TECHNISCHE UNIVERSITÄT WIEN
Vienna | Austria

Open Source und Datenschutz

Luis & Thomas

29. Mai 2025

Was ist Open Source Software (FOSS)

- **Definition**: Quellcode ist öffentlich zugänglich, kann genutzt, verändert und weitergegeben werden.
- **Philosophie**: Zusammenarbeit, Transparenz und Freiheit stehen im Mittelpunkt.
- **Vorteile**: Sicherheit, Anpassbarkeit, keine Lizenzkosten, große Community.
- **Open Source vs. Free Software**: Open Source = praktischer Ansatz, Free Software = ethische/philosophische Grundlage (Stichwort: "Free as in freedom, not as in free beer").
- **Bedeutung für die Gesellschaft**: Digitale Souveränität, Datenschutz, Unabhängigkeit von großen Konzernen.

Die Geschichte von FOSS

- **1950er–1970er**: Software wurde oft frei geteilt, insbesondere in der akademischen Welt.
- **1983**: Richard Stallman startet das GNU-Projekt und begründet die Free Software Foundation (FSF).
- **1991**: Linus Torvalds veröffentlicht den ersten Linux-Kernel.
- **1998**: Der Begriff "Open Source" entsteht als Alternative zu "Free Software".
- **2000er–heute**: Open Source wird Mainstream – von Unternehmen (Google, Microsoft) bis zu Regierungen.

Von UNIX zu GNU: Der Weg zur Open-Source-Bewegung

- **1970er**: UNIX wird an Universitäten verbreitet, BSD (Berkeley Software Distribution) entsteht als modifizierte Version.
- **1980er**: AT&T beginnt, UNIX kommerziell zu lizenzieren, BSD enthält noch proprietären UNIX-Code.
- **1983**: Richard Stallman startet das GNU-Projekt, um ein komplett freies UNIX-ähnliches System zu entwickeln.
- **1990er**: Nach rechtlichen Streitigkeiten wird BSD von proprietären UNIX-Teilen befreit, parallel entwickelt sich GNU weiter.
- **Linux-Kernel (1991)**: GNU fehlte ein Kernel, Linus Torvalds veröffentlicht Linux – GNU/Linux entsteht.

Was ist jetzt GNU?

- **GNU (GNU's Not Unix)**: Ein freies, UNIX-ähnliches Betriebssystem, gestartet von Richard Stallman 1983.
- **Ziel**: Ein komplett freies Software-Ökosystem ohne proprietäre Einschränkungen.
- **Bestandteile**: Compiler (GCC), Editor (Emacs), Shell (Bash), viele UNIX-Tools.
- **GNU Hurd**: Eigentlich als Kernel für GNU gedacht, aber bis heute nicht fertiggestellt.
- **GPL-Lizenz**: Sichert, dass Software frei bleibt (Copyleft-Prinzip).

...und was ist Linux?

- **Linux-Kernel**: 1991 von Linus Torvalds entwickelt, ein freier, monolithischer Betriebssystemkern.
- **Ersatz für GNU Hurd**: Da Hurd nie wirklich fertig wurde, wurde Linux als Kernel für GNU genutzt – so entstand GNU/Linux.
- **Distributionen**: Debian, Ubuntu, Arch, Fedora, openSUSE – unterschiedliche Ansätze und Zielgruppen.
- **Einsatzbereiche**: Server, Embedded Systems, Supercomputer, Smartphones (Android), Desktop.
- **Philosophie**: Open Source, Anpassbarkeit, Stabilität, Sicherheit.

GNU, Linux... ja gut, aber was ist BSD?

- **BSD (Berkeley Software Distribution)** – Unix-Derivat, entwickelt ab den 1970er Jahren an der UC Berkeley
- **AT&T vs. BSD** – Rechtsstreit in den 1990ern, führte zur vollständigen freien Veröffentlichung von BSD
- **Lizenz** – BSD-Lizenz erlaubt freie Nutzung, Modifikation und proprietäre Nutzung (weniger restriktiv als GPL)
- **Forks** – FreeBSD, OpenBSD, NetBSD als eigenständige Weiterentwicklungen
- **Einfluss** – TCP/IP-Stack von BSD prägt moderne Netzwerktechnologie
- **macOS & iOS** – Basieren teilweise auf BSD-Komponenten
- **PlayStation 4 & 5** – Betriebssystem "Orbis OS" basiert auf FreeBSD

Die wichtigsten Lizenzen

- **GPL (GNU General Public License)**: Copyleft, Änderungen müssen ebenfalls unter GPL veröffentlicht werden.
- **MIT License**: Sehr permissiv, erlaubt fast alles, solange der ursprüngliche Autor genannt wird.
- **Apache License 2.0**: Ähnlich wie MIT, aber mit Patentklausel zum Schutz vor Patentstreitigkeiten.
- **BSD License (2-/3-Clause)**: Minimalistische Lizenz, erlaubt fast uneingeschränkte Nutzung.
- **Creative Commons (CC)**: Für nicht-softwarebasierte Werke, verschiedene Varianten mit Einschränkungen wie Namensnennung oder nicht-kommerzielle Nutzung.

