

# Alterantive Apps und Tools

Willst du im grossen Ozean der Main Stream Apps untergehen oder lieber auf der einsamen Insel verhungern? Diese Frage stellt sich (leider) immer häufiger in der heutigen IT-Welt - und es gibt kein Richtig oder Falsch. Dennoch versuchen wir in diesem Dokument, einige Tipps und Tricks weiterzugeben, um im IT-Dschungel einigermaßen gesund überleben zu können.

Dieses Dokument ist weder abschliessend noch vollständig, was die Apps und Tools betrifft. Viel mehr ist dies der aktuelle Stand, was zur Zeit an Sicherheit und persönlichem Datenschutz genutzt oder verwendet werden kann. Da sich die IT-Welt rasend schnell weiterentwickelt, werden laufend neue Apps dazukommen oder aufgeführte «sichere» Apps doch nicht mehr so sicher sein - der eingeschlagene Weg sollte dennoch zum eigenen Schutz weiterverfolgt werden!

Das Dokument soll - ganz im Zeichen von Open Source - von deinem Feedback und deinen Beiträgen leben und weiterentwickelt werden. Zu diesem Zweck ist es offen und (im privaten Rahmen) von dir editier- und erweiterbar. Wende dich an [Christoph G.](#), damit du den Link und die notwendige Berechtigung zur Mitarbeit erhältst.

## Versionsverlauf

Version	Datum	Author(en)	Beschreibung
V1	25.01.2025	<a href="#">Christoph G.</a>	Initiale Version des Dokuments

## Browser

Der Browser wird von verschiedenen Betriebssystemen per Default zur Verfügung gestellt. Dennoch - oder gerade deshalb - macht es Sinn, sich über die Sicherheit und den persönlichen Datenschutz Gedanken zu machen, da der Browser wohl zu den meist genutzten Apps gehört.

Apps	Beschreibung
Microsoft Edge	Standard Browser unter Windows, Nachfolger des Internet Explorers
Safari (Apple)	Standard Browser für Apple Produkte (iPhone, iPad, MacBook, Desktop)
Google Chrome	Weit verbreiteter Browser von Google, markführender Browser für Windows, macOS, Linux, Andriod, iOS

## Alternativen

Apps	Beschreibung
Brave	Open Source Browser ohne Tracking und Werbung für Windows, macOS, Linux, Android und iOS
Chromium	Basiert auf den Open Source-Bestandteilen von Google Chrome für Windows, Linux, macOS, iOS und Andriod
Mozilla Firefox	Open Source Browser für Linux, Windows, macOS, Android, iOS, FreeBSD
Opera	Proprietärer Browser auf Basis von Chromium für Linux, Windows, macOS, Android, iOS, FreeBSD
Startpage	Mobile App unterstützt die gleichnamige Search Engine, um den privaten Datenschutz zu gewährleisten.

Apps	Beschreibung
DuckDuckGo	Mobile App der gleichnamigen Search Engine mit Fokus auf Privatsphäre, blockiert Tracker, nutzt verschlüsselte Verbindungen, privater Datenschutz

## Quellen

- [https://de.wikipedia.org/wiki/Liste\\_von\\_Webbrowsern](https://de.wikipedia.org/wiki/Liste_von_Webbrowsern)
- <https://www.swisscom.ch/de/privatkunden/blog/internet/mit-welchem-browser-surft-es-sich-am-besten>

## Search Engine

Ebenso wichtig wie die Browser App ist die verwendete Suchmaschine (Search Engine). Hier spielen nicht nur die Suchresultate eine Rolle, sondern vor allem die Sicherheit sowie die Privatsphäre.

