Digitale Selbstverteidigung

gegen den technologischen Angriff

#1

Digitale Selbstverteidigung

Info zur Förderung des Widerstands gegen den technologischen Angriff

Inhalt

Kontakt: feedforward@riseup.net

Wir schreiben gerne verschlüsselt mit dir, wenn du das auch kannst: PGP

Fingerprint: 33FF 1619 EAEA 991F F39A 77CE E027 308A 2B56 9493

Einleitende Worte zu Kontext und Nutzung

Wir leben in Zeiten schnell voran schreitender technischer Neuerungen und in einer Atmosphäre, die von autoritärer Sicherheitspolitik und dem kommerziellen Willen der BigTech's dominiert wird. In vielen deutschen Bundesländern wurden bereits neue Polizeigesetze auf Landesebene verabschiedet, die in Kombination mit Lockerungen im Datenschutz zu massiven Eingriffen im privaten und öffentlichen Raum sorgen. Erweiterten präventiven Befugnissen für Verfolgungsbehörden folgen nun Gesetze auf Bundesebene, von der alten Leier Vorratsdatenspeicherung bis zu KI-gestützter Videoüberwachung und dem Einsatz von Überwachungssoftware für die Ermittlungsbehörden, ob nun von Palantir oder nicht.

Mit der Ausgangslage, die wie in Berlin mit der Verschärfung des ASOG (Allgemeines Sicherheits- und Ordnungsgesetz) einhergeht, stehen Aktivist:innen vor großen Herausforderungen. Wie ist eine politische Opposition noch möglich in Zeiten von militärischer Mobilmachung, fortschreitender Ausbeutung von Mensch und Natur und einer globalen faschistischen Bedrohungslage?

Klar ist, wir haben etwas dagegen! … und nun auch dafür - in dieser Broschüre für die digitale Selbstverteidigung und Selbstermächtigung:

Digitales Wissen und die Kenntnisse von simplen Techniken des Eigen- und Strukturschutzes sollten mehr und mehr Alltagswissen werden. Angriffe auf unsere Privatsphäre gibt es zu Genüge, ob aus Staat oder von Unternehmen – um diese ins Leere laufen zu lassen und Handlungen bewusst zu machen gibt es hier eine praxisnahe Handreichung, die auf eigenen Erfahrungen, Recherchen und der eigenen Lernkurve basiert. Vorgestellt werden Open-Source-Tools und Konzepte, die besonders für kritische oder aktivistische Zusammenhänge geeignet sind und Wissen vermittelt, das es ermöglicht, ein eigenes digitales Schutz-Setup zu entwickeln.

Wie du unsere Tipps letztlich nutzt bleibt dir als User:in vorbehalten, wir verweisen auch darauf sich an unterstützende Strukturen zu wenden um Hürden zu überwinden und sich bei Installationen oder Fragen an diese zu wenden. In Berlin gibt es hierfür z.B.:

- Cryptosprechstunde
- Resist Berlin
- Penguin Padlock Party
- Skills for Utopia

Wir möchten noch betonen, dass sich die Broschüre auf den Jetzt-Zustand bezieht und sich Bedrohungslage, Angriffspunkte und Sicherherheitsarchitekturen ständig verändern. Digitale Selbstverteidigung ist ein andauernder Prozess.

So freuen wir uns auch über Feedback in Form von Aktualisierungen, Ergänzungen und Korrekturen!

Die wichtigsten Grundprinzipien

Digitale Sicherheit ist nicht nur eine Frage von Technik, sondern vor allem der richtigen Herangehensweise. Bevor du konkrete Tools auswählst, solltest du dir einen Überblick über die eigene Situation verschaffen.

💡 **Stelle dir grundlegende Fragen:**

- Was möchte ich schützen?
- Vor wem möchte ich es schützen?
- Wie wahrscheinlich ist ein Angriff?
- Welche Folgen hätte ein Sicherheitsvorfall?
- Wie viel Aufwand bin ich bereit zu investieren?

→ Die Antworten helfen dir oder auch deiner Gruppe, einen individuellen Sicherheitsplan (Bedrohungsmodellierung) zu entwickeln und an dein Aktionslevel anzupassen.

💡 **Sicherheit ist nur so stark wie ihr schwächster Teil: eine verschlüsselte App nützt z.B. wenig, wenn Daten ungeschützt gespeichert sind.**

Betrachte deine gesamte digitale Nutzung (privat, politisch, Arbeitskontexte) und deine Umwelt (z.B. Leute/Kontexte mit denen du kommunizierst).

💡 **Trenne Identitäten (Kompartmentalisierung):** durch Trennung von verschiedenen Bereichen deines Lebens machst du dich weniger angreifbar. Ist eine Sphäre gehackt, trifft es nicht gleich die anderen. Bspw. Privatleben/Aktivismus auf zwei verschiedenen Geräten.

💡 **Daten die nicht anfallen, können nicht missbraucht werden.** Seien es Kommunikationsdaten, Bilddaten, Funkdaten, Accountdaten...

💡 **Überlege genau, wem du welche Daten anvertraust** (z. B. Cloud-Dienste). Jede Weitergabe erhöht das Risiko. Je weniger Mitwisser, desto sicherer.

💡 **Zu viele komplexe Tools können unübersichtlich werden:** Einfache, gut verstandene Lösungen sind oft effektiver. Und manchmal ist eine nicht-technische Lösung leichter zu kontrollieren.

💡 **Sicherheit entsteht nicht durch Tools, sondern indem du verstehst wo deren Grenzen sind.** Nur wenn du weißt, was ein Tool (Betriebssystem, Messanger, VPN...) kann oder nicht, weißt du auch vor was du geschützt bist und vor was eben nicht.

💡 **Sicherheit muss alltagstauglich sein:** Ein theoretisch perfektes Konzept hilft nicht, wenn es nicht umgesetzt wird. Stell dir die Frage welche Sicherheitsstandards du konsequent anwenden kannst.?

💡 **Bedrohungen verändern sich ständig:** Überprüfe deine Maßnahmen regelmäßig. Passe deine Strategie bei Bedarf an.

💡 **Es gilt immer noch die alte Regel für klandestine Aktionen:** geht lieber zusammen spazieren und lasst alles technische Gerät gleich Zuhause - keine Spuren, keine Aussagen, kein Problem.

Angriffspunkte

Digitale Angriffe im politischen Kontext sind oft gezielt und persönlich. Neben allgemeiner Cyberkriminalität gibt es auch gezielte Einschüchterungs- und Überwachungsversuche. Hier ein Überblick möglicher Angriffspunkte:

Phishing und Spear-Phishing: Während normales Phishing massenhaft versendet wird, richtet sich Spear-Phishing gezielt an Einzelpersonen oder Gruppen. Angreifer geben sich z.B. als bekannte Kontakte oder Organisationen aus und versuchen, Zugang zu E-Mail-Konten oder Social-Media-Accounts zu erhalten, in dem sie z.B. Webseiten und Formulare nahezu perfekt nachbilden. Du merkst also unter Umständen nicht, dass du deine Daten auf einer Fakeseite eingibst und so z.B. Benutzername und Passwort an Angreifende weitergibst.

Malware und Spyware können zur Überwachung eingesetzt werden. Besonders gefährlich sind staatlich eingesetzte Überwachungsprogramme (“Staatstrojaner”) wie Pegasus der NSO Group, die Smartphones heimlich ausspionieren können. Aber auch einfachere Schadsoftware, die über Messenger-Links oder kompromittierte Webseiten verbreitet wird, kann Chats, Kontakte oder Standorte auslesen.

Account-Übernahmen (Account Hijacking): Angreifer versuchen, Social-Media-Konten zu übernehmen, um Desinformation zu verbreiten, interne Kommunikation offenzulegen oder Personen öffentlich zu diskreditieren (Doxxing).

Kennwortangriffe und Datenlecks: Viele Menschen nutzen gleiche oder ähnliche Passwörter für mehrere Dienste. Wird ein Dienst gehackt, können diese Daten für weitere Zugriffe missbraucht werden.