Vorteile von Open Source in der Forschung

- **Reproduzierbarkeit**: Offen zugänglicher Code sorgt für überprüfbare Ergebnisse.
- **Kosteneffizienz**: Keine teuren Lizenzen, volle Kontrolle über die Tools.
- **Transparenz**: Keine Black-Box-Algorithmen – jeder kann nachprüfen, was passiert.
- **Kollaboration**: Forschungsteams weltweit können gemeinsam weiterentwickeln.
- **Nachhaltigkeit**: Software bleibt nutzbar, auch wenn Unternehmen verschwinden.
- **Anpassbarkeit**: Code kann spezifisch für Forschungsfragen modifiziert werden.

Setzen wir FOSS ein? JA!

- **Python** – Eine weit verbreitete Programmiersprache für Datenanalyse, Automatisierung und wissenschaftliches Rechnen.
- **Octave** – Freie MATLAB-Alternative für numerische Berechnungen.
- **UGENE** – Open-Source-Software für Bioinformatik, Sequenzanalyse und Genomanalysen.
- **OpenChrom** – Freie Software zur Auswertung chromatographischer Daten (z. B. GC/MS, HPLC).
- **Zotero** – Open-Source-Tool zur Verwaltung von Literatur und Quellen.
- **LaTeX** – Ein Schriftsatzsystem für wissenschaftliche Arbeiten – inklusive dieser Präsentation!

Open Source und BigTech

- **Microsoft** – Nutzt und unterstützt Open Source (z. B. Linux auf Azure, WSL, VS Code) und ist größter GitHub-Sponsor.
- **Apple** – Setzt Open-Source-Technologien ein (z. B. WebKit, Swift, Darwin), aber hält viele Teile proprietär.
- **Google** – Entwickelt und fördert Open Source (z. B. Android, Chromium, TensorFlow, Kubernetes), doch sammelt viele Nutzerdaten.
- **Tesla** – Verwendet Linux in seinen Autos, musste Open-Source-Code veröffentlichen, hält aber viele Softwarekomponenten geschlossen.
- **Meta (Facebook)** – Entwickelt Open-Source-Projekte wie React, PyTorch und HHVM, steht aber wegen Datenschutz und Tracking in der Kritik.
- **Red Hat** – Einer der größten Open-Source-Anbieter, entwickelt Linux-Distributionen (z. B. RHEL, Fedora) und verdient mit Support und Dienstleistungen.

Was ist GitHub?

- **GitHub** – Die größte Plattform für Open-Source-Software-Entwicklung.
- **2018 von Microsoft übernommen** – Seitdem gemischte Reaktionen aus der Open-Source-Community.
- **Features** – Code-Hosting, Kollaboration, Versionskontrolle mit Git, CI/CD, Codespaces.
- **GitHub Copilot** – KI-gestütztes Coding-Tool, aber umstritten wegen Trainingsdaten aus Open-Source-Code.
- **Alternativen** – GitLab (selbst hostbar), Gitea, Codeberg (FOSS-freundlich, unabhängig).

Hands-on: GitHub

Nehmt euch **10 Minuten** Zeit und überlegt:

- Öffnet **GitHub** (`https://github.com`) und sucht nach spannenden Projekten.
- Schaut euch an:
  - Beschreibung (README)
  - Programmiersprache
  - Lizenz
  - Aktivität (Commits, Issues, Pull Requests)
- Beispiele für bekannte Open-Source-Projekte:
  - **Linux Kernel** (`https://github.com/torvalds/linux`)
  - **Python** (`https://github.com/python/cpython`)
  - **Blender** (`https://github.com/blender/blender`)
  - **OBS Studio** (`https://github.com/obsproject/obs-studio`)
- Welche interessanten Projekte findet ihr?

Open-Source-Anwendungssoftware

- **Open Source im Alltag:**
  - **Firefox** – Datenschutzfreundlicher Webbrowser.
  - **E-Mail:** Thunderbird – Open-Source-E-Mail-Client mit vielen Erweiterungen.
  - **LibreOffice** – Kostenlose Alternative zu Microsoft Office.
  - **VLC** – Mediaplayer für fast alle Formate.
  - **7-Zip** – Dateiarchivierer für `.zip`, `.rar`, `.7z`, etc.
- **Open Source für spezielle Anwendungen:**
  - **Kdenlive** – Videobearbeitung.
  - **Darktable** – Foto-Entwicklung (Alternative zu Adobe Lightroom).
  - **Audacity** – Audio-Editor.
  - **Ardour** – Professionelle DAW für Audio-Produktion.
  - **Blender** – 3D-Modellierung und Animation.
  - **OBS Studio** – Livestreaming und Bildschirmaufnahme.

