Programme nutzen

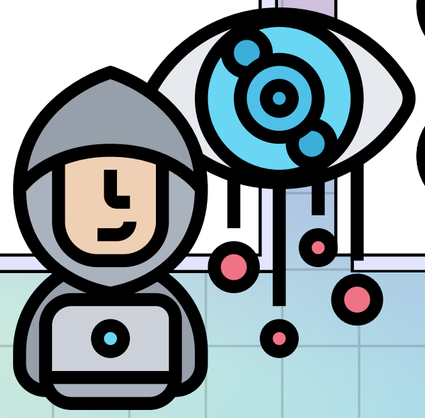
Zugriff über:



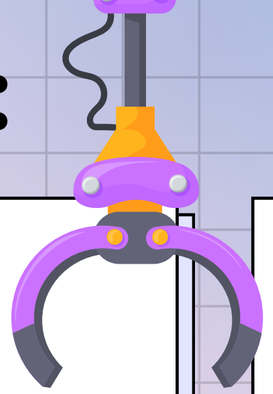
Gefahr durch gezielte Angriffe auf Ihre Person oder Ihre Einrichtung:

- Cyberstalking
- Identitäts-diebstahl
- Erpressung

1. Direkter Zugriff auf das Gerät
2. Indirekter Zugriff über Zugänge (Anmeldedaten)
3. Indirekter Zugriff über Apps, die Standort preisgeben
4. Smartphone-Funktionen wie Cloud
5. Vernetzte Geräte (Smart Watch, Smart Home)
6. Stalkerware (Spionage-Apps)
7. Datenbanken im Darknet



Zugriff über:



1

Direkter Zugriff auf das Gerät

- Geräte im Blick behalten & durch Display-Sperre sichern
- häufige Gründe für Zugriffe: Einrichtung von Geräten
- besser: externe Angebote nutzen (Smartphone/ Computer-Kurs) & Unterstützung beim Einrichten der Geräte anbieten

2 3 4

Indirekter Zugriff über Zugänge (Anmeldedaten), Apps, Cloud

- Datenschutzeinstellungen: kein Zugriff von Apps/ Cloud auf Standort, Mikrofon, Kamera
- WhatsApp: Abmeldung aller Geräte (WhatsApp Web)
- aus Cloud abmelden (z.B. Google) & neues Google-Konto einrichten (häufig Suchanfragen, Fotos etc. mit Cloud verknüpft)
- Google-Einstellungen: Standort-/Suchverlauf nicht speichern
- besser: Tor Browser & Signal

Zugriff über:

5

Vernetzte Geräte

- auf Smart Speaker verzichten
- Abhören bzw. Standortverfolgung ist möglich über Zugriff auf Smart Speaker, smartes Spielzeug, smarte Kleidung & Accessoires (z.B. Schulranzen oder SmartWatch mit GPS-Funktion) oder Smartphone/ Laptop
- unbedingt Kamera-Schieber für smarte Geräte nutzen!

6

Stalkerware/ Spionage-Apps

- Auflistung aller auf dem Smartphone installierten Apps über die App “Exodus”: verdächtige Apps dabei?
- AirGuard App: erkennt AirTags in der Nähe
- wichtig: Verdächtiges dokumentieren

Merkwürdiges Verhalten des Smartphones:

- Akku entlädt sich schnell
- genutztes Datenvolumen ist ungewöhnlich hoch
- Smartphone läuft langsamer als gewohnt
- Hintergrundgeräusche beim Telefonieren
- unbekannte Apps

2. Verdacht: Fragenkatalog

- Was ist passiert / was stellst Du fest? Schreibe die Beobachtung möglichst genau auf.
  - Führe ein Tagebuch über die Vorkommnisse und Begebenheiten. Dies kann auf Papier in einem Schulheft stattfinden.
  - Das Aufschreiben dient dazu, eine zeitliche Dokumentation der Ereignisse zu haben, die später z.B. auch der Polizei vorgelegt werden kann.
  - Niemand kann beliebig viele Vorfälle über lange Zeit im Kopf behalten.
  - Der Weiße Ring Linktipp: Weisser Ring (externe Seite) stellt auch eine App zur Verfügung, die die Daten nicht auf dem Smartphone speichert, die NoStalk-App:
  - Linktipp: Die Nostalking App des Weissen Ring (externe Seite)

Weitere Fragen & Anleitungen auf: antistalking.haecksen.org

- Passiert das öfter (reproduzierbar)? Passiert das immer in bestimmten Situationen?
- Kannst Du ausschließen, dass die Beobachtung darauf zurückzuführen ist, dass Deine Software veraltet oder falsch eingestellt ist?
- Kannst Du ausschließen, dass die Beobachtung darauf zurückzuführen ist, dass Deine Hardware (Rechner, Smartphone, DSL-Router, Splitter) defekt ist?
- Kannst Du ausschließen, dass eine Webseite eines Anbieters schlicht und einfach kaputt ist und daher komische Dinge anzeigt?
- Haben andere Menschen innerhalb und außerhalb Deines Haushaltes Zugriff auf Deine Geräte und können diese "verstellt" haben?

Dokumentation sowohl für Privatpersonen als auch Einrichtungen wichtig!

Warum nicht mal Selbstbestimmung verschenken?
Hier bestellen

Merci!

digitale.selbstfuersorge

http:// www.luisegoerlach.de

hallo@luisegoerlach.de