💡 **Daher sind für dich besonders wichtig:**

- starke, einzigartige Passwörter und Passwortmanager
- Zwei-Faktor-Authentifizierung (möglichst mit App oder Hardware-Token)
- Verschlüsselung von Datenspeichern
- regelmäßige Software-Updates
- verschlüsselte Kommunikation
- bewusster Umgang mit persönlichen Informationen und Metadaten

Rückschlüsse auf deine Identität

Einer der einfachsten Wege zur digitalen Identifizierung ist die Verwendung von **Klarnamen** und **Profilbildern** auf sozialen Netzwerken, in Messengern, Foren oder anderen Online-Plattformen. Auch Spitznamen, Namenskürzel und persönliche Fotos, auch Bilder von deinem Haustier, deiner Umgebung oder von Friends, können auf dich zurückgeführt werden und sollten besonders in Gruppen, die politisch und offen sind vermieden werden. Mache dir bewusst, dass offene Gruppen Netzwerke sichtbar machen und Rückschlüsse auf Strukturen zulassen können und überlege dir wie du darin präsent bist und kommunizierst.

💡 Wenn nicht notwendig, auf Klarnamen, Namenskürzel und zuordenbare Profilbilder verzichten und die Privatsphäre-Einstellungen so wählen, dass nur begrenzte Daten sichtbar sind.

Doch Profile können oft auch ohne explizite Namen durch Verknüpfungen zu anderen Daten, wie etwa geografischen Standortinformationen oder Vorlieben, identifiziert werden. Selbst wenn du auf verschiedenen Plattformen unterschiedliche Profile und Benutzernamen verwendest, gibt es oft indirekte Möglichkeiten, diese zu verknüpfen (z.B. gleiche IP-Adresse, gleiche Browser-Konfigurationen, ähnliche Zeitpunkte der Nutzung).

Aber auch ohne ein explizites Profil können Nutzer durch technische Mittel identifiziert und verfolgt werden.

- Die **IP-Adresse** (*Internet Protocol Address*) identifiziert dein Gerät in einem Netzwerk, um per Datenaustausch mit anderen Geräten zu kommunizieren (Postadresse für Computer). Es verrät geographische Informationen wie die Stadt oder den Provider eines Nutzers.
- **MAC-Adressen** (Media Access Control) sind eindeutige Kennungen von Geräten im lokalen Netzwerk (z.B. WLAN zuhause). Sie können primär vom Netzwerkadministrator, dem Router (in der Client-Liste) oder dem

Gerätebesitzer selbst ausgelesen werden. Außerhalb des eigenen Netzwerks (im Internet) ist eine direkte Rückverfolgung auf den Nutzer jedoch nicht möglich, da MAC-Adressen nicht über Router hinweg ins Internet gesendet werden. MAC-Adressen können oft softwareseitig geändert/spoofed werden (mehr dazu im Kapitel MAC-Adressen Spoofing/Randomisierung)

- Der **IMSEI / IMEI** ist eine eindeutige Nummer, die jedem mobilen Gerät zugewiesen wird. Sie identifiziert ein mobiles Gerät und kann zur Wiederherstellung des Geräts oder zur Sperrung verwendet werden. Der **IMSI** ist eine eindeutige Identifikationsnummer, die einem Mobilfunkgerät zugewiesen wird, wenn es sich in einem Mobilfunknetz anmeldet. Er wird in der SIM-Karte gespeichert und von Mobilfunkanbietern verwendet, um den Nutzer und dessen Abonnement zu identifizieren. IMSIs können z.B. mit IMSI-Catchern, Geräte, die wie ein falscher Mobilfunkmast fungieren und neben IMSIs auch den Datenverkehr zwischen Handy und Mobilfunknetz überwachen.
- **Fingerprinting** ist eine Methode, bei der verschiedene Informationen über das Gerät eines Nutzers (wie Bildschirmauflösung, installierte Schriftarten, Betriebssystem und Browser) gesammelt werden, um einen einzigartigen „Fingerabdruck“ zu erstellen, der auch ohne die Verwendung von Cookies eine Identifikation ermöglicht.
- **Tracking** kann durch Cookies, Web Beacons oder durch die vorher genannten Technologien erfolgen. Es erlaubt Unternehmen, Nutzer über verschiedene Websites hinweg zu verfolgen und so Verhaltensmuster zu erkennen.

💡 Verwende **VPNs** (Virtuelle Private Netzwerke), Anonymisierungsdienste wie **Tor** (mehr dazu im Kapitel VPN & TOR) und blockiere Cookies und Tracker (z.B. mit Browser-Erweiterung uBlock Origin).

Viele **Apps** sammeln und teilen ohne dein Wissen Daten über dein Verhalten.

💡 Überprüfe die Berechtigungen deiner Apps und deaktiviere alle, die unnötig Standortdaten oder andere persönliche Informationen sammeln. Nutze nur vertrauenswürdige Apps!

Auch über eingebaute Smartphone-**Sensoren wie Beschleunigungs-, Lage- oder Kompasssensoren** können indirekt Informationen gesammelt werden, etwa über Bewegungsmuster, typische Tagesabläufe oder die grobe Richtung und Art der Bewegung. Solche Daten können im Zuge forensischer Ermittlungen ausgewertet werden, um Nutzer:innen zu erkennen oder zu profilieren, zum Beispiel zur Rekonstruktion von Abläufen, etwa um Bewegungen oder Aufenthaltszeiten nachzuvollziehen.

Metadaten, die mit jeder Datei (z.B. Fotos oder Dokumente) verbunden sind, stellen ein oft unterschätztes Risiko dar. Fotos beispielsweise enthalten oft Geodaten, die den exakten Standort angeben, an dem das Bild aufgenommen wurde und können auch Informationen über das Gerät und das Datum enthalten und damit weitere Details zu deinem Verhalten preisgeben. Es ist wichtig dich der digitalen Spuren, die du bei der Kommunikation mit anderen hinterlässt bewusst zu machen und zu minimieren.

💡 Entferne Metadaten mit Metadaten-Entfernen (wie z.B. Exiftools), bevor du sie veröffentlichst.

Funk- und Standortdaten

Deine Geräte, insbesondere dein Smartphone, sind ständig mit Netzwerken verbunden und können daher Informationen über deinen Standort sammeln. Dein Smartphone kann auf zwei Arten geortet werden: aktiv durch das Gerät selbst – und nachträglich durch die Auswertung von Mobilfunkdaten.

Bei der **aktiven Ortung** bestimmt dein Smartphone seinen Standort selbst. Es nutzt dafür **GPS** sowie Signale aus **WLAN-Netzwerken** und **Mobilfunkmasten**. Besonders in Städten ist die Ortung über WLAN und Mobilfunk oft sehr genau, weil viele bekannte Netzwerke und Funkzellen in der Nähe sind. Viele Apps kombinieren diese Datenquellen, um den Standort möglichst präzise zu berechnen. Auf diese Standortdaten können Apps zugreifen, wenn du ihnen die entsprechende Berechtigung erteilt hast; je nach Dienst werden sie auch an Anbieter im Hintergrund übertragen. In bestimmten Fällen können Strafverfolgungsbehörden mit richterlicher Anordnung ebenfalls auf solche Daten zugreifen, etwa durch die Auswertung eines beschlagnahmten Geräts oder durch spezielle Software (“Staatstroyaner”).

Daneben gibt es die **nachträgliche Ortung** über das Mobilfunknetz. Dabei wird nicht dein Handy direkt abgefragt. Stattdessen werden Verbindungsdaten ausgewertet, die automatisch entstehen, wenn dein Gerät mit Funkmasten kommuniziert. Diese Daten zeigen, in welcher Funkzelle sich dein Handy zu bestimmten Zeitpunkten aufgehalten hat.

Bei einer sogenannten **Funkzellenabfrage** werden für einen Ort und Zeitraum alle Geräte erfasst, die dort ins Netz eingewählt waren. Anschließend lassen sich daraus Bewegungen rekonstruieren, indem man die Abfolge der genutzten Funkzellen analysiert. So kann zum Beispiel eine Route grob nachvollzogen werden.

Die Genauigkeit ist dabei unterschiedlich: Während GPS oft sehr präzise ist, liegt die Ortung über Funkmasten meist im Bereich von einigen Dutzend bis mehreren hundert Metern – in Städten genauer als auf dem Land.