Open Source für Web & Content

Frameworks

- **Bootstrap** – CSS-Framework für responsive Webentwicklung
- **React** – JavaScript-Framework für UI-Komponenten
- **Vue.js** – Fortschrittliches JavaScript-Framework für Web-Apps

Plattformen & CMS

- **WordPress** – Weltweit meistgenutztes Content-Management-System
- **Moodle** – Open-Source-Lernplattform für Bildungseinrichtungen
- **Nextcloud** – Selbstgehostete Cloud-Lösung als Alternative zu Google Drive
- **Joomla!** – Flexibles Open-Source-CMS

Open-Source-Server-Software

- **Apache** – Der Klassiker unter den Webservern. (Bedient etwa 23,04 % der meistbesuchten Websites)
- **Nginx** – Leistungsstarker Webserver und Reverse Proxy. (Bedient etwa 22,01 % der meistbesuchten Websites)
- **Bind** – Einer der meistgenutzten DNS-Server weltweit.
- **OpenVPN / WireGuard** – VPN-Lösungen für sichere Verbindungen.

Open Source in europäischen Verwaltungen

- **Deutschland:** Bundescloud basiert auf Open-Source-Technologien (Nextcloud, Matrix, Jitsi).
- **Frankreich:** GendBuntu – eigene Ubuntu-Variante der französischen Gendarmerie.
- **Spanien:** LiMux-Projekt in München inspirierte Initiativen in Spanien (z. B. Guadalinex in Andalusien).
- **Niederlande:** Verpflichtung zur Nutzung von Open Source, wenn möglich (Open Government Act).
- **EU-Kommission:** Nutzung von Open-Source-Software (z. B. LibreOffice) und Open-Source-Strategie zur digitalen Souveränität.

→ Open Source stärkt digitale Souveränität und reduziert Abhängigkeiten von US-Konzernen.

Open Source in österreichischen Verwaltungen

- **Österreichische Justiz:**
  - Einsatz von Linux-Servern und Open-Source-Technologien zur Verwaltung von Justizdaten.
- **Stadt Wien:**
  - Nutzung von Open-Source-Software in verschiedenen IT-Bereichen der Verwaltung, z. B. LibreOffice statt Microsoft Office.
  - Förderung von Open Data-Initiativen über data.gv.at.
- **Österreichische Bundesverwaltung:**
  - Verwendung von Nextcloud für interne Dokumentenverwaltung (z. B. im Parlament).
  - Unterstützung von Open-Source-Projekten durch Förderprogramme.
- **Forschungsprojekte:**
  - TU Wien, FHs und andere Institutionen setzen verstärkt auf Open-Source-Software in der Forschung und Lehre.

Hands-on: Welche Open-Source-Programme nutzt ihr?

Nehmt euch **10 Minuten** Zeit und überlegt:

- Welche Programme nutzt ihr täglich?
- Welche davon sind Open Source?
- Gibt es Alternativen, die Open Source sind?

Diskutiert anschließend eure Ergebnisse!

Open Source als Treiber für KI

Open Source hat viele Bereiche revolutioniert – von Betriebssystemen bis hin zu wissenschaftlicher Software. Doch eine der größten aktuellen Entwicklungen ist Open-Source-KI. Wie verändert sie die Forschung, Unternehmen und unsere digitale Welt?

Open Source in der Künstlichen Intelligenz

- **Transparenz und Reproduzierbarkeit** – Wissenschaftliche Forschung profitiert von offenen Modellen und Algorithmen.
- **Community-getriebene Innovation** – Open-Source-Projekte ermöglichen schnelle Weiterentwicklung durch eine globale Entwicklergemeinschaft.
- **Zugänglichkeit** – Open-Source-KI-Modelle ermöglichen es kleinen Unternehmen, Universitäten und Einzelpersonen, KI-Technologien zu nutzen.
- **Beispiele für Open-Source-KI:**
  - LLaMA (Meta) – Sprachmodell-Alternative zu GPT
  - Mistral – Leichtgewichtige und effiziente KI-Modelle
  - Stable Diffusion – Generative KI für Bilder
  - BLIP – Bild-Text-Verständnis
  - GPT-2, DistilBERT – Textverarbeitung
  - Real-ESRGAN – KI-gestützte Bildverbesserung
  - EasyOCR – Optische Zeichenerkennung

Warum veröffentlichen Unternehmen Open-Source-KI?

Open-Source-KI fördert Innovation, aber Unternehmen verfolgen oft auch eigene strategische Ziele.

- **Marktdominanz & Einfluss** – Firmen wie Meta wollen Standards setzen und sicherstellen, dass ihre Technologie von Entwicklern weltweit genutzt wird.
- **Daten & Feedback sammeln** – Durch Open-Source-Modelle können Unternehmen beobachten, wie ihre KI in der Praxis eingesetzt wird und so indirekt ihre eigenen Modelle verbessern.
- **Kosten sparen** – Externe Entwickler tragen zur Weiterentwicklung bei, ohne dass das Unternehmen alles selbst finanzieren muss.
- **Regulatorischer Druck** – Open-Source kann als Strategie genutzt werden, um sich als transparent zu präsentieren und Kritik an KI-Monopolen zu entschärfen.
- **Konkurrenz zu geschlossenen Systemen** – Meta mit LLaMA gegen OpenAI mit GPT, Mistral gegen Claude usw. $\rightarrow$ Wettbewerb um Entwickler und Marktanteile.
- **Lock-In-Effekte erzeugen** – Unternehmen wollen, dass ihre Infrastruktur genutzt wird (z. B. Meta: LLaMA + PyTorch $\rightarrow$ stärkere Bindung an Meta-Ökosystem).

