Was ist eigentlich…

Inhalt

… der späte Mausklick 3
… der God Mode in Windows 11 4
… Linux 5
… ChatGPT 7
… ein Bot 8
… Everything 9
… Freefilesync 10
… Startpage 11
… Calibre 13
… Native Alpha 14
… Samsung Good Lock 15
… die Entwickleroption bei Samsung 16
… PhotoSync 18
… eine Echo Chamber 19
… der Idetity Leak Checker 21
… Swiss Transfer 22
… ein QR-Code 23
… der „Kartoffel-Test“ 24
… ein VPN 26
… VoIP 27
… eine SSD 29
… ein persönlicher Hotspot 30
… ein Passkey 31
… ein Notch 33
... ein Hoax 34
… ein Meme 36
… ein haptisches Feedback 37
… eine Drittanbietersperre 38
… ein Cookie 39
… Clickbait 40
… ein Captcha 41
… AR 42

… das gängigste Videoformat 43
… NTFS 44
… Tailscale 45
… das BFID Verfahren 51

… der späte Mausklick

Der Begriff **„Später Mausklick“** bezeichnet kein technisches Problem oder einen IT-Fachbegriff, sondern ist der Name einer bekannten **Computer-Selbsthilfegruppe für Senioren**.

Was steckt dahinter?

Das Projekt wurde bereits vor über 20 Jahren in **Köln** (speziell im Stadtteil Riehl) ins Leben gerufen. Es richtet sich an Menschen ab etwa 55 Jahren, die Unterstützung im Umgang mit moderner Technik suchen.

- **Zielgruppe:** Seniorinnen und Senioren („Späteinsteiger“), die fit am PC, Tablet oder Smartphone werden wollen.
- **Angebot:** Es handelt sich um einen offenen Treff, bei dem ehrenamtliche Experten bei Fragen zu Internet, Apps, Online-Banking oder Sicherheit helfen.
- **Konzept:** Anstatt starrer Kurse steht das gemeinsame Ausprobieren und der Austausch in ruhiger Atmosphäre im Vordergrund.

Standorte und Treffen

Der wohl bekannteste „Späte Mausklick“ findet regelmäßig im **Riehler Treff** der Sozial-Betriebe-Köln (SBK) statt.

- **Wann:** Meist dienstagnachmittags von16:30-18:00 Uhr.
- **Wo:** Boltensternstraße 16, 50735 Köln.

… der God Mode in Windows 11

Der God Mode in Windows 11 ist ein versteckter Ordner, der dir zentralen Zugriff auf über 200 Verwaltungseinstellungen bietet.

Er dient als bequemer Sammelort für Systemwerkzeuge, administrative Optionen und Konfigurationen.

So wird der God Mode aktiviert:

1. **Rechtsklick** auf eine freie Stelle auf dem Desktop.
2. Wählen Sie **Neu** > **Ordner**.
3. Benennen Sie den Ordner mit folgendem exakten Text (am besten kopieren): GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}
4. Drücken Sie **Enter**. Das Ordnersymbol ändert sich, und der Name verschwindet.

Funktionen und Hinweise:

- **Zentraler Zugriff:** Schneller Zugriff auf Verwaltungstools wie BitLocker, Geräte, Energieoptionen und Benutzerkonten.
- **Suche:** Optionen können innerhalb des Ordners direkt durchsucht werden.
- **Ort:** Der Ordner kann auch an anderen Speicherorten erstellt werden, am Desktop ist er jedoch am leichtesten erreichbar.

Wichtiger Hinweis:

Der God Mode ist praktisch für erfahrene Nutzer oder Administratoren. Finde die richtigen Tools dort schnell, aber sei vorsichtig, Änderungen betreffen tiefere System- und Sicherheitseinstellungen.

... Linux

Linux ist ein kostenloses und quelloffenes **Betriebssystem**, das genau wie Windows oder macOS die Verbindung zwischen der Hardware deines Computers und deiner Software herstellt. Der Name Linux bezeichnet im Kern den sogenannten **Kernel** – das Herzstück des Systems, das Rechenleistung und Speicher verwaltet.

Was macht Linux besonders?

- **Open Source:** Jede Zeile des Programmcodes ist öffentlich einsehbar. Das bedeutet, eine weltweite Community prüft, verbessert und teilt das System ständig, was es besonders **sicher und stabil** macht.
- **Kostenlos:** Du kannst Linux gratis herunterladen und auf so vielen Geräten installieren, wie du möchtest – ohne teure Lizenzen oder Abos.
- **Vielfalt (Distributionen):** Es gibt nicht „das eine“ Linux. Stattdessen existieren hunderte Varianten, sogenannte **Distributionen**, für jeden Zweck: vom schicken Desktop bis zum Rechenzentrum.
- **Überall im Einsatz:** Auch wenn du es auf dem PC selten siehst – das Internet, fast alle Webserver, Supercomputer und auch **Android-Smartphones** basieren auf Linux.

Linux vs. Windows: Ein kurzer Vergleich

Merkmal	Windows	Linux
Kosten	Kostenpflichtig (Lizenz)	Meist völlig kostenlos
Privatsphäre	Sammelt viele Nutzerdaten	Hoher Datenschutz, keine Spionage
Software	Riesige Auswahl (Office, Adobe)	Viele Gratis-Alternativen (LibreOffice, GIMP)
Gaming	Standard-Plattform	Dank Steam/Proton gut, aber nicht perfekt
Freiheit	Starr, kaum anpassbar	Extrem modular und nach Wunsch gestaltbar

Einsteiger-Empfehlungen

Wenn du Linux ausprobieren möchtest, ohne direkt ein Profi sein zu müssen, empfehlen Experten oft Linux Mint Cinnamon oder Ubuntu. Diese Systeme sehen Windows optisch ähnlich und lassen sich bequem per Maus bedienen.

Es gibt drei einfache Wege, Linux auszuprobieren, ohne dein bestehendes Windows-System zu gefährden. Der sicherste und flexibelste Weg ist das sogenannte **Live-System** via USB-Stick.

1. Der Klassiker: Das Live-System (USB-Stick)

Dies ist die beste Methode, um zu sehen, wie Linux auf deiner echten Hardware (WLAN, Grafikkarte, Drucker) funktioniert. Dein Windows bleibt dabei völlig unberührt.

1. **Vorbereitung:** Besorge dir einen leeren USB-Stick (mind. 8 GB).
2. **Download:** Lade eine Linux-Version (ISO-Datei) herunter, z. B. Linux Mint.
3. **Stick erstellen:** Nutze ein Tool wie Rufus oder Etcher, um die ISO-Datei auf den Stick zu „flashen“.
4. **Booten:** Starte deinen PC neu und drücke während des Hochfahrens eine Taste (oft F12, F10 oder F8), um das Boot-Menü zu öffnen und den **USB-Stick auszuwählen**.
5. **Testen:** Wähle „Linux ausprobieren“. Wenn du fertig bist, fährst du den PC einfach herunter und ziehst den Stick ab – beim nächsten Start ist alles wie vorher.

2. Die „Sandkasten“-Variante: Virtuelle Maschine

Wenn du Linux direkt unter Windows wie ein normales Programm in einem Fenster nutzen möchtest, ist eine virtuelle Maschine ideal.

- **Software:** Installiere ein Programm wie Oracle VirtualBox.
- **Vorteil:** Du kannst Linux und Windows **gleichzeitig** nutzen und Dateien zwischen beiden Welten austauschen.
- **Voraussetzung:** Dein PC sollte über genügend Arbeitsspeicher verfügen (empfohlen sind mind. 8 GB RAM insgesamt).

3. Für Schnelle: Das Windows Subsystem for Linux (WSL2)

Wenn es dir weniger um die Optik und mehr um die Linux-Werkzeuge geht, bietet Windows 10 und 11 eine eingebaute Funktion.

- **Installation:** Öffne das „Windows Terminal“ als Administrator und gib wsl --install ein.
- **Ergebnis:** Nach einem Neustart hast du ein vollwertiges Linux-Terminal (standardmäßig Ubuntu) direkt in Windows zur Verfügung.

Tipp für den Start: Probier es zuerst mit der **Live-USB-Methode** und Linux Mint. Es sieht Windows sehr ähnlich und ist extrem einsteigerfreundlich.

… ChatGPT

ChatGPT ist ein im November 2022 veröffentlichter **KI-Chatbot** des US-Unternehmens OpenAI. Er basiert auf einem sogenannten „Large Language Model“ (LLM) und ist darauf trainiert, menschenähnliche Gespräche zu führen, Fragen zu beantworten und Texte aller Art zu erstellen.

Was bedeutet der Name?

Der Name setzt sich aus zwei Teilen zusammen:

- **Chat**: Die Interaktion erfolgt über ein Dialogfenster, wie man es von Messengern kennt.
- **GPT**: Steht für *Generative Pre-trained Transformer*.
    - *Generative*: Er kann neue Inhalte (Texte, Codes, Bilder) erzeugen.
    - *Pre-trained*: Er wurde vorab mit riesigen Datenmengen aus dem Internet trainiert.
    - *Transformer*: Bezeichnet die technische Architektur (ein neuronales Netz), die Zusammenhänge in der Sprache besonders gut versteht.

Wie funktioniert es?

Technisch gesehen ist ChatGPT ein **„Next Token Predictor“**. Wenn du eine Frage stellst, berechnet das Modell Wort für Wort (bzw. in kleinen Einheiten, den „Tokens“), welches Wort statistisch gesehen am wahrscheinlichsten als nächstes folgt.

Wichtige Merkmale:

- **Kein echtes Wissen:** ChatGPT „weiß“ nichts im menschlichen Sinne; es erkennt lediglich Muster in den Trainingsdaten und berechnet Wahrscheinlichkeiten.
- **Vielseitigkeit:** Es kann Gedichte schreiben, Programmiercode verfassen, komplexe Themen einfach erklären oder beim Planen von Reisen helfen.
- **Halluzinationen:** Da das Modell auf Wahrscheinlichkeiten basiert, kann es Fakten frei erfinden, die jedoch sehr überzeugend klingen.

Wer steckt dahinter?

Entwickelt wurde das Tool von OpenAI unter der Leitung von **Sam Altman** (CEO) und **Mira Murati** (CTO). Das Unternehmen wird massiv von Microsoft unterstützt. Inzwischen nutzt ChatGPT modernste Modelle wie **GPT-4o** oder das aktuellste **GPT-5.2**

… ein Bot

Ein **Bot** (kurz für Robot) ist ein Computerprogramm, das **automatisierte Aufgaben** abarbeitet, die sich ständig wiederholen. Stell dir einen Bot wie einen digitalen Assistenten vor, der niemals schläft und Befehle viel schneller ausführen kann als ein Mensch.

Es gibt „gute“ und „weniger gute“ Bots, je nachdem, was ihr Ziel ist:

1. Die nützlichen Bots

- **Suchmaschinen-Bots (Crawler):** Google nutzt Bots, die das ganze Internet durchforsten, um Webseiten zu indexieren. Ohne sie würdest du bei einer Suche keine Ergebnisse finden.
- **Chatbots:** Diese begegnen dir oft im Kundenservice. Sie beantworten Standardfragen oder helfen dir bei einer Bestellung (wie z. B. ChatGPT).
- **Gaming-Bots:** In Videospielen steuern sie computergesteuerte Gegner oder Teammitglieder.

2. Die nervigen oder schädlichen Bots

- **Spam-Bots:** Sie fluten Kommentarspalten oder dein E-Mail-Postfach mit Werbung.
- **Social-Media-Bots:** Diese faken Likes, Abonnenten oder verbreiten massenhaft politische Meinungen, um Trends zu beeinflussen.
- **Scalper-Bots:** Das sind die Programme, die innerhalb von Sekunden Konzerttickets oder neue Playstation-Konsolen aufkaufen, bevor echte Fans eine Chance haben.

Wie erkennt man einen Bot?