Bluetooth kann ebenfalls zur Standortbestimmung genutzt werden, insbesondere bei der Nutzung von Bluetooth Low Energy (BLE) Geräten, die in vielen modernen Smartphones und Geräten verbaut sind. Diese Schnittstelle wird zunehmend

verwendet, um Nutzer:innen zu erkennen und zu verfolgen, auch wenn sie keine direkten Interaktionen mit einer App haben.

→ Deaktiviere **WLAN**-Ortungsdienste und **Bluetooth**-Funktionen, wenn du sie nicht aktiv benutzt. Wenn du dich in öffentlichen Bereichen aufhälst, stelle sicher, dass dein Gerät nicht unnötig **Standortdaten**überträgt. Die meisten Geräte bieten in ihren Einstellungen die Möglichkeit, Standortdienste selektiv zu aktivieren oder zu deaktivieren.

Sichere Passwörter

"*Das Entsperrmuster lässt sich an der Fettspur auf dem Handy-Display ablesen, den Fingerabdruck bekommt man zum Beispiel von einem Getränkebehälter oder aus einer erkennungsdienstlichen Behandlung. Ein Porträtfoto für die Gesichtserkennung lässt sich mit einer guten Kamera aus der Ferne machen: Die meisten Entsperrmechanismen sind recht simpel zu umgehen." (Netzpolitik)*

Daher brauchen wir unbedingt sichere Passwörter!

Hier das wichtigste auf einen Blick:

Nutze nie das gleiche Passwort für verschiedene Accounts - vergib immer ein neues Passwort!

Die Länge ist entscheidend: Mindestens 20 Zeichen.

Ausnahme Smartphone: Hier sagt man mind 6 Zeichen. Aktuelle iPhones und aktuelle Google-Pixel-Telefone sind mit einem Sicherheitschip ausgerüstet, der hardwareseitig dafür sorgt, dass die Wartezeit zwischen den PIN-Eingaben von Fehlversuch zu Fehlversuch immer weiter steigt (Rate-Limiting), was ein sehr hoher Schutz gegen sogenannte Brute-Force-Angriffe darstellt.

Passwort im Zweifelsfall ändern:solltest du dich auf einem nicht vertrauenswürdigen Gerät eingeloggt haben, oder dein Passwort wurde in einem Datenleck veröffentlicht, ändere dein Passwort so schnell wie möglich. Ob deine E-Mail-Accounts in solchen Datenlecks enthalten sind kannst du hier checken: https://haveibeenpwned.com/ . Generell schadet es nicht Passwörter regelmäßig zu ändern.

Passwortmanager: Um deine vielen, langen Passwörter zu verwalten, nutze einen Passwortmanager. Hier kannst du nicht nur deine sicheren Passwörter geschützt speichern, sondern auch genrieren und schnell neue vergeben.

💡 Empfehlung: die KeePassfamilie

KeePassXC (Windows, macOS und Linux)ist ein quelloffenes (OpenSource) Projekt und der Quellcode auf GitHub einsehbar. Dies gilt auch für die Anwendungen KeePassDX (Android, GrapheneOS) und KeePassium (iOS), die du auf deinem Smartphone nutzen kannst.

Mit diesen Anwendungen kannst du eine Passwort-Datenbank erzeugen, in der all deine Passwörter liegen. Die Datenbank ist durch ein Passwort und, wenn du willst, zusätzlich noch durch einen zweiten Faktor wie z.B. eine Schlüsseldatei geschützt. Im Netz findest du diverse Anleitungen zur Installation auf verschiedenen Betriebssystemen und zur Einrichtung .

Es gibt auch eine Firefox-Integration, sodass deine Passwörter automatisch im Browser zur Verfügung stehen. Dies kann allerdings die Sicherheit deiner Passwort-Datenbank gefährden.

Willst du deine Passwort-Datenbank über mehrere Geräte/Betriebssysteme hinweg nutzen, musst du dich um die Synchronisation selbst kümmern – entweder manuell oder z.B. durch die Ablage deiner verschlüsselten Passwortdatenbank in einer sicheren Cloud.

❗ **Wichtig**: Erstelle regelmäßig Backups deiner Passwort-Datenbank und das am Besten auf unterschiedlichen Speichermedien – wenn möglich deponiere diese Speichermedien an verschiedenen Orten, sodass du noch Zugriff auf deine (Zugangs)Daten hast, sollten deine Datenträger abhanden kommen.

Alternative: Bitwarden ist ein cloudbasierter Passwortmanager, der als sicher gilt und dir die manuelle Synchronisation über deine verschiedenen Geräte hinweg erspart.

Spezielle Passwörter: Es gibt Passwörter, die du dir einfach merken musst, da du sie brauchst bevor du deinen Passwortmanager nutzen kannst. Z.B.

- Passwörter zum Entschlüsseln von Systemfestplatten
- Passwort zum Einloggen in dein System
- Hauptpasswort deiner Passwortdatenbank

  Hier kannst du z.B. sehr gut auf folgende Methoden zurückgreifen:

  Würfelmethode (Diceware-Methode)

  Eselsbrücken

Betriebssysteme jenseits von BigTech

Desktop/Laptop

Linux

Linux ist ein sehr sicheres Betriebssystem, das sich vor allem durch seine Open-Source-Natur, regelmäßige Updates und starke Sicherheitsfunktionen auszeichnet. Hier die wichtigsten Punkte:

- **Offener Quellcode**: Der Quellcode von Linux ist öffentlich, sodass Sicherheitslücken schnell erkannt und behoben werden können.
- **Paketquellen und Updates:** Software wird in Linux über Paketmanager (z.B. apt, yum, dnf) aus vertrauenswürdigen Quellen installiert. Diese Quellen sind sicherheitsgeprüft, und Updates werden regelmäßig angeboten, um bekannte Sicherheitslücken zu schließen.
- **Verschlüsselung:** Linux bietet einfache Lösungen zur Verschlüsselung von Festplatten (z.B. LUKS) und Dateien (z.B. ecryptfs), um Daten auch im Falle eines Diebstahls zu schützen.
- **Firewall & Netzwerksicherheit**: Linux hat leistungsstarke Firewall-Tools wie iptables, mit denen Administratoren den Datenverkehr genau steuern können. Tools wie fail2ban blockieren automatisch IP-Adressen bei wiederholten Sicherheitsverletzungen, z.B. Brute-Force-Angriffen.
- **Sicherheits-Tools:** Tools wie SELinux und AppArmor bieten erweiterte Sicherheitsfunktionen, um den Zugriff auf Systemressourcen weiter einzuschränken und Missbrauch zu verhindern.

Insgesamt bietet Linux ein hohes Maß an Sicherheit durch Transparenz, starke Verschlüsselung und eine einfache, aber effektive Verwaltung von Software und Updates.

Tails

Tails (kurz für Tails Amnesic Incognito Live System) ist ein auf Sicherheit und Anonymität spezialisiertes Live-Betriebssystem, das auf Linux basiert. Es ist darauf ausgelegt, von einem USB-Stick oder einer DVD aus zu booten, ohne Spuren auf dem genutzten Computer zu hinterlassen ("amnesic" = vergesslich).

Weitere Eigenschaften von Tails:

- **Anonymität durch Tor**: Der gesamte Internetverkehr wird zwangsweise über das Tor-Netzwerk geleitet, wodurch die IP-Adresse verschleiert und Online-Überwachung verhindert wird.

- **Keine Datenspuren:** Tails läuft vollständig im Arbeitsspeicher (RAM). Nach dem Herunterfahren werden alle flüchtigen Daten gelöscht. Es wird nichts auf der Festplatte des Computers gespeichert.
- **Portabilität:**Tails verwandelt jeden PC in einen sicheren Computer, da es nicht installiert werden muss, sondern als Live-System genutzt wird.
- **Vorinstallierte Sicherheits-Tools**: Das System enthält Werkzeuge für verschlüsselte Kommunikation, darunter der Tor Browser, KeePassXC (Passwortmanager), GnuPG (Verschlüsselung) und LibreOffice.
- **MAC-Adressen-Spoofing:** Tails verschleiert automatisch die MAC-Adresse der Netzwerkkarte, um die Hardware im Netzwerk unkenntlich zu machen.
- **Persistenter Speicher (optional):** Auf dem USB-Stick kann ein verschlüsselter Bereich eingerichtet werden, um Dateien und Konfigurationen dauerhaft zu speichern.