Hands-on: Erkunde das Open-Source-KI-Projekt!

Aufgabe:

- Öffne das Webinterface des KI-Projekts.
- Teste die verschiedenen Modelle und Funktionen.
- Überlege: Was macht welche KI? Wo könnte man sie einsetzen?

Dauer: 10 Minuten

In meinem ursprünglichen Konzept hättet ihr das alles selber programmieren müssen, aber das ging nicht durch... also klickt einfach ein bisschen herum :P

Open Source und Datenschutz – Ein natürliches Duo?

- Open Source bedeutet Transparenz: Jeder kann den Code überprüfen.
- Proprietäre Software kann versteckte Datensammlungen enthalten.
- Kontrolle über Software und Infrastruktur ist essenziell für Datenschutz.
- Open-Source-Tools bieten Alternativen zu datenhungrigen Big-Tech-Diensten.
- Datenschutz ist Freiheit – und die sollte man nicht kampflos aufgeben.

Open Source schafft Transparenz: Wer den Code einsehen kann, kann überprüfen, ob Daten sicher verarbeitet werden. Doch: Bedeutet Open Source automatisch besseren Datenschutz? Wer prüft den Code tatsächlich?
→ Datenschutz erfordert mehr als nur quelloffene Software – es geht um Verschlüsselung, Infrastruktur und digitale Selbstbestimmung.

Warum ist Datenschutz wichtig?

- **Daten sind Macht:** Wer Informationen kontrolliert, kontrolliert Menschen.
- **"Ich habe nichts zu verbergen" ist ein Trugschluss:** Datenschutz schützt nicht nur dich, sondern auch andere.
- **Überwachung verändert Verhalten:** Menschen passen ihr Verhalten an, wenn sie beobachtet werden.
- **Personalisierte Manipulation:** Werbung, Meinungsbildung und Wahlbeeinflussung durch gezielte Datenanalyse.
- **Datenunternehmen und Profilerstellung:** Unternehmen und Staaten speichern riesige Datenmengen – oft ohne unser Wissen.

Cambridge Analytica und Trumps Wahl – Ein Datenschutzskandal

Was ist passiert?

- 2014: Cambridge Analytica sammelt Millionen Facebook-Profile ohne Zustimmung.
- Psychometrische Analysen zur gezielten Wahlwerbung für Trump 2016.
- Microtargeting: Individuelle Botschaften basierend auf Persönlichkeitstests.

Warum war das problematisch?

- Daten wurden ohne Wissen der Nutzer missbraucht.
- Wähler wurden manipuliert, ohne es zu bemerken.
- Datenschutzrechtliche Verstöße und Facebooks Rolle.

Folgen:

- Facebook wurde zu hohen Strafen verurteilt.
- Stärkere Datenschutzregulierungen wie die DSGVO wurden relevanter.
- Bewusstsein für digitale Manipulation und Datenschutz wuchs.

DSGVO – Datenschutz in der EU

- Seit 25. Mai 2018 in Kraft – schützt personenbezogene Daten.
- Ziel: Mehr Kontrolle für Bürger über ihre Daten.

Wichtige Prinzipien:

- **Recht auf Auskunft** – Nutzer können erfahren, welche Daten gespeichert sind.
- **Recht auf Löschung** – Personen können verlangen, dass ihre Daten gelöscht werden ("Recht auf Vergessenwerden").
- **Datenminimierung** – Unternehmen dürfen nur notwendige Daten erheben.
- **Einwilligung** – Datenverarbeitung erfordert eine aktive Zustimmung.
- **Recht auf Datenübertragbarkeit** – Nutzer können ihre Daten in einem gängigen Format anfordern.

Strafen: Verstöße gegen die DSGVO können mit hohen Bußgeldern geahndet werden (bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes).

Datenhandel – Unsere Informationen als Ware

- Daten sind ein Milliardengeschäft: Unternehmen handeln mit Nutzerdaten für gezielte Werbung, Profilbildung und Marktanalysen.
- Große Konzerne (z. B. Google, Meta, Amazon) verdienen durch personalisierte Werbung.
- Datenbroker sammeln und verkaufen Informationen aus verschiedensten Quellen (Webtracking, Kundenkarten, Social Media).
- Konsequenzen: Preisdiskriminierung, Manipulation (z. B. politische Werbung), Datenschutzverletzungen.
- DSGVO schafft strengere Regeln, aber viele Unternehmen umgehen sie oder operieren in Ländern mit schwächeren Gesetzen.

Frage: Haben wir noch Kontrolle über unsere eigenen Daten, oder sind sie längst eine Handelsware?