Oft stößt du im Internet auf **CAPTCHAs** (diese kleinen Rätsel, bei denen du Ampeln oder Brücken anklicken musst). Diese sind genau dazu da, um Bots auszusperren, weil Programme (noch) Schwierigkeiten haben, Bilder wie ein Mensch zu interpretieren.

Wichtig zu wissen: Ein Bot ist keine künstliche Intelligenz (KI) an sich. Viele einfache Bots folgen nur einer starren „Wenn-Dann“-Logik. Erst moderne Chatbots nutzen KI, um menschliche Sprache wirklich zu verstehen.

Bist du im Netz schon mal auf ein Verhalten gestoßen, bei dem du dich gefragt hast: **„Ist das ein Mensch oder ein Bot?“**

... Everything

"Everything" ist ein extrem schnelles, kostenloses Suchprogramm für Windows, entwickelt von voidtools. Es dient als **effizienter Ersatz für die integrierte Windows-Suche**, da es Dateien und Ordner auf dem Computer in Sekundenbruchteilen findet.

Hier sind die wichtigsten Fakten zu Everything:

- **Funktionsweise:** Im Gegensatz zur Windows-Suche indiziert "Everything" nur Datei- und Ordnernamen (nicht den Inhalt) und nutzt dafür die Master File Table (MFT) von NTFS-Laufwerken.
- **Echtzeitsuche:** Sobald man den Suchbegriff eingibt, werden Ergebnisse sofort angezeigt. Es überwacht Änderungen im Dateisystem in Echtzeit, sodass neue Dateien sofort gefunden werden.
- **Schnelle Indizierung:** Die erste Indexierung dauert selbst bei einer Million Dateien meist nur etwa eine Minute.
- **Ressourcenschonend:** Das Programm ist sehr leichtgewichtig (weniger als 5 MB RAM).
- **Funktionen:** Es unterstützt Platzhalter (Wildcards), logische Operatoren (AND, OR, NOT) und reguläre Ausdrücke (Regex).
- **Portable Version:** Es ist keine Installation erforderlich; eine portable Version (ZIP-Archiv) kann direkt ausgeführt werden.

  Unterschied zur Windows-Suche:
  Während die Standard-Windows-Suche oft langsam ist und lange nach Inhalten sucht, ist "Everything" darauf spezialisiert, **Dateinamen** sofort zu finden, selbst wenn das System extrem unübersichtlich ist.

  Hinweis: Das Programm ist primär für NTFS-formatierte Laufwerke gedacht, kann aber auch andere Formate durchsuchen.

… Freefilesync

FreeFileSync ist ein kostenloses Open-Source-Tool zur Synchronisation und Datensicherung, das Ordner, Festplatten oder Netzwerklaufwerke (via FTP, SFTP, Google Drive) unter ***Windows, macOS und Linux*** abgleicht. Es vergleicht Inhalte nach Größe/Datum, spiegelt Daten und erkennt verschobene Dateien. Es ist einfach zu bedienen und ideal für Backups.

Wesentliche Funktionen und Eigenschaften:

- **Synchronisationsmethoden:** Es werden verschiedene Methoden wie "Zwei Wege", "Spiegeln" (Spiegelung) und "Aktualisieren" angeboten.
- **Unterstützte Speicherorte:** Es können lokale Ordner, externe Festplatten, USB-Sticks sowie Netzlaufwerke (über SFTP/FTP oder Google Drive) synchronisiert werden.
- **Datensicherung:** Es eignet sich gut, um Backups auf externen Festplatten oder NAS-Systemen zu erstellen.
- **Effizienz:** Die Software erkennt Änderungen und überträgt nur die notwendigen Daten, was Zeit spart.
- **Filterfunktionen:** Über Filter (F7) können bestimmte Dateien oder Ordner von der Synchronisation ausgeschlossen werden.
- **Kostenfrei:** Es ist Open-Source-Software, die jedoch durch Spenden finanziert wird.

FreeFileSync ist besonders nützlich, um Datenbestände zwischen verschiedenen Computern oder auf externe Speichermedien aktuell zu halten, ohne Dateien manuell kopieren zu müssen.

… Startpage

Startpage ist eine diskrete Suchmaschine aus den **Niederlanden**, die dir quasi das Beste aus zwei Welten bietet: die Suchergebnisse von **Google** und den Datenschutz einer anonymen Suche.

Hier ist das Wichtigste in Kürze:

- **Google-Power ohne Tracking:** Startpage fungiert als Schutzschild zwischen dir und Google. Deine Suchanfrage wird anonymisiert weitergeleitet, sodass Google weder deine IP-Adresse sieht noch ein Profil von dir erstellen kann.
- **Anonyme Ansicht:** Ein echtes Highlight ist die Funktion, Webseiten direkt über einen Proxy-Server von Startpage zu besuchen. So bleibst du auch nach dem Klick auf ein Suchergebnis für den Webseitenbetreiber unsichtbar.
- **Keine Filterblase:** Da keine persönlichen Daten gespeichert werden, erhältst du neutrale Ergebnisse, die nicht durch dein bisheriges Surfverhalten beeinflusst sind.
- **Top-Bewertungen:** Der Dienst wird regelmäßig für seinen Datenschutz gelobt und wurde von der Stiftung Warentest bereits als sicherste Suchmaschine ausgezeichnet.

Im Gegensatz zu Konkurrenten wie DuckDuckGo, die eigene Indizes oder Bing nutzen, setzt Startpage voll auf die gewohnte Google-Qualität, ohne dass du dabei "gläsern" wirst.

Das Einrichten von Startpage als Standardsuchmaschine funktioniert am einfachsten über die offizielle Add-on-Seite von Startpage, die deinen Browser automatisch erkennt.

Hier sind die gängigsten Methoden für verschiedene Browser:

1. Über die offizielle Startpage-Erweiterung (Empfohlen)

Besuche die Seite add.startpage.com. Dort wird dir direkt eine Schaltfläche wie **„Zu [Browsername] hinzufügen“** angezeigt.

- **Vorteil:** Die Erweiterung konfiguriert die Adresszeile automatisch so, dass alle Suchen über Startpage laufen.
- **Browser:** Funktioniert hervorragend für Google Chrome, Firefox und Microsoft Edge.

2. Manuelle Einrichtung (Ohne Erweiterung)

Wenn du keine Browser-Erweiterung installieren möchtest, kannst du Startpage in vielen Browsern manuell hinterlegen:

- **Firefox:** Rufe startpage.com auf, mache einen **Rechtsklick in die Adresszeile** und wähle **„Startpage-Suche hinzufügen“**. Danach kannst du sie in den Firefox-Einstellungen unter „Suche“ als Standard festlegen.
- **Chrome (Android/iOS):** Führe zuerst eine Suche auf der Webseite durch. Gehe dann in die **Einstellungen > Suchmaschine**; Startpage sollte dort nun unter den „kürzlich besuchten“ Seiten zur Auswahl stehen.

- **Brave:** Hier ist Startpage oft schon in der Liste der verfügbaren Suchmaschinen unter **Einstellungen > Suchmaschine** enthalten und muss nur ausgewählt werden.

3. Startpage als Startseite festlegen

Damit Startpage erscheint, sobald du ein neues Fenster öffnest:

- Kopiere die URL https://www.startpage.com.
- Gehe in die Browsereinstellungen zur Kategorie **Startseite** (oder „Darstellung“ bei Chrome).
- Wähle „Benutzerdefinierte Adresse“ und füge den Link ein.

Tipp: Falls du deine Sucheinstellungen (wie das Design oder die Region) ohne Cookies dauerhaft speichern willst, bietet Startpage auf seiner Einstellungsseite die Möglichkeit, eine spezielle **Einstellungs-URL** zu generieren.

Welchen **Browser** nutzt du gerade? Ich kann dir dann eine exakte Schritt-für-Schritt-Anleitung für dein Gerät geben.

… Calibre

Calibre ist eine kostenlose Open-Source-Software zur umfassenden **Verwaltung digitaler Buchsammlungen**. Es gilt in der E-Book-Community als das „Schweizer Taschenmesser“, da es nahezu jedes Dateiformat unterstützt und zahlreiche Funktionen unter einer Oberfläche vereint.

Die Software wird primär auf Desktop-Rechnern (Windows, macOS, Linux) genutzt und bietet folgende Kernfunktionen:

- **Bibliotheksverwaltung:** Organisieren von E-Books nach Titeln, Autoren, Verlagen oder eigenen Schlagwörtern.
- **Format-Konvertierung:** Umwandlung von E-Books in verschiedene Formate (z. B. von PDF zu EPUB oder MOBI), um sie auf unterschiedlichen Geräten wie dem Amazon Kindle oder Tolino lesbar zu machen.
- **Metadaten-Editor:** Automatisches Herunterladen von Buchcovern, Klappentexten und Bewertungen aus dem Internet.
- **Geräte-Synchronisation:** Einfaches Übertragen von Büchern auf E-Reader per USB-Kabel.
- **Integrierter Reader:** Direktes Lesen von E-Books am Computerbildschirm.
- **Nachrichten-Abruf:** Automatisches Umwandeln von RSS-Feeds oder Nachrichten-Webseiten in ein E-Book-Format für die spätere Lektüre.

Obwohl die Benutzeroberfläche oft als funktional und weniger modern empfunden wird, bleibt es aufgrund seiner Vielseitigkeit für viele E-Book-Nutzer unverzichtbar

… Native Alpha

Native Alpha ist eine quelloffene Android-App, mit der du jede beliebige Website in eine **vollwertige Web-App** (Web-Wrapper) verwandeln kannst.

Hier sind die wichtigsten Funktionen im Überblick:

- **Vollbild-Erlebnis:** Die Webseiten werden in einem randlosen Fenster ohne Browser-Menüleisten angezeigt, sodass sie sich wie echte native Apps anfühlen.
- **Datenschutz durch Sandboxing:** Die Premium-Version ermöglicht es, Web-Apps in isolierten „Sandboxes“ auszuführen. Das verhindert, dass Cookies oder andere Daten zwischen verschiedenen Web-Apps geteilt werden.
- **Individuelle Steuerung:** Du kannst für jede erstellte Web-App einzeln festlegen, ob JavaScript, Cookies oder der Zugriff auf Kamera und Standort erlaubt sind.
- **Performance:** Da die App das Android System WebView nutzt, ist sie oft deutlich ressourcensparender als das Installieren zahlreicher großer nativer Apps.

Die App ist als **Open-Source-Software** verfügbar und kann über das Cylonid-Repository auf GitHub oder spezialisierte App-Stores wie F-Droid (via IzzyOnDroid) bezogen werden.

… Samsung Good Lock

Samsung Good Lock ist eine offizielle, modulare Anwendungssammlung von Samsung, die tiefgreifende Personalisierungs- und Optimierungsmöglichkeiten für Galaxy-Smartphones bietet. Sie ermöglicht Nutzern, UI-Elemente wie Sperrbildschirm, Schnellleiste, Navigationsleiste, Tastatur und Homescreen (via Home Up) weit über die Standardeinstellungen hinaus anzupassen.

Die wichtigsten Fakten zu Good Lock:

- **Funktionsweise:** Die App fungiert als Oberfläche (Launcher) für verschiedene Module (Plugins), die einzeln heruntergeladen werden können, um Speicherplatz zu sparen.
- **Wichtige Module (Plugins):**
    - **LockStar:** Anpassung von Sperrbildschirm und Always-On-Display (AOD).
    - **QuickStar:** Individualisierung der Schnelleinstellungen und der oberen Statusleiste.
    - **Home Up:** Erweiterte Einstellungen für den Homescreen, Ordner und Animationen.
    - **NavStar:** Anpassung der Navigationsleiste (Buttons/Gesten).
    - **Theme Park:** Erstellen eigener Themes.
    - **Keys Cafe:** Umfassende Tastaturkonfiguration.
    - **One Hand Operation+:** Erweiterte Gestensteuerung.
- **Verfügbarkeit:** Hauptsächlich im **Samsung Galaxy Store** verfügbar, mit One UI 7 wird eine breitere Verfügbarkeit, auch im Google Play Store, erwartet. Es funktioniert auf den meisten Samsung Galaxy-Geräten.
- **Alternative:** In Regionen, in denen Good Lock nicht direkt im Store verfügbar ist, können Module über Apps wie *Fine Lock* oder *Nice Lock* genutzt werden.

Good Lock ist ideal für Nutzer, die ihr Samsung-Handy bis ins kleinste Detail an ihre eigenen Bedürfnisse anpassen möchten.

… die Entwickleroption bei Samsung

Die **Entwickleroptionen** sind ein verstecktes Menü in den Android-Einstellungen deines Samsung-Geräts, das zusätzliche Werkzeuge und Konfigurationen freischaltet. Ursprünglich sind sie dafür gedacht, dass Programmierer ihre Apps testen und debuggen können, aber auch für normale Nutzer bieten sie praktische Möglichkeiten.

Das kannst du mit den Entwickleroptionen machen:

- **Handy „schneller“ machen:** Du kannst die Geschwindigkeit der System-Animationen (z. B. beim App-Wechsel) halbieren oder ganz ausschalten, wodurch sich das Gerät deutlich reaktionsschneller anfühlt.
- **USB-Debugging:** Diese Funktion erlaubt es deinem PC, tiefgreifend mit deinem Handy zu kommunizieren – etwa um Daten zu retten, Apps manuell zu installieren oder das System zu sichern.
- **Bluetooth-Optimierung:** Du kannst feinere Einstellungen für Audio-Codecs oder die Bluetooth-Version vornehmen, um die Klangqualität oder Verbindung zu verbessern.
- **Simulierter Standort:** Du kannst Apps vorgaukeln, dass du dich an einem anderen Ort auf der Welt befindest.

So aktivierst du sie bei Samsung:

Da das Menü versteckt ist, musst du es erst „freischalten“:

1. Öffne die **Einstellungen** und gehe ganz unten auf **Telefoninfo**.
2. Tippe auf **Softwareinformationen**.
3. Tippe nun **7-mal schnell hintereinander** auf die **Buildnummer**.
4. Gib deine PIN ein – nun erscheint in den Haupteinstellungen ganz unten der neue Punkt **Entwickleroptionen**.

Sicherheitshinweis

Gehe vorsichtig mit den Einstellungen um. Während das bloße Aktivieren des Modus harmlos ist, können falsche Einstellungen die Systemstabilität beeinträchtigen oder bei aktiviertem **USB-Debugging** die Sicherheit deiner Daten verringern, wenn du das Handy an fremde Computer anschließt.

Gibt es diese Funktion auch bei Apple?

Nein, ein direktes Gegenstück zu den Android-Entwickleroptionen gibt es bei Apple in dieser Form **nicht**. Apple hält sein System (iOS) deutlich geschlossener.

Es gibt jedoch zwei Dinge, die in diese Richtung gehen:

1. Das „Entwickler“-Menü (Nur mit Mac/PC)

Apple blendet ein „Entwickler“-Menü in den iPhone-Einstellungen erst ein, wenn du das Gerät mit einem Mac verbindet, auf dem die Software **Xcode** (Apples Entwicklungsumgebung) läuft.

- **Was ist drin?** Hauptsächlich Tools zum Testen von Apps, Netzwerk-Simulationen (um schlechtes Internet zu testen) und Performance-Analysen.
- **Kein USB-Debugging:** Es gibt keine Funktion, die so weitreichend ist wie das USB-Debugging bei Android, um das Dateisystem komplett freizugeben.

2. Der „Entwicklermodus“ (Seit iOS 16)

Seit iOS 16 gibt es unter **Einstellungen > Datenschutz & Sicherheit** ganz unten den Punkt **Entwicklermodus**.

- **Zweck:** Dieser muss aktiviert werden, wenn man Apps installieren möchte, die nicht aus dem App Store stammen (z. B. selbst programmierte Apps oder Apps aus Firmen-Netzwerken).
- **Keine Tuning-Tools:** Im Gegensatz zu Samsung kannst du hier **keine** Animationen beschleunigen oder die Hardware-Leistung beeinflussen.

3. Bedienungshilfen (Der „Tuning“-Ersatz)

Wenn es dir darum geht, das iPhone (wie bei Samsung) „schneller“ zu machen, nutzt man bei Apple die **Bedienungshilfen**:

- Unter **Einstellungen > Bedienungshilfen > Bewegung > Bewegung reduzieren** kannst du die Zoomeffekte ausschalten. Das lässt das iPhone direkter und flotter wirken, ähnlich wie das Anpassen der Animationsgeschwindigkeit bei Android.

Kurz gesagt: Apple erlaubt dir nicht, „unter die Haube“ zu schauen, es sei denn, du bist ein registrierter App-Entwickler mit der entsprechenden Software auf dem Computer.

… PhotoSync

PhotoSync ist eine populäre, plattformübergreifende Anwendung, mit der Fotos und Videos drahtlos zwischen Mobilgeräten (Android/iOS), Computern (Windows/Mac/Linux), NAS-Geräten und Cloud-Diensten übertragen, gesichert und verwaltet werden können. Sie wird oft als flexible Alternative zu iCloud oder Google Fotos genutzt, um mehr Kontrolle über die Speicherung zu haben.

Hauptfunktionen und Vorteile von PhotoSync:

- **Drahtlose Übertragung:** Überträgt Fotos und Videos via Wi-Fi oder mobilen Hotspot zwischen Smartphones, Tablets und Computern.
- **Automatisches Backup:** Kann Aufnahmen automatisch im Hintergrund sichern, sobald ein festgelegtes Ziel (z.B. NAS, Cloud) erreicht wird.
- **Plattformübergreifend:** Funktioniert nahtlos zwischen Android und iOS sowie Mac und Windows.
- **Unterstützung von Cloud-Diensten:** Unterstützt eine Vielzahl von Cloud-Diensten wie Dropbox, Google Drive, OneDrive, Amazon Cloud Drive, SmugMug und Box.
- **Übertragung in voller Qualität:** Fotos und Videos werden in der Originalauflösung inklusive Metadaten (EXIF, Geodaten) übertragen.
- **Unterstützung für RAW-Formate:** Ermöglicht die Verwaltung von RAW-Bilddateien.
- **Kamera-Funktion:** Die Pro-Version bietet eine "PhotoSync Kamera", mit der direkt in der App Fotos aufgenommen werden, die sofort an das Ziel gesendet werden.

Wie funktioniert es?
Die App verwendet das lokale WLAN-Netzwerk, um Geräte direkt miteinander zu verbinden, ohne dass Fotos über externe Server im Internet umgeleitet werden müssen. Die Übertragung zum Computer ist oft kostenlos, während für erweiterte Cloud-Funktionen in der Regel eine Pro-Lizenz (Einmalkauf oder Abo) erforderlich ist.

… eine Echo Chamber

Eine **Echo Chamber** (deutsch: *Echokammer*) ist ein Umfeld – meist in sozialen Medien oder bestimmten Gruppen – in dem Menschen fast nur noch Meinungen hören, die ihre eigene Sichtweise bestätigen.

Warum heißt das so?

Wie in einer echten Kammer mit Echo:
Du sagst etwas – und bekommst im Grunde nur deine eigene Meinung zurückgespiegelt.

Typisches Beispiel

In sozialen Netzwerken wie:

- Facebook
- X
- YouTube

zeigen Algorithmen häufig Inhalte, die zu deinem bisherigen Klick- und Like-Verhalten passen.
Dadurch siehst du überwiegend Beiträge, die deine Überzeugungen bestätigen – andere Perspektiven tauchen kaum noch auf.

Was passiert dabei?

In einer Echokammer:

- Eigene Meinung wird ständig bestätigt
- Kritik oder Gegenargumente werden ausgeblendet
- Extreme Positionen können sich verstärken
- Gruppen fühlen sich „im Recht“ und geschlossen

Das kann zu **Polarisierung** führen – also zu stärkerer gesellschaftlicher Spaltung.

Unterschied zu „Filterblase“

- **Filterblase** → entsteht technisch durch Algorithmen
- **Echo Chamber** → entsteht sozial, durch Austausch gleichdenkender Menschen

Oft wirken beide Effekte zusammen.

… der Idetity Leak Checker

Der **Identity Leak Checker (ILC)** ist ein kostenloses Online-Tool des Hasso-Plattner-Instituts (HPI), mit dem Sie überprüfen können, ob Ihre persönlichen Daten (wie E-Mail-Adressen oder Passwörter) durch Datenpannen im Internet veröffentlicht wurden.

So funktioniert der Dienst

- **Eingabe:** Sie geben auf der offiziellen Webseite Ihre E-Mail-Adresse ein.
- **Abgleich:** Das System gleicht diese Adresse mit einer riesigen Datenbank ab, die über **14,5 Milliarden kompromittierte Nutzerkonten** aus fast 2.000 bekannten Datenleaks enthält (Stand März 2026).
- **Ergebnis:** Sie erhalten eine detaillierte Antwort per E-Mail. Darin wird aufgelistet, welche Art von Daten (z. B. Passwort, Geburtsdatum, Telefonnummer) in welchem Leak aufgetaucht sind.

Warum ist das wichtig?

Hacker nutzen solche „Leaked Credentials“, um sich Zugang zu anderen Konten zu verschaffen (Credential Stuffing), Identitätsdiebstahl zu begehen oder gezielte Phishing-Angriffe durchzuführen. Wenn Ihre Daten in der Liste auftauchen, sollten Sie sofort die Passwörter der betroffenen Dienste ändern und, falls möglich, eine **Zwei-Faktor-Authentisierung (2FA)** aktivieren.

Alternativen und Ergänzungen

Neben dem deutschen Angebot des HPI gibt es weitere seriöse Dienste:

- Have I Been Pwned?: Der weltweit bekannteste Dienst des Sicherheitsforschers Troy Hunt.
- Leak Checker der Uni Bonn: Ein ähnliches akademisches Projekt aus Deutschland.

… Swiss Transfer

SwissTransfer ist ein kostenloser Online-Dienst zum sicheren Versenden großer Dateien, der vom Schweizer Webhosting-Anbieter **Infomaniak** betrieben wird. Er gilt als eine der bekanntesten europäischen Alternativen zu Diensten wie WeTransfer.

Hier sind die wichtigsten Merkmale des Dienstes:

- **Hohe Kapazität:** Sie können Dateien mit einer Größe von bis zu **50 GB** pro Übertragung versenden.
- **Keine Anmeldung erforderlich:** Der Dienst kann direkt im Browser ohne das Erstellen eines Benutzerkontos genutzt werden.
- **Datenschutz & Standort:** Alle Daten werden auf Servern in der **Schweiz** gespeichert, was eine hohe Datensicherheit und DSGVO-Konformität gewährleistet.
- **Flexibilität:** Der Versand ist sowohl per **E-Mail** als auch über einen direkt generierten **Link** möglich.
- **Zusatzfunktionen:** Nutzer können Übertragungen mit einem **Passwort** schützen, ein Ablaufdatum festlegen (bis zu 30 Tage Gültigkeit) oder die Anzahl der Downloads beschränken.
- **Verfügbarkeit:** Neben der Web-Version gibt es auch Apps für iOS und Android.

Der Dienst finanziert sich laut Infomaniak durch deren andere kostenpflichtige Produkte, wodurch SwissTransfer selbst werbefrei und ohne den Verkauf von Nutzerdaten bleibt.

… ein QR-Code

Ein **QR-Code** (steht für „Quick Response“, also „schnelle Antwort“) ist ein **zweidimensionaler Barcode**, der Informationen in einer quadratischen Matrix aus schwarzen und weißen Punkten speichert.

Im Gegensatz zum herkömmlichen Strichcode (1D), der nur horizontal gelesen wird, speichert ein QR-Code Daten sowohl horizontal als auch vertikal. Dadurch kann er deutlich mehr Informationen enthalten, wie etwa lange URLs, Kontaktdaten oder WLAN-Zugänge.

Die wichtigsten Fakten im Überblick:

- **Herkunft:** Er wurde **1994** von der japanischen Firma **Denso Wave** (einer Toyota-Tochter) entwickelt, um Autoteile in der Produktion effizienter zu verfolgen.
- **Aufbau:** Die drei markanten **Quadrate in den Ecken** dienen dem Scanner zur Orientierung, damit der Code aus jedem Winkel korrekt gelesen werden kann.
- **Fehlerkorrektur:** Ein QR-Code funktioniert oft selbst dann noch, wenn er bis zu **30 % beschädigt** oder verschmutzt ist.
- **Inhalt:** Er kann bis zu **4.296 Zeichen** oder 7.089 Ziffern speichern.
- **Nutzung:** Heutzutage verfügen fast alle Smartphones über eine integrierte Scan-Funktion in der Kamera-App.

… der „Kartoffel-Test“

Man kann die Kommunikation mit einem KI-Bot oft an bestimmten Mustern im Schreibstil, der Reaktionsgeschwindigkeit und der Art der Argumentation erkennen. Da moderne KI-Modelle jedoch immer menschlicher wirken, hilft meist eine Kombination aus Beobachtung und gezielten Fangfragen.

1. Sprachliche Merkmale

- **Perfekte Grammatik und Rechtschreibung:** während Menschen beim Tippen oft Flüchtigkeitsfehler machen oder Abkürzungen nutzen, schreiben Bots meist in fehlerfreiem, fast schon zu korrektem Deutsch.
- **Wiederholungen und Floskeln:** KI neigt dazu, bestimmte Phrasen oder Satzstrukturen häufig zu wiederholen oder sehr förmlich und allgemein zu klingen.
- **Fehlende Empathie mit Tiefgang:** Bots können zwar Empathie vortäuschen (z. B. „Es tut mir leid zu hören...“), diese wirkt aber oft oberflächlich oder formelhaft.
- **Mangel an Humor oder Sarkasmus:** Komplexe Witze, Ironie oder feine sprachliche Nuancen werden von KI-Systemen oft nicht oder nur sehr flach verstanden.

2. Technisches Verhalten

- **Unnatürliche Geschwindigkeit:** Ein Bot antwortet oft sofort mit langen, perfekt formatierten Textblöcken, was die menschliche Tippgeschwindigkeit bei weitem übersteigt.
- **Verzögerungen bei Sprach-Bots:** Bei Telefonaten brauchen KI-Systeme manchmal einen Moment, um das Gesagte zu verarbeiten, was zu kurzen, unnatürlichen Pausen vor jeder Antwort führt.
- **Profil-Checks:** In sozialen Medien haben Bots oft generische Namen, keine Biografie oder nutzen KI-generierte Profilbilder, die bei genauerem Hinsehen Fehler (z. B. bei Haaren oder Hintergründen) aufweisen.

3. Gezielte Testfragen

Um einen Bot zu entlarven, kannst du versuchen, ihn aus seinem programmierten Schema zu locken:

- **Fangfragen mit erfundenen Fakten:** Stelle eine Frage zu einem Ereignis, das nie stattgefunden hat (z. B. „Was sagst du zum Sieg der deutschen Nationalmannschaft bei der WM 2025?“). Eine KI könnte anfangen zu halluzinieren und eine plausible Antwort erfinden (ja, das geht).
- **Themenwechsel:** Springe mitten im Satz zu einem völlig anderen Thema. Viele Bots verlieren dann den Faden oder reagieren verwirrt.
- **Visuelle Tests:** Sende eine Video-Nachricht oder ein Bild und frage nach Details daraus. Einfache Automatisierungen können den Inhalt oft nicht „sehen“.

- **Der „Kartoffel-Test“:** Bitte das Gegenüber, ein völlig unzusammenhängendes Wort wie „Kartoffel“ oder einen spezifischen Satz zu schreiben, um zu beweisen, dass es kein Skript ist.

... ein VPN

Ein **VPN** steht für „Virtual Private Network“ (virtuelles privates Netzwerk). Kurz gesagt: Es sorgt dafür, dass deine Internetverbindung **verschlüsselt und über einen anderen Server geleitet** wird.

So funktioniert’s in der Praxis:

- Normalerweise gehst du direkt von deinem Gerät ins Internet
- Mit VPN gehst du zuerst zu einem VPN-Server
- Von dort wird deine Anfrage weitergeleitet

Dadurch passiert Folgendes:

1. Deine Daten werden verschlüsselt
Niemand im selben WLAN (z. B. im Café oder Hotel) kann einfach mitlesen, was du machst.

2. Deine IP-Adresse wird „versteckt“
Websites sehen nicht deine echte IP, sondern die des VPN-Servers. Dadurch wirkst du z. B. so, als wärst du in einem anderen Land.

3. Mehr Privatsphäre
Dein Internetanbieter kann schwerer nachvollziehen, welche Seiten du genau besuchst.

Typische Gründe, ein VPN zu nutzen:

- Sicher surfen in öffentlichen WLANs
- Geoblocking umgehen (z. B. Inhalte aus anderen Ländern anschauen)
- Mehr Anonymität im Netz
- Zugriff auf Firmennetzwerke von unterwegs

Aber wichtig:
Ein VPN macht dich **nicht komplett anonym**. Anbieter selbst könnten theoretisch Daten sehen, und manche Websites erkennen VPNs trotzdem.

... VoIP

VoIP steht für „Voice over Internet Protocol“ – also **Telefonieren über das Internet statt über klassische Telefonleitungen**.

Statt dass deine Stimme über das alte Telefonnetz läuft, passiert bei VoIP Folgendes:

- Deine Stimme wird in **digitale Datenpakete** umgewandelt
- Diese werden über das Internet verschickt
- Beim Empfänger wieder in Ton zurückverwandelt

Einfaches Beispiel

Wenn du z. B. über Apps wie WhatsApp, Skype oder Zoom telefonierst, nutzt du VoIP – oft ohne es zu merken.

Vorteile von VoIP

- **Günstiger** als klassische Telefonie (vor allem international)
- **Flexibel** – funktioniert auf Handy, Laptop oder Tablet
- **Zusatzfunktionen** wie Videoanrufe, Konferenzen, Bildschirmfreigabe

Nachteile

- **Abhängig vom Internet** – schlechte Verbindung = schlechte Qualität
- Kann **Verzögerungen oder Aussetzer** geben
- Notrufe sind manchmal komplizierter als bei Festnetz

Unterschied zu VPN (falls du vergleichst)

- **VoIP** = *wie* du kommunizierst (Telefon über Internet)
- **VPN** = *wie sicher / über welchen Weg* deine Daten gehen

Privat lohnt sich **VoIP** nicht immer automatisch – aber in bestimmten Situationen ist es richtig praktisch.

Sinnvoll ist VoIP für dich, wenn:

1. Du viel ins Ausland telefonierst
Mit Apps wie WhatsApp oder Skype kannst du kostenlos oder sehr günstig weltweit telefonieren – solange beide Internet haben.

2. Du sowieso viel über Apps kommunizierst
Wenn du eh Messenger nutzt, ist VoIP quasi schon integriert. Du brauchst keinen extra Telefonanschluss mehr.

3. Du oft im WLAN bist (z. B. zuhause oder unterwegs)
Dann sparst du mobile Daten und Telefonkosten, besonders bei längeren Gesprächen oder Videoanrufen (z. B. mit Zoom).

4. Du flexibel bleiben willst
Du kannst auf verschiedenen Geräten telefonieren – Handy, Laptop, Tablet – egal wo du bist.

Weniger sinnvoll ist es, wenn:

1. Deine Internetverbindung instabil ist
Dann nerven Aussetzer oder schlechte Sprachqualität.

2. Du nur selten telefonierst
Dann bringt dir der Umstieg kaum Vorteile.

3. Du Wert auf absolut zuverlässige Erreichbarkeit legst
Für Notrufe oder wichtige Gespräche ist klassisches Telefon oft stabiler.

Kurz gesagt:

- **Lohnt sich:** Viel Internetnutzung + internationale Kontakte + Messenger ohnehin im Einsatz
- **Weniger nötig:** Wenig telefonieren + schlechtes Internet + einfache Nutzung reicht dir

… eine SSD

Eine **SSD** (Solid-State-Drive) ist ein modernes Speichermedium für Computer, das die klassische mechanische Festplatte (HDD) weitgehend ersetzt hat. Der entscheidende Unterschied: Während eine HDD Daten auf rotierenden Magnetscheiben speichert, nutzt eine SSD **Flash-Speicher-Chips** – ähnlich wie ein USB-Stick, nur viel schneller und langlebiger.

Warum sind SSDs so beliebt?

- **Extreme Geschwindigkeit**: Da keine mechanischen Teile bewegt werden müssen, kann die SSD sofort auf Daten zugreifen. Das sorgt für blitzschnelle Systemstarts und kurze Ladezeiten in Programmen und Spielen.
- **Robustheit**: Ohne bewegliche Teile sind SSDs unempfindlich gegenüber Erschütterungen oder Stürzen, was sie ideal für Laptops macht.
- **Geräuschlosigkeit**: Eine SSD arbeitet völlig lautlos, während HDDs oft ein leises Surren oder Rattern von sich geben.
- **Energieeffizienz**: Sie verbrauchen weniger Strom, was die Akkulaufzeit mobiler Geräte verlängert.

Die Technik dahinter

Im Inneren einer SSD arbeiten zwei Hauptkomponenten:

1. **NAND-Flash-Speicher**: Hier werden die eigentlichen Daten in Form elektrischer Ladungen gespeichert.
2. **Controller**: Er fungiert als „Gehirn“ der SSD, verwaltet die Datenströme und sorgt dafür, dass die Speicherzellen gleichmäßig abgenutzt werden.

Gibt es auch Nachteile?

- **Preis**: Pro Gigabyte sind SSDs teurer als herkömmliche HDDs, auch wenn die Preise stetig sinken.
- **Verschleiß**: Flash-Zellen lassen sich nur eine begrenzte Anzahl oft beschreiben. Moderne SSDs halten bei normaler Nutzung jedoch problemlos **5 bis 10 Jahre** oder länger.

… ein persönlicher Hotspot

Ein **persönlicher Hotspot** (auch „Mobiler Hotspot“ oder „Tethering“ genannt) ist eine Funktion deines Smartphones oder Tablets, die das Gerät in einen kleinen, tragbaren WLAN-Router verwandelt.

Dabei nutzt das Handy seine eigene mobile Datenverbindung (z. B. LTE oder 5G), um ein WLAN-Signal für andere Geräte in der Nähe bereitzustellen. So können Geräte ohne eigene SIM-Karte – wie Laptops oder Tablets – überall dort im Internet surfen, wo dein Handy Mobilfunkempfang hat.

Wie funktioniert es?

1. **Aktivierung**: Du schaltest die Funktion in den Einstellungen deines Handys (oft unter „Verbindungen“ oder „Mobiles Netz“) ein.
2. **Sicherheit**: Du legst einen Netzwerknamen (SSID) und ein sicheres Passwort fest, damit nur befugte Personen mitsurfen können.
3. **Verbindung**: Das andere Gerät sucht nach WLAN-Netzwerken, findet dein Handy und verbindet sich nach Eingabe des Passworts.

Die wichtigsten Vor- und Nachteile

- **Vorteile**:
    - **Internet überall**: Ideal für Reisen, im Zug oder im Café, wenn kein öffentliches WLAN verfügbar ist.
    - **Sicherheit**: Ein eigener Hotspot ist sicherer als unverschlüsselte öffentliche WLAN-Netzwerke.
    - **Mehrere Geräte**: Du kannst meist mehrere Geräte gleichzeitig verbinden.
- **Nachteile**:
    - **Datenverbrauch**: Alle verbundenen Geräte verbrauchen das Inklusiv-Volumen deines Mobilfunktarifs.
    - **Akku-Fresser**: Die Funktion benötigt viel Energie und leert den Handy-Akku deutlich schneller.
    - **Geschwindigkeit**: Die Surf-Geschwindigkeit hängt stark von deinem aktuellen Mobilfunkempfang ab.

Tipp: Schalte den Hotspot nach der Nutzung wieder aus, um deinen **Akku** und dein **Datenvolumen** zu schonen.

… ein Passkey

Ein **Passkey** ist eine moderne, passwortlose Alternative zur klassischen Anmeldung bei Webseiten oder Apps. Er soll das herkömmliche Passwort langfristig ersetzen, da er deutlich sicherer und bequemer ist.

Wie funktioniert das?

Anstatt sich eine komplexe Zeichenfolge zu merken, nutzt ein Passkey die **biometrischen Merkmale** deines Geräts (wie FaceID, TouchID oder den Fingerabdrucksensor) oder die **PIN**, mit der du dein Gerät entsperrst.

Technisch gesehen basiert ein Passkey auf Kryptografie:

1. **Privater Schlüssel**: Dieser bleibt sicher auf deinem Gerät gespeichert und wird niemals geteilt.
2. **Öffentlicher Schlüssel**: Dieser liegt auf dem Server des Dienstes (z. B. Google oder Amazon).
   Eine Anmeldung funktioniert nur, wenn beide Teile mathematisch zusammenpassen – was durch deine Biometrie bestätigt wird.

Die Vorteile gegenüber Passwörtern

- **Phishing-resistent**: Da der Passkey fest an eine Webseite oder App gebunden ist, kannst du ihn nicht versehentlich auf einer gefälschten Betrüger-Seite eingeben.
- **Kein Merken mehr**: Du musst dir keine langen Passwörter mehr ausdenken oder merken.
- **Sicher vor Server-Hacks**: Wenn eine Firma gehackt wird, können Diebe nichts mit dem dort gespeicherten „öffentlichen Schlüssel“ anfangen, da dein privater Schlüssel sicher auf deinem Handy oder Computer bleibt.

Wo werden Passkeys gespeichert?

Passkeys werden meistens in der **Cloud** deines Betriebssystems gespeichert (z. B. im iCloud-Schlüsselbund bei Apple oder im Google Passwort-Manager bei Android). Dadurch sind sie auf allen deinen Geräten verfügbar, solange du mit deinem Hauptkonto angemeldet bist.

Hier ist eine kurze Anleitung, wie du **Passkeys** bei den gängigsten Diensten einrichtest. In der Regel musst du dich einmalig klassisch mit deinem Passwort anmelden, um die Funktion zu aktivieren.

1. Google (für Gmail, YouTube etc.)

Google ermöglicht es dir, Passkeys direkt für dein gesamtes Konto zu nutzen.

- Öffne die Google Passkey-Seite in deinem Browser.
- Klicke auf **„Passkey erstellen“**.

- Bestätige die Einrichtung mit deiner Displaysperre (Fingerabdruck, Gesicht oder PIN).
- Alternativ findest du die Option in deinem Google-Konto unter dem Reiter **„Sicherheit“** → **„Passkeys und Sicherheitsschlüssel“**.

2. Amazon

Amazon bietet Passkeys als sichere Login-Option in den Kontoeinstellungen an.

- Logge dich bei Amazon ein und gehe zu **„Mein Konto“**.
- Wähle **„Anmelden und Sicherheit“**.
- Suche den Punkt **„Passkey“** und klicke daneben auf **„Einrichten“**.
- Folge den Bildschirmanweisungen, um dein Gerät zu verknüpfen.

3. PayPal

Bei PayPal kannst du Passkeys sowohl im Browser als auch in der App aktivieren.

- **Im Browser:** Gehe zu den Sicherheitseinstellungen und klicke auf **„Passkeys“** → **„Verwalten“**.
- **In der App:** Tippe auf dein Profil-Icon oder das Menü, gehe zu **„Login und Sicherheit“** und wähle **„Passkey“**.
- Klicke auf **„Passkey erstellen“** und bestätige dies mit deiner biometrischen Sperre.

Wichtig zu wissen

- **Synchronisation:** Wenn du ein iPhone nutzt, werden Passkeys im **iCloud-Schlüsselbund** gespeichert; bei Android im **Google Passwort-Manager**. So sind sie automatisch auf deinen anderen Geräten desselben Herstellers verfügbar.
- **Voraussetzung:** Dein Gerät muss eine Displaysperre (PIN, Muster, Fingerabdruck oder Gesichtserkennung) aktiv haben.

… ein Notch

Ein **Notch** (englisch für „Kerbe“ oder „Einkerbung“) bezeichnet die kleine Aussparung am oberen Rand eines Smartphone-Displays oder Laptop-Bildschirms.

Dort wird der Bildschirm unterbrochen, um Platz für wichtige Hardware-Komponenten zu schaffen, ohne den Rand (Bezel) des Geräts insgesamt dicker machen zu müssen.

Was steckt im Notch?

Meistens befinden sich darin:

- Die **Frontkamera** (für Selfies und Videocalls).
- **Sensoren** für die Gesichtserkennung (wie FaceID beim iPhone).
- Der **Näherungssensor** (der das Display ausschaltet, wenn du das Handy ans Ohr hältst).
- Der **Umgebungslichtsensor** zur automatischen Helligkeitssteuerung.

Warum gibt es ihn überhaupt?

Die Hersteller möchten die Vorderseite des Geräts fast vollständig mit dem Display füllen (**„Edge-to-Edge“**). Da die Technik für Kameras und Sensoren unter dem Display lange Zeit nicht gut genug war, war der Notch der Kompromiss: Man zieht das Display so weit wie möglich nach oben und lässt nur eine kleine „Insel“ für die Technik frei.

Die Entwicklung

- **Der Klassiker:** Bekannt wurde der Notch vor allem durch das **iPhone X** (2017).
- **Waterdrop-Notch:** Eine sehr kleine, tropfenförmige Aussparung, die oft nur die Kamera enthält.
- **Punch-Hole:** Ein freistehendes „Loch“ im Display (oft bei Samsung oder Google Pixel).
- **Dynamic Island:** Apples Weiterentwicklung beim iPhone, bei der Software-Elemente den Notch umspielen und ihn für Benachrichtigungen nutzen.

... ein Hoax

Ein **Hoax** (englisch für „Schabernack“, „Scherz“ oder „Schwindel“) ist eine bewusst in Umlauf gebrachte Falschmeldung. Im Gegensatz zu reiner Desinformation, die oft politische Ziele verfolgt, zielt ein Hoax meist darauf ab, Menschen zu täuschen, zu erschrecken oder sie dazu zu bringen, eine Nachricht massenhaft weiterzuleiten.

Typische Merkmale eines Hoax

Sie erkennen einen Hoax oft an diesen Anzeichen:

- **Aufforderung zur Weiterleitung**: Es wird massiv dazu aufgerufen, die Nachricht an möglichst viele Freunde oder Kontakte zu senden („Bitte teilen!“).
- **Dringlichkeit oder Drohung**: Es wird oft Zeitdruck aufgebaut oder mit negativen Konsequenzen gedroht, falls man die Nachricht nicht teilt.
- **Vage Zeitangaben**: Statt eines konkreten Datums werden Begriffe wie „gestern“ oder „ab nächstem Montag“ verwendet, damit die Meldung jahrelang aktuell wirkt.
- **Fehlende Quellen**: Es gibt keine seriösen Belege oder Links zu offiziellen Stellen oder Nachrichtenportalen.

Klassische Beispiele

- **Falsche Warnungen**: Meldungen über angebliche Computerviren (die man durch das Löschen wichtiger Systemdateien selbst „bekämpfen“ soll) oder Warnungen vor vergifteten Werbegeschenken.
- **Angebliche Kosten**: Nachrichten, die behaupten, dass Dienste wie WhatsApp oder Facebook bald kostenpflichtig werden, es sei denn, man leitet die Warnung weiter.
- **Mitleids-Hoaxes**: Berichte über schwer kranke Kinder, für deren Heilung ein Konzern angeblich pro „Geteilt“-Klick Geld spendet.

Abgrenzung zu anderen Begriffen

Begriff	Kerninhalt
Fake News	Gezielte politische oder manipulative Desinformation.
Urban Legend	„Moderne Sagen“ (wie die Spinne in der Yucca-Palme), die eher als unterhaltsame Gruselgeschichten weitererzählt werden.
Phishing	Betrugsversuche, bei denen Kriminelle versuchen, Passwörter oder Bankdaten abzugreifen.

Tipp: Wenn Sie eine verdächtige Nachricht erhalten, kopieren Sie einen markanten Satz daraus in eine Suchmaschine zusammen mit dem Wort „Hoax“. Seiten wie der Verbraucherzentrale Phishing-Radar oder das BSI entlarven solche Meldungen meist sehr schnell.

… ein Meme

Ein **Meme** (ausgesprochen: *Miem*) ist im Grunde ein Insider-Witz des Internets, der sich rasend schnell verbreitet. Meistens handelt es sich um ein Bild, ein Video oder einen kurzen Text, das von anderen aufgegriffen, leicht abgewandelt und immer wieder neu geteilt wird.

Hier sind die wichtigsten Merkmale:

- **Wiedererkennung**: Ein Meme nutzt oft ein bekanntes Bild (z. B. ein lustiges Tier oder eine Filmszene), das eine ganz bestimmte Emotion oder Situation ausdrückt.
- **Variation**: Der Witz entsteht dadurch, dass Leute den Text ändern, um ihn auf ihren eigenen Alltag oder aktuelle Ereignisse zu beziehen.
- **Kulturphänomen**: Memes sind die „Sprache“ sozialer Medien (Instagram, TikTok, Reddit). Sie kommentieren oft sarkastisch oder humorvoll Politik, Gesellschaft oder banale Alltagsprobleme.

Woher kommt das Wort?

Der Begriff stammt ursprünglich gar nicht aus dem Internet, sondern von dem Evolutionsbiologen **Richard Dawkins** (1976). Er bezeichnete damit eine kulturelle Idee, die sich wie ein Gen von Mensch zu Mensch verbreitet und dabei mutiert.

Berühmte Beispiele

- **Grumpy Cat**: Die Katze mit dem chronisch schlecht gelaunten Gesichtsausdruck.
- **Distracted Boyfriend**: Der Mann, der einer Frau hinterherguckt, während seine Freundin ihn empört ansieht.
- **Rickrolling**: Ein Video-Link, der vorgibt, etwas Spannendes zu sein, aber dann das Musikvideo von Rick Astley abspielt.

… ein haptisches Feedback

Ein **haptisches Feedback** (oder haptische Rückmeldung) ist die spürbare Antwort eines Geräts auf eine Eingabe von dir.

Statt nur etwas auf einem Bildschirm zu sehen oder zu hören, **fühlst** du eine Vibration oder einen kurzen Widerstand. Das simuliert das Gefühl eines echten, physischen Knopfes, auch wenn du eigentlich nur eine glatte Glasfläche berührst.

Wo begegnet dir das im Alltag?

- **Smartphones**: Wenn du eine Nachricht tippst und bei jedem Buchstaben ein minimales Vibrieren spürst, oder wenn das Handy kurz „klopft“, wenn du einen Regler verschiebst.
- **Controller (Gaming)**: Wenn der Controller bei einer Explosion im Spiel heftig rüttelt oder der Abzugswiderstand sich verändert (z. B. beim PS5-Controller).
- **Trackpads**: Bei modernen Laptops (wie dem MacBook) bewegt sich das Touchpad gar nicht mehr mechanisch. Ein kleiner Motor im Inneren erzeugt ein so präzises haptisches Feedback, dass dein Gehirn glaubt, du hättest einen echten Klick gemacht.

Warum macht man das?

- **Bestätigung**: Du weißt sofort, dass das Gerät deinen Befehl registriert hat, ohne hinsehen zu müssen.
- **Immersion**: In Spielen macht es das Erlebnis realistischer (z. B. das Gefühl von Regen oder Schritten).
- **Barrierefreiheit**: Menschen mit Sehbehinderung erhalten so wichtige Signale über den Zustand des Geräts.

Der Unterschied zur normalen Vibration

Früher gab es meist nur plumpe Vibrationsmotoren, die einfach das ganze Gerät geschüttelt haben. Modernes haptisches Feedback ist **präzise und nuanciert** – es fühlt sich eher wie ein Tippen, Klopfen oder Klicken an als wie ein klassisches Summen.

… eine Drittanbietersperre

Eine **Drittanbietersperre** ist ein kostenloser Schutzmechanismus deines Mobilfunkanbieters, der verhindert, dass externe Unternehmen Geld über deine Handyrechnung abbuchen können.

Warum ist das sinnvoll?

Sie dient vor allem als Schutz vor sogenannten **Abofallen**. Ohne Sperre kann es passieren, dass ein unvorsichtiger Klick auf einen Werbebanner oder einen Link in einer App ausreicht, um ein kostenpflichtiges Abo (z. B. für Spiele, Klingeltöne oder Erotik-Inhalte) abzuschließen. Der Betrag taucht dann einfach am Ende des Monats auf deiner Mobilfunkrechnung auf.

Was genau wird gesperrt?

Wenn die Sperre aktiv ist, können folgende Dienste nicht mehr über die Handyrechnung bezahlt werden:

- **Abos & Downloads**: Klingeltöne, Wallpaper oder mobile Spiele.
- **In-App-Käufe**: Käufe in Stores wie Google Play oder dem Apple App Store.
- **Service-Dienste**: Parkscheine, ÖPNV-Tickets oder Spenden via SMS.

Wichtig: Du kannst diese Dinge oft immer noch nutzen, musst dann aber eine andere Bezahlmethode wie Kreditkarte oder PayPal hinterlegen.

Wie richtest du sie ein?

Mobilfunkanbieter wie die Telekom, Vodafone oder O2 sind gesetzlich verpflichtet, diese Sperre auf Wunsch kostenlos einzurichten. Das geht meistens:

1. **Online** im Kundenportal deines Anbieters.
2. In der jeweiligen **Service-App** (z. B. "Mein O2" oder "MeinMagenta").
3. Über die **Kunden-Hotline** deines Mobilfunknetzes.

Oft kannst du auch nur **bestimmte Kategorien** (z. B. nur Abos oder nur Erotik) sperren lassen, damit du praktische Dinge wie Parktickets weiterhin über das Handy bezahlen kannst.

… ein Cookie

Ein **Cookie** (englisch für „Plätzchen“) ist eine kleine Textdatei, die eine Webseite auf deinem Gerät (Computer, Handy oder Tablet) speichert, wenn du sie besuchst.

Stell dir einen Cookie wie eine Art **digitalen Merkzettel** vor. Er hilft der Webseite dabei, dich wiederzuerkennen und sich bestimmte Informationen über deinen Besuch zu merken.

Wofür werden Cookies genutzt?

Es gibt drei Hauptgründe, warum Webseiten Cookies einsetzen:

1. **Funktionalität (Notwendige Cookies)**: Ohne sie würden viele Seiten nicht funktionieren. Sie merken sich zum Beispiel, dass du eingeloggt bist oder welche Produkte du bereits in den **Warenkorb** gelegt hast, während du weiter auf der Seite stöberst.

2. **Einstellungen**: Hier werden Dinge wie deine bevorzugte **Sprache**, das Design (Dark Mode) oder deine Region gespeichert, damit du sie nicht bei jedem Besuch neu einstellen musst.

3. **Tracking & Werbung**: Diese Cookies verfolgen dein Surfverhalten über mehrere Webseiten hinweg. So können Firmen Profile erstellen, um dir **personalisierte Werbung** anzuzeigen (z. B. wenn du Schuhe suchst und danach auf allen anderen Seiten Schuh-Werbung siehst).

Sind Cookies gefährlich?

Nein, Cookies sind an sich keine Viren oder Schadprogramme. Sie können keine Dateien auf deiner Festplatte lesen. Das Problem ist eher der **Datenschutz**: Da Tracking-Cookies dein Verhalten genau analysieren können, empfinden viele Nutzer dies als Eingriff in ihre Privatsphäre.

Was hat es mit den Bannern auf sich?

Wegen strenger Gesetze (wie der DSGVO) müssen Webseiten dich heute meistens fragen, welche Cookies sie speichern dürfen. Deshalb siehst du fast überall diese **Cookie-Banner**, auf denen du „Alle akzeptieren“ oder „Ablehnen“ klicken kannst.

Tipp: In deinen Browser-Einstellungen (Chrome, Safari, Firefox) kannst du jederzeit alle gespeicherten Cookies löschen oder einstellen, dass Tracking-Cookies automatisch blockiert werden.

… Clickbait

Clickbait (von englisch *click* für Klick und *bait* für Köder) bezeichnet Inhalte im Internet, die mit reißerischen Überschriften oder Bildern Nutzer dazu verleiten sollen, einen Link anzuklicken.

Das Ziel ist es, möglichst viele Seitenaufrufe (Traffic) zu generieren, um Werbeeinnahmen zu steigern oder die Markenbekanntheit zu erhöhen.

Wie funktioniert Clickbait?

Die Methode nutzt psychologische Tricks, um eine sogenannte **Neugierlücke** (*curiosity gap*) zu erzeugen. Dem Nutzer wird gerade so viel Information gegeben, dass er neugierig wird, aber nicht genug, um diese Neugier ohne einen Klick zu stillen.

Typische Merkmale

- **Übertreibungen & Superlative**: Verwendung von Wörtern wie „unglaublich“, „schockierend“, „sensationell“ oder „das Beste, was du je sehen wirst“.
- **Cliffhanger**: Sätze, die ein Ereignis ankündigen, aber das Ergebnis offen lassen, z. B. „Du wirst nicht glauben, was als Nächstes passierte ...“.
- **Emotionale Trigger**: Es wird gezielt mit Neugier, Angst oder Mitleid gespielt.
- **Reißerische Vorschaubilder (Thumbnails)**: Oft werden bunte, schockierende oder sogar irreführende Bilder verwendet, die kaum etwas mit dem eigentlichen Inhalt zu tun haben.

Warum ist Clickbait oft enttäuschend?

Hinter den spektakulären Versprechungen steckt meist ein qualitativ minderwertiger Inhalt. Oft hält der Artikel oder das Video das Versprechen der Überschrift nicht ein, was beim Nutzer zu Frust führt. In manchen Fällen dienen Clickbaits auch dazu, Nutzer auf dubiose Seiten zu locken, auf denen sie persönliche Daten preisgeben sollen.

Tipp: Wenn eine Schlagzeile extrem vage bleibt oder „Unglaubliches“ verspricht, ohne konkret zu werden, lohnt sich oft ein zweiter, kritischer Blick, bevor man klickt.

… ein Captcha

Ein **CAPTCHA** ist dieser kleine Test auf Webseiten, mit dem überprüft wird, ob du ein echter Mensch oder ein automatisierter Computer (ein „Bot“) bist.

Der Name ist eine Abkürzung für: *„Completely Automated Public Turing test to tell Computers and Humans Apart“*.

Warum gibt es das?

Webseiten wollen sich vor Spam und Missbrauch schützen. Ohne Captchas könnten Bots in Sekundenschnelle tausende Fake-Accounts erstellen, massenhaft Spam-Kommentare posten oder bei Konzerten alle Tickets aufkaufen, um sie teuer weiterzuverkaufen.

Die verschiedenen Arten

Sicher hast du schon alle davon mal gesehen:

- **Bilderrätsel**: „Wähle alle Quadrate mit Hydranten, Ampeln oder Zebrastreifen aus.“ (Das nutzt Google übrigens oft gleichzeitig, um seine KI für autonomes Fahren zu trainieren).
- **Verzerrter Text**: Du musst krumme Buchstaben oder Zahlen abtippen, die für Computer schwer lesbar sind.
- **Die Checkbox**: Ein einfaches Feld „Ich bin kein Roboter“. Hier analysiert das System dein Mausverhalten kurz vor dem Klick – Bots bewegen die Maus oft zu perfekt oder gar nicht.
- **Unsichtbare Captchas**: Moderne Systeme (wie reCAPTCHA v3) arbeiten im Hintergrund. Sie beobachten dein Verhalten auf der Seite und lassen dich einfach gewähren, wenn alles nach einem normalen Menschen aussieht.

Warum werden sie immer schwerer?

Da die **Künstliche Intelligenz** immer besser darin wird, Bilder und Texte zu erkennen, müssen auch die Captchas komplizierter werden, um die Bots weiterhin auszusperren. Das ist ein ständiges Wettrüsten.

... AR

AR steht für **Augmented Reality** (auf Deutsch: „Erweiterte Realität“).

Im Gegensatz zur *Virtual Reality (VR)*, bei der du komplett in eine digitale Welt eintauchst und nichts mehr von deiner Umgebung siehst, vermischt AR die echte Welt mit digitalen Elementen. Du siehst also deine normale Umgebung, die durch virtuelle Objekte, Texte oder Bilder ergänzt wird.

Wie funktioniert das?

Meistens nutzt du dafür dein **Smartphone**, ein Tablet oder eine spezielle **AR-Brille**. Die Kamera erfasst den Raum, und die Software platziert digitale Objekte so darin, als stünden sie wirklich da.

Bekannte Beispiele aus dem Alltag

- **Pokémon GO**: Das wohl bekannteste Beispiel. Du siehst die echte Straße durch dein Handy-Display, aber plötzlich steht dort ein kleines Monster.
- **IKEA Kreativ**: Du kannst virtuelle Möbelstücke maßstabsgetreu in dein echtes Wohnzimmer projizieren, um zu sehen, ob das Sofa passt.
- **Social Media Filter**: Wenn du auf Instagram oder TikTok einen Filter nutzt, der dir Katzenohren aufsetzt oder dein Gesicht verändert, ist das AR.
- **Navigation**: Google Maps kann dir im Live-Bild der Kamera Pfeile direkt auf die Straße einblenden, damit du weißt, wo du abbiegen musst.
- **Industrie**: Mechaniker können sich Reparaturanleitungen direkt über das Bauteil legen lassen, an dem sie gerade arbeiten.

Der Unterschied kurz gefasst

- **VR (Virtual Reality)**: Alles ist digital, du bist „weg“ aus der echten Welt.
- **AR (Augmented Reality)**: Die echte Welt bleibt sichtbar, wird aber digital „aufgepeppt“.

… das gängigste Videoformat

Das gängigste Videoformat im Jahr 2026 ist nach wie vor **MP4** (MPEG-4 Part 14). Es gilt als der universelle Standard, da es eine hervorragende Balance zwischen hoher Bildqualität und geringer Dateigröße bietet und auf fast jedem Gerät (Smartphones, Smart-TVs, Browser) problemlos abgespielt werden kann.

Die wichtigsten Videoformate (Container) im Überblick

Neben MP4 gibt es weitere Formate, die je nach Zweck ihre Stärken ausspielen:

- **MOV (QuickTime Movie)**: Von Apple entwickelt, ist es der Standard für iPhones und Macs. Es bietet eine sehr hohe Qualität und wird deshalb oft in der professionellen Videobearbeitung genutzt, erzeugt aber deutlich größere Dateien als MP4.
- **MKV (Matroska)**: Ein extrem flexibles Open-Source-Format. Es kann unbegrenzt viele Video- und Audiospuren sowie Untertitel in einer einzigen Datei speichern. Es ist besonders bei Film-Enthusiasten beliebt, wird aber nicht von allen Standard-Playern unterstützt.
- **WebM**: Ein von Google entwickeltes, lizenzfreies Format, das speziell für die Nutzung im Internet optimiert ist. Es bietet bei sehr kleinen Dateigrößen eine gute Qualität für Webbrowser.
- **AVI (Audio Video Interleave)**: Eines der ältesten Formate von Microsoft. Es ist zwar sehr weit kompatibel, technisch aber veraltet, da es im Vergleich zu modernen Formaten sehr große Dateien bei gleicher Qualität erzeugt.
- **WMV (Windows Media Video)**: Ebenfalls von Microsoft, primär für Windows-Systeme gedacht, spielt heute im Vergleich zu MP4 jedoch eine eher untergeordnete Rolle.

Wichtig: Der Unterschied zwischen Format und Codec

Oft werden Begriffe vermischt. Das Format (z. B. MP4) ist nur der **Container** – wie eine Schachtel. Was darin liegt, ist der **Codec** (die Kompressionsmethode).

- **H.264 (AVC)**: Der aktuell am weitesten verbreitete Standard in MP4-Dateien.
- **H.265 (HEVC)**: Der modernere Nachfolger für 4K- und 8K-Inhalte, der Videos bei gleicher Qualität noch stärker schrumpft.
- **AV1**: Ein neuer, lizenzfreier Codec, der 2026 zunehmend an Bedeutung gewinnt und eine noch bessere Effizienz als H.265 verspricht.

... NTFS

NTFS steht für **New Technology File System** und ist das Standard-Dateisystem für moderne Windows-Betriebssysteme. Es fungiert quasi als das „Inhaltsverzeichnis“ und der „Ordnungshüter“ deiner Festplatte, indem es festlegt, wie Daten gespeichert, benannt und organisiert werden.

Die wichtigsten Merkmale

- **Hohe Kapazität:** Im Gegensatz zum alten FAT32-System, das Dateien nur bis zu einer Größe von 4 GB speichern kann, unterstützt NTFS riesige Dateien und Partitionen (theoretisch bis zu 16 Exabyte).
- **Sicherheit & Rechte:** Du kannst für jede Datei und jeden Ordner präzise festlegen, welcher Benutzer sie lesen, ändern oder löschen darf.
- **Fehlertoleranz (Journaling):** NTFS führt ein „Tagebuch“ (Journal) über alle Dateiänderungen. Wenn der PC plötzlich abstürzt oder der Strom ausfällt, kann das System Fehler beim nächsten Start viel schneller reparieren und Datenverlust verhindern.
- **Zusatzfunktionen:** Es bietet integrierte Komprimierung (um Platz zu sparen) und Verschlüsselung (wie BitLocker), um sensible Daten zu schützen.

Vor- und Nachteile im Überblick

Vorteil	Nachteil
Enorme Dateigrößen möglich (über 4 GB)	**Eingeschränkte Kompatibilität:** macOS kann NTFS-Platten meist nur lesen, nicht beschreiben.
Hohe Datensicherheit durch Zugriffsberechtigungen	**Overhead:** Für sehr kleine USB-Sticks ist es oft zu „schwerfällig“.
Robustheit gegenüber Systemabstürzen	Nicht optimal für den Datenaustausch mit Spielekonsolen oder Kameras.

Wann solltest du es nutzen?

NTFS ist die beste Wahl für alle **internen Festplatten** unter Windows, da das Betriebssystem selbst dieses System zwingend benötigt, um stabil und sicher zu laufen. Für **externe Datenträger** (USB-Sticks, SD-Karten), die du auch an einem Mac, Fernseher oder Tablet nutzen möchtest, ist oft das Format **exFAT** die bessere Alternative, da es modern ist, aber eine viel höhere Kompatibilität bietet.

... Tailscale

Tailscale ist eine moderne VPN-Lösung, die deine Geräte (Laptops, Handys, Server) so miteinander verbindet, als wären sie alle im selben lokalen WLAN zu Hause – egal, wo sie sich gerade befinden.

Die wichtigsten Merkmale:

- **Keine Konfiguration ("Zero Config"):** Im Gegensatz zu klassischen VPNs musst du keine Ports am Router öffnen oder komplexe Firewall-Regeln erstellen. Du installierst einfach die App und meldest dich an.
- **Mesh-Netzwerk (Peer-to-Peer):** Deine Geräte kommunizieren direkt miteinander (P2P), anstatt den gesamten Datenverkehr über einen zentralen Server zu schicken. Das macht die Verbindung schnell und stabil.
- **Sicherheit:** Es basiert auf dem modernen **WireGuard-Protokoll**, das für seine hohe Geschwindigkeit und starke Verschlüsselung bekannt ist.
- **Identity-Based:** Du loggst dich mit bestehenden Accounts (z. B. Google, Microsoft oder Apple) ein. Das System erkennt automatisch, welche Geräte zu dir gehören.

Typische Anwendungsfälle:

- **Sicherer Zugriff von unterwegs:** Du kannst im Urlaub auf deine Dateien auf dem PC zu Hause oder dein NAS (Netzwerkspeicher) zugreifen.
- **Home-Server & Home Labs:** Bastler nutzen es, um ihre Smart-Home-Zentralen oder Server sicher erreichbar zu machen, ohne sie öffentlich ins Internet stellen zu müssen.
- **Exit-Nodes:** Du kannst ein Gerät zu Hause als "Ausgang" festlegen. Wenn du dann im öffentlichen Café-WLAN surfst, läuft dein gesamter Internetverkehr verschlüsselt über deinen heimischen Anschluss.

Kosten und Privatsphäre:

- **Kostenlos für Privatnutzer:** Für den persönlichen Gebrauch (bis zu 100 Geräte und 3 Benutzer) ist Tailscale dauerhaft kostenlos.
- **Zentraler Koordinator:** Ein kleiner Nachteil für absolute Sicherheits-Puristen ist, dass Tailscale einen zentralen "Koordinationsserver" nutzt, um die Verbindungen zwischen deinen Geräten zu vermitteln (der eigentliche Datenverkehr bleibt jedoch verschlüsselt und für Tailscale unlesbar).

Hier ist eine kompakte Anleitung für die Einrichtung von Tailscale auf den beliebtesten Heimnetz-Geräten.

1. Raspberry Pi (Linux)

Die Installation auf dem Raspberry Pi ist sehr einfach über das Terminal möglich.

1. **Installation:** Öffne das Terminal und gib diesen Befehl ein, um das offizielle Installationsskript auszuführen:

   bash

   curl -fsSL https://tailscale.com/install.sh | sh

   Verwende Code mit Vorsicht.

2. **Starten:** Aktiviere Tailscale mit:

   bash

   sudo tailscale up

   Verwende Code mit Vorsicht.

3. **Anmelden:** Es erscheint ein Link im Terminal. Kopiere diesen, öffne ihn im Browser deines PCs/Handys und logge dich ein.

2. Synology NAS

Für Synology-Geräte gibt es ein offizielles Paket im **Paketzentrum**.

1. Öffne das **Paketzentrum** in deiner Synology-Oberfläche (DSM).
2. Suche nach **"Tailscale"** und klicke auf **Installieren**.
3. Öffne die App nach der Installation und klicke auf **Log in**. Du wirst zur Tailscale-Webseite weitergeleitet, um das NAS mit deinem Account zu verknüpfen.
4. **Tipp:** Um das NAS auch als Ausgangspunkt für deinen Internetverkehr zu nutzen, kannst du es in der Tailscale Admin Konsole als **Exit Node** festlegen.

3. QNAP NAS

Auch für QNAP ist die Installation unkompliziert.

1. Öffne das **App Center** auf deinem QNAP NAS.
2. Suche unter dem Bereich "Kommunikation" nach der **Tailscale-App** und installiere sie.
3. Klicke nach der Installation auf das Icon, wähle **Öffnen** und folge dem Anmeldelink, um das Gerät zu autorisieren.

4. Windows & Smartphones

- **Windows:** Lade den Installer von der Tailscale-Webseite herunter und melde dich nach der Installation über das Icon in der Taskleiste an.
- **Handys:** Lade die App einfach aus dem Apple App Store oder Google Play Store herunter.

Sobald zwei Geräte angemeldet sind, können sie über ihre speziellen **Tailscale-IPs** (beginnen meist mit 100.x.x.x) direkt kommunizieren, egal ob du im mobilen Netz oder im fremden WLAN bist.]

Das Einrichten eines **Exit Nodes** ist ein zweistufiger Prozess: Erst sagst du dem Gerät, dass es sein Internet teilen darf, und dann erlaubst du es in der zentralen Verwaltung.

Schritt 1: Das Gerät als Exit Node vorbereiten

Je nach Gerät unterscheidet sich der Befehl oder der Klickweg:

- **Linux / Raspberry Pi:**
  Zuerst musst du das IP-Forwarding im System aktivieren. Gib danach diesen Befehl ein:

  bash

  sudo tailscale up --advertise-exit-node

  Verwende Code mit Vorsicht.

- Synology NAS**:**
  Öffne die Tailscale-App im DSM und klicke auf **"Advertise as Exit Node"**. Falls das nicht geht, kannst du den Befehl sudo tailscale up --advertise-exit-node auch per SSH oder über die Aufgabenplanung ausführen.

- **Windows:**
  Mache einen Rechtsklick auf das Tailscale-Icon in der Taskleiste und wähle **"Run exit node"**. Bestätige die Sicherheitswarnung.

Schritt 2: Den Exit Node in der Admin Konsole freischalten

Das ist der wichtigste Sicherheitscheck, damit nicht jeder einfach dein Internet nutzen kann.

1. Gehe auf die Tailscale Admin Console.
2. Suche dein Gerät in der Liste (es hat jetzt ein graues Label "Exit Node").
3. Klicke rechts auf die **drei Punkte (⋮)** und wähle **"Edit route settings"**.
4. Aktiviere den Schalter bei **"Use as exit node"** und speichere.

Schritt 3: Den Exit Node auf deinem Handy/Laptop nutzen

Jetzt kannst du von überall aus (z. B. im Ausland oder im Café) dein heimisches Internet nutzen:

- **Smartphone:** Öffne die Tailscale-App, tippe auf **"Exit Node"** und wähle dein zu Hause stehendes Gerät aus.
- **Laptop:** Klicke auf das Tailscale-Icon, gehe zu **"Exit Node"** und wähle das Gerät aus der Liste.

Was passiert dann? Dein gesamter Datenverkehr wird verschlüsselt zu deinem Gerät nach Hause geschickt und geht von dort aus ins Internet. Webseiten denken nun, du wärst zu Hause an deinem Anschluss.

Um Geräte in deinem Heimnetz zu erreichen, die selbst kein Tailscale installiert haben (wie Drucker, Smart-Home-Bridges oder alte IP-Kameras), nutzt du die Funktion **Subnet Routing**.

Dabei fungiert ein Gerät (z. B. dein Raspberry Pi oder dein NAS) als „Brücke“ (Subnet Router) in dein lokales Netzwerk.

Schritt 1: Das Subnet am Gerät freigeben

Du musst Tailscale sagen, welchen Adressbereich es in das VPN „holen“ soll. Meistens ist das heimische Netz 192.168.178.0/24 (FritzBox) oder 192.168.1.0/24.

- **Linux / Raspberry Pi:**
  Gib den Befehl ein (ersetze den Bereich durch dein lokales Netz):

  bash

  sudo tailscale up --advertise-routes=192.168.178.0/24

  Verwende Code mit Vorsicht.

- **Synology NAS:**
  Hier ist es am einfachsten, die Admin-Konsole zu nutzen oder den Befehl über die Aufgabenplanung/SSH abzusetzen.

Schritt 2: In der Admin Konsole aktivieren

Wie beim Exit Node muss diese Route aus Sicherheitsgründen manuell bestätigt werden:

1. Gehe zur Tailscale Admin Console.
2. Klicke bei dem Gerät, das du gerade konfiguriert hast, auf die **drei Punkte (⋮)** -> **Edit route settings**.
3. Unter **Subnet routes** siehst du nun den Bereich (z. B. 192.168.178.0/24). Aktiviere den Schalter daneben.

Schritt 3: Zugriff testen

Ab sofort kannst du von unterwegs (wenn Tailscale auf deinem Handy/Laptop an ist) einfach die normale lokale IP deines Druckers oder Smart-Home-Geräts in den Browser eingeben. Tailscale leitet die Anfrage automatisch über deinen Subnet Router nach Hause weiter.

Kleiner Profi-Tipp: DNS-Namen nutzen (MagicDNS)

Damit du dir keine IP-Adressen merken musst, kannst du in der Admin Konsole unter **DNS** das "MagicDNS" aktivieren. Dann kannst du deine Geräte einfach über ihren Namen ansprechen (z.B. http://mein-nas/).

Wenn du Tailscale und **Pi-hole** (oder AdGuard Home) kombinierst, hast du deinen eigenen privaten Werbeblocker immer in der Tasche. Egal ob du im Mobilfunknetz oder in einem Hotel-WLAN bist – dein Handy fragt für jede Webseite erst bei deinem Pi-hole zu Hause nach, ob die Adresse auf einer Sperrliste steht.

So richtest du es ein:

1. Pi-hole für Tailscale öffnen

Standardmäßig blockiert Pi-hole Anfragen, die nicht aus dem direkten lokalen Netzwerk kommen. Da Tailscale ein eigenes virtuelles Netzwerk nutzt, musst du das erlauben:

1. Öffne dein **Pi-hole Dashboard** im Browser.
2. Gehe zu **Settings** > **DNS**.
3. Wähle unter "Interface settings" die Option **"Permit all origins"** (oder "Respond only on interface tailscale0", falls verfügbar).
    - *Sicherheitshinweis:* Das ist sicher, solange dein Pi-hole nicht direkt per Port-Forwarding im offenen Internet steht.

2. Pi-hole als DNS-Server in Tailscale eintragen

Jetzt musst du Tailscale sagen, dass alle Geräte diesen Pi-hole fragen sollen:

1. Logge dich in die Tailscale Admin Console ein.
2. Klicke auf den Tab **DNS**.
3. Suche den Bereich **Nameservers** und klicke auf **Add nameserver** > **Custom...**.
4. Gib hier die **Tailscale-IP** deines Pi-hole-Geräts ein (die 100.x.x.x Adresse) und speichere.
5. Aktiviere den Schalter **Override local DNS**. Das zwingt deine Geräte, den Pi-hole zu nutzen, anstatt den DNS-Server des aktuellen WLANs.

3. MagicDNS (Optional aber empfohlen)

Aktiviere in den DNS-Einstellungen auch **MagicDNS**. Damit kannst du deine Geräte im Browser einfach mit ihrem Namen aufrufen (z. B. http://pihole/admin statt der IP).

Das Ergebnis:
Sobald du Tailscale auf deinem Handy einschaltest, siehst du in der Pi-hole Statistik die Anfragen deines Handys. Werbung in Apps und auf Webseiten wird nun auch unterwegs gefiltert, ohne dass du einen öffentlichen (und oft langsameren) Werbeblocker-Dienst nutzen musst.

Um bestimmte Geräte von der Filterung auszunehmen, hast du zwei Möglichkeiten: entweder direkt am Gerät oder über die zentrale Steuerung in Tailscale.

Methode 1: "Override local DNS" am Gerät deaktivieren

Wenn du möchtest, dass ein bestimmter Laptop oder ein Handy den Pi-hole **gar nicht** nutzt, kannst du das in der jeweiligen Tailscale-App einstellen:

1. Öffne die **Tailscale-App** auf dem Gerät.
2. Suche in den Einstellungen nach **"Use Tailscale DNS settings"** (oder ähnlich, je nach System).
3. Schalte diesen Regler **aus**.
    - **Effekt:** Dieses Gerät ignoriert den in der Admin-Konsole festgelegten Pi-hole und nutzt wieder den DNS-Server des lokalen Netzwerks (z. B. den deiner FritzBox).

Methode 2: Tailscale ACLs (für Profis)

Du kannst über die **Access Control Lists (ACLs)** in der Admin-Konsole sehr feingranular festlegen, wer den DNS-Server nutzen darf. Das ist jedoch etwas technischer, da man hier Code-Zeilen im JSON-Format bearbeitet.

Methode 3: Die "Pause"-Funktion im Pi-hole (Einfachste Lösung)

Falls der Werbeblocker gerade eine Seite blockiert, die du dringend brauchst, ist es oft einfacher, den Filter kurz für alle zu pausieren:

1. Öffne dein **Pi-hole Dashboard**.
2. Klicke links auf **Disable**.
3. Wähle eine Zeitspanne (z. B. "For 5 minutes").
    - **Vorteil:** Du musst nichts an den Tailscale-Einstellungen ändern und nach 5 Minuten ist der Schutz automatisch wieder für alle aktiv.

Methode 4: Die Whitelist im Pi-hole

Wenn eine bestimmte Webseite (z. B. ein Shopping-Portal oder ein Streaming-Dienst) auf allen Geräten funktionieren soll, füge sie einfach zur **Whitelist** in deinem Pi-hole hinzu. Dann wird sie trotz aktivem Tailscale-Tunnel auf keinem Gerät mehr geblockt.

Ein wichtiger Hinweis noch:
Falls du auf einem Gerät (z. B. Android oder im Chrome-Browser) **"Sicheres DNS" (DNS-over-HTTPS)** aktiviert hast, kann das den Pi-hole umgehen. Schalte diese Funktion in den Browser- oder Systemeinstellungen aus, wenn der Pi-hole-Filter dort greifen soll.

… das BFId Verfahren

Das **BFId-Verfahren** (eine Abkürzung für *Beamforming Feedback Identity*) ist eine hochpräzise Forschungsmethode aus der IT-Sicherheit, mit der Personen **allein über gewöhnliche WLAN-Signale fast fehlerfrei identifiziert werden können**.

Entwickelt wurde das Verfahren von einem Forschungsteam des Karlsruher Instituts für Technologie (KIT). Es nutzt eine Funktion im WLAN-Standard (ab WiFi 5), um Menschen ohne Kameras, Sensoren oder gar ein eigenes Smartphone zu erkennen.

Wie funktioniert das Verfahren?

1. **Beamforming ausnutzen**: Moderne WLAN-Router nutzen "Beamforming", um Funksignale gezielt in die Richtung der verbundenen Endgeräte (wie Smartphones oder Laptops) zu lenken. Dafür senden diese Geräte fortlaufend Rückmeldungen über die Kanalcharakteristik an den Router.
2. **Körpersignale erfassen**: Bewegt sich ein Mensch durch den Raum, verändern und reflektieren sich diese Funkwellen minimal durch seinen Körper.
3. **Mustererkennung per KI**: Ein passives Empfangsgerät fängt diese offen übertragenen Signale im Raum ab. Ein darauf trainiertes maschinelles Lernmodell verwandelt die Signaländerungen in eine Art **digitale Signatur der Person**.

Warum ist das BFId-Verfahren so bemerkenswert?

- **Enorme Treffsicherheit**: In Tests mit knapp 200 Personen erreichte das System eine Erkennungsgenauigkeit von rund 99,5 Prozent.
- **Kein Handy nötig**: Es reicht, wenn *andere* Geräte im Raum mit dem WLAN kommunizieren. Der eigene Körper reflektiert die Wellen sowieso – man muss also selbst kein Smartphone bei sich tragen.
- **Blickwinkelunabhängig**: Das System erkennt die Person unabhängig von Schritten, Gangbild, Blickwinkel oder Hindernissen wie Wänden.
- **Unsichtbarer Angriff**: Da für das Abfangen der Funksignale ein handelsübliches Empfangsgerät ausreicht, bleibt der "Angriff" auf die Privatsphäre völlig unbemerkt.

Aktueller Status

Das Verfahren ist aktuell ein **akademischer Machbarkeitsnachweis (Proof of Concept)**. Es findet noch keine flächendeckende Überwachung statt. Die Forscher haben das Risiko bewusst frühzeitig aufgezeigt, damit zukünftige WLAN-Standards durch Verschlüsselung dieser Rückmeldungen sicherer gestaltet werden können.

Da das BFId-Verfahren eine passive Abhörmethode ist, bei der die Funksignale unverschlüsselt durch die Luft fliegen, kannst du dich als Einzelperson im Alltag **aktuell leider kaum selbst dagegen schützen**. Selbst wenn du dein eigenes Smartphone

ausschaltest, reicht es aus, wenn andere Geräte in deiner Nähe (z. B. der Router im Café oder das Handy eines Passanten) WLAN-Signale austauschen.

Dennoch gibt es technische Lösungsansätze, die auf unterschiedlichen Ebenen ansetzen, um dieses Tracking in Zukunft zu verhindern:

1. Die echte Lösung: Technische Standards ändern (In Arbeit)

Das Kernproblem ist, dass die Beamforming-Daten (BFI) im aktuellen WLAN-Standard **völlig unverschlüsselt (im Klartext) übertragen werden**. Jeder im Raum kann sie mitlesen.

- **Der neue WLAN-Standard (IEEE 802.11bf)**: Das KIT-Forschungsteam und andere Wissenschaftler fordern vehement, Sicherheits- und Datenschutzmechanismen direkt in den kommenden WLAN-Standard zu integrieren, der speziell für "WiFi-Sensing" (WLAN-Raumüberwachung) entwickelt wird.
- **Verschlüsselung der Feedback-Daten**: Würden Router und Smartphone die Daten über die Funkkanal-Beschaffenheit verschlüsselt austauschen, könnte ein Angreifer mit den abgefangenen Datenpaketen nichts mehr anfangen.

2. Schutzmechanismen aus der Forschung (Obfuskation)

Wissenschaftler arbeiten bereits an Software-Abwehrmethoden, die auf Routern oder Endgeräten installiert werden könnten:

- **"LeakyBeam"-Verteidigung**: Forscher haben Prototypen entwickelt, die BFI-Pakete künstlich verschleiern (Obfuskation). Dabei werden minimale, künstliche Störungen in die Rückmeldungen eingebaut. Für die Internetverbindung reicht das Signal immer noch völlig aus, aber die KI des Angreifers kann daraus kein klares "Körperbild" oder Bewegungsmuster mehr berechnen.

3. Was du heute schon tun kannst (Eingeschränkter Schutz)

Wenn du deine Privatsphäre in den eigenen vier Wänden maximal schützen willst, helfen derzeit nur radikale oder klassische Methoden gegen Funkwellen:

- **WLAN ausschalten**: Wenn zu Hause kein Gerät funkt (z. B. nachts per Zeitschaltuhr am Router), gibt es auch keine Beamforming-Signale, die reflektiert und abgefangen werden können.
- **Auf Kabel umsteigen (LAN)**: Geräte, die fest an einem Ort stehen (Fernseher, PC, Spielekonsolen), über ein Ethernet-Kabel statt über WLAN zu betreiben, reduziert den Funkverkehr drastisch.
- **Alte WLAN-Standards nutzen (Notlösung)**: Das BFId-Verfahren benötigt das moderne, gezielte Beamforming. Ältere Standards (wie das sehr alte Wi-Fi 4 / 802.11n) nutzen diese präzise Technologie noch nicht – allerdings erkauft man sich diesen Schutz mit deutlich langsamerem Internet.

Da das BFId-Verfahren bisher nur im Labor existiert, besteht im Moment **kein Grund zur Panik**. Es zeigt jedoch, dass die Cybersicherheit bei zukünftigen Funkstandards dringend nachbessern muss.