❗ **Achtung:** Wie alle Betriebssysteme ist auch Tails abhängig von der Firmware und Hardware des Geräts. Ist diese Komprimitiert, wurde z.B. Spionagesoftware aufgespielt, kann auch Tails nicht mehr als sicher gelten

Es gibt Rund um Tails eine sehr nützliche Broschüre, die auch als Download zur Verfügung steht.

QubesOS

QubesOS bietet herausragende Sicherheit und lässt sich mit Whonix kombinieren, um den Schutz vor Überwachung und Angriffen weiter zu verstärken. Es ist jedoch für technisch versierte Nutzer konzipiert.

- **Isolierte VMs:** Anwendungen laufen in eigenen VMs (virtuelle Maschinen), wodurch Angriffe auf eine VM nicht das ganze System gefährden können.
- **Minimale Rechte & Kompartimentierung:** VMs haben nur die nötigen Berechtigungen, was das Risiko eines Systemdurchbruchs minimiert.
- **Hardware-Virtualisierung:** Schützt vor tiefgehenden Angriffen durch Xen-Virtualisierung.
- **Open Source:** Der Quellcode ist öffentlich zugänglich, was Transparenz und Kontrolle ermöglicht.
- **Starke Verschlüsselung:** Alle Daten sind standardmäßig verschlüsselt.
- Regelmäßige Updates: Sicherheitsupdates werden kontinuierlich bereitgestellt.

Integration mit Whonix:

Qubes OS kann mit Whonix kombiniert werden, einem Betriebssystem, das speziell für Anonymität entwickelt wurde. Whonix leitet den gesamten Internetverkehr über das Tor-Netzwerk, um die Privatsphäre zu schützen. Die Architektur trennt zusätzlich

Tor-Netzwerkzugang (Whonix-Gateway) und Anwendungsbetrieb (Whonix-Workstation) in zwei separate virtuelle Maschinen. So bleibt die Integrität des Tor-Prozesses selbst bei kompromittierten Anwendungen erhalten. Whonix verhindert zuverlässig IP- und DNS-Leaks, schützt gegen Traffic-Korrelation, bietet vorkonfigurierte Sicherheitseinstellungen und unterstützt zahlreiche Tunneling-Varianten, etwa VPN-over-Tor oder SSH-Kaskadierungen. In Kombination mit Qubes OS bietet Whonix einen extrem hohen Schutz.

Whonix ist auch ohne Qubes nutzbar, läuft dann in einer eigenen VM oder als virtuelle Maschine auf anderen Betriebssystemen. Aber in Kombination mit Qubes OS erreicht Whonix eine nochmal höhere Isolation und geringere Angriffsfläche als im Standalone-Betrieb.

Smartphone

GrapheneOS

GrapheneOS ist das seit Jahren sicherste und datensparsamste mobile Betriebssystem. Es basiert auf dem Android Open Source Project (AOSP) und läuft derzeit nur auf Googles Pixel-Geräten, da nur diese den Sicherheitsanforderungen des Entwickler:innenteams an die Hardware gerecht werden. Soweit bekannt sind GrapheneOS-Geräte derzeit die einzigen Mobilgeräte, die in den letzten Jahren weder bei physischem Zugriff geknackt, noch remote kompromittiert werden konnten.

- Durch Spenden finanziert, kleines Entwickler:innenteam
- Dreiteilige Sicherheitsarchitektur:
  - Verkleinerung der Angriffsfläche: **nur absolut notwendige Features** sind im Grundzustand enthalten und aktiviert, alles Unnötige entfernt
  - Durch **moderne, sichere Softwareentwicklung** wird versucht, ganze Klassen von Programmfehlern (Bugs) auszuschließen (z.B. memory corruption oder dynamic code loading/execution) und fundamentale Schutzgräben ins Betriebssystem einzuziehen, statt nur auf bekannte Sicherheitslücken zu reagieren – Proaktiver statt reaktiver Sicherheitsansatz
- Durch **Containment und Isolation** werden die Auswirkungen minimiert, die es hat, wenn ein Angreifer doch mal eine Sicherheitslücke ausnutzen kann, weil jeder Prozess nur minimale Zugriffsrechte hat.
- **Keine Google-Dienste** im System, aber Nutzer:innen entscheiden selbst über Funktionen; Apps, die Google Play Services benötigen, können sicher in einer isolierten Sandbox laufen.
- **Schutz vor Exploits** (also Angriffen, die Sicherheitslücken ausnutzen) durch

    - räumliche Einschränkung (Apps haben nur Zugriff auf bestimmte Ressourcen, getrennte Benutzerprofile möglich) und
    - zeitliche Einschränkung (bei jedem Neustart sorgt Verified Boot dafür, dass das System wieder sicher ist).
- **Sicherheitsfeatures:**
    - **Auto-Reboot:** wenn sich die Nutzer:in für eine konfigurierbare Zeit nicht eingeloggt hat. Dadurch geht das Gerät wieder in den sichereren Before First Unlock (BFU)-Zustand über, in dem keine Geheimnisse im RAM liegen
    - keine unnötigen Netzwerkverbindungen: automatisches Abschalten der Schnittstellen (Wlan, Bluetooth etc.) bei Nicht-Verbindung, sodass darüber keine Angriffe mehr stattfinden können
    - **Duress-PIN** möglich → die bei (erzwungener) Eingabe alle Daten vom Gerät löscht
    - Zwei-Faktor-Authentifizierung zum Entsperren des Geräts möglich

Bei Resist Berlin findest du Infos, wie lange die verschiedenen Pixelmodelle noch durch Sicherheitsupdates supportet werden und wass dich das kostet.

Es gibt auch noch andere Betriebssysteme für Smartphones, die ohne Google als Basis funktionieren und doch die Nutzung ausgewählter Google-Apps ermöglichen. Sie reichen in Sachen Sicherheit jedoch nicht an GrapheneOS heran. Beispielsweise:

- **CalyxOS**: Schützt dein Handy stärker vor Angriffen als Android und sammelt kaum Daten. Viele Sicherheitsfunktionen sind standardmäßig aktiviert. Einfach zu installieren.
- **LineageOS:** Auch besser für Datenschutz als normales Android, aber mehr auf Freiheit und Anpassung ausgelegt. Sicherheit hängt stärker davon ab, wie du es einstellst.

Sichere Kommunikation

Messenger

Signal

Signal ist die sicherste Messenger-App für mobile Kommunikation. Das Ziel der Signal Technology Foundation ist es, private Kommunikation mit starker Verschlüsselung für alle zugänglich zu machen.

Wichtige Eigenschaften von Signal:

- **Ende-zu-Ende-Verschlüsselung:** Alle Nachrichten und Anrufe sind verschlüsselt, sodass niemand außer dem Sender und Empfänger die Inhalte lesen kann.

- Signal gibt **nur zwei Datenpunkte** an Behörden weiter: Wann der Account erstellt wurde und wann er zuletzt online war.
- **Double-Ratchet-Schlüsselmanagement:**Für jede Nachricht wird ein neuer Schlüssel verwendet, sodass selbst wenn jemand einen Schlüssel bekommt, nur eine Nachricht entschlüsselt werden kann.
- **Desktop-Version:** Signal kann auch auf dem Computer verwendet werden.
- **Open Source:** Der Code ist öffentlich und wird regelmäßig von Sicherheitsexperten überprüft.
- **Metadaten von Medien löschen:** Beim Versenden von Fotos und Videos werden Metadaten wie Gerätemodell, Betriebssystem oder Standort entfernt.
- **Telefonieren:** Signal eignet sich auch besonders gut für sichere Anrufe und Gruppenvideoanrufe bis 8 Personen.

Nachteil: Du benötigst eine Telefonnummer zur Anmeldung (die aber anonymisiert und nur für gespeicherte Kontakte sichtbar sein kann).