Search Engines	Beschreibung
Bing	Suchmaschine von Microsoft
Google	grösste Suchmaschine von Google, technisch hervorragend, Datenschutz lässt zu wünschen übrig, z.B. Sammeln von Nutzerdaten für personalisierte Werbung
Yahoo	Suchergebnisse von Bing (Proxy Search Engine)

## Alternativen

Search Engines	Beschreibung
Startpage	Suchmaschine ohne Tracking und Werbung, «sicherste Suchmaschine der Welt» (Eigenwerbung), anonymisierte Suchergebnisse von Google (Proxy Search Engine)
Brave Search	Suchmaschine ohne Tracking und Werbung, Standard-Suchmaschine des gleichnamigen Browsers Brave
Ecosia	Generiert Spendengelder für Baumpflanzungen, Server werden klimaneutral betrieben, Ergebnisse von Bing und Google (Proxy Search Engine)
DuckDuckGo	Wenig Werbung, Kombination aus Meta Search Engine und eigenem Web Crawler

## Quellen

- [https://de.wikipedia.org/wiki/Liste\\_von\\_Websuchmaschinen](https://de.wikipedia.org/wiki/Liste_von_Websuchmaschinen)
- <https://mind-force.de/knowhow/suchmaschinen-vergleich/#startpage>

## Mail

Auch wenn sich die sichere Übertragung von Mails etabliert hat, ist der Inhalt längst nicht so sicher aufbewahrt wie im Allgemeinen angenommen. Erst End-to-End-Verschlüsselung machen den Austausch von Mails wirklich sicher.

Apps	Beschreibung
Gmail	Kostenloser E-Mail-Dienst von Google, mögliche Verstösse gegen europäische Datenschutzbestimmungen
Outlook	Teil des Microsoft-365-Pakets, weder werbefrei noch DSGVO konform
Bluewin / Bluemail	Kostenloser E-Mail-Dienst von Swisscom inkl. Kalender und Adressbuch (light), kostenpflichtige Version im Abo

## Alternativen

Apps	Beschreibung
Proton	Open Source basierter E-Mail-Dienst aus der Schweiz, End-to-End-Verschlüsselung, Zero-Access-Architektur (nur Nutzer:innen haben Zugriff auf den privaten Schlüssel), keine Aktivitätsprotokolle, Nutzer:innen bleiben anonym, kostenlos bis 500 MB Speicherplatz, kostenpflichtige Versionen bieten weitere Dienste wie Proton Drive, VPN, Password Manager etc. an
StartMail	Sicherer E-Mail-Dienst von denselben Entwicklern wie die private Suchmaschine Startpage, PGP-Verschlüsselung, kostenpflichtig

## Quellen

- <https://de.wikipedia.org/wiki/Kategorie:Webmail-Anbieter>
- <https://www.metanet.ch/de/email/grundlagen/email-anbieter>
- <https://kinsta.com/de/blog/sicheren-email-anbieter/>

## Instant Messenger

Apps	Beschreibung
WhatsApp	mit über zwei Milliarden Nutzer:innen am weitesten verbreitet, sammelt Daten rund um deine Aktivitäten inkl. komplettes Adressbuch
Telegram	zweitgrösste Messenger weltweit mit rund einer Milliarde Nutzer:innen ist ein Open-Source-App, was bei Telegram mit den gesammelten Daten passiert, ist nicht bekannt

## Alternativen

Apps	Beschreibung
Threema	erste Schweizer Open Source Messenger App, auch ohne Mobile Nummer verwendbar, einmalige Kosten beim Herunterladen der App, Privacy by Design, End-to-End-Verschlüsselung
Signal	Open Source App entstand 2018 als Alternative zu WhatsApp, ohne Metadaten zu sammeln, vergleichsweise sicher mit End-to-End-Verschlüsselung

## Quellen

- <https://threema.com/de/products/private/messenger-comparison>
- <https://community.swisscom.ch/de/d/719962-5-beliebte-messenger-apps-im-vergleich>

## Chat Bot

Goolest du noch oder unterhältst du dich schon mit einem Chat Bot? Nebst den Chat Bots der grossen Player gibt es durchaus geeignete Alternativen, welche deine Privatsphäre respektieren.