Tracking und Personalisierte Werbung

- Webseiten und Apps nutzen Tracker, um Nutzerverhalten zu analysieren (Cookies, Fingerprinting, Pixel).
- Werbenetzwerke (z. B. Google Ads, Meta Ads) erstellen detaillierte Profile für gezielte Werbung.
- Dynamische Preisgestaltung: Nutzer sehen je nach Profil unterschiedliche Preise.
- Psychologische Beeinflussung: Werbung wird so platziert, dass sie maximal effektiv ist.
- Datenschutzprobleme: Nutzer wissen oft nicht, welche Daten gesammelt werden und wie sie verwendet werden.

Frage: Wo liegt die Grenze zwischen Personalisierung und Manipulation?

Dark Patterns – Manipulation durch Design

- **Zwangsregistrierung** – Nutzung einer Website nur mit Account möglich.
- **Versteckte Einwilligungen** – Opt-in riesig, Opt-out winzig.
- **Fake Countdown-Timer** – "Nur noch 5 Minuten!" (bleibt aber immer gleich).
- **Mikro-Transparenz** – Wichtige Optionen tief in den Einstellungen versteckt.
- **Dunkle UX-Farben** – "Ablehnen"-Button unscheinbar grau, "Akzeptieren" leuchtet.
- **Schwerer Ausstieg** – Kündigen kompliziert, Anmelden super einfach.
- **Nudging** – "Du bist der Einzige, der noch keine Freunde eingeladen hat!"

Datenabsaugung durch soziale Netzwerke

- **Totalüberwachung**: WhatsApp, Facebook & Co. sammeln massenhaft Nutzerdaten.
- **Erfasste Daten**:
  - Nachrichten, Kontakte, Standortverläufe
  - Geräte-IDs, App-Nutzung, Online-Aktivitäten
- **Tracking-Methoden**:
  - **Bluetooth-Tracking**: Begegnungen mit anderen Nutzern erfassbar
  - **Geofencing**: Erkennung von Aufenthaltsorten für gezielte Werbung
  - **MAC-Adress-Tracking**: Bewegungsprofile über WLAN-Netze
- **Datenhandel**: Verknüpfung mit anderen Quellen & Verkauf an Werbefirmen.
- **Folgen**: Verhaltensüberwachung, gezielte Manipulation, mögliche Weitergabe an Behörden.

TikTok: Datenschutz & Tracking

- Umfangreiche Datensammlung: Standort, Kontakte, Tastatureingaben, Metadaten.
- Nutzerverhalten wird analysiert, um detaillierte Profile zu erstellen.
- Fingerprinting-Techniken ermöglichen eindeutige Identifikation der Nutzer.
- Zugriff auf die Zwischenablage – mehrfach nachgewiesen.

TikTok: Algorithmus & Einflussnahme

- Hochgradig personalisierte Inhalte – Nutzer werden gezielt gelenkt.
- Manipulationspotenzial: Unterdrückung oder Verstärkung bestimmter Inhalte.
- Förderung von viralen Trends, unabhängig von Wahrheitsgehalt.
- Verstärkung von extremen Meinungen und Radikalisierung möglich.

TikTok: Herkunft & Bedenken

- Gehört zum chinesischen Konzern ByteDance.
- Chinesische Regierung könnte Zugriff auf Nutzerdaten verlangen.
- Sicherheitsbedenken führten zu Verboten/Diskussionen in mehreren Ländern.
- Datenschutzregelungen in der EU stehen im Konflikt mit TikToks Praktiken.

TikTok: Jugendschutz & Suchtfaktor

- Endlos-Scroll-Mechanik sorgt für extrem hohe Verweildauer.
- Suchtpotenzial durch Dopamin-gesteuertes Belohnungssystem.
- Gefährliche Challenges verbreiten sich oft unkontrolliert.
- Minderjährige sind besonders von Datenschutzrisiken betroffen.

Influencer: Manipulation als Geschäftsmodell

- **Gehirnwäsche durch Algorithmen**: Plattformen pushen extreme Inhalte, weil sie mehr Klicks bringen.
- **Schleichwerbung & Fake-Authentizität**: "Empfohlene" Produkte sind oft nur bezahlte Deals.
- **Perfekte Lügenwelt**: Gefilterte Realität erzeugt Druck und unrealistische Erwartungen.
- **Kaufzwang durch FOMO**: "Nur heute! Nur hier! Nur für dich!" – alles Marketingtricks.
- **Macht & Einfluss**: Einige Influencer verbreiten Desinformationen und Verschwörungstheorien.
- **Alles für die Kohle**: Viele Influencer verkaufen euch alles, solange die Bezahlung stimmt.

Wie können wir uns jetzt schützen?

- **Fact-Checker**: Nutze Plattformen wie *Mimikama* oder *correctiv.org*, um Informationen zu prüfen.
- **Open-Source-Alternativen**: Verwende sicherere Optionen wie *Mastodon* oder *PeerTube*.
- **Passwort-Management**: Setze Passwort-Manager ein, um deine Konten zu schützen.
- **Datenschutz**: Überprüfe regelmäßig deine Privatsphäre-Einstellungen in sozialen Netzwerken.
- **Bewusster Umgang mit Medien**: Hinterfrage Inhalte und sei dir bewusst, wie Algorithmen dein Verhalten beeinflussen können.
- **Daten sind dauerhaft**: Alles, was einmal im Internet ist, bleibt dort oft für immer – sei dir der Folgen bewusst.