→ **Lösung**: vorregistrierte SIM-Karte organisieren, um Signal auf eine Nummer zu registrieren, die nicht mit einem selbst identifiziert wird

❗ Die richtigen Einstellungen in deiner App sind wichtig und machen einen großen Unterschied in Sachen Sicherheit aus.

💡 Es ist immer ratsam, zumindest in einem begrenzten Personenkreis, auf alternative Kommunikationsstrukturen zugreifen zu können, falls der Dienst, den du standardmäßig nutzt mal ausfällt. Daher hier noch eine Alternative:

Elements

- Sehr sicher, wenn richtig genutzt (z. B. eigener Server, Verschlüsselung aktiv)
- Für „normale Nutzung“: sicher, aber deutlich komplizierter als z. B. Signal
- In der Vergangenheit gab es immer wieder Sicherheitslücken, die jedoch auch relativ schnell wieder geschlossen wurden

Email-Provider

Viele große Anbieter wie Gmail, Yahoo oder GMX bieten zwar Komfort, haben aber erhebliche Nachteile für den Datenschutz - Sie scannen E-Mails für Werbezwecke, speichern umfangreiche Metadaten, verfolgen Nutzer:innen über Dienste hinweg und geben auf Behördenanfrage Daten heraus. Wer Kommunikation ernsthaft schützen möchte, sollte auf Anbieter setzen, die Privatsphäre konsequent respektieren und Ende-zu-Ende-Verschlüsselung unterstützen. Bei dieser Verschlüsselung werden E-Mails bereits auf dem Gerät der Absender:innen verschlüsselt und erst auf dem Gerät der Empfänger:innen wieder entschlüsselt – selbst der Anbieter kann die Inhalte nicht

einsehen. Weitere wichtige Aspekte sind eine No-Logs-Politik, verschlüsselte Speicherung auf den Servern und datensparsame Registrierung.

Empfohlene Anbieter mit Eigenschaften:

- **Riseup**
  - Ende-zu-Ende-Verschlüsselung standardmäßig
  - Verschlüsselte Speicherung, offene Infrastruktur
  - Registrierung nur auf Einladung, keine personenbezogenen Daten erforderlich
  - Fokus auf Aktivist:innen und kritische Gruppen
- **Systemli**
  - Optional Ende-zu-Ende-Verschlüsselung über PGP
  - Verschlüsselte Speicherung, Open-Source-Clients
  - Registrierung nur auf Einladung, keine personenbezogenen Daten erforderlich
  - Nachhaltige Infrastruktur, datensparsame Nutzung
- **Posteo**
  - Ende-zu-Ende-Verschlüsselung optional
  - Verschlüsselte Speicherung von E-Mails und Kalenderdaten
  - Registrierung frei möglich, keine personenbezogenen Daten erforderlich
  - Umweltfreundlich, kostenpflichtig: 1 € pro Monat, anonyme Zahlung möglich
- **ProtonMail**
  - Ende-zu-Ende-Verschlüsselung standardmäßig
  - Verschlüsselte Speicherung auf Servern in der Schweiz
  - Strikte No-Logs-Politik
  - Registrierung frei möglich, nur notwendige Account-Daten
  - Zwei-Faktor-Authentifizierung, Open-Source-Clients
- **Immerda.ch**
  - Ende-zu-Ende-Verschlüsselung optional
  - Verschlüsselte Speicherung, strikte No-Logs-Politik
  - Registrierung frei möglich, keine personenbezogenen Daten erforderlich
  - Schweizer Anbieter mit Fokus auf Datenschutz

PGP-Verschlüsselung
PGP (Pretty Good Privacy) und S/MIME sind Standards, um einzelne E-Mails stark zu verschlüsseln. Jede Person besitzt ein Schlüsselpaar: einen öffentlichen Schlüssel zum Verschlüsseln und einen privaten Schlüssel zum Entschlüsseln. PGP schützt zuverlässig den Inhalt der Nachricht, verschlüsselt aber nicht standardmäßig die

Betreffzeile. Auch Metadaten wie Zeitstempel oder Absender-/Empfängeradressen bleiben sichtbar. Dadurch kann PGP auch über Standardanbieter hinweg eingesetzt werden, bietet aber nur dann vollen Schutz, wenn Absender:in und Empfänger:in es konsequent nutzen.

Eine Anleitung zur Einrichtung von PGP-Verschlüsselung findest du hier: https://mail.de/de/hilfe/nachrichten/pgp-verschluesselung/pgp_in_thunderbird

Tuta – quantensicher
Tuta Mail nutzt ein eigenes Verschlüsselungssystem, das PGP nicht kompatibel ist. Der Grund: PGP ist komplex, alt und nicht quantensicher. Tutanota bietet dafür:

- **Ende-zu-Ende-Verschlüsselung** für Inhalte, Betreffzeilen, Anhänge und Kalenderdaten
- **Post-Quantum-Kryptographie** zum Schutz gegen zukünftige Quantenangriffe
- Keine Speicherung von IP-Adressen, strikte **No-Logs-Politik**
- Eigenes **Open-Source**-Mailclient-System (Web, Desktop, Mobile)
- Optionale **Zwei-Faktor-Authentifizierung**, inkl. Hardware-Token
- Verschlüsselte Kontakte und sichere externe Nachrichten via **Passwortschutz**

Sicherung und Löschen von Daten

Festplattenverschlüsselung

Je nach Betriebssystem gibt es verschiedene integrierte Möglichkeiten zur vollständigen Festplattenverschlüsselung:

- **Mac:** Option File Vault.
- **Linux:** Unified Key Setup (LUKS).
- **Windows Pro/Home**: Bitlocker/Geräteverschlüsselung.

  Achtung: Beim Booten von Windows wird automatisch der Verschlüsselungs-Key in den Systemspeicher geladen. Um einen potentiellen Angriff durch physisches Auslesen des Schlüssels zu unterbinden, sollte man die "Pre-Boot-Authentifzierung" aktivieren.

Wenn du die Verschlüsselung auf einem bereits laufendem System aktivierst, sichere zuvor unbedingt deine Daten auf einem anderen Datenträger.

- **Smartphones:** Pixel-Handys ab Serie 6 und Iphones ab iOS 8 gelten als sehr sicher. Beide Systeme bieten automatische Gerätespeicher-Verschlüsselung – du musst sie nicht extra aktivieren. Außerdem liegt u.a. der Schlüssel in der Hardware – der eigentliche Schlüssel ist nicht einfach im Speicher gespeichert,

was dein Telefon auch vor physischen Angriffen schützt. Es ist nicht möglich den Speicher direkt auszulesen (also z.B. Chip ausbauen oder kopieren). Der wichtigste Faktor bleibt dein starkes Passwort/PIN.

Verschlüsselte Datencontainer

Sobald du das Passwort eingibst und dein verschlüsseltes System entschlüsselst, liegt alles offen. Daher ist es ratsam kritische Daten in einer verschlüsselten Festplattenpartition oder Datencontainern zu speichern.

Empfehlung: VeraCrypt

VeraCrypt ist eine quelloffene (OpenSourcce) Software zur starken Datenverschlüsselung. Als Weiterentwicklung von TrueCrypt ermöglicht es die Verschlüsselung von ganzen Partitionen, Datenträgern (USB-Sticks, Festplatten) oder die Erstellung virtueller, verschlüsselter Containerdateien. Es gilt als sehr sicher und bietet "On-the-Fly"-Verschlüsselung. Die Installation und Einrichtung ist gut handhabbar.

❗ **Achtung:** Vergessene Passwörter führen zu unwiederbringlichem Datenverlust.

In Veracrypt kannst du auch sogenannte **Hidden Container** anlegen. Solch ein versteckter Container basiert auf dem Prinzip der „plausible deniability“, also der glaubhaften Abstreitbarkeit. Das bedeutet, dass ein verschlüsselter Container so aufgebaut ist, dass er nach außen nur wie zufällige Daten aussieht. Je nach eingegebenem Passwort wird entweder ein äußeres Volume oder ein darin verstecktes zweites Volume geöffnet, ohne dass technisch eindeutig nachweisbar ist, dass dieses zweite Volume überhaupt existiert.

Sinnvoll ist dieses Konzept vor allem in Situationen, in denen jemand unter Zwang stehen könnte, ein Passwort preiszugeben – etwa bei Kontrollen, Beschlagnahmungen oder in repressiven Umgebungen. So besteht die Möglichkeit nur das Passwort des äußere Volumes und so “harmlose” Inhalte preiszugeben, während besonders sensible Daten im versteckten Volume weiterhin verborgen bleiben.

Ein Hidden Container in VeraCrypt ist ein versteckter, verschlüsselter Bereich innerhalb eines normalen Containers. Nach außen wirkt die Datei wie zufällige Daten, ohne erkennbare Struktur. Je nach Passwort wird entweder das äußere oder das versteckte Volume geöffnet („plausible deniability“).

❗ **Wichtige Grenzen:**

- kein Schutz vor sehr tiefer forensischer Analyse oder Metadaten-Auswertung
- Hidden Volume kann durch falsche Nutzung (z. B. Schreiben ins äußere Volume) beschädigt werden

Tella ist ein **Open Source-Tool** zur Verschlüsselung sensibler Daten für Smartphones und ist speziell das Speichern und die sofortige Verbreiten von Bild- und Videodokumentation ausgelegt:

- **Videoaufnahme und Bildschirmaufzeichnung:** Erlaubt das Erstellen von Videos, inklusive Kommentaren oder Erklärungen, direkt über Kamera oder Bildschirm.
- **Offline-Modus:** Inhalte können aufgenommen und vorbereitet werden, bevor sie online geteilt werden – nützlich in Regionen mit unsicherer oder eingeschränkter Internetverbindung.
- **Kontrolliertes Teilen:** Videos können über spezifische Links oder Plattformen geteilt werden, wobei Zugriffsrechte genau bestimmt werden.
- **Verschlüsselung & Datenschutz:** Die App speichert Inhalte lokal und verwendet Verschlüsselung, um Daten vor unbefugtem Zugriff zu schützen.
- **Einfache Bearbeitung:** Grundfunktionen wie Schneiden, Kommentieren oder Markieren von Videos direkt in der App.
- **Plattformübergreifend:** Verfügbar für gängige Smartphones und Betriebssysteme, sodass Inhalte flexibel erstellt und geteilt werden können.

Bei der Nutzung von **Cloud-Diensten** bietet die App **Cryptomator** plattformübergreifend als zusätzliche Sicherheitsebene die Möglichkeit deine Dateien und Dateinamen in einem lokalen Tresor oder in der Cloud mit AES-256 zu verschlüsseln. Die Verschlüsselung passiert auf dem Gerät bevor die Daten in die Cloud gesendet werden. Der Anbieter speichert also lediglich verschlüsselte Daten

Backups

Die **3-2-1-Backup-Regel** ist eine bewährte Strategie zur Datensicherung:

- **3 Kopien:** Neben dem Original solltest du zwei weitere (verschlüsselte) Sicherungskopien deiner Daten besitzen.
- **2 Medientypen:** Speicher deine Daten auf zwei unterschiedlichen Arten von Speichermedien (z.B. primär auf dem Laptop, die Backups auf einer externen Festplatte).
- **1 externer Standort:** Bewahre die Backups räumlich getrennt von deinem Hauptstandort auf (z.B. bei nicht gefährdeten friends oder family)

Daten löschen

Gelöschte Dateien sind nicht einfach weg: Die Löschfunktionen der Betriebssysteme entfernen oft nur die Beschriftung der Dateien und markieren sie als überschreibbar, während die eigentlichen Daten physisch noch auf dem Speichermedium vorhanden sind. Das Entfernen des Markers geht schnell, im laufenden Betrieb wird die Datei dann irgendwann überschrieben. Echtes Überschreiben ist hingegen aufwendig, zeitintensiv – und daher nicht alltagstauglich, weil es zu viele Ressourcen des Computers binden würde. Jeder Block des Datenträgers, auf dem die Datei lag, müsste mehrfach überschrieben werden.

Auch das Formatieren einer Festplatte oder eines Datenträgers reicht oft nicht aus, um die Daten vollständig zu löschen. Das System löscht dabei meist nur das bestehende Inhaltsverzeichnis und ersetzt es mit einem neuen – das heißt nur die Dateisystemstruktur wird verändert und Dateien bleiben auf dem Datenträger bestehen.

Einzeldateien können mit spezieller Datenschredder-Software (in Linux mit dem *shred*-Befehl) sicher gelöscht werden, indem sie vor dem Löschen mehrfach mit zufälligen Datenfolgen überschrieben werden. **Shredden** ist jedoch unsicher, da oft noch Metadaten oder Referenzen in anderen Teilen des Systems (z. B. in „Zuletzt verwendete Dokumente"-Listen oder temporären Dateien) zurückbleiben. Um sicherzugehen, dass alle Spuren einschließlich Dateinamen entfernt sind überschreibe die gesamte Festplatte (**Wipen**) und installiere das Betriebssystem neu. Hierbei gibt es je nach Speichermedium Besonderheiten zu beachten:

HDD (klassische Festplatte):

- Überschreiben des gesamten Datenträgers mit speziellen Tools wie *BleachBit* oder *Darik's Boot and Nuke*.
- Das Überschreiben schadet den magnetischen Platten nicht und hinterlässt keinen messbaren Verschleiß.

SSD Hier ist es komplizierter:

- SSDs haben begrenzte **Schreibzyklen** (P/E-Cycles) pro Zelle. Ein vollständiges Wipen verbraucht davon einen Zyklus auf jeder Zelle — das verkürzt die Lebensdauer, ist aber bei einmaligem Wipen vernachlässigbar.
- SSDs haben auch **Reservebereiche** (Over-Provisioning), auf die man beim normalen Wipen gar nicht zugreift — dort können theoretisch noch Daten liegen.
- Lösung: Festplatte vorab verschlüsseln und anschließend den Verschlüsselungsschlüssel löschen („**kryptografisches Löschen**"), was die Daten sofort unlesbar macht.

- Alternativ bieten einige SSD-Hersteller sichere Löschfunktionen im BIOS an – z.B. **ATA Secure Erase** oder **NVMe Sanitize**, welches komplett auf der SSD selbst innerhalb von Sekunden abläuft.

USB-Sticks: am Besten physisch zerstören oder von Anfang an verschlüsselt betreiben – dann reicht normales Formatieren.

Tools fürs Android Handy: *CCleaner*, um temporäre und versteckte Dateien zu entfernen, gefolgt von *Extirpater*, um den freien Speicherplatz sicher zu überschreiben.

💡**Allgemein gilt:** Regelmäßiges Überprüfen und Säubern von temporären Dateien, Browserverläufen, Zwischenablage-Inhalten und alten Protokolldateien.

❗Es gibt keine 100%-ige Sicherheit das Daten nicht wiederhergestellt werden können. Bei sensiblen Daten hilft deshalb nur - **Hammer statt Schredder!**

Sicher und anonym im Netz

VPN & TOR

Tor-Netzwerk und Orbot

Tor-Netzwerk:
Tor (The Onion Router) ist ein Netzwerk, das Internetverkehr durch mehrere Knotenpunkte weltweit weiterleitet, um Anonymität zu gewährleisten. Der Verkehr wird dreifach verschlüsselt, wobei jeder Knoten nur eine Schicht der Verschlüsselung entfernt, sodass erstmal niemand den Ursprung des Datenverkehrs nachvollziehen kann und deine echte IP verborgen bleibt. Außerdem sehen alle TOR-User gleich aus. So schützt TOR vor Überwachung und Zensur.

Dein Internetdienstanbieter, sowie die Zieladresse (Webseite, die du aufrufst) sehen allerdings, dass du TOR nutzt. Um dem entgegen zu wirken kannst du TOR-Bridges nutzen.

❗Aber auch Tor hat Grenzen und deine Anonymität kann gefährdet sein, durch

- unverschlüsselte Verbindungen zur Zieladresse (HTTP statt HTTPS)
- Man-in-the Middle Angriffe
- Zeitanalyse
- Verkehrskorrelation (durch die Überwachung von Teilen des Netzwerks)

Orbot:
Orbot ist eine Android-App, die Tor auf Mobilgeräten verfügbar macht. Sie leitet den gesamten Internetverkehr deines Geräts sicher und anonym über das Tor-Netzwerk. Dadurch kannst du deine IP-Adresse verschleiern, auch in Apps, die keine eigene Anonymisierung unterstützen.