Apps	Beschreibung
ChatGPT (OpenAI)	Grösstes Ökosystem von Zusatz-Apps, wenig Wissen zu Schweizer Themen, keine Quellenangaben und keine Hinweise auf Richtigkeit der Antwort
Gemini (Google)	Guter Bildgenerator, viel Wissen zu Schweizer Themen, gute Integration mit Google-Produkten
Copilot (Microsoft)	Entwickelt von Microsoft mit dem Ziel, die Entwicklungsarbeit (von Software) zu unterstützen, gute Integration mit Microsoft-Produkten

## Alternativen

Apps	Beschreibung
Claude (Anthropic)	Gute Resultate, viel Wissen zu Schweizer Themen, verschiedene Sprachmodelle und Varianten, wird kritisiert, sich nicht an die Regeln im Internet zu halten (z.B. Crawler Policies)
Lumo (Proton)	Hervorragender Datenschutz, verschlüsselte Kommunikation, keine Daten für KI-Training, kann nur Text, quelloffene Software
Public AI (Apertus)	Schweizer Chat Bot, entwickelt an der ETH Zürich und am EPF Lausanne, vollständig als Open Source verfügbar inkl. Trainingsprozess und Trainingsdaten

## Quellen

- [https://de.wikipedia.org/wiki/Liste\\_von\\_Chatbots](https://de.wikipedia.org/wiki/Liste_von_Chatbots)
- <https://www.srf.ch/sendungen/kassensturz-espresso/tests/gadgets-elektronik/ki-sprachmodelle-im-vergleich-chatbot-duell-chatgpt-landet-nur-im-mittelfeld>

## Virenschutz

Virenschutz ist auf Windows- und macOS-Rechner ein MUSS: Windows- und macOS-Rechner werden aufgrund ihrer weiten Verbreitung am häufigsten angegriffen. Für Linux sind bislang kaum Schadprogramme bekannt, die «kommerziell» genutzt werden. Bereits gibt es auch verschiedene Apps für mobile Geräte, was in Zukunft zunehmen und notwendig sein wird.

Eine beliebte Betrugsmasche ist zudem, falsche Antiviren-Software zu verbreiten. Im besten Fall sind diese Apps harmlos und verunsichern dich mit immer wieder auftauchenden Falschmeldungen, dass dein Rechner mit Schad-Software infiziert ist. Harmlos und teurer sind diese Apps, wenn sie dich aufgrund von Falschmeldungen zur Bezahlung einer «Lizenz» auffordern. Fatal sind diese Apps, wenn sie deine Privatsphäre ausspionieren und / oder deine Festplatte verschlüsseln und du deine Daten mit viel Geld wieder «freikaufen» musst. Anstelle der Zahlung eines «Lösegelds» solltest du dir die Meldung beim [BACS](#) überlegen.

Empfehlenswert sind seriöse Anbieter von Virenschutz-Software, die zwischen gratis und einer mässigen Jahresgebühr im Internet angepriesen werden, z.B.

Apps	Beschreibung
Bitdefender	hervorragender Schutz, einfache Bedienung

Apps	Beschreibung
Norton 360	vielseitiger Antiviren-Schutz ohne allzu viel Ballast
Avira Internet Security	umfassendes und benutzerfreundliches Antivirus-Programm
McAfee Total Protection	hervorragendes Antiviren-Programm mit Datenschutz-Fokus

Als **nicht-empfehlenswert** gilt das Antiviren-Programm von Kaspersky, welchem unerwünschte Backdoor-Eigenschaften und damit Spionage der Privatsphäre nachgesagt werden. Seit dem 15. März 2022 warnt das deutsche Bundesamt für Sicherheit vor dem Einsatz der Virenschutz-Software des Anbieters Kaspersky. Die Warnung besteht heute immer noch, trotz Intervention von Kaspersky.