Anonyme Anmeldung: Fake E-Mail & Identitätsgeneratoren

- **Fake E-Mail Generatoren**: Tools, die temporäre E-Mail-Adressen erstellen, um sich ohne Angabe persönlicher Daten auf Websites anzumelden.
- **Temporäre Identitäten**: Webseiten, die es ermöglichen, pseudonyme Identitäten zu erstellen, um online anonym zu bleiben und die wahre Identität zu verschleiern.
- **Vorteil**: Diese Dienste bieten Schutz vor Spam, unerwünschter Werbung und Tracking.
- **Beispiele**: `10minutemail.com`, `guerrillamail.com`, `mailinator.com` (für Fake E-Mail) und `fakenamegenerator.com` (für Pseudonyme).

Wie erkenne ich Fake News?

- **Quelle prüfen**: Kommt die Information von einer vertrauenswürdigen Quelle?
- **Fehlende Quellenangabe**: Gibt es keine verlinkten, überprüfbaren Quellen oder Studien?
- **Emotionaler Inhalt**: Wird versucht, eine starke emotionale Reaktion (Angst, Wut) zu erzeugen?
- **Falsche oder manipulierte Bilder**: Achte auf Bildbearbeitung oder alte Bilder, die neu präsentiert werden.
- **Sensationsgier**: Ist die Nachricht zu dramatisch oder extrem, um wahr zu sein?
- **Bestätigungsfehler**: Bestätigt die Nachricht nur deine eigenen Überzeugungen ohne echte Beweise?
- **Faktencheck-Websites**: Nutze Seiten wie `mimikama.at` oder `correctiv.org` zur Überprüfung.

Mimikama: Faktencheck leicht gemacht

- **Unabhängige Plattform**: Mimikama ist ein gemeinnütziger Verein, der sich der Aufklärung über Falschmeldungen widmet.
- **Faktenbasierte Recherche**: Alle Artikel basieren auf gründlicher Recherche und überprüfbaren Quellen.
- **Expertennetzwerk**: Das Team besteht aus Fachleuten aus verschiedenen Bereichen, die fundierte Analysen liefern.
- **Transparenz**: Mimikama gibt klare Quellen an und erklärt ihre Rechercheprozesse transparent.
- **Nicht kommerziell**: Keine kommerziellen Interessen – es geht ausschließlich um Aufklärung und den Schutz vor Fake News.

Fediverse: Alternativen zu zentralisierten Plattformen

- **Mastodon**: Alternative zu *Twitter* – Mikroblogging mit Fokus auf Datenschutz und Dezentralisierung.
- **Friendica**: Alternative zu *Facebook* – Soziales Netzwerk mit Schwerpunkt auf Privatsphäre und Dezentralisierung.
- **Pixelfed**: Alternative zu *Instagram* – Dezentrales Foto-Sharing ohne Werbung.
- **Lemmy**: Alternative zu *Reddit* – Dezentrale Plattform für Foren und Diskussionen.
- **Loops**: Alternative zu *YouTube Shorts* – Dezentrale Plattform für kurze, kreative Videos.
- PeerTube: Alternative zu *YouTube* – Dezentrales Video-Hosting ohne Werbung und Zensur.
- Funkwhale: Alternative zu *Spotify* – Musikstreaming-Plattform im Fediverse.
- Mobilizon: Alternative zu *Eventbrite* – Dezentrale Event-Planung ohne kommerzielle Interessen.

Vorteile des Fediverse

- **Keine Werbung**: Keine kommerziellen Interessen, keine Anzeigen, die den Inhalt beeinflussen.
- **Kein Tracking**: Nutzer haben die Kontrolle über ihre Daten, keine umfassende Datensammlung durch Dritte.
- **Keine Algorithmen**: Keine Algorithmen, die den Feed kuratieren oder versteckte Inhalte priorisieren – alles ist transparent.
- **Dezentralität**: Jeder kann seinen eigenen Server betreiben und die Plattform nach seinen Wünschen gestalten.
- **Privatsphäre**: Fokus auf Datenschutz und Kontrolle über persönliche Informationen.
- **Weniger Zensur**: Geringere Kontrolle durch zentrale Instanzen, aber dennoch Community-Regeln für verantwortungsbewusstes Verhalten.
- **Plattformübergreifendes Interagieren**: Dank des offenen Protokolls (ActivityPub) können Nutzer auf verschiedenen Plattformen liken, teilen und kommunizieren

Sichere Kommunikation

- **Signal**: Verschlüsselte Nachrichten-App mit End-to-End-Verschlüsselung, Open Source und kostenlos.
- **Matrix**: Dezentrales Kommunikationsprotokoll für Chat, Sprach- und Videoanrufe mit Ende-zu-Ende-Verschlüsselung. Plattformen wie *Element* nutzen Matrix.
- **Threema**: Sicherer Messenger mit End-to-End-Verschlüsselung, kostenpflichtig, aber ohne die Notwendigkeit einer Telefonnummer.

Signal: Die sichere Kommunikations-App

- **Ende-zu-Ende-Verschlüsselung**: Alle Nachrichten sind sicher verschlüsselt und können nur vom Empfänger gelesen werden.
- **Open Source**: Der Quellcode ist öffentlich einsehbar und wird regelmäßig von der Community überprüft.
- **Keine Werbung**: Signal wird nicht durch Werbung oder Datenverkauf finanziert, was die Privatsphäre schützt.
- **Keine Sammlung von Metadaten**: Signal speichert keine Daten über den Nutzer, wie z.B. Kontakte oder Nachrichteninhalte.
- **Kostenlos**: Signal ist eine kostenlose App, die keine versteckten Kosten oder Premium-Versionen bietet.
- **Multiplattform**: Verfügbar auf iOS, Android und Desktop, ermöglicht sichere Kommunikation auf allen Geräten.
- **Gruppen- und Sprach-/Videoanrufe**: Erlaubt sichere Gruppen-Chats sowie Sprach- und Videoanrufe mit End-to-End-Verschlüsselung.

Wie schütze ich mich beim Surfen?

- **Warum ist Chrome schlecht?**
  - Google sammelt viele Daten über dein Surfverhalten, was deine Privatsphäre gefährdet.
  - Chrome verwendet einen zentralisierten Ansatz, der deine Daten mit Google-Servern verbindet.
  - Zukünftige Änderungen (Manifest V3) könnten Adblocker wie uBlock Origin weniger effektiv machen.
- **Warum lieber Firefox?**
  - Firefox ist Open Source und hat Datenschutz als Kernprinzip.
  - Der Browser bietet erweiterte Datenschutzfunktionen wie Tracking-Schutz und ist nicht von Werbung abhängig.
- **uBlock Origin:**
  - Erweiterung, die Werbung und Tracker blockiert und so deine Privatsphäre schützt.
  - Reduziert die Ladezeiten von Webseiten und verbessert die Sicherheit beim Surfen.

Alternativen zu Google & Bing

- **Ecosia, DuckDuckGo, Startpage:**
  - Alle drei bieten Suchergebnisse ohne das Sammeln persönlicher Daten.
  - **Achtung:** Sie nutzen entweder Bing (Ecosia, DuckDuckGo) oder Google (Startpage) für die Suchergebnisse, sodass trotzdem einige Daten an Microsoft bzw. Google weitergegeben werden.
  - **Vorteil:** Sie schützen vor Tracking und minimieren die Datensammlung im Vergleich zu Google oder Bing.
- **Qwant:**
  - Europäische Suchmaschine, die keine persönlichen Daten speichert und keine Tracker verwendet.
  - Besonders empfehlenswert für Datenschutz und Privatsphäre.

ProtonMail: Sichere E-Mail

- **Ende-zu-Ende-Verschlüsselung:**
  - Alle E-Mails sind standardmäßig verschlüsselt, sodass nur der Empfänger die Nachricht lesen kann.
- **Schweizer Datenschutzgesetze:**
  - ProtonMail unterliegt den strengen Datenschutzbestimmungen der Schweiz, die die Privatsphäre der Nutzer besser schützen als viele andere Länder.
- **Keine Werbung, keine Tracking:**
  - ProtonMail sammelt keine persönlichen Daten und zeigt keine Werbung.
- **Open Source:**
  - Der Code von ProtonMail ist Open Source, was zusätzliche Transparenz bietet und von der Community überprüft werden kann.
- **Kostenlos & Premium-Optionen:**
  - ProtonMail bietet ein kostenloses Konto mit grundlegenden Funktionen sowie kostenpflichtige Pläne mit erweiterten Features.

Sicheres Passwortmanagement

- **Länge**: Mindestens 16 Zeichen, besser 20+.
- **Komplexität**: Mischung aus Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen.
- **Einzigartigkeit**: Jedes Konto sollte ein eigenes Passwort haben.
- **Kein Wörterbuch-Passwort**: "Passwort123" oder "qwertz" sind unsicher.
- **Passwortmanager nutzen**: Keepass (offline, Open Source) oder Firefox Lockwise.
- **2FA aktivieren**: Wo möglich, Zwei-Faktor-Authentifizierung (z. B. TOTP) nutzen.

Passwortsicherheit überprüfen

- **CheckDeinPasswort.de**: Hier kannst du dein Passwort auf Sicherheitslücken prüfen. Der Service zeigt dir, wie stark dein Passwort ist und gibt dir Tipps, wie du es sicherer machen kannst, indem du z.B. stärkere Kombinationen verwendest. Besuche die Seite unter: checkdeinpasswort.de
- **Have I Been Pwned?**: Mit diesem Tool kannst du überprüfen, ob deine E-Mail-Adresse oder dein Passwort in einer bekannten Datenpanne veröffentlicht wurde. So erfährst du, ob deine Anmeldedaten in einem Leck auftauchen und kannst entsprechende Maßnahmen ergreifen. Besuche die Seite unter: haveibeenpwned.com

Sicheres Smartphone: Apps für den Datenschutz

- **F-Droid:** Open-Source App-Store für Android, bietet datenschutzfreundliche Alternativen.
- **NewPipe:** Open-Source YouTube-Client ohne Werbung und Tracking.
- **K-9 Mail:** Sichere und datenschutzfreundliche E-Mail-App für Android.
- **LineageOS:** Android-Betriebssystem, datenschutzfreundlich und ohne Google-Dienste.
- **GrapheneOS:** Android-basierte, datenschutzorientierte ROM mit verstärkter Sicherheit und Privatsphäre.

Warum Apple keine echte Alternative ist

- **Geschlossenes Ökosystem**: Apple erlaubt nur Apps aus dem eigenen App Store.
- **Kein echtes Open Source**: iOS ist proprietär, und der Code kann nicht überprüft werden.
- **Vendor Lock-in**: Nutzer werden in die Apple-Infrastruktur gezwungen (iCloud, Safari, Apple Mail etc.).
- **Tracking & Werbung**: Trotz Datenschutz-Versprechen sammelt Apple Daten für personalisierte Werbung.
- **Keine unabhängigen App-Stores**: F-Droid, NewPipe und andere datenschutzfreundliche Apps sind nicht erlaubt.

Anonymes Surfen: Tor

- **Was ist Tor?**
  - Tor (The Onion Router) ist ein Open-Source-Netzwerk, das für anonymes Surfen entwickelt wurde.
  - Es verschlüsselt deine Internetverbindung und leitet sie über mehrere zufällige Knotenpunkte weltweit.
  - Ziel: Deine Identität und Aktivität im Internet zu verschleiern, sodass niemand (einschließlich Internetanbieter oder Websites) dich zurückverfolgen kann.
- **Vorteile von Tor:**
  - Schutz vor Zensur und Überwachung.
  - Bietet Anonymität, besonders für Journalisten, Aktivisten und Menschen in autoritären Staaten.
  - Ermöglicht Zugang zu gesperrten Webseiten ("Great Firewall" in China).
- **Wie funktioniert Tor?**
  - Deine Verbindung wird durch mehrere Knoten (Relays) im Tor-Netzwerk weitergeleitet, wobei jeder Knoten nur einen Teil der Verbindung kennt.
  - Diese Verschlüsselung macht es für Dritte nahezu unmöglich, die Verbindung bis zu ihrem Ursprung zurückzuverfolgen.

Clear Web, Deep Web und Dark Web

- **Clear Web:**
  - Das "normale" Web, das von Suchmaschinen indexiert wird.
  - Öffentlich zugängliche Webseiten wie Google, Wikipedia, Nachrichtenportale.
  - Jeder kann diese Inhalte durchsuchen und darauf zugreifen.
- **Deep Web:**
  - Der Teil des Webs, der nicht von Suchmaschinen indexiert wird.
  - Beinhaltet private Datenbanken, E-Mail-Konten und andere nicht öffentlich zugängliche Informationen.
  - Der Zugriff erfolgt in der Regel über Passwörter oder spezielle Berechtigungen.
- **Dark Web:**
  - Ein Teil des Deep Webs, der absichtlich verborgen ist und Anonymität bietet.
  - Meist über das Tor-Netzwerk zugänglich, um die Privatsphäre zu schützen.
  - Wird von Personen genutzt, die Anonymität benötigen, z.B. in Ländern mit Zensur oder für den sicheren Austausch von Informationen.

Das Dark Web und sichere Kommunikation

- **Warum das Dark Web?**
  - Bietet Schutz vor Zensur und Überwachung, besonders für Whistleblower.
  - Anonymität bei der Weitergabe von Informationen, z.B. über das Tor-Netzwerk.
- **Beispiel: SecureDrop**
  - Plattform für den sicheren Austausch von Informationen zwischen Whistleblowern und Journalisten.
  - Über Tor erreichbar, schützt vor Verfolgung.
- **Bedeutung für die Gesellschaft:**
  - Whistleblower decken Missstände auf und spielen eine wichtige Rolle bei der Aufklärung von Korruption und Verbrechen.
  - Sie helfen, gesellschaftliche Missstände zu beseitigen und Verantwortliche zur Rechenschaft zu ziehen.
  - Ohne Whistleblower könnten viele Skandale, wie die Massenüberwachung durch die NSA oder Kriegsverbrechen, unentdeckt bleiben.

Whistleblower: Schutz und Anonymität

- **Whistleblower:**
  - Personen, die geheime oder illegale Aktivitäten aufdecken.
  - Sie benötigen sichere Kanäle, um ohne Gefahr von Vergeltungsmaßnahmen Informationen weiterzugeben.
- **Beispiel: Bradley (Chelsea) Manning**
  - Manning leakte geheime US-Militärdokumente, die Kriegsverbrechen dokumentierten.
  - Brauchte sichere und anonyme Kanäle, um seine Identität zu schützen.
- **Beispiel: Edward Snowden**
  - Snowden enthüllte die Massenüberwachung durch die NSA.
  - Nutze anonyme Plattformen, um sicher zu kommunizieren.