VPN (Virtual Private Network):

Ein VPN verschlüsselt deinen Internetverkehr und leitet ihn über einen sicheren Server. Dadurch wird deine echte IP-Adresse durch die des VPN-Servers ersetzt, was deine Identität schützt und geografische Sperren umgehen kann. Während VPNs den Datenverkehr sichern, bieten sie weniger Anonymität als Tor, da der VPN-Anbieter den Verkehr einsehen könnte.

❗ Achtung: VPN sind keine Anonymisierungsdienste! Eine VPN verschiebt in erster Linie wer deine IP kennt, sie wird durch einen VPN-Dienst nicht unsichtbar! Daher ist es sehr wichtig einen vertrauensvollen VPN-Anbieter zu wählen und so wenig wie möglich Daten überhaupt erst preiszugeben.

Mullvad VPN

Plattformen: Windows, macOS, Linux, Android und iOS

Sitz: Schweden

Mullvad VPN ist ein radikal anonymitätsorientierter VPN-Dienst mit starkem Fokus auf Privatsphäre, moderner Verschlüsselung, Schutz vor Datenlecks, Zensurumgehung sowie hoher Transparenz und zusätzlichen Sicherheitsfunktionen.

- **Keine persönlichen Daten für die Kontoerstellung erforderlich** (nur zufällige Kontonummer) und anonyme Bezahlung möglich (in Bar per Post); ergänzt durch eine strikte **No-Logs-Politik** ohne Speicherung von Verbindungs- oder Aktivitätsdaten
- Einsatz moderner Sicherheitsstandards **wie WireGuard sowie starker Verschlüsselung (AES-256, ChaCha20) und teilweise zukunftsorientierter Technologien wie quantenresistente Tunnel**
- Integrierte Schutzmechanismen wie **Kill Switch,** durchgehender **DNS-Leak-Schutz** und vollständige Weiterleitung des Datenverkehrs durch den VPN-Tunnel
- Funktionen zur Umgehung von Zensur, etwa durch **Verschleierungstechniken** und optionale **Multihop-Verbindungen** über mehrere Server
- Hohe Transparenz durch **Open-Source**-Software und regelmäßige unabhängige Audits

- Zusätzliche Sicherheitsfeatures wie automatische Schlüsselrotation, DNS-Filter gegen Tracking und Malware sowie optionales Split Tunneling
- Mullvad VPN in Kombination mit dem darauf abgestimmten Mullvad Browser bietet außerdem einen hohen Trackingschutz
- hohe Geschwindigkeit
- Kosten 5€/Monat (zur Finanzierung der Infrastruktur)

Proton VPN

Plattformen: Windows, macOS, Linux, Android und iOS

Sitz: Schweiz

Proton VPN gilt als sehr sicherer Mainstream-Privacy-Dienst mit Fokus auf Privatsphäre, starker Verschlüsselung, Schutz vor Datenlecks, Zensurumgehung sowie Transparenz; er ist in das Proton-Ökosystem (z. B. Proton Mail) integriert und eignet sich z.B. gut, wenn du Zensur und Geoblocking umgehen willst:

- **Kontoerstellung mit E-Mail** erforderlich
- Keine vollständig anonyme Bezahlung
- Strikte **No-Logs-Politik**

  ❗ rechtliche Unsicherheit durch geplante Überwachungsgesetze (Verpflichtung zur Datenspeicherung) in der Schweiz; teilweise Verlagerung von Infrastruktur ins Ausland (u. a. EU)
- Einsatz moderner Protokolle (**WireGuard, OpenVPN**) und **starker Verschlüsselung** (AES-256)
- Schutzmechanismen wie **Kill Switch, DNS-Leak-Schutz** und **„Always-on“-Funktion**
- Erweiterte Features wie „Secure Core“ (**Multihop** über sichere Server)
- Gute Zensurumgehung und Geoblocking-Funktionalität
- **Open-Source**-Clients und unabhängige Audits für Transparenz
- hohe Geschwindigkeit bei der kostenpflichtigen Pro-Version
- kostenlose Basisversion und kostenpflichtige Erweiterungen (10€/Monat, oft angebote ab 3€/Monat)

Weitere VPNs:

Riseup & sytemli bieten auch kostenlose VPN-Dienste an. Beide werden von kollektiven Diensten betrieben, bringen einen **hohen ideellen Anspruch** mit und zielen auf die Unterstützung von Aktivismus ab. Sie verfolgen beide den **No-Logs-Ansatz**. Bei Riseup ist keine Registrierung nötig und bei Systemli kannst du anonym eine Mailadresse registrieren und erhältst so auch Zugriff auf die VPN. Die

Infrastruktur ist kleiner ausgelegt, was tendenziell niedrigere Geschwindigkeiten und weniger Serverstandorte mit sich bringt.

VPN vor Tor

Es ist möglich, Tor und VPN miteinander zu kombinieren, um eine doppelte Sicherheitsebene zu schaffen, indem du zuerst dein VPN aktivierst und anschließend Orbot/Tor für die Anonymisierung deines Datenverkehrs einsetzt. So wird der Internetverkehr zuerst über das VPN umgeleitet und dann in das Tor-Netzwerk weitergeleitet. Dies bietet den Vorteil, dass dein Internetanbieter (ISP) nicht sehen kann, dass du Tor verwendest, da der gesamte Verkehr zuerst verschlüsselt über das VPN läuft.
Deine IP wird außerdem vor dem Tor-Netzwerk verborgen und die Zielwebseite weiß nicht, dass du Tor benutzt.
Einschränkung: Diese Konfiguration kann die Verbindungsgeschwindigkeit erheblich verlangsamen, da der Verkehr zuerst über das VPN und dann durch Tor läuft.

Browser

Die Wahl des Browsers ist wichtig, weil der Browser die zentrale Schnittstelle zwischen dir und dem Internet ist und damit bestimmt, wie viele Daten überhaupt entstehen und wie stark du vor Tracking, Fingerprinting und schädlichen Inhalten geschützt bist.

Einige Browser haben bereits starke integrierte Schutzmechanismen gegen Tracker, Cookies und Fingerprinting, während andere mehr auf Erweiterungen angewiesen sind. Gleichzeitig beeinflusst der Browser auch, wie einzigartig dein Gerät im Netz wirkt – und damit, wie leicht du wiedererkannt werden kannst.

Das Tor Project beschreibt dabei ein Paradox: „By wanting to increase online privacy, you install extensions that in the end make you even more visible than before.“

Kurz gesagt: Der Browser entscheidet mit darüber, wie viel du preisgibst, bevor überhaupt zusätzliche Sicherheitsmaßnahmen greifen können.

Tor Browser

Plattformen: Windows, macOS, Linux, Android

Schutz der Privatsphäre: Der Tor Browser ist besonders für Nutzer geeignet, die maximale Anonymität und Datenschutz wünschen. Er basiert auf Firefox und verschleiert die IP-Adresse, indem er Anfragen verschlüsselt über drei Server leitet. Dies schützt vor Nachverfolgbarkeit und ermöglicht Standortverschleierung und Zensurumgehung. Im Tor-Netzwerk sind außerdem alle Nutzer hinsichtlich ihrer Browser- und Systemmerkmale weitgehend standardisiert, sodass sie sich im

Fingerprinting nicht unterscheiden und dadurch schwer individuell identifizierbar sind.

Einschränkungen: Er ist kein "Alltagsbrowser", da viele Websites den Zugang blockieren und Captchas häufiger auftreten. Auf Android ist der Tor Browser weniger sicher als Chromium-basierte Browser.

Tipp: Vermeide personalisierte Einstellungen, um die Anonymität zu bewahren. Wähle mindestens die Einstellung “sicherer/saver” . Gib nie in der gleichen Session persönliche Daten ein, anhand denen du identifiziert werden kannst, wenn du noch andere Sachen machst bei denen du anonym bleiben willst.

Mullvad Browser

Plattformen: Windows, macOS, Linux

Schutz der Privatsphäre: Der Mullvad Browser wurde in Zusammenarbeit mit dem Tor Project entwickelt und nutzt viele der Anonymisierungsfunktionen von Tor, um die Privatsphäre der Nutzer zu schützen. Er blockiert Tracking, Fingerprinting und sorgt für eine standardisierte Darstellung von Browserdaten, um eine eindeutige Identifizierung zu verhindern, aber ohne die direkte Nutzung des Tor-Netzwerks – er wurde zur Nutzung mit einer VPN entwickelt.

VPN-Integration: Der Mullvad Browser ist besonders effektiv in Kombination mit Mullvad VPN, aber er kann auch mit anderen vertrauenswürdigen VPNs verwendet werden.

Kein anonymisierendes Netzwerk wie bei Tor, dafür weniger Captchas, die es zu lösen gilt und schnelleres Surfen, besonders in Kombination mit Mullvad VPN.

Vanadium

Plattformen: GrapheneOS

Schutz der Privatsphäre: Vanadium ist ein Chromium-basierter Browser, der speziell für Sicherheit und Datenschutz auf dem GrapheneOS-Betriebssystem optimiert wurde. Er verwendet eigene Filterlisten und DuckDuckGo als Standardsuchmaschine.

Vorteil: Sehr schnelle Sicherheitsupdates und umfassende Datenschutzfunktionen.

Firefox

Plattformen: Windows, macOS, Linux, Android, iOS

Schutz der Privatsphäre: Firefox ist Open-Source und bietet eine Vielzahl an Anpassungen, die den Datenschutz verbessern können. Standardmäßig sind jedoch Telemetrie und Werbefunktionen aktiv, die deaktiviert werden müssen.

Vorteil: Userfreundlich, bekannt

Nachteile: Auf Android gibt es Sicherheitsprobleme und der Browser ist zunehmend in Werbeindustrie-Aktivitäten involviert.

Empfehlung: Nicht zu viele Ad-Ons installieren! Auf jeden Fall: uBlock Origin und Datenschutzeinstellung “streng” verwenden.

Brave

Plattformen: Windows, macOS, Linux, Android, iOS

Schutz der Privatsphäre: Brave Browser blockiert standardmäßig Tracker, Werbung, Cross-Site-Cookies und viele Fingerprinting-Techniken direkt im Browser („Shields“). Dadurch werden zahlreiche Tracking-Skripte gar nicht erst geladen. Zusätzlich unterstützt Brave moderne Sicherheitsarchitekturen wie Site Isolation, bei der Websites in getrennten Prozessen ausgeführt werden, um Datenabgriffe zwischen Seiten zu verhindern. Weitere Funktionen sind integriertes HTTPS-Upgrade, Cookie-Isolation pro Site und optionales DNS-over-HTTPS.

Sicherheitsarchitektur: Brave basiert auf Chromium und profitiert dadurch von einer ausgereiften Sandbox-Architektur sowie regelmäßigen, schnellen Sicherheitsupdates. Die Kombination aus Prozessisolation, Sandbox und Site Isolation reduziert die Angriffsfläche durch kompromittierte Webseiten deutlich.

Auf Android stärker als Firefoxbasierte Browser.

Privatsphäre-Optionen: Zusätzlich bietet Brave private Fenster mit optionaler Tor-Anbindung (nur Desktop), die den Netzwerkverkehr über das Tor-Netzwerk leiten, jedoch ohne vollständigen Funktionsumfang des separaten Tor Browsers.

Einordnung: Unabhängig von der technischen Funktion des Browsers, steht das Projekt immer wieder in der Kritik. Der Browser blockiert Werbung, ersetzt sie aber stattdessen mit eigenen Brave-Anzeigen, URLs wurden automatisch vervollständigt und Code großer Krypto-Börsen eingefügt und der CEO Brendan Eich unterstützte 2008 eine Volksabstimmung gegen gleichgeschlechtliche Ehe.

MAC-Adressen spoofing/randomization

Die MAC-Adresse kann per Software vorgetäuscht (temporär überschrieben) werden — dein Gerät gibt sich dann im Netzwerk als ein anderes aus und wird vom Router als ein neues Gerät erkannt.

Das Spoofen der MAC-Adresse unter **Linux** erfolgt meist temporär über das Terminal mit macchanger oder ip link: https://wiki.archlinux.org/title/MAC_address_spoofing

Ab **Android 10** sind zufällige MAC-Adressen als Datenschutzfunktion eingebaut:

- Einstellungen → WLAN → Netzwerkname antippen → Stift/Details
- Option: „Zufällige MAC" (Standard seit Android 10) oder „Geräte-MAC"
- Pro Netzwerk einstellbar

Seit **Android 12** wird die MAC sogar **regelmäßig automatisch rotiert**, auch ohne Verbindungswechsel.

SET-UP Vorschlag

Der folgende Setup-Vorschlag ist als Orientierung gedacht und ersetzt keine Auseinandersetzung mit deinen Tools und deiner digitalen Umgebung. Wir empfehlen mindestens das erste Kapitel der Broschüre oder andere Grundlagentexte zu lesen.

PC/Laptop

Standardlevel:

Linux mit LUKS Systemverschlüsselung und/oder VeraCrypt + Keepass + Mullvad-Browser / -VPN (Firefox & TOR Browser als Alternative)

Toplevel:

Tails (VeraCrypt + Keepass + TOR Browser - schon vorinstalliert bzw. Teil des Designs)

+ externer verschlüsselter Datenspeicher und backups

für **Technik-Versierte**: QubesOS mit Whonix

Smartphone

💡 **Grundsätzlich:** Achte darauf möglichst wenige Funkdaten zu senden und nutze ein aktuelles Betriebssystem mit laufenden Sicherheitsupdates und VPN.

❗ Nutze mehrere Geräte für verschiedene Anlässe:

Alltagshandy: Wenn möglich Pixelhandy mit GrapheneOS und mehreren Profilen für verschiedene Bereiche deines Lebens

Polithandy (abhängig von deinem Bedrohungslevel)**:** für deine politischen Kontakte, Gruppen oder Online-Präsenz mit kritischen Inhalten. Am Besten mit GrapheneOS und vorregistrierter Prepaid SIM-Karte, evtl. Tella.

Relevant könnte außerdem sein, wo du das Gerät anmachst – Funkdaten geben Informationen über deinen Standort preis!

Aktionshandy: mit vorregistrierter Wegwerf-SIM-Karte. Wichtig – schalte das Handy nie zuhause oder an politischen Orten an - nur bei der Aktion!

Kommunikation:

Standardlevel:

Wenn möglich, nutze immer Signal (auch zum telefonieren) und schaffe für den Ausfall mit deinen Bezugsmenschen eine Alternative.

Außerdem: Sicherer Email-Provider, Mailprogramm Thunderbird mit geschütztem Passwort und wenn möglich Mails immer verschlüsseln.

Toplevel:

gezielt z.B. Tuta Mail für bestimmte Zusammenhänge

*** Die Beste und sicherste Kommunikation ist immer noch: **Live & ohne Technik :)** ***

Zum Weiterlesen

Auflistung & Beschreibung Open-Source-Tools: https://opensourcealternative.to

Clouddienst: Nextcloud

E-Mail-Programm: Thunderbird

Share Dienste: wetransfer, OnionShare

Suchmaschine: DuckDuckgo >> In Firefox als Standardsuchmaschine festlegen

Videocalls: Senfcall oder Jitsi

Pads: Systemli, Cryptpad, RiseUp

Ausführliche Online-"Handbücher":

https://ssd.eff.org/ (EN, spezifisch für Aktivist*innen)

https://securityinabox.org/en/ (EN, spezifisch für Aktivist*innen)

https://activisthandbook.org/tools/security (EN)

https://activistchecklist.org/essentials/ (EN, ES)

https://privacy-handbuch.de/index.htm (DE, für technisch Versierte)

https://digitalcourage.de/digitale-selbstverteidigung (DE, weniger spezifisch)

https://netzpolitik.org/digitale-selbstverteidigung/ (DE, weniger spezifisch)