## Quellen

- [https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Virenschutz-Firewall/Virenschutzprogramme/virenschutzprogramme\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Virenschutz-Firewall/Virenschutzprogramme/virenschutzprogramme_node.html)
- <https://www.av-test.org/de/antivirus/privat-windows/>
- <https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/FAQ-Kaspersky/faq-kaspersky.html>

## VPN

Virtual Private Network (VPN) erlaubt eine sichere, verschlüsselte Internet-Verbindung, indem der Internetverkehr über einen (externen) Server umgeleitet wird. Dadurch kannst du deine Privatsphäre schützen, indem du deine IP-Adresse verbirgst und verhinderst, dass dein Internetverkehr von Hackern, Regierungen und Internetdiensteanbietern überwacht und misbraucht wird. Alternativ hilft dir eine VPN-Verbindung, um z.B. eine geschützte, sichere Internet-Verbindung zu deinem Arbeitgeber zu nutzen, was vor allem für Homeoffice ein häufig genutztes Verfahren ist.

Zudem ist VPN eine gute Lösung, wenn du im öffentlichen WLAN unterwegs bist, da die öffentlichen WLANs meist ungeschützt sind und damit auch deine Daten ungeschützt sind.

VPN-Lösungen für deinen Rechner gibt es verschiedene; häufig werden diese in einem Paket kombiniert und angeboten, z.B. zusammen mit oben aufgeführten Virenschutz-Programmen (Bitdefender, Norton (Testsieger 2026), Avira, McAfee) oder Gesamtlösungen (Proton).

## Quellen

- <https://surfshark.com/de/blog/antivirus-mit-vpn>
- <https://softwarelab.org/de/antivirus-mit-vpn-test/>

## Password Manager

Damit du den Sicherheitsanforderungen von Passwörtern gerecht wirst (z.B. starke, einmalige Passwörter), kommst du nicht mehr ohne einen Password Manager aus. Es gibt eine Vielzahl von Lösungen, von einfachen Standalone Apps bis zu cloud-basierten Lösungen für mehrere unterschiedlichste Geräte.

Damit du die «richtige» Lösung für dich findest, solltest du folgende Fragen beantworten und danach die dazu passende Lösung suchen:

- Auf wievielen Geräten (Desktop, Laptop, Smartphone, Tablet) möchtest du einen Password Manger verwenden?
- Willst du die Passwörter unter den Geräten synchronisieren? Oder führst du auf jedem Gerät einen eigenständigen Password Store, der nur die notwendigen Passwörter enthält?
- Verwendest du zusätzliche Funktionen wie 2FA-Generator, Kreditkarten-Speicher, Dark-Web-Überwachung?
- Wie wichtig ist dir die Integration in dein bestehendes Ökosystem (Browser-Erweiterungen, Cloud-Dienste)?
- Legst du Wert auf Datenschutz-Standorte (Server in der Schweiz, EU, USA)?

Mögliche, empfehlenswerte Lösungen:

Apps	Beschreibung
Proton Pass	alle gängigen Betriebssysteme und Browser, Zero-Knowledge (End-to-End-Verschlüsselung), 2FA-Optionen, teilweise Open Source, gute Integration in das Proton-Ökosystem (Mail, VPN, Drive), kostenlos oder Abo bei grösseren Datenmengen
Bitwarden	alle gängigen Betriebssysteme und Browser, Zero-Knowledge, 2FA-Optionen, Open Source, self hosting möglich, Password Sharing für Teams, Gratis-Plan und Abos
1Password	alle gängigen Betriebssysteme und Browser, Zero-Knowledge, 2FA-Optionen, Quell-Code proprietär, Travel-Mode, Familien- und Team-Pläne, Sieger bei SRF

## Quellen

- <https://proton.me/de/pass>
- [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/passwortmanager\\_\\_sicherheit\\_datenschutz.pdf?\\_\\_blob=publicationFile&v=3](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/passwortmanager__sicherheit_datenschutz.pdf?__blob=publicationFile&v=3)
- <https://www.srf.ch/sendungen/kassensturz-espresso/tests/gadgets-elektronik/security-test-diese-passwortmanager-schuetzen-vor-hackern>