ZAV-Fachgruppe Opfervertretung, 9. April 2026 in Zürich

Opfer in Strafverfahren: Schutz der digitalen Privatsphäre

Rechtsanwalt Martin Steiger

Steiger Legal

Wie können Opfer in Strafverfahren ihre digitale Privatsphäre schützen?

Ziel: Schutz von Menschen vor der missbräuchlichen, nachteiligen oder unerwünschten Verwendung ihrer Daten

Mittel: Geeignete Massnahmen für den «digitalen Flankenschutz»

Besonders verwundbare «Flanken»:

- Handlungen der Täterschaft im digitalen Raum
- «Victim Blaming» durch die gegnerische Rechtsvertretung, insbesondere durch die Strafverteidigung
- Selbstschädigendes Verhalten in Verfahren, insbesondere mit unbedachten Beweisanträgen in Strafverfahren

Doxing

Doxing (von englisch *dox*, Abkürzung für *documents* ‚Dokumente'), auch *Doxxing*, ist das internetbasierte Zusammentragen und anschließende Veröffentlichen personenbezogener Daten, typischerweise mit bösartigen Absichten gegenüber den Betroffenen.[1][2] Zum Teil geht damit auch die Identifizierung anonymer Personen einher.

Die Gründe für das Doxing können unterschiedlicher Natur sein, darunter etwa Selbstjustiz, öffentliches Bloßstellen sowie Belästigung. Personen, die vom Doxing betroffen sind, sind oft auf den veröffentlichten Daten basierenden Folgeattacken ausgesetzt.

Informationsgewinnung

[Bearbeiten | Quelltext bearbeiten]

Die personenbezogenen Daten können auf vielfältige Weise gesammelt werden. Eine Herangehensweise zur Informationsgewinnung besteht in der Durchsuchung öffentlich zugänglicher Datenbanken. Darunter fallen etwa Onlinemedien sowie Telefon-, Adress- und Mitgliederverzeichnisse.

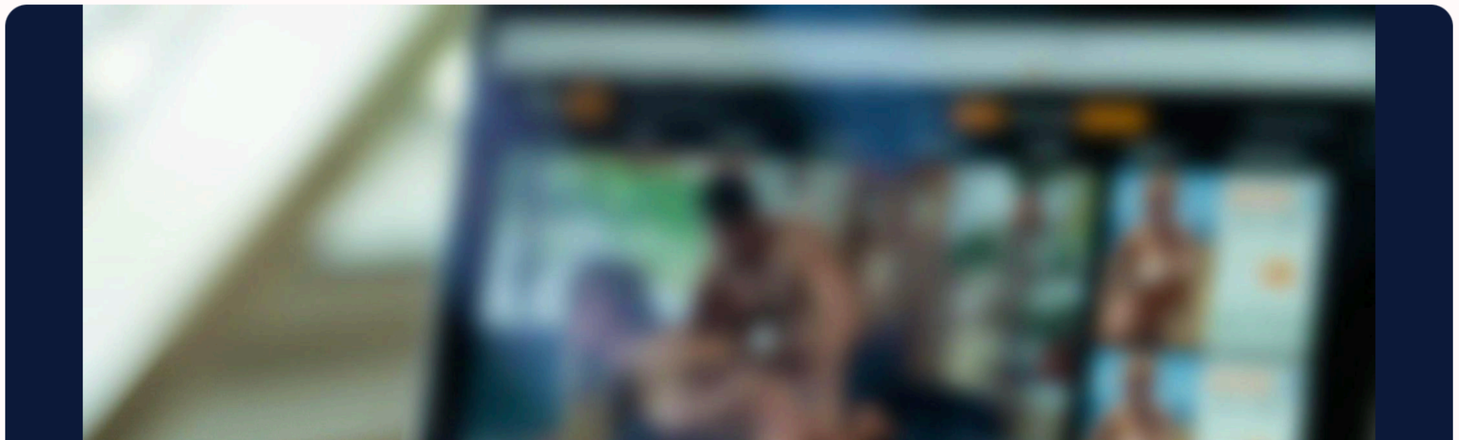
Publiziert 23. Oktober 2022, 16:10

REVENGE PORN

Wurden schon Nacktbilder von dir veröffentlicht?

Die Konsequenzen von Rachepornografie können zerstörerisch sein. Wurden schon einmal Nacktbilder ohne Erlaubnis von dir verschickt? Oder auf eine Porno-Plattform hochgeladen? Für eine Videoreportage sind wir auf der Suche nach Betroffenen, die ihre Geschichte erzählen.

von
Helena Müller



Was tun bei Stalking? | Schwei

https://www.skppsc.ch/de/themen/gewalt/stalking/

SKPPSC

Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

Stalking

Stalking, auch Cyberstalking, im Schweizerischen Strafgesetzbuch als «Nachstellung» bezeichnet, kann betroffene Personen in ihrer Lebensführung stark beeinträchtigen. Sie erleiden oft richtiggehenden Psychoterror bis hin zu körperlichen Übergriffen. Stalking kann beim Opfer schwere seelische Leiden hervorrufen und soziale Isolation zur Folge haben.

Idealfall: Bestehende Schutzmassnahmen

Häufige Realität: Ungenügende Schutzmassnahmen, gerade bei Opfern digitaler Straftaten

Aber: Besser spät als nie!

Fokus: Smartphone

Smartphone: Wer Zugriff auf diesen «Personal Computer» einer Person hat, kennt und kontrolliert das ganze «digitale Leben» dieser Person …

… und die Kommunikation mit der Anwältin oder dem Anwalt! 😬

- Zugriff auf grundsätzlich alle Daten auf dem Smartphone einschliesslich SMS
- Direkter Zugriff auf Daten bei Dritten über Apps auf dem Smartphone: Dating, E-Mail, Fotos und Videos, E-Banking, Messaging, Social-Media, …
- Indirekter Zugriff auf Daten bei Dritten über Passwörter auf dem Smartphone: Passwort-Manager oder System-eigener Schlüsselbund

Ziel: Smartphone als «Safe House»
in der eigenen Hand und Tasche

Faustregel: Ein Smartphone darf nie in fremde Hände geraten – auch nicht als «Beilage» zu einem Strafantrag … 💡

Grundlagen der Smartphone-Sicherheit:

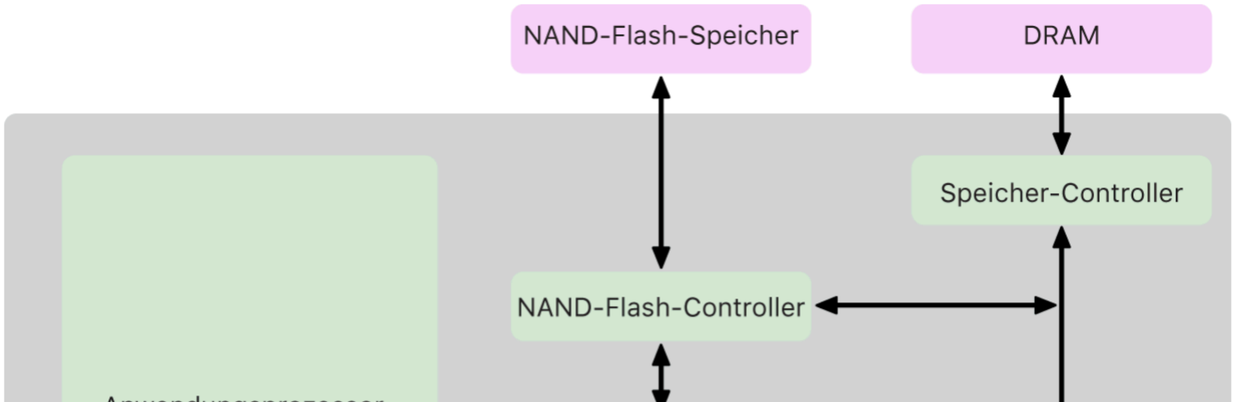
- Halbwegs aktuelle Hardware, insbesondere iPhone 12 (2020) oder neuer, im Idealfall das neuste iPhone 17 (2025) 💰💰💰
- Aktuelles Betriebssystem, insbesondere aktuelles iOS 26 mit allen Aktualisierungen

Secure Enclave

Die Secure Enclave ist ein dediziertes sicheres Subsystem in den aktuellen Versionen von iPhone, iPad, Mac, Apple TV, Apple Watch, Apple Vision Pro und HomePod.

Übersicht

Die Secure Enclave ist ein dediziertes sicheres Subsystem, das bei Apple in die SoCs (Systems on Chip) integriert ist. Die Secure Enclave ist vom Hauptprozessor isoliert, was eine zusätzliche Sicherheitsebene mit sich bringt, und ist darauf ausgelegt, die Sicherheit sensibler Benutzerdaten selbst dann zu gewährleisten, wenn der Kernel des Anwendungsprozessors kompromittiert werden sollte. Sie folgt denselben Designprinzipien wie das SoC insgesamt – ein Boot-ROM, das einen Hardware-Vertrauensanker etabliert, eine AES-Engine für effiziente und sichere kryptografische Operationen und geschützter Speicher. Die Secure Enclave umfasst keinen Speicher, verfügt aber über einen Mechanismus zum sicheren Speichern von Informationen auf dem angeschlossenen Speicher, der unabhängig von dem vom Anwendungsprozessor und dem Betriebssystem verwendeten NAND-Flashspeicher ist.



«… und was ist mit Android»?

Threat Intelligence

The Proliferation of DarkSword: iOS Exploit Chain Adopted by Multiple Threat Actors

March 18, 2026

Google Threat Intelligence Group

Google Threat Intelligence

Introduction

Visibility and

«DarkSword supports iOS versions 18.4 through 18.7 and utilizes six different vulnerabilities to deploy final-stage payloads. […] GTIG reported the vulnerabilities used in DarkSword to Apple in late 2025, and all vulnerabilities were patched with the release of iOS 26.3 (although most were patched prior).

Google Threat Intelligence Group (GTIG), 18. März 2026

Darksword kursiert im Netz

Hacking-Tool bedroht Millionen iPhones – deines auch?

Ein Hacking-Tool für iPhones gibt es nun kostenlos im Internet. Bisher nutzten es Geheimdienste, jetzt kann es jeder herunterladen. Wer betroffen ist, was das Tool anrichtet – und wie du dich schützt.

Publiziert: 24.03.2026 um 11:05 Uhr | Aktualisiert: 25.03.2026 um 06:35 Uhr

Android: Diverse Hardware- und Software-Landschaft im Guten wie im Schlechten

Private

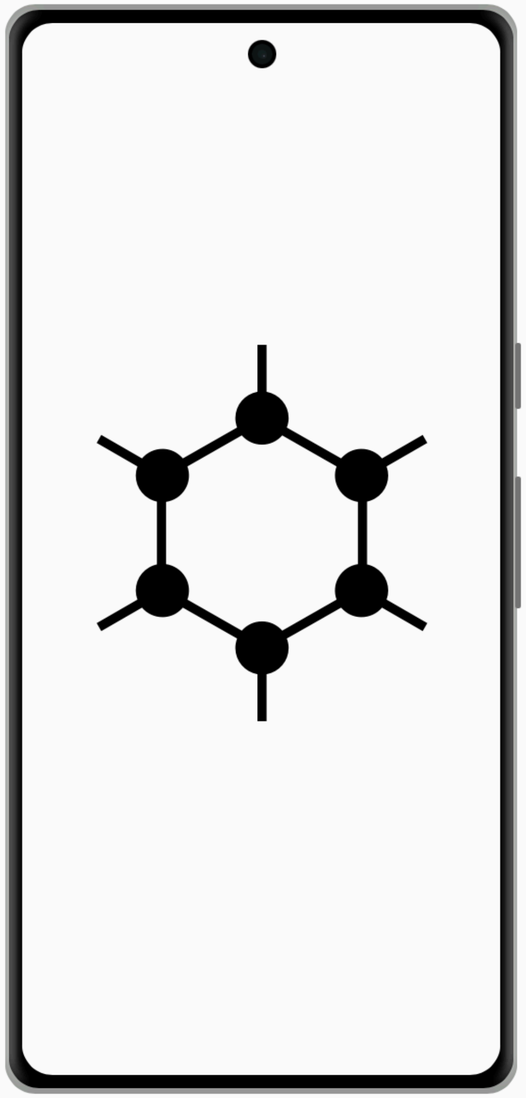
grapheneos.org

GrapheneOS Features Install Build Usage FAQ Releases Source History Articles Donate Contact

GrapheneOS

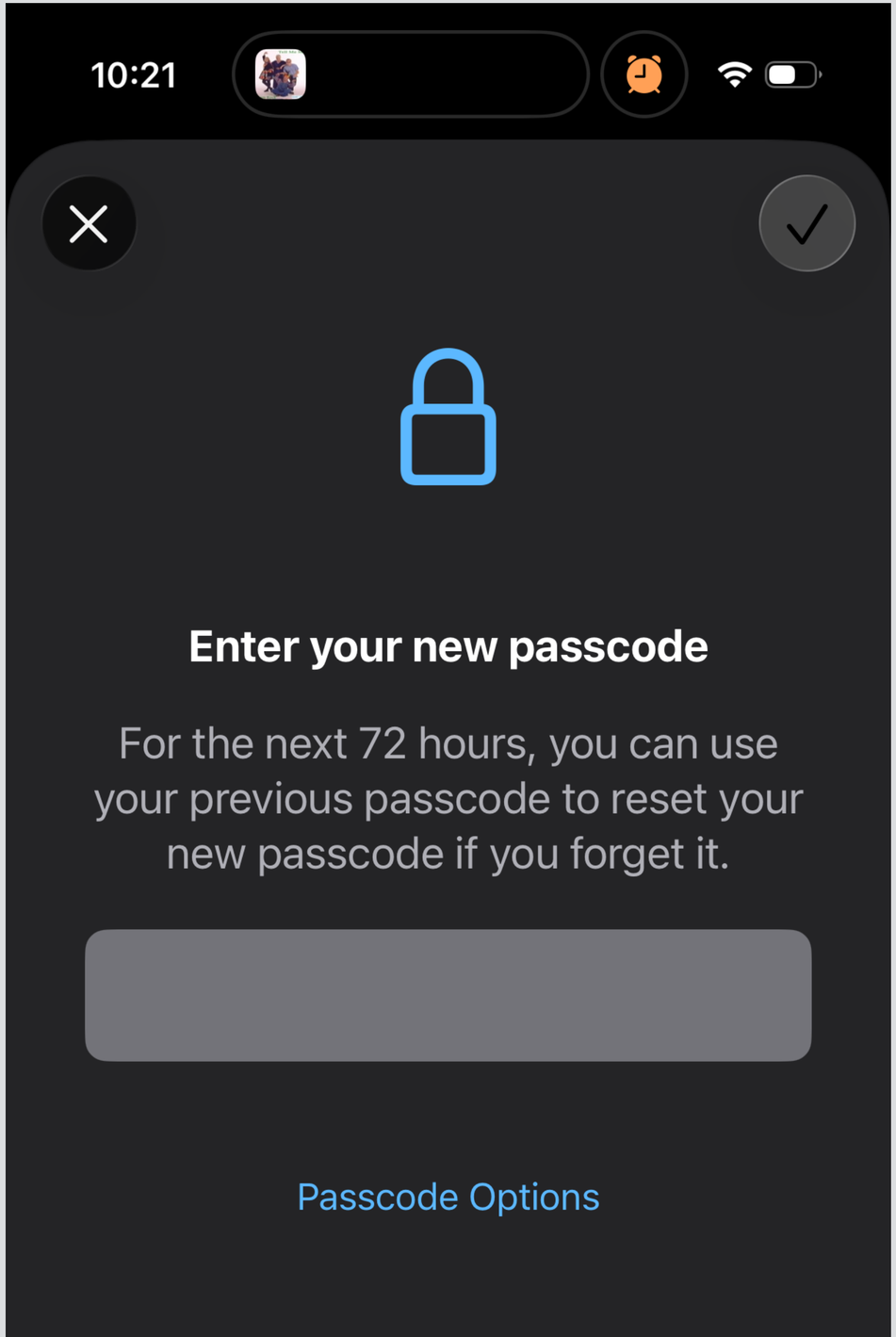
The private and secure mobile operating system with Android app compatibility. Developed as a non-profit open source project.

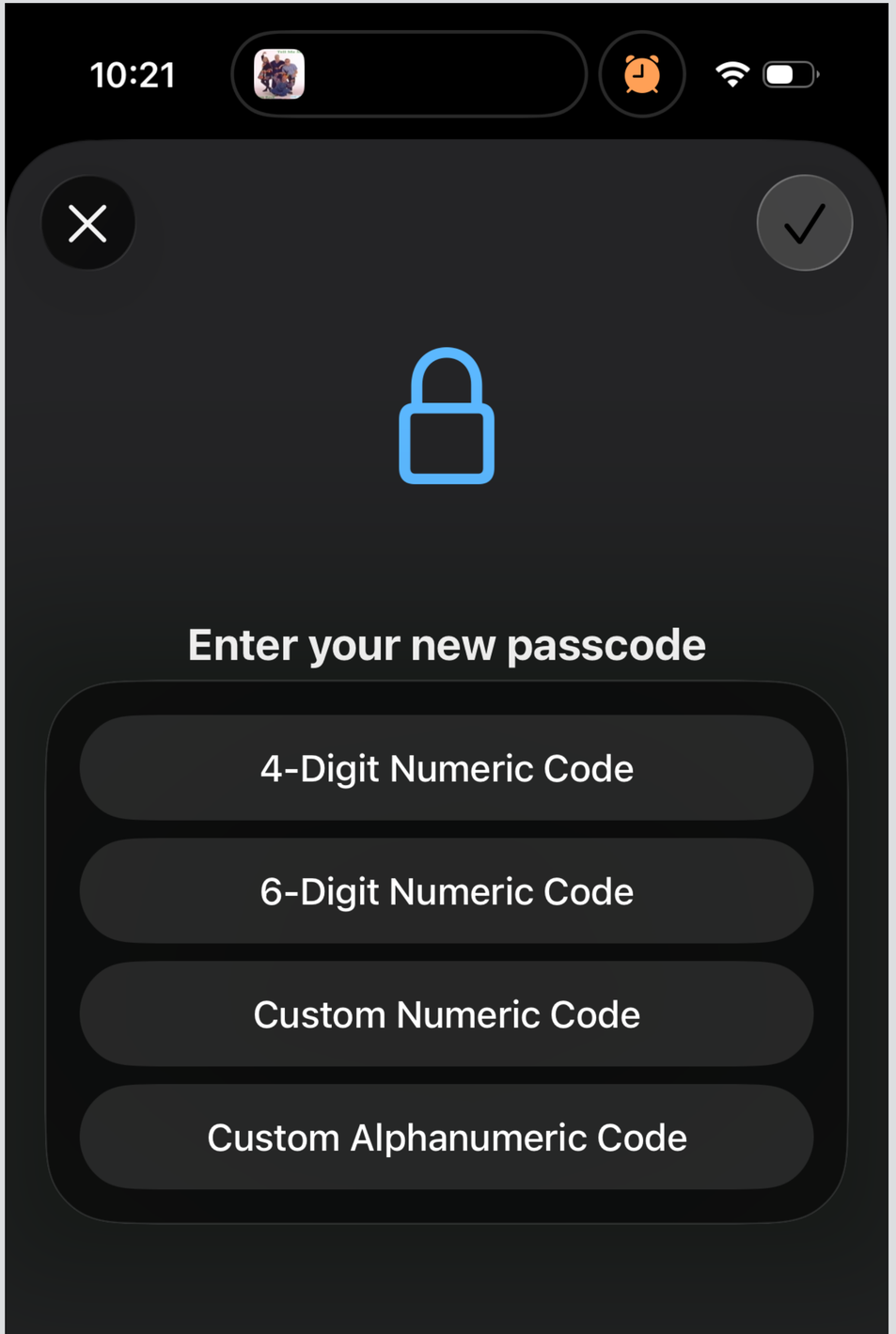
Install GrapheneOS



Immer: Geheimes und genügend langes Passwort in Verbindung mit biometrischer Entsperrung («Face ID» und «Touch ID»)

Deshalb: Keine PIN aus 4–6 Zahlen,
sondern ein Passcode mit Buchstaben
und Ziffern – und im Zweifelsfall
nicht komplex, sondern 16+ Zeichen


10:21
Enter your new passcode
For the next 72 hours, you can use your previous passcode to reset your new passcode if you forget it.
Passcode Options


10:21
Enter your new passcode
4-Digit Numeric Code
6-Digit Numeric Code
Custom Numeric Code
Custom Alphanumeric Code

Pragmatische Möglichkeit:

Aktuelle PIN «vervierfachen»

PIN-PIN-PIN-PIN

Problem: Gängige PIN wie «123456»

The Data

I was able to find almost *3.4 million* four digit passwords. Every single one of the of the 10,000 combinations of digits from 0000 through to 9999 were represented in the dataset.

The most popular password is 1234 …

… it's *staggering* how popular this password appears to be. Utterly *staggering* at the lack of imagination …

… nearly 11% of the 3.4 million passwords are 1234 *!!!*

The next most popular 4-digit PIN in use is 1111 with over 6% of passwords being this.

In third place is 0000 with almost 2%.

A table of the top 20 found passwords in shown at the right. A staggering 26.83% of all passwords could be guessed by attempting these 20 combinations!

(Statistically, with 10,000 possible combination, if passwords were uniformly randomly distributed, we would expect the these twenty passwords to account for just 0.2% of the total, not the 26.83% encountered)

Looking more closely at the top few records, all the usual suspects are present 1111 2222 3333 … 9999 as well as 1212 and (snigger) 6969 .

It's not a surprise to see patterns like 1122 and 1313 occurring high up in the list, nor 4321 or 1010 .

2001 makes an appearance at #19. 1984 follows not far behind in position #26, and James Bond fans may be interested to know 0007 is found between the two of them in position #23 (another variant 0070 follows not much further behind at #28).

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

The first "puzzling" password I encountered was 2580 in position #22. What is the significance of these digits? Why should so many people select this code to make it appear so high up the list?

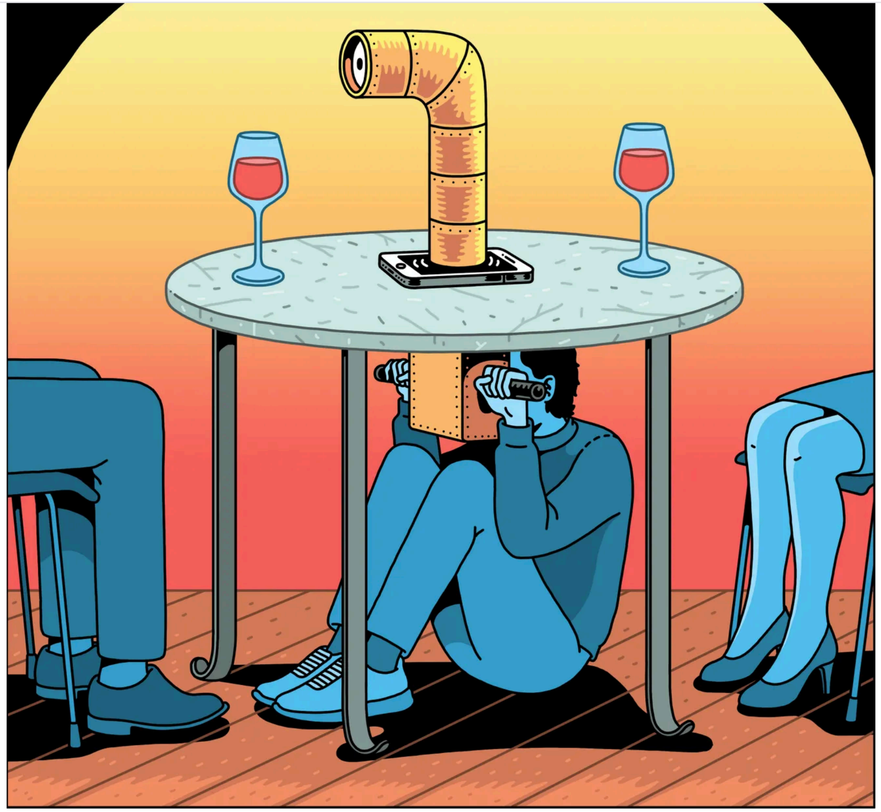
Then I realized that 2580 is a straight down the middle of a telephone keypad!

(Interestingly, this is very compelling evidence confirming the hypothesis that a 4-digit password list is a great proxy for a PIN number database. If you look at the numeric keypad on a PC-keyboard you'll see that 2580 is slightly more awkward to type on the PC than a phone because the order of keys on a keyboard is the inverted. Cash machines and other terminals that take credit cards use a phone style numeric pads. It appears that many people have an easy to type/remember PIN number for their credit card and are re-using the same four digits for their online passwords, where the *"straight down the middle"* mnemonic no longer applies).

(Another fascinating piece of trivia is that people seem to prefer even numbers over odd, and codes like 2468 occur higher than a odd number equivalent, such as 1357).

«Wie häufig muss ich mein Passwort ändern?»

Problem: Stalkerware (Schadsoftware)



Mit dieser App weiss Ihr Partner alles über Sie

Ein Datenleck der kommerziellen Überwachungssoftware mSpy zeigt: Auch in der Schweiz ist digitales Ausspionieren in Beziehungen und Familien gang und gäbe. Teil 1.

Normalfall: Installation durch Opfer (unfreiwillig) oder durch Täterschaft mit Zugriff auf Smartphone

Möglich, aber selten: Hacking

www.mspy.com/de/

mSPY

FUNKTIONEN LÖSUNGEN FAQ BLOG EINLOGGEN DEMO DE JETZT TESTEN

Die beste Mobiltelefonverfolgung

für die Kindersicherung

WAHL NR. 1 IN DER SCHWEIZ*

Mehr erfahren. Weniger Sorgen machen. Genau das ist die Stärke von mSpy, der App, mit der Sie herausfinden können, was Ihr Gegenüber auf seinem Telefon und im Internet macht. Und sie werden nicht einmal wissen, dass Sie die App benutzen.

JETZT TESTEN

DEMO ANSEHEN

KOMPATIBEL

www.mspy.com/de/iphone-monitoring.html

mSPY

FUNKTIONEN LÖSUNGEN FAQ BLOG EINLOGGEN DEMO DE JETZT TESTEN

- WhatsApp
- SMS Ein- / Ausgang
- iMessage
- Facebook Messenger
- Instagram
- Snapchat
- Keylogger
- Screenrecorder
- GPS-Tracker
- Android Anrufrekorder
- Live Bildschirm-Streaming
- Fernstandortverfolgung
- KI-Werkzeuge
- **Alle Funktionen**

MIT ALLEN IPHONES KOMPATIBEL

iPhone-Überwach App

iPhones sind einfach zu bedienen. U o
einfach, herauszufinden, was vor si

JETZT TESTEN

So leicht war eine

RESEARCH → TARGETED SURVEILLANCE

The Predator in Your Pocket

A Multidisciplinary Assessment of the Stalkerware Application Industry

This report was collaboratively written by researchers from computer science, political science, criminology, law, and journalism studies. As befits their expertise, the report is divided into several parts, with each focusing on specific aspects of the consumer spyware ecosystem, which includes: technical elements associated stalkerware

Anlassbezogene und Regelmässige Prüfung:

Installierte Apps und erteilte Freigaben auf dem Smartphone

mSpy-Leak

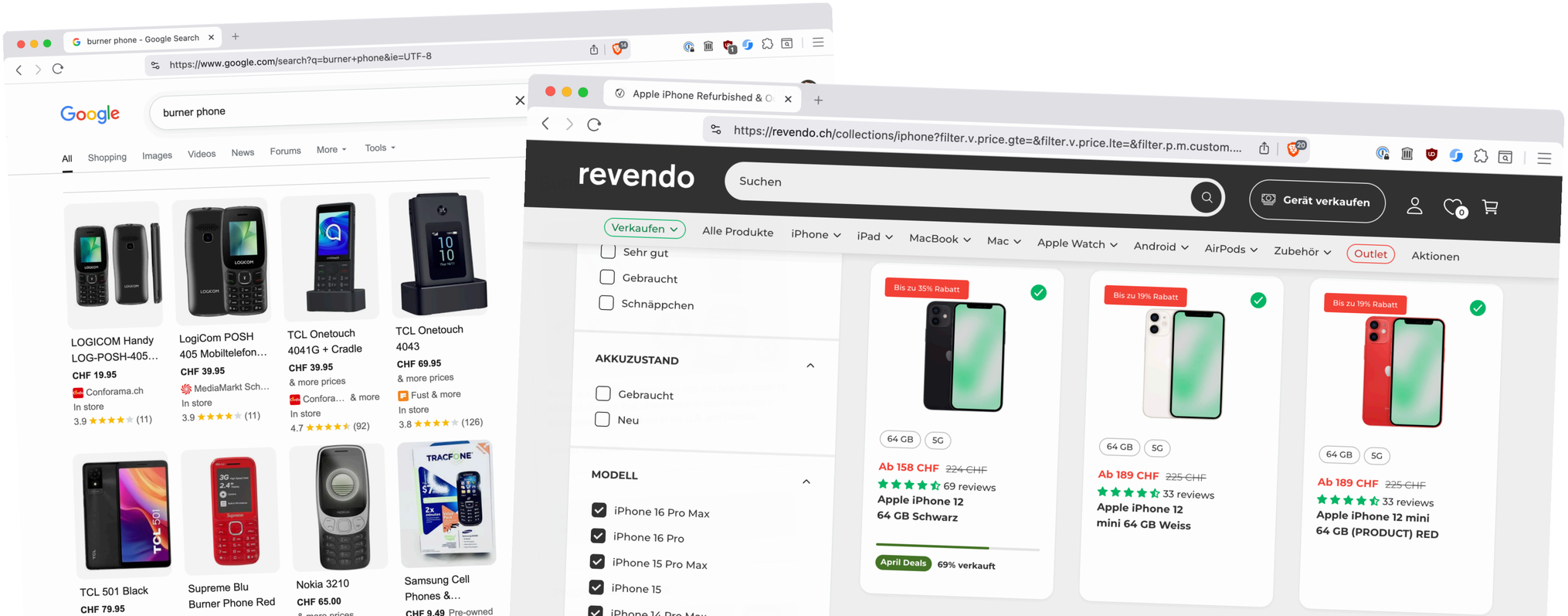
So stoppt man Spionage-Apps

Mit Überwachungs-Programmen wie mSpy können Privatpersonen einander ausspionieren. Wir erklären, wie man solche Angriffe aufdecken und abwehren kann.

27.01.2025 um 05:00 Uhr - Martin Schwarzbeck, Chris Köver - in Überwachung - 3 Ergänzungen

Im Zweifelsfall: Smartphone muss neu aufgesetzt werden!

Alternative: Günstiges «Burner Phone» mit Prepaid-Karte und minimaler Software



Version wählen:

iOS 26

Dieses Handbuch durchsuchen

Inhaltsverzeichnis

Standort mit Familienmitgliedern teilen und ihre vermissten Geräte auf dem iPhone orten

Mit der Familienfreigabe kannst du deinen Standort mit Mitgliedern deiner Familienfreigabegruppe teilen und ihnen helfen, vermisste Geräte zu finden. Wenn die Person, die als Familienorganisator:in eingetragen ist, die Standortfreigabe in den Einstellungen für die Familienfreigabe konfiguriert, wird der Standort dieser Person automatisch mit allen Mitgliedern der Familie geteilt. Das gilt auch für alle Mitglieder, die später zur Gruppe hinzugefügt werden. Die Familienmitglieder können dann entscheiden, ob sie ihren Standort teilen möchten oder nicht.

Deinen Standort mit Familienmitgliedern teilen

Wenn du Standorte mit deiner Familie teilst, können die Mitglieder deinen Standort in der App „Wo ist?“

AirTag

25 languages

From Wikipedia, the free encyclopedia

Not to be confused with AirTag (company).

AirTag is a tracking device developed by Apple.[1] AirTag is designed to act as a key finder, which helps people find personal objects such as keys, bags, apparel, small electronic devices and vehicles. To locate lost or stolen items, AirTags use Apple's crowdsourced Find My network, estimated in early 2021 to consist of approximately one billion devices worldwide that detect and anonymously report emitted Bluetooth signals.[2]

AirTags are compatible with any iPhone, iPad, or iPod Touch device capable of running iOS/iPadOS 14.5 or later, including iPhone 6S or later (including iPhone SE 1, 2 and 3). Using the built-in U1 chip on iPhone 11 or later (except iPhone SE models iPhone 16e and iPhone 17e models), users can more precisely locate items using ultra-wideband (UWB) technology. AirTag has been available since 2021.[3][4]

An updated model with the U2 chip, upgraded Bluetooth, and a louder speaker was released in January 2026. It has enhanced range for precision detection with iPhones equipped with a U2 chip such as the iPhone 15/Pro or later (excluding iPhone 16e and 17e), and also allows an Apple Watch with a U2 chip such as the Apple Watch Series 9 or later, or Apple Watch Ultra 2 or later (excluding Apple Watch SE), to precisely locate items. The second generation AirTag is compatible with devices running iOS/iPadOS/watchOS 26.2.1 or later.[5]

AirTag

An Apple AirTag

Developer	Apple
Manufacturer	Foxconn
Type	Key finder
Released	April 30, 2021; 4 years ago (1st

Immerhin: Viele Anbieter bieten Hilfe!

Private

www.apple.com/chde/privacy/control/

Store Mac iPad iPhone Watch AirPods TV & Home Entertainment Zubehör Support

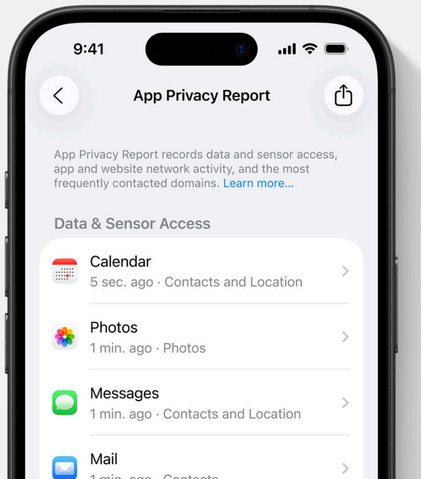
Datenschutz

Überblick Features Kontrolle Label Transparenzbericht Datenschutzrichtlinie

Du hast die Kontrolle.

Datenschutz ist integriert – ab dem Moment, wo du dein neues Gerät öffnest, und jedes Mal, wenn du eine App nutzt. Hier sind ein paar Informationen, wie du für noch mehr Sicherheit sorgen kannst.

Mehr über die Einstellungen zur Privat-sphäre.



Private

support.apple.com/en-az/guide/iphone/iph

Lock an app

Locking an app requires Face ID, Touch ID, or your passcode to open the app.

1. Go to the Home Screen.
2. Locate the app you want to lock.
3. Touch and hold the app icon until the Quick Actions menu opens.
4. Tap Require Face ID (or Touch ID or Passcode).

   Note: Some of the apps that come with iPhone can't be locked—including Calculator, Camera, Clock, Contacts, Find My, Maps, Shortcuts, and Settings.

Open a locked app without unlocking it

You can open and use an app you locked without permanently unlocking it.

1. Go to the Home Screen.
2. Locate the app you want to open.
3. Tap the app, then authenticate using Face ID (or Touch ID or a passcode).

   After you quit the app, it relocks. To reopen it, you need to reauthenticate with Face ID, (or Touch ID or a passcode).

Unlock an app

You can unlock an app so you no longer need to use Face ID, Touch ID, or a passcode to open it.

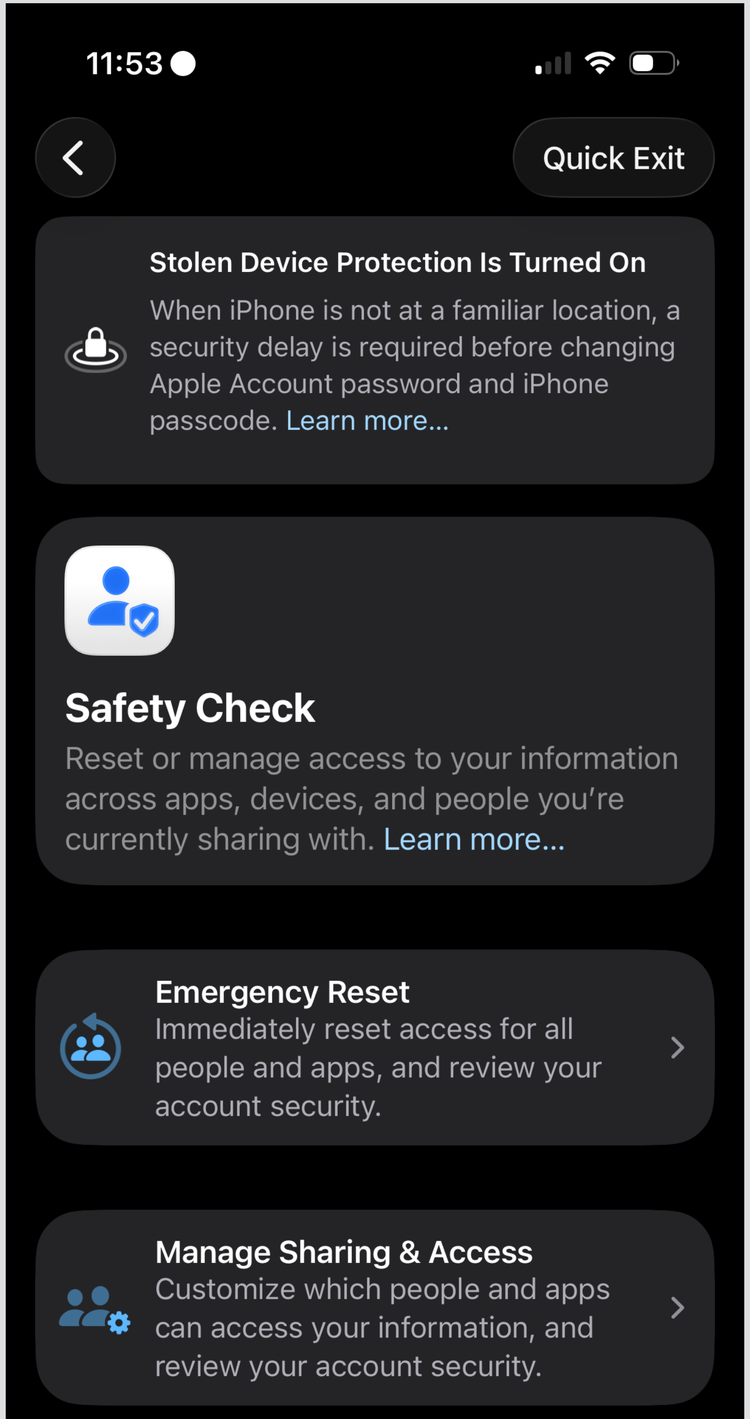
1. Go to the Home Screen.
2. Locate the app you want to unlock.
3. Touch and hold the app icon until the menu opens.
4. Tap Don't Require Face ID (or Touch ID or Passcode), then authenticate using Face ID (or Touch ID or a passcode).

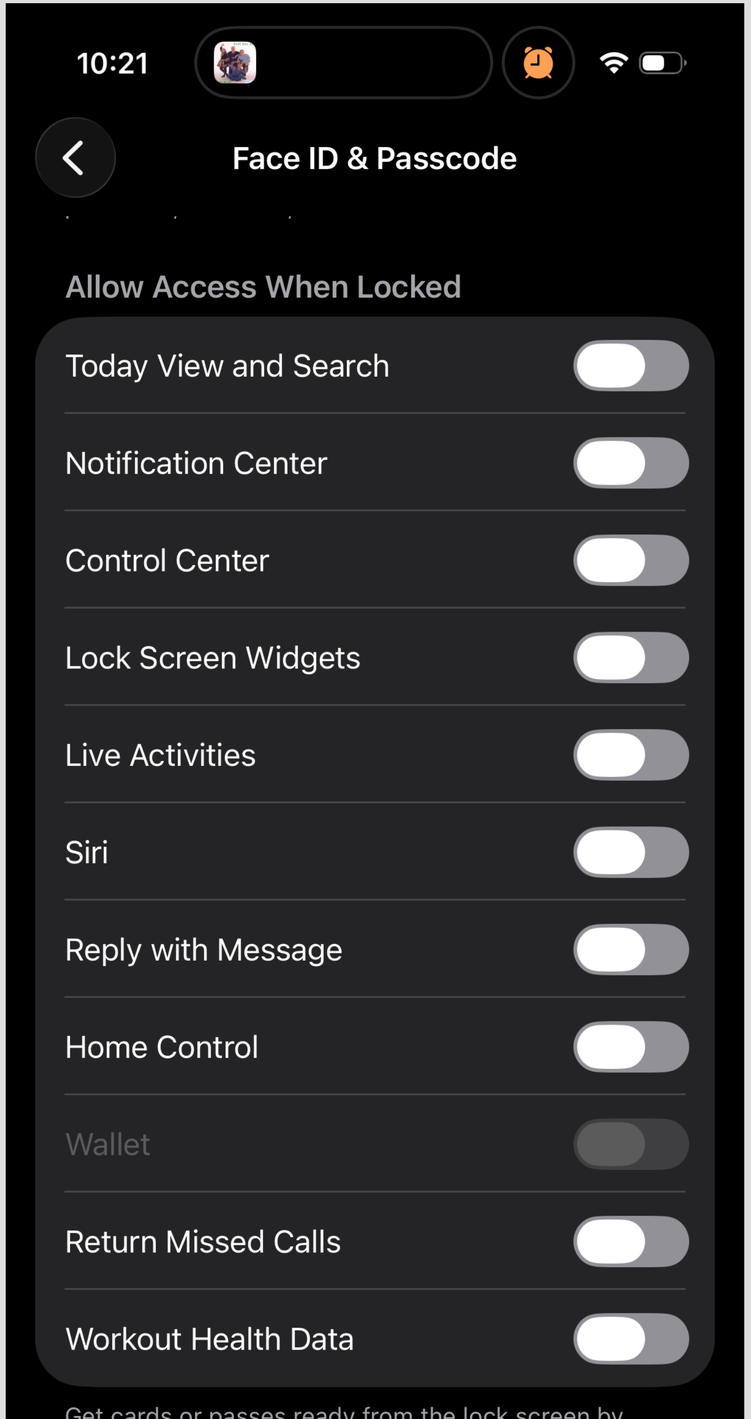
Hide an app

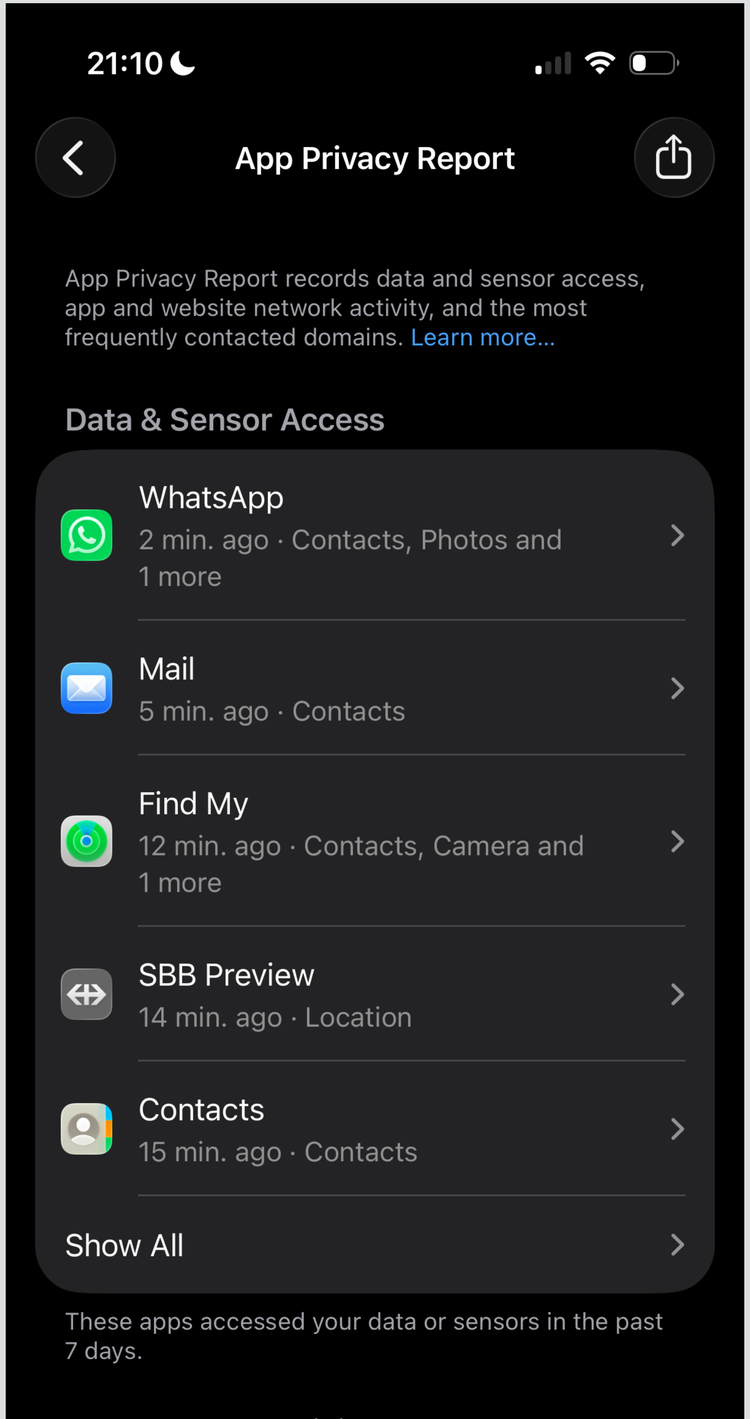
Hiding an app prevents others from seeing or opening it (unless they have a way to authenticate your iPhone using Face ID, Touch ID, or a passcode).

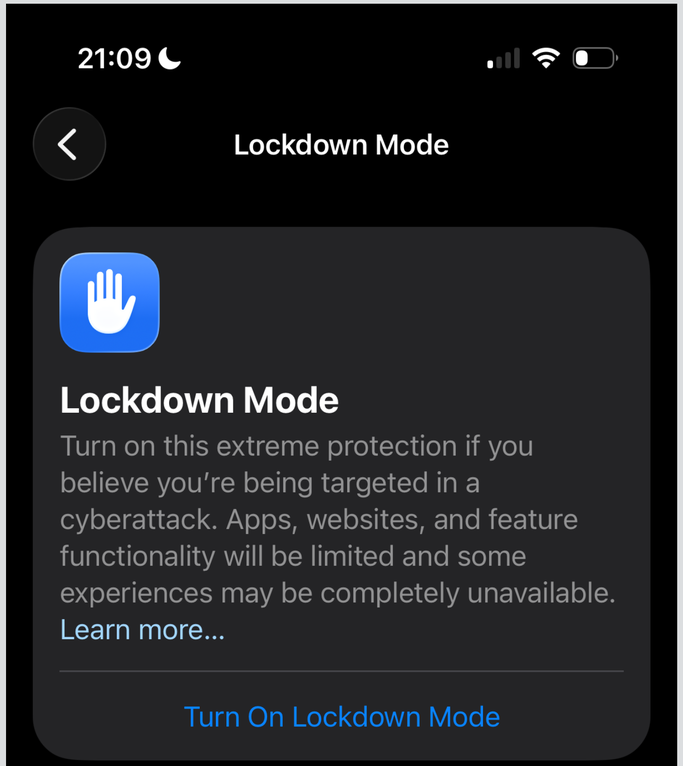
When you hide an app, its name is still visible in some places, such as Screen Time, Battery Usage By App (in Settings), and your App Store purchase history.

Note: Apps that come installed can't be hidden—only apps you download separately from the App Store can be hidden. Apps that are set by the user as default web browser or app marketplace (available only in the EU) can't be hidden either.


11:53
Quick Exit
Stolen Device Protection Is Turned On
When iPhone is not at a familiar location, a security delay is required before changing Apple Account password and iPhone passcode. Learn more...
Safety Check
Reset or manage access to your information across apps, devices, and people you're currently sharing with. Learn more...
Emergency Reset
Immediately reset access for all people and apps, and review your account security.
Manage Sharing & Access
Customize which people and apps can access your information, and review your account security.


10:21
Face ID & Passcode
Allow Access When Locked
Today View and Search
Notification Center
Control Center
Lock Screen Widgets
Live Activities
Siri
Reply with Message
Home Control
Wallet
Return Missed Calls
Workout Health Data


21:10
App Privacy Report
App Privacy Report records data and sensor access, app and website network activity, and the most frequently contacted domains. Learn more...
Data & Sensor Access
WhatsApp
2 min. ago · Contacts, Photos and 1 more
Mail
5 min. ago · Contacts
Find My
12 min. ago · Contacts, Camera and 1 more
SBB Preview
14 min. ago · Location
Contacts
15 min. ago · Contacts
Show All
These apps accessed your data or sensors in the past 7 days.



Private
support.apple.com/en-us/105120

Store Mac iPad iPhone Watch Vision AirPods TV & Home Entertainment Accessories Support

About Lockdown Mode

Lockdown Mode helps protect devices against extremely rare and highly sophisticated cyber attacks.

What is Lockdown Mode?

Lockdown Mode is an optional, extreme protection that's designed for the very few individuals who, because of who they are or what they do, might be personally targeted by some of the most sophisticated digital threats. Most people are never targeted by attacks of this nature.

When Lockdown Mode is enabled, your device won't function like it typically does. To reduce the attack surface that potentially could be exploited by highly targeted mercenary spyware, certain apps, websites, and features are strictly limited for security and some experiences might not be available at all.

Lockdown Mode is available in iOS 16 or later, iPadOS 16 or later, watchOS 10 or later, and macOS Ventura or later. Additional protections are available starting in iOS 17, iPadOS 17, watchOS 10, and macOS Sonoma.

For a complete set of protections, update your devices to the latest software before turning on Lockdown Mode.

How Lockdown Mode protects your device

When Lockdown Mode is enabled, some apps and features will function differently, including:

- **Messages:** Most message attachment types are blocked, other than certain images, video, and audio. Some features, such as links and link previews, are unavailable.
- **Web browsing:** Certain complex web technologies are blocked, which might cause some websites to load more slowly or not operate correctly. In addition, web fonts might not be displayed, and images might be replaced with a missing image icon.
- **FaceTime:** Incoming FaceTime calls are blocked unless you have previously called that person or contact within the past 30 days. Features such as SharePlay and Live Photos are unavailable.
- **Apple services:** Incoming invitations for Apple services, such as invitations to manage a home in the Home app, are blocked unless you have previously invited that person. Focus and any related status will not work as expected. Game Center is also disabled.
- **Photos:** When you share photos, location information is excluded. Shared albums are removed from the Photos app, and new Shared Album invitations are blocked. You can still view these shared albums on other devices that don't have Lockdown Mode enabled.
- **Device connections:** To connect your iPhone or iPad to an accessory or another computer, the device

Nicht vergessen: Traditionelle Computer und einzelne Datenträger (USB-Sticks, externe Festplatten / SSDs, …)

support.microsoft.com/en-us/windows/bitlocker-o

Microsoft | Support Microsoft 365 Office Products More Try Copilot Chat All Microsoft

Windows security, safety, and privacy

- Overview
- Windows security
- Windows safety
- Windows privacy
- BitLocker
  - Overview
  - Device Encryption
  - BitLocker Drive Encryption
  - Find your recovery key
  - Back up your recovery key
- Windows Security app

BitLocker overview

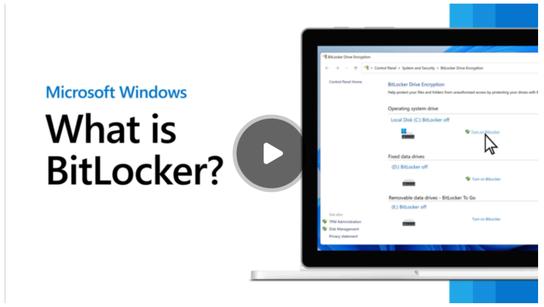
▶ *Applies To*

BitLocker is a Windows security feature that protects your data by encrypting your drives. This encryption ensures that if someone tries to access a disk offline, they won't be able to read any of its content.

BitLocker is particularly valuable if your device is lost or stolen, as it keeps your sensitive information secure. It's designed to be user-friendly and integrates seamlessly with the Windows operating system, making it easy to set up and manage.

BitLocker offers two functionalities:

- *Device Encryption* , which is designed for simplicity of use, and it's usually enabled automatically
- *BitLocker Drive Encryption* , which is designed for advanced scenarios, and it allows you to manually encrypt drives



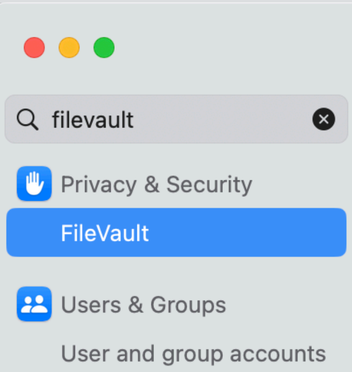
Having trouble playing the video? Watch it on YouTube.

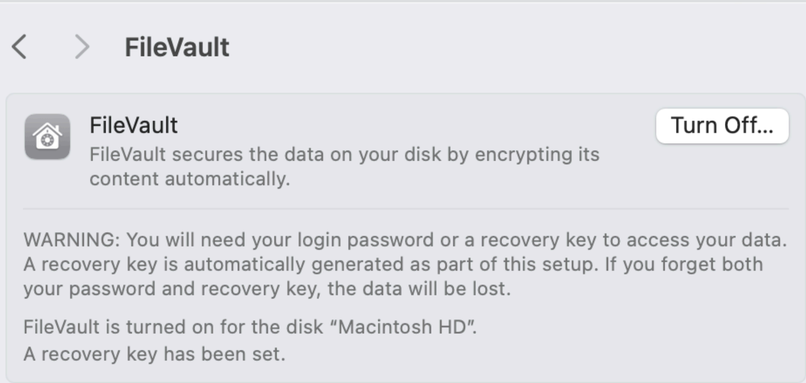
If you have BitLocker turned on for any of your drives, it's important to be sure you have the *BitLocker recovery key* backed up somewhere. If BitLocker detects an unauthorized access to the drive or changes in the hardware, it will prevent access to the disk, asking for the recovery key. If you don't have that key, you won't be able to access the drive.

It only takes a few moments to back up your recovery key. For more information, see Back up your BitLocker recovery key.

BitLocker frequently asked questions (FAQs)

Here's a collection of common questions related to BitLocker. Expand each question to read the answer:





Heute: Viele Daten liegen bei Dritten!

(«Cloud», «Software-as-a-Service»,
Social-Media, …)

Unverzichtbar: Einzigartiges und genügend langes Passwort für jedes Nutzerkonto

Plus: 2-Faktor-Authentifizierung

Private

apps.apple.com/ch/app/passwords/id6473799789

App Store
Open in the App Store app

Open

App Store für iPhone

Suchen

- Heute
- Spiele
- Apps
- Arcade

Kategorien

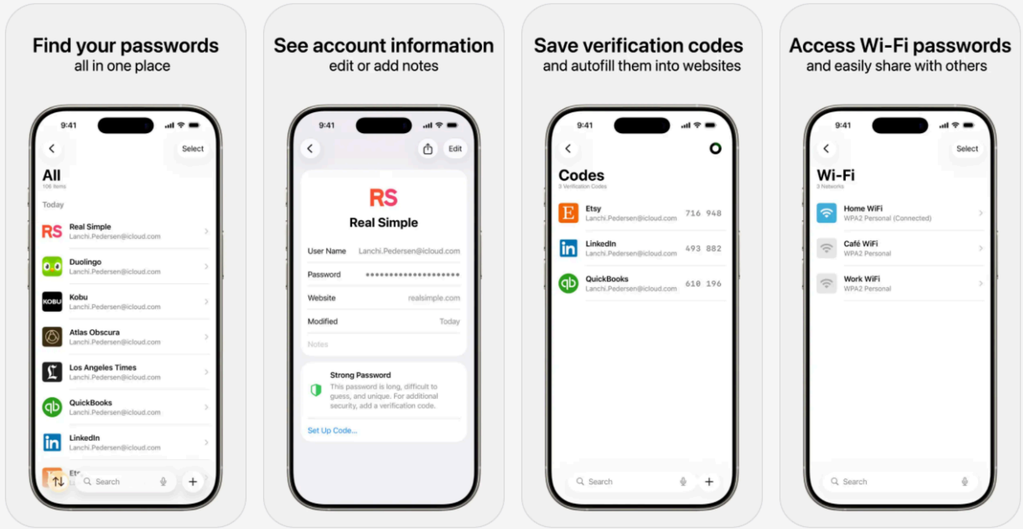
- Kategorien
- Foto und Video
- Gesundheit und Fitness
- Produktivität
- Unterhaltung
- Action
- Abenteuer
- Puzzle
- Indie

Passwords

Dienstprogramme
Kostenlos

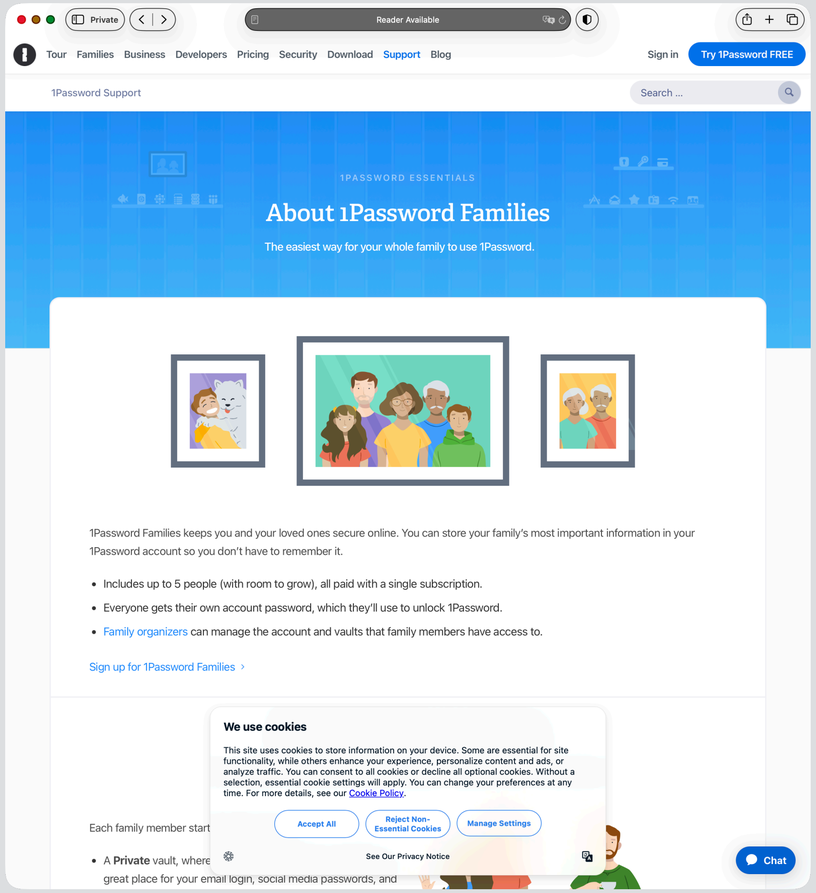
Teilen

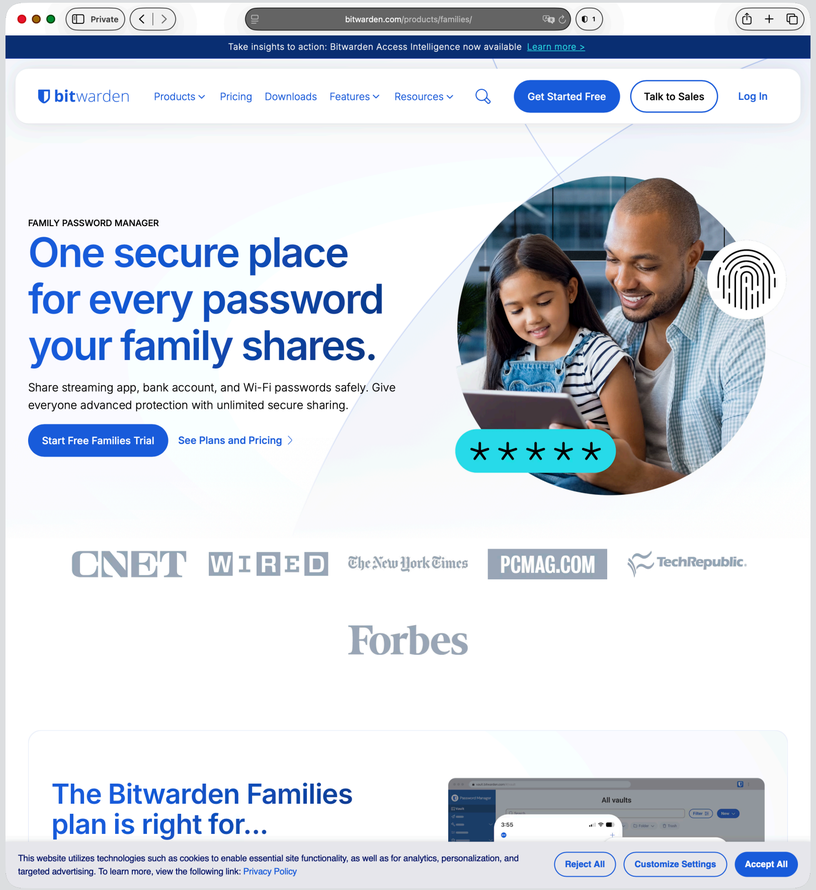
18'593 BEWERTUNGEN	ALTER	KATEGORIE	ENTWICKLUNGSTEAM	SPRACHE
4.7 ★★★★★	4+ Jahre	Dienstprogramme	Apple	EN Englisch

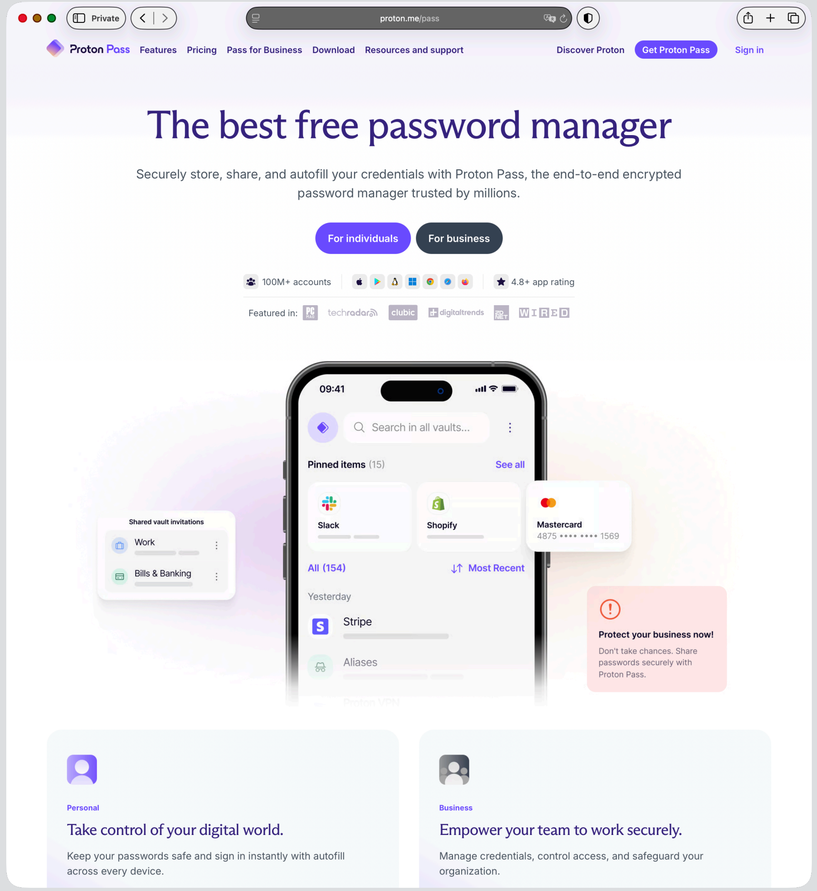


iPhone, iPad

Passwörter


Private
Reader Available
Tour Families Business Developers Pricing Security Download Support Blog
Sign in
Try 1Password FREE
1Password Support
Search ...
1PASSWORD ESSENTIALS
About 1Password Families
The easiest way for your whole family to use 1Password.
1Password Families keeps you and your loved ones secure online. You can store your family's most important information in your 1Password account so you don't have to remember it.
Includes up to 5 people (with room to grow), all paid with a single subscription.
Everyone gets their own account password, which they'll use to unlock 1Password.
Family organizers can manage the account and vaults that family members have access to.
Sign up for 1Password Families
We use cookies
This site uses cookies to store information on your device. Some are essential for site functionality, while others enhance your experience, personalize content and ads, or analyze traffic. You can consent to all cookies or decline all optional cookies. Without a selection, essential cookie settings will apply. You can change your preferences at any time. For more details, see our Cookie Policy.
Accept All
Reject Non-Essential Cookies
Manage Settings
See Our Privacy Notice
Each family member start
A Private vault, where
great place for your email login, social media passwords, and
Chat


Private
bitwarden.com/products/families/
Take insights to action: Bitwarden Access Intelligence now available Learn more >
bitwarden
Products
Pricing
Downloads
Features
Resources
Get Started Free
Talk to Sales
Log In
FAMILY PASSWORD MANAGER
One secure place for every password your family shares.
Share streaming app, bank account, and Wi-Fi passwords safely. Give everyone advanced protection with unlimited secure sharing.
Start Free Families Trial
See Plans and Pricing
CNET
WIRED
The New York Times
PCMAG.COM
TechRepublic.
Forbes
The Bitwarden Families plan is right for...
All vaults
This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. To learn more, view the following link: Privacy Policy
Reject All
Customize Settings
Accept All


Private
proton.me/pass
Proton Pass
Features
Pricing
Pass for Business
Download
Resources and support
Discover Proton
Get Proton Pass
Sign in
The best free password manager
Securely store, share, and autofill your credentials with Proton Pass, the end-to-end encrypted password manager trusted by millions.
For individuals
For business
100M+ accounts
4.8+ app rating
Featured in:
09:41
Search in all vaults...
Pinned items (15)
See all
Slack
Shopify
Mastercard
4875 •••• •••• 1569
Shared vault invitations
Work
Bills & Banking
All (154)
Most Recent
Yesterday
Stripe
Aliases
Protect your business now!
Don't take chances. Share passwords securely with Proton Pass.
Personal
Take control of your digital world.
Keep your passwords safe and sign in instantly with autofill across every device.
Business
Empower your team to work securely.
Manage credentials, control access, and safeguard your organization.

Mit einem Passwort-Manager muss man sich nur noch folgende Passwörter merken:

- Zugang zum Smartphone und anderen Computern
- Zugriff auf Passwort-Manager / Schlüsselbund

Messaging & Social Media

Idealfall: Nutzung von datensparsamen Messaging-Diensten mit Ende-zu-Ende-Verschlüsselung

Private

signal.org

Signal

Get Signal Help Blog Developers Careers Donate English

Speak Freely

Say "hello" to a different messaging experience. An unexpected focus on privacy, combined with all of the features you expect.

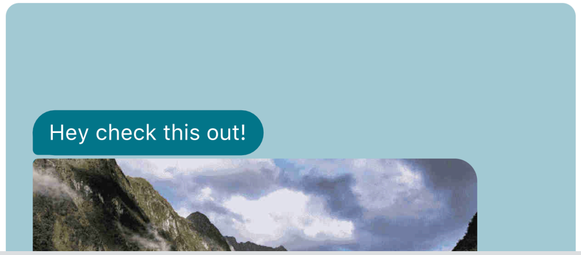
Get Signal

Why use Signal?

Explore below to see why Signal is a simple, powerful, and secure messenger

Share Without Insecurity

State-of-the-art end-to-end encryption (powered by the open source Signal Protocol) keeps your conversations secure. We can't read your messages or listen to your calls, and no one else can either. Privacy



Private

Reader Available

THREEMA

ANMELDEN DE

ÜBER UNS PRODUKTE LÖSUNGEN RESSOURCEN PREISE

JETZT LOSLEGEN

THREEMA PRIVATE

PRIVATSPHÄRE OHNE KOMPROMISSE

Mit Freunden und Familie in völliger Vertraulichkeit kommunizieren – ohne Datenschnüffelei, ohne Metadatensammlung, ohne Kompromisse.

APP HERUNTERLADEN

EIN STARKES FUNDAMENT FÜR IHRE KOMMUNIKATION

Alle unsere Threema-Lösungen sind einzigartig in ihrer Ausführung, doch sie basieren auf dem gleichen starken Fundament. Die drei Aspekte **Vertrauen**, **Transparenz** und **Technologie** bilden das Herzstück unserer Philosophie und schaffen die Basis für sichere, souveräne und zukunftsfähige Kommunikationslösungen.

TRUST

Sichere Kommunikation beginnt mit Vertrauen. Threema schützt Ihre Inhalte durch konsequente Ende-zu-Ende-Verschlüsselung – ganz ohne Angabe persönlicher Daten wie Telefonnummer oder E-Mail-Adresse. Das Prinzip der Datensparsamkeit steht im Mittelpunkt. Millionen Nutzer weltweit, ob privat oder geschäftlich, setzen täglich auf diese Sicherheit.

TRANSPARENCY

Wer Sicherheit verspricht, muss sie nachweislich gewährleisten. Threema ist Open Source, wird regelmässig von unabhängigen Experten geprüft und erfüllt alle Anforderungen der DSGVO. Statt Tracking oder versteckter Datennutzung in unseren Anwendungen setzen wir auf konsequente Datensparsamkeit und transparente Prozesse – für volle Nachvollziehbarkeit.

TECHNOLOGY

Modern, leistungsstark, vielseitig: Threema setzt auf zukunftsfähige Technologie für eine stabile, plattformübergreifende Kommunikation – egal, ob privat, im Unternehmen oder komplett selbstgehostet. Dank Active-Directory- und MDM-Anbindung, APIs und flexibler Infrastruktur passt sich Threema nahtlos an jede Umgebung an. Sichere Kommunikation «made in Switzerland».

Tabelle filtern + -

Messenger

Letzte Aktualisierung: 07. Januar 2026

	Briar	Conversations (XMPP)	Delta Chat	Discord	Element (Matrix)	Facebook Messenger	Google Messages	iMessage
Allgemeine Informationen								
Entwickler	Briar Team	Daniel Gultsch	Merlinux	Discord Inc.	New Vector	Meta Platforms	Google	Apple
Erscheinungsjahr	2017	2014	2017	2015	2016	2011	2014	2011
Anzahl Downloads (Play Store)	1 Million	100 Tausend	1 Million	500 Millionen	1 Million	5 Milliarden	5 Milliarden	—
Kosten	—	4,99 € / keine (F-Droid)	—	—	—	—	—	—
Systemunterstützung								
Android	ja	ja	ja	ja	ja	ja	ja	nein
iOS	nein	nein (siehe Monal)	ja	ja	ja	ja	nein	ja
Desktop	Windows, macOS,	ja (diverse	Windows, macOS,	Windows, macOS,	ja (diverse	Windows,	nein	nur macOS

Häufige Realität: WhatsApp ohne datensparsame Einstellungen und mit extensiver «Status»-Nutzung

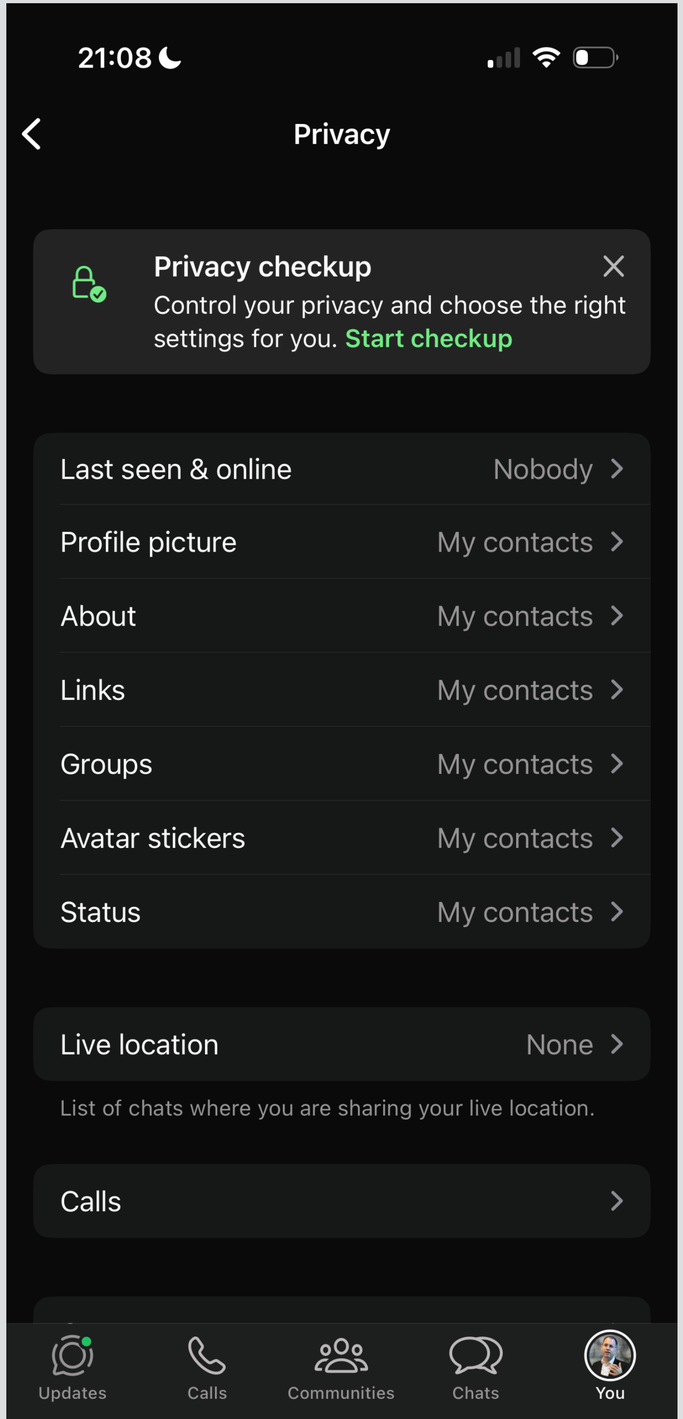
Private

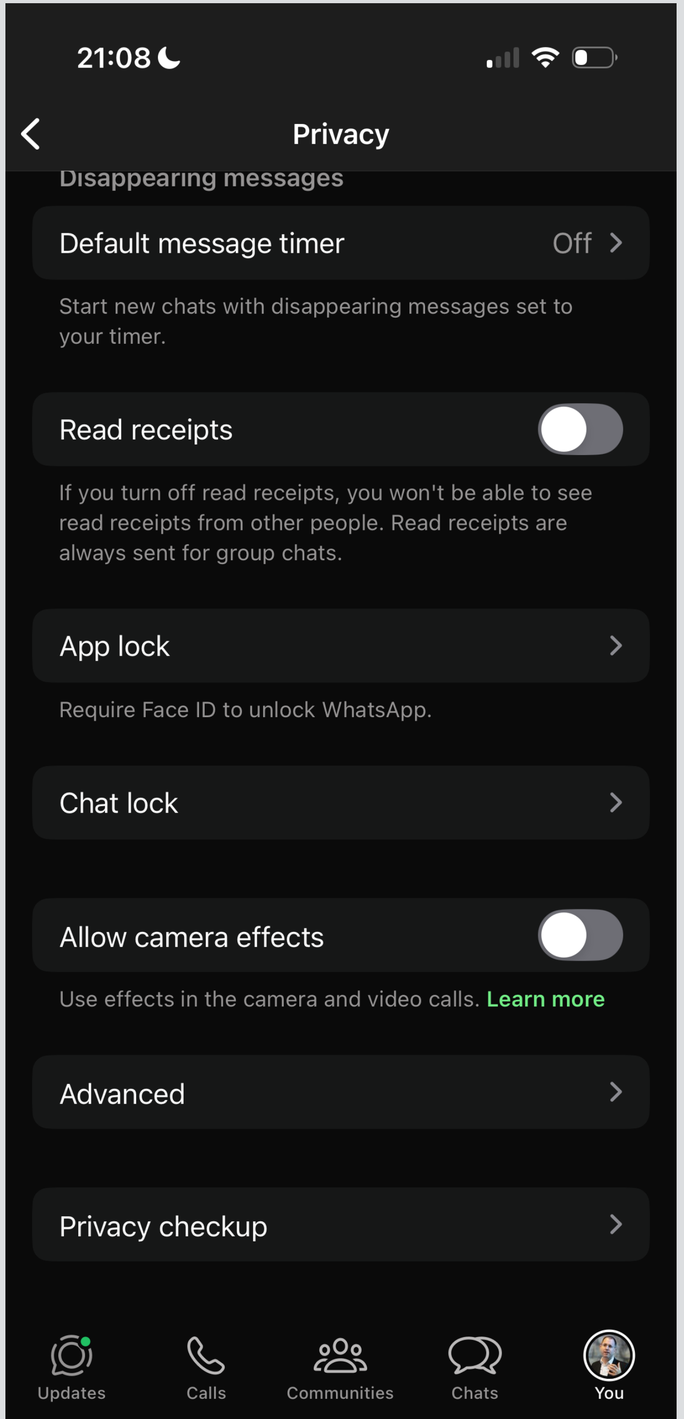
www.whatsapp.com/status?lang=de

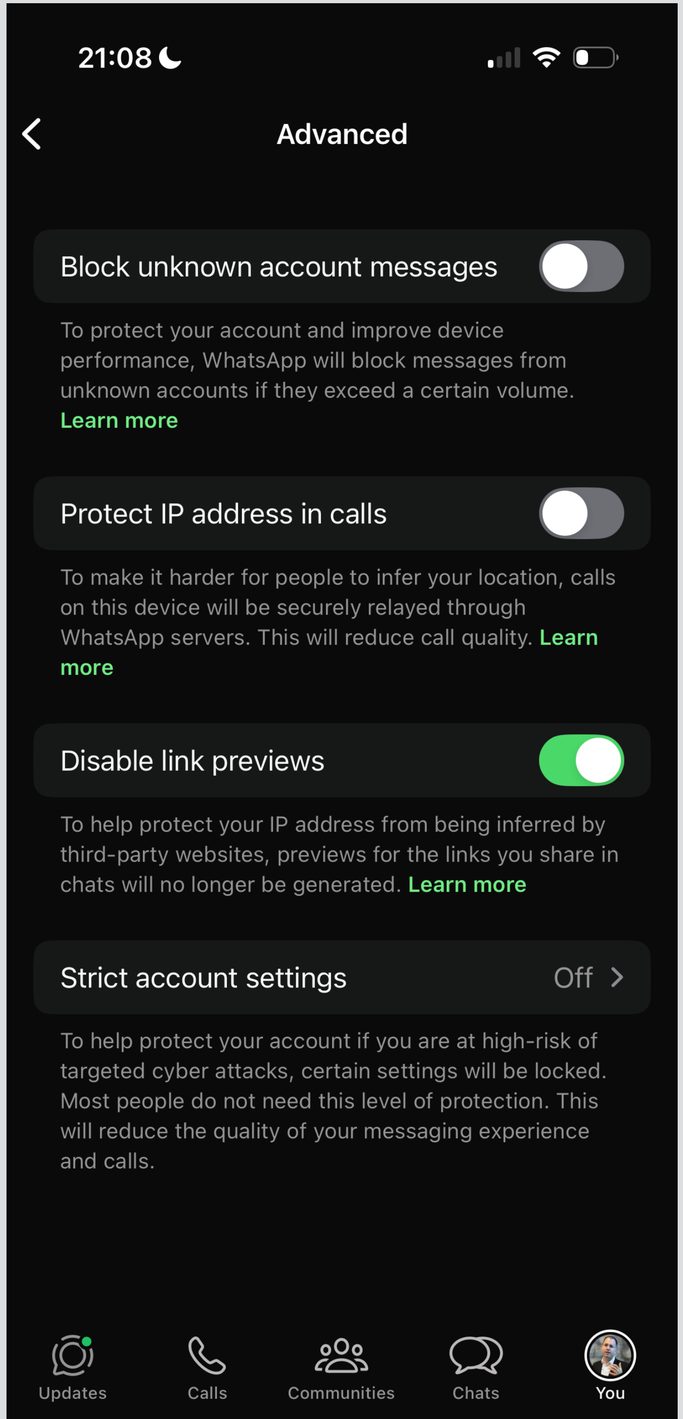
WhatsApp

Bleibe mit Statusmeldunge auf dem Laufenden

Teile mit deinen Liebsten deinen WhatsApp-Status, der Fotos, Videos, Sprachnachrichten und Text enthalten kann. Personalisiere deinen Status mit


21:08
Privacy
Privacy checkup
Control your privacy and choose the right settings for you. Start checkup
Last seen & online
Nobody
Profile picture
My contacts
About
My contacts
Links
My contacts
Groups
My contacts
Avatar stickers
My contacts
Status
My contacts
Live location
None
List of chats where you are sharing your live location.
Calls
Updates
Calls
Communities
Chats
You

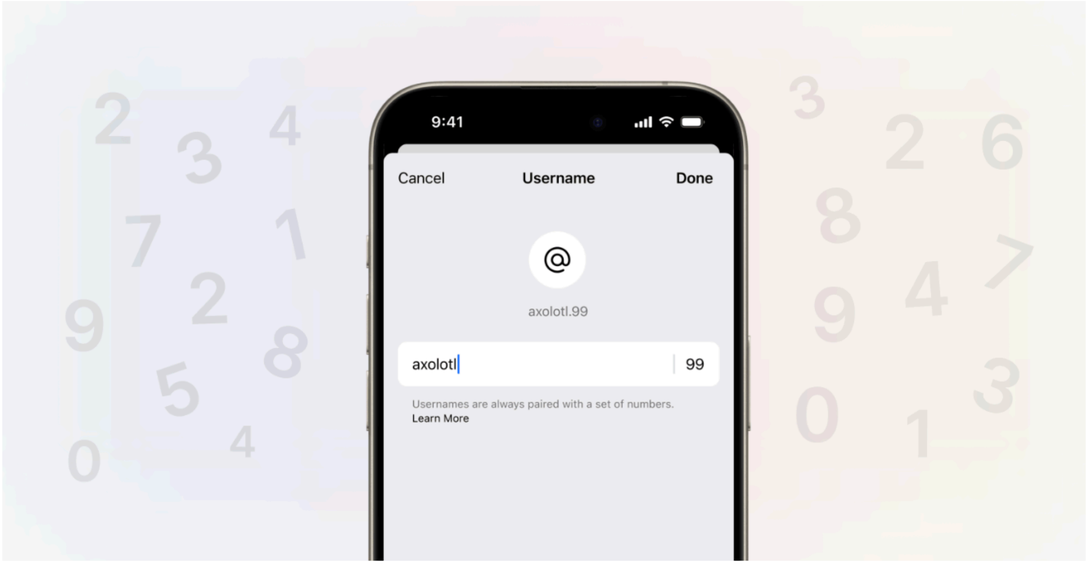

21:08
Privacy
Disappearing messages
Default message timer
Off
Start new chats with disappearing messages set to your timer.
Read receipts
If you turn off read receipts, you won't be able to see read receipts from other people. Read receipts are always sent for group chats.
App lock
Require Face ID to unlock WhatsApp.
Chat lock
Allow camera effects
Use effects in the camera and video calls. Learn more
Advanced
Privacy checkup
Updates
Calls
Communities
Chats
You

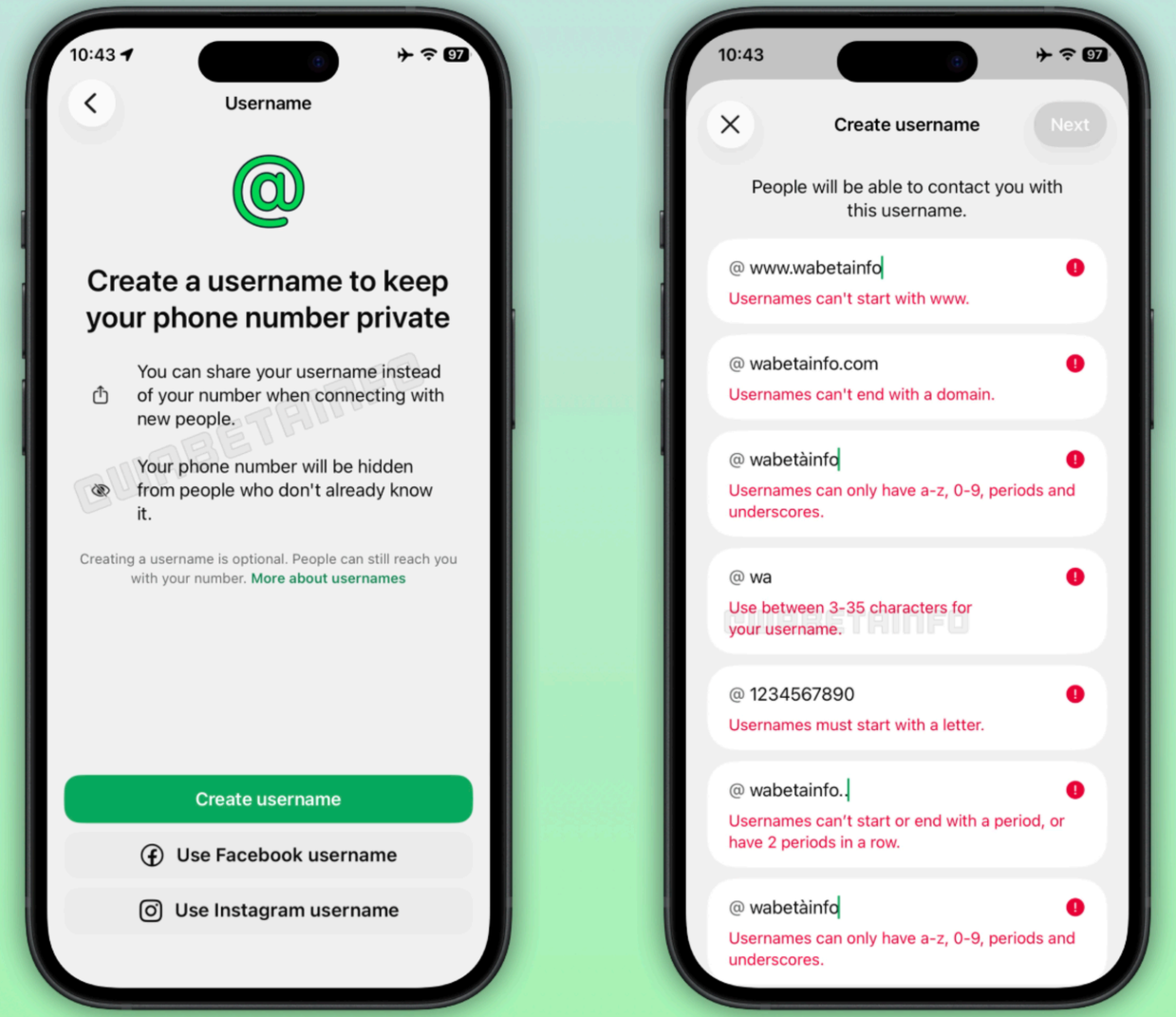

21:08
Advanced
Block unknown account messages
To protect your account and improve device performance, WhatsApp will block messages from unknown accounts if they exceed a certain volume. Learn more
Protect IP address in calls
To make it harder for people to infer your location, calls on this device will be securely relayed through WhatsApp servers. This will reduce call quality. Learn more
Disable link previews
To help protect your IP address from being inferred by third-party websites, previews for the links you share in chats will no longer be generated. Learn more
Strict account settings
Off
To help protect your account if you are at high-risk of targeted cyber attacks, certain settings will be locked. Most people do not need this level of protection. This will reduce the quality of your messaging experience and calls.
Updates
Calls
Communities
Chats
You

Messaging: Nutzerkonten basieren vielfach auf Telefonnummern, aber das Bewusstsein bei den Anbietern wächst

Keep your phone number private with Signal usernames

Signal on 20 Feb 2024




10:43
97
Username
Create a username to keep your phone number private
You can share your username instead of your number when connecting with new people.
Your phone number will be hidden from people who don't already know it.
Creating a username is optional. People can still reach you with your number. More about usernames
Create username
Use Facebook username
Use Instagram username
10:43
97
Create username
Next
People will be able to contact you with this username.
@ www.wabetainfo
Usernames can't start with www.
@ wabetainfo.com
Usernames can't end with a domain.
@ wabetàinfo
Usernames can only have a-z, 0-9, periods and underscores.
@ wa
Use between 3-35 characters for your username.
@ 1234567890
Usernames must start with a letter.
@ wabetainfo.
Usernames can't start or end with a period, or have 2 periods in a row.
@ wabetàinfo
Usernames can only have a-z, 0-9, periods and underscores.

Messaging ➡️ Social-Media

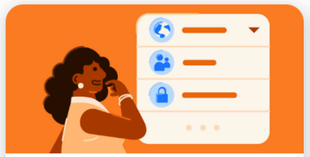
(6) Facebook

https://www.facebook.com/privacy/unified_checkup/

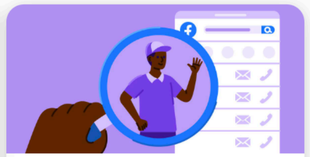
Privatsphäre-Check

Wir zeigen dir einige Einstellungen und helfen dir dabei, die richtige Auswahl für dein Konto zu treffen.

Mit welchem Thema möchtest du starten?



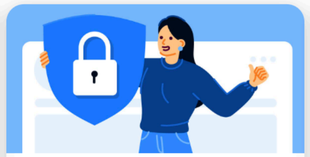
Wer sehen kann, was du teilst



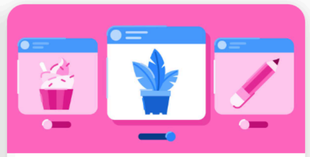
So können andere dich auf Facebook finden

Deine Daten-Einstellungen auf Facebook

Vor einem Jahr



So kannst du dein Konto schützen



Deine Werbepräferenzen auf Facebook

Weitere Privatsphäre-Einstellungen findest du auf Facebook in den **Einstellungen**

10:41 5:44

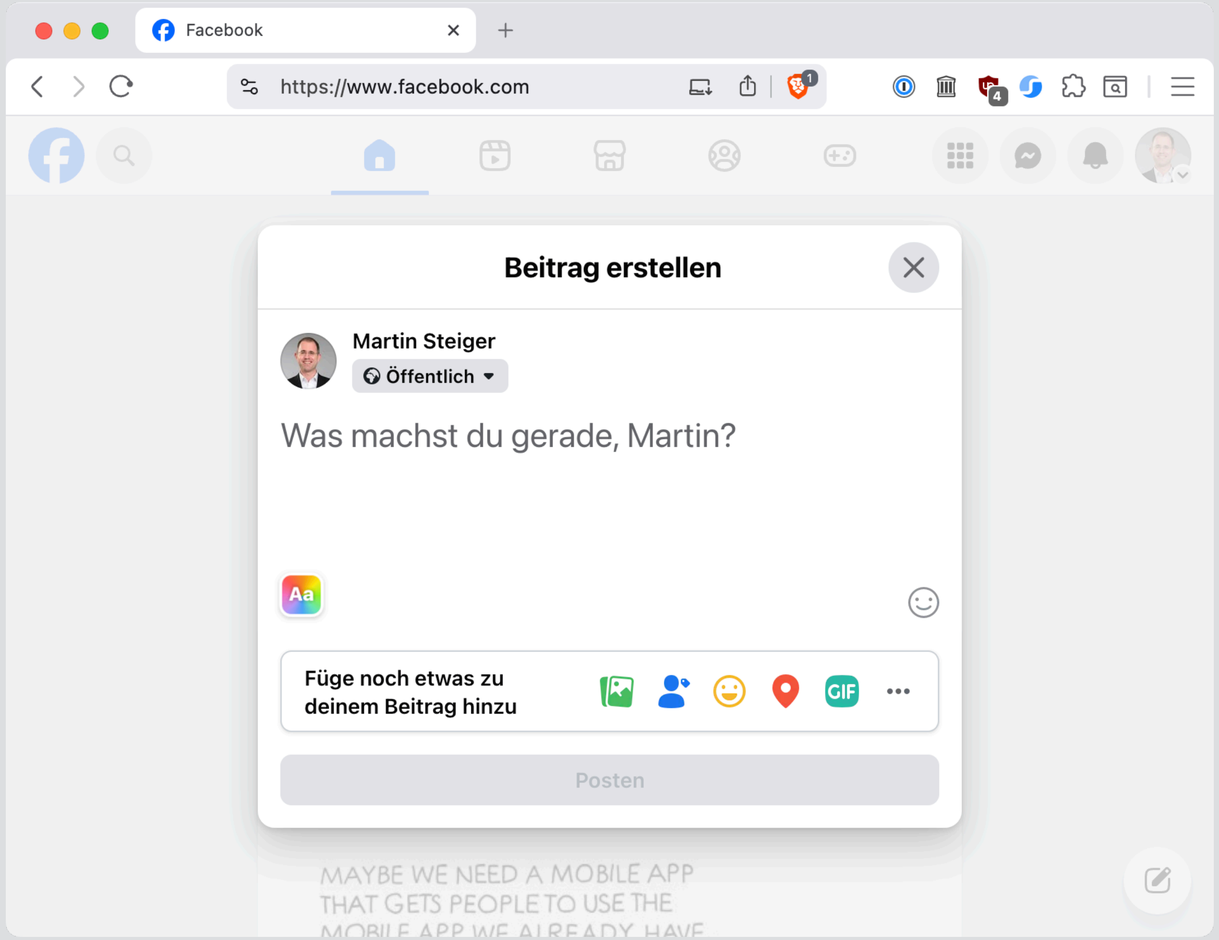
Help

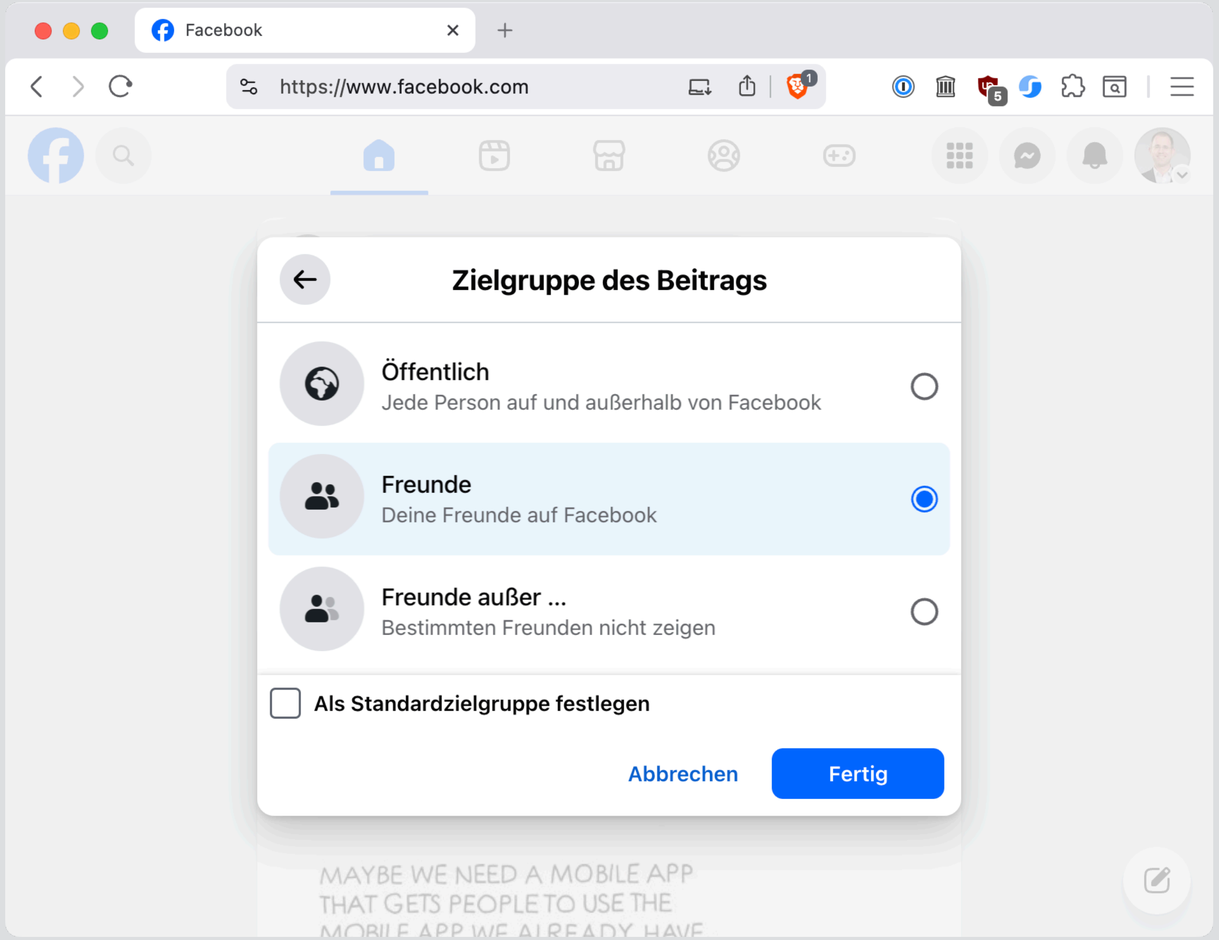
Security checkup

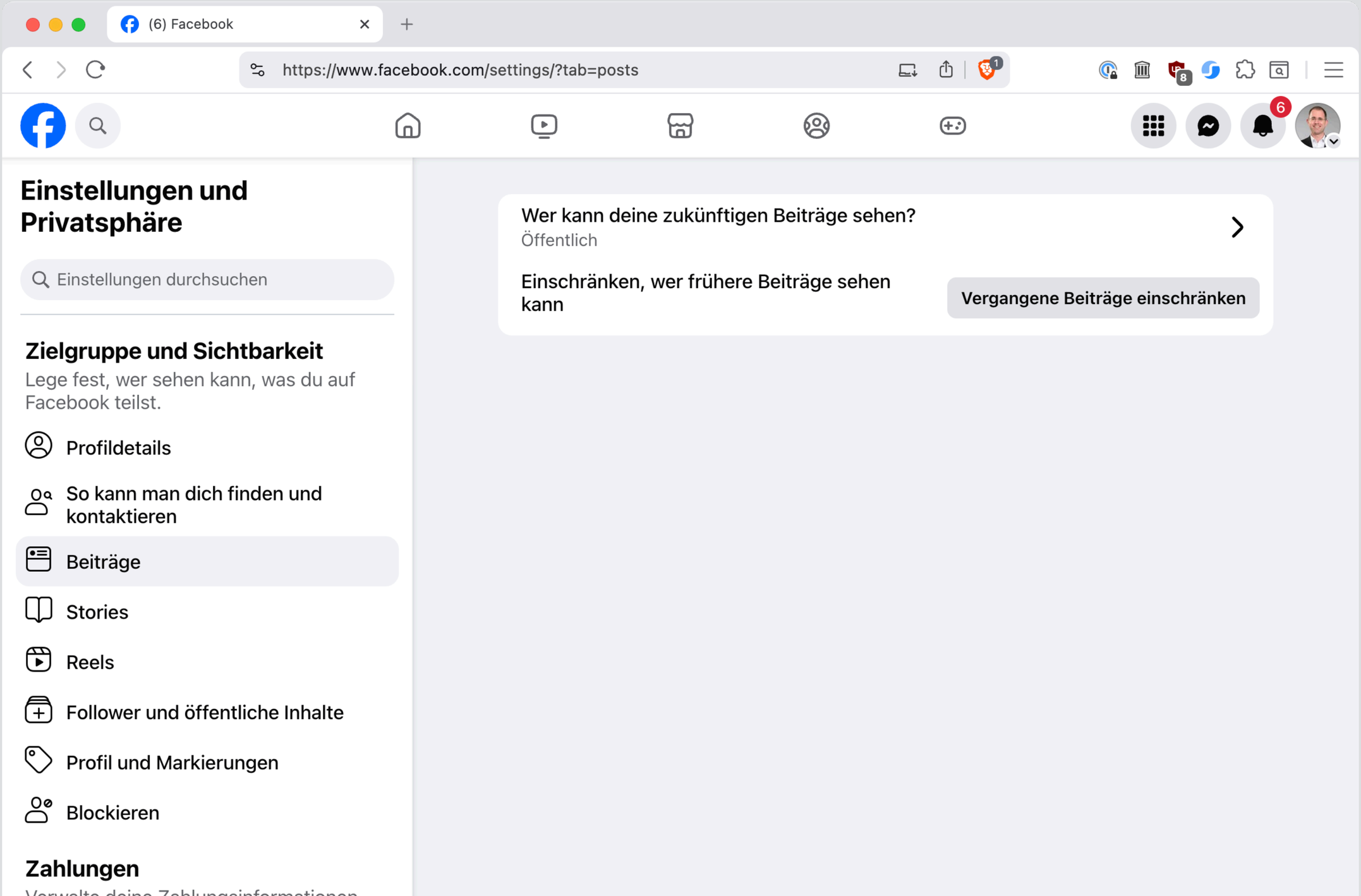
Well done checking off the security tips to keep your account safe.

- **Phone** [redacted]
- **Email** [redacted]
- **2-step verification** [redacted]
- **Your devices** [redacted]
- **Security activity**
  No unusual activity in the last 30 days.
- **Passkey**
  You've created a passkey for a quicker and safer login.

Erneut: Besser spät als nie!

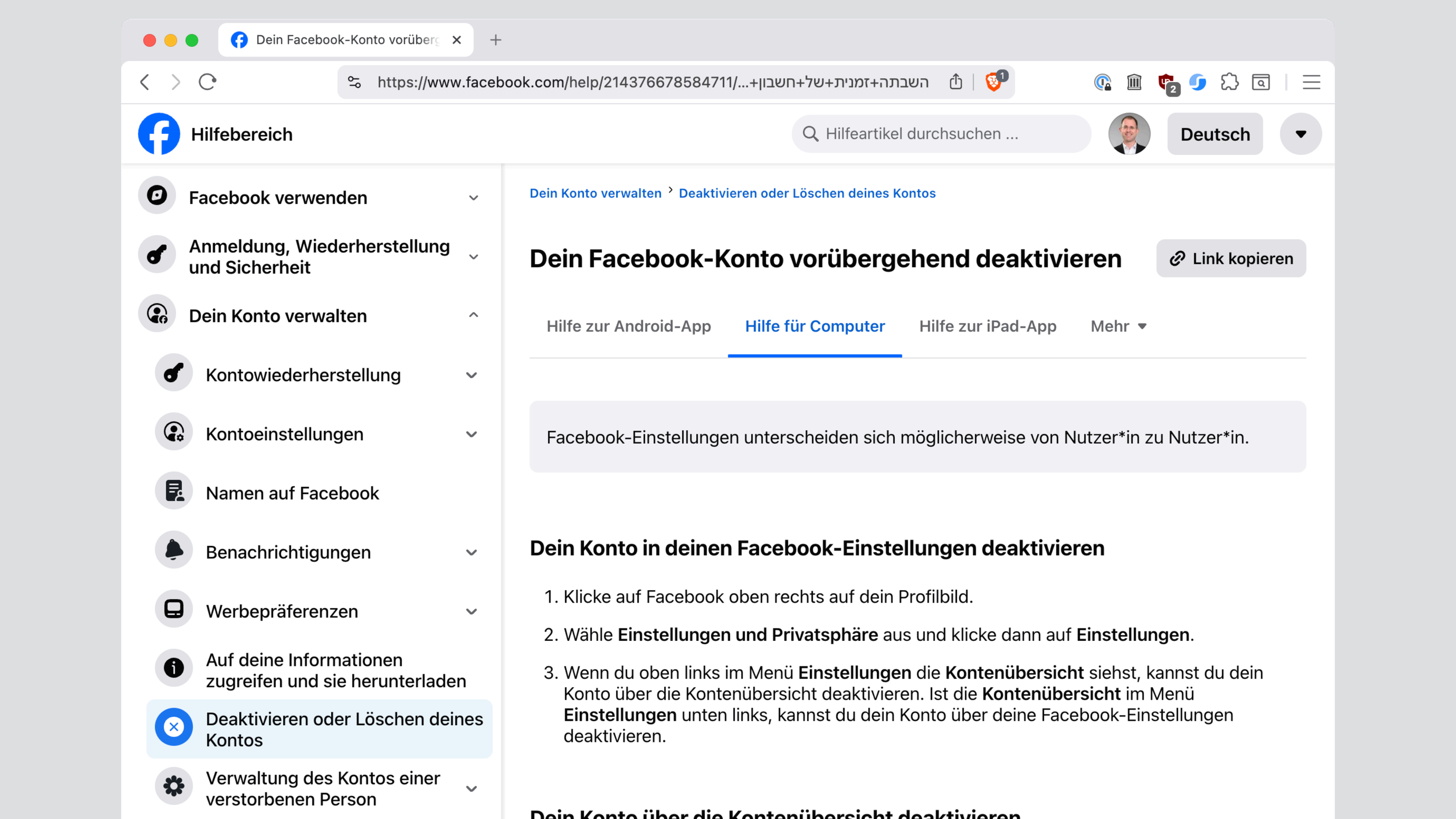

Facebook
https://www.facebook.com
Beitrag erstellen
Martin Steiger
Öffentlich
Was machst du gerade, Martin?
Füge noch etwas zu deinem Beitrag hinzu
Posten
MAYBE WE NEED A MOBILE APP
THAT GETS PEOPLE TO USE THE


Facebook
https://www.facebook.com
Zielgruppe des Beitrags
Öffentlich
Jede Person auf und außerhalb von Facebook
Freunde
Deine Freunde auf Facebook
Freunde außer ...
Bestimmten Freunden nicht zeigen
Als Standardzielgruppe festlegen
Abbrechen
Fertig
MAYBE WE NEED A MOBILE APP
THAT GETS PEOPLE TO USE THE


(6) Facebook
https://www.facebook.com/settings/?tab=posts
6
Einstellungen und Privatsphäre
Einstellungen durchsuchen
Zielgruppe und Sichtbarkeit
Lege fest, wer sehen kann, was du auf Facebook teilst.
Profildetails
So kann man dich finden und kontaktieren
Beiträge
Stories
Reels
Follower und öffentliche Inhalte
Profil und Markierungen
Blockieren
Zahlungen
Wer kann deine zukünftigen Beiträge sehen?
Öffentlich
Einschränken, wer frühere Beiträge sehen kann
Vergangene Beiträge einschränken

Im Ernstfall: «Going dark!»

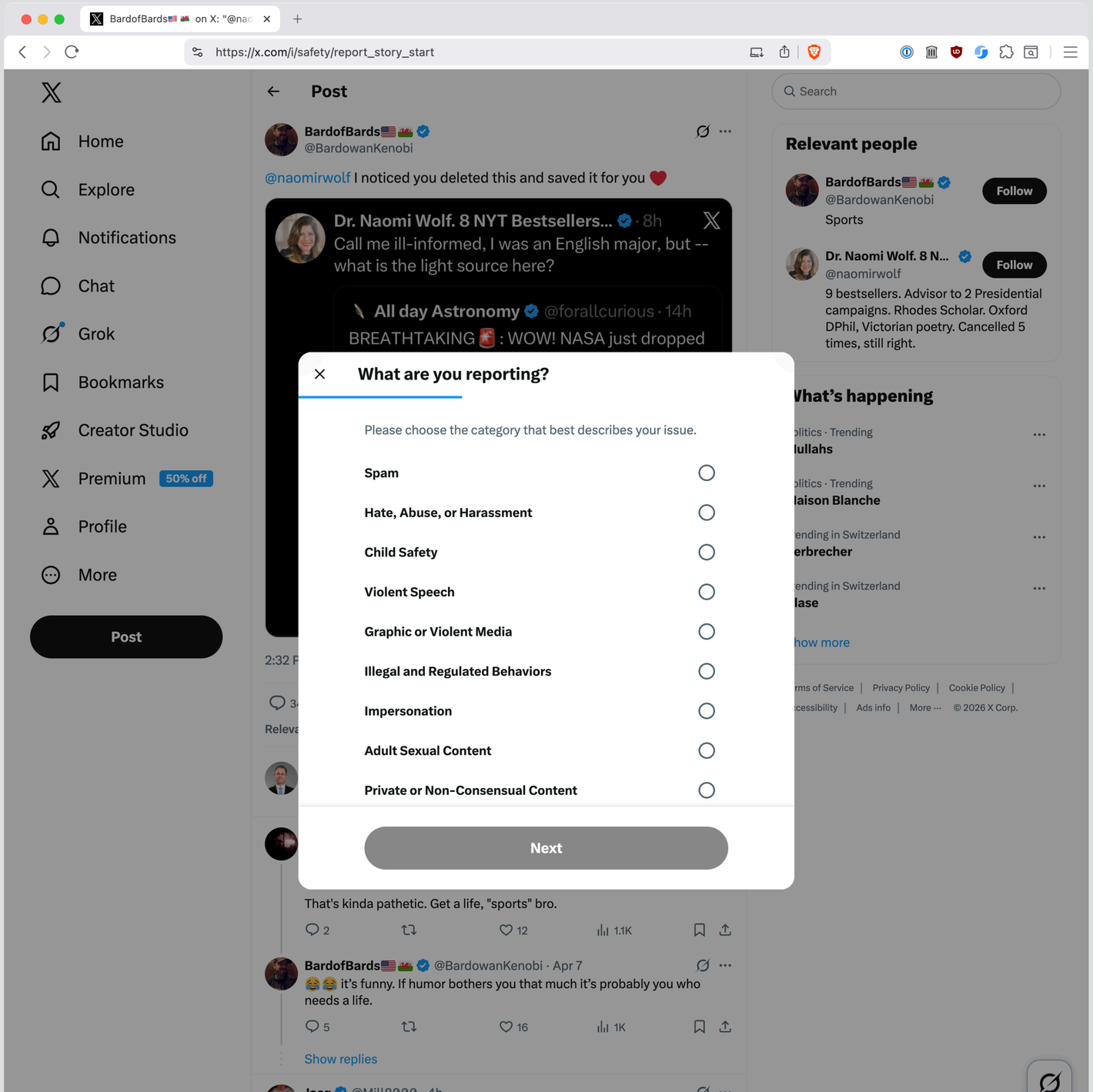
(Gegner:innen dokumentieren
häufig nicht rechtzeitig …)

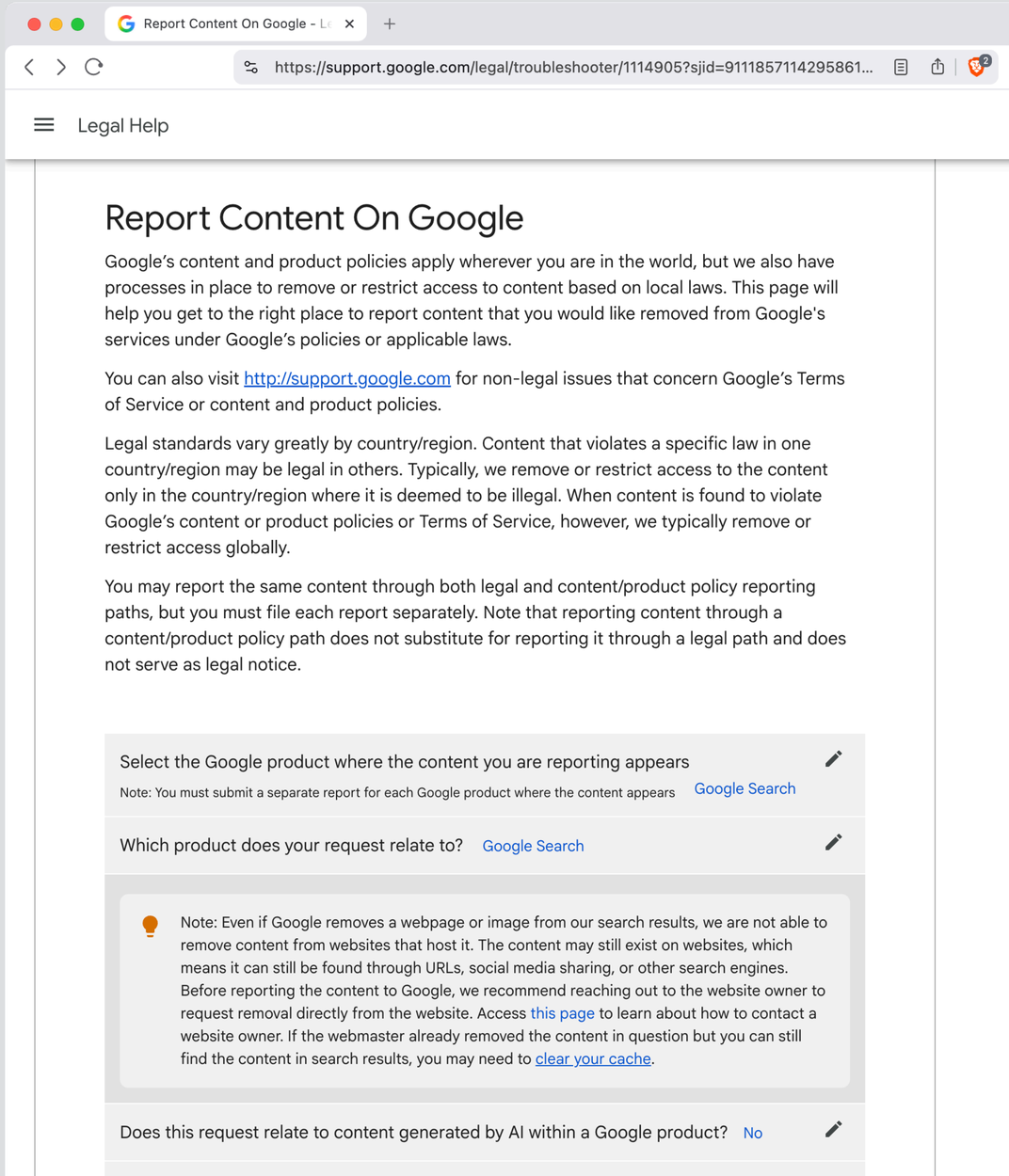

Dein Facebook-Konto vorüberg
https://www.facebook.com/help/214376678584711/...+השבתה+זמנית+של+חשבון
Hilfebereich
Hilfeartikel durchsuchen ...
Deutsch
Facebook verwenden
Anmeldung, Wiederherstellung und Sicherheit
Dein Konto verwalten
Kontowiederherstellung
Kontoeinstellungen
Namen auf Facebook
Benachrichtigungen
Werbepräferenzen
Auf deine Informationen zugreifen und sie herunterladen
Deaktivieren oder Löschen deines Kontos
Verwaltung des Kontos einer verstorbenen Person
Dein Konto verwalten › Deaktivieren oder Löschen deines Kontos
Dein Facebook-Konto vorübergehend deaktivieren
Link kopieren
Hilfe zur Android-App
Hilfe für Computer
Hilfe zur iPad-App
Mehr
Facebook-Einstellungen unterscheiden sich möglicherweise von Nutzer*in zu Nutzer*in.
Dein Konto in deinen Facebook-Einstellungen deaktivieren
1. Klicke auf Facebook oben rechts auf dein Profilbild.
2. Wähle Einstellungen und Privatsphäre aus und klicke dann auf Einstellungen.
3. Wenn du oben links im Menü Einstellungen die Kontenübersicht siehst, kannst du dein Konto über die Kontenübersicht deaktivieren. Ist die Kontenübersicht im Menü Einstellungen unten links, kannst du dein Konto über deine Facebook-Einstellungen deaktivieren.

Unerwünschte Inhalte bei Plattformen und auf Websites

Sofern möglich: Beschwerde über Mechanismen der Plattformen und Website-Betreiberinnen

Hilfreich: Inhalte sind klar strafbar oder verstossen klar gegen die Richtlinien der jeweiligen Plattform


BardofBards on X: "@nac
https://x.com/i/safety/report_story_start
Home
Explore
Notifications
Chat
Grok
Bookmarks
Creator Studio
Premium
50% off
Profile
More
Post
Post
BardofBards
@BardowanKenobi
@naomirwolf I noticed you deleted this and saved it for you
Dr. Naomi Wolf. 8 NYT Bestsellers... · 8h
Call me ill-informed, I was an English major, but -- what is the light source here?
All day Astronomy @forallcurious · 14h
BREATHTAKING : WOW! NASA just dropped
What are you reporting?
Please choose the category that best describes your issue.
Spam
Hate, Abuse, or Harassment
Child Safety
Violent Speech
Graphic or Violent Media
Illegal and Regulated Behaviors
Impersonation
Adult Sexual Content
Private or Non-Consensual Content
Next
That's kinda pathetic. Get a life, "sports" bro.
BardofBards @BardowanKenobi · Apr 7
it's funny. If humor bothers you that much it's probably you who needs a life.
Show replies
Search
Relevant people
BardofBards
@BardowanKenobi
Sports
Follow
Dr. Naomi Wolf. 8 N...
@naomirwolf
9 bestsellers. Advisor to 2 Presidential campaigns. Rhodes Scholar. Oxford DPhil, Victorian poetry. Cancelled 5 times, still right.
Follow
What's happening
Trending
Trending
Trending in Switzerland
Trending in Switzerland
Show more
Terms of Service | Privacy Policy | Cookie Policy |
Accessibility | Ads info | More ··· | © 2026 X Corp.


Report Content On Google - Le
https://support.google.com/legal/troubleshooter/1114905?sjid=9111857114295861...
Legal Help
Report Content On Google
Google's content and product policies apply wherever you are in the world, but we also have processes in place to remove or restrict access to content based on local laws. This page will help you get to the right place to report content that you would like removed from Google's services under Google's policies or applicable laws.
You can also visit http://support.google.com for non-legal issues that concern Google's Terms of Service or content and product policies.
Legal standards vary greatly by country/region. Content that violates a specific law in one country/region may be legal in others. Typically, we remove or restrict access to the content only in the country/region where it is deemed to be illegal. When content is found to violate Google's content or product policies or Terms of Service, however, we typically remove or restrict access globally.
You may report the same content through both legal and content/product policy reporting paths, but you must file each report separately. Note that reporting content through a content/product policy path does not substitute for reporting it through a legal path and does not serve as legal notice.
Select the Google product where the content you are reporting appears
Note: You must submit a separate report for each Google product where the content appears Google Search
Which product does your request relate to? Google Search
Note: Even if Google removes a webpage or image from our search results, we are not able to remove content from websites that host it. The content may still exist on websites, which means it can still be found through URLs, social media sharing, or other search engines. Before reporting the content to Google, we recommend reaching out to the website owner to request removal directly from the website. Access this page to learn about how to contact a website owner. If the webmaster already removed the content in question but you can still find the content in search results, you may need to clear your cache.
Does this request relate to content generated by AI within a Google product? No

Alltag: Viele Plattform- oder Website-Betreiberinnen lehnen Beschwerden direkt ab oder reagieren gar nicht

TikTok verliert vor Gericht m

https://www.youtube.com/watch?v=rGxYE2...

Premium CH

Search

Create

TikTok verliert vor Gericht mit seinem Fake-Meldesystem

Anwalt Jun
46.6K subscribers

1.6K | Share | Save | Download

14K views 1 year ago
/ anwaltjun

Ebenfalls Alltag: Reaktion kann auch im besten Fall sofort Tage dauern!

Anwaltliche Abmahnung: Gleiches Problem … aber dauert allenfalls noch länger …

Superprovisorische vorsorgliche Massnahmen: Aufwendig 💰💰💰, aber je nach Gericht relativ schnell verfügt, doch wie wird vollstreckt? 😬

Strafrecht: Viel zu langsam … aber je nach Inhalten kann das kantonale Bedrohungsmanagement helfen 💡

Faktisch: Die meisten betroffenen Personen können sich nur im Einzelfall oder gar nicht wirksam zur Wehr setzen 🤷

Auf den Punkt gebracht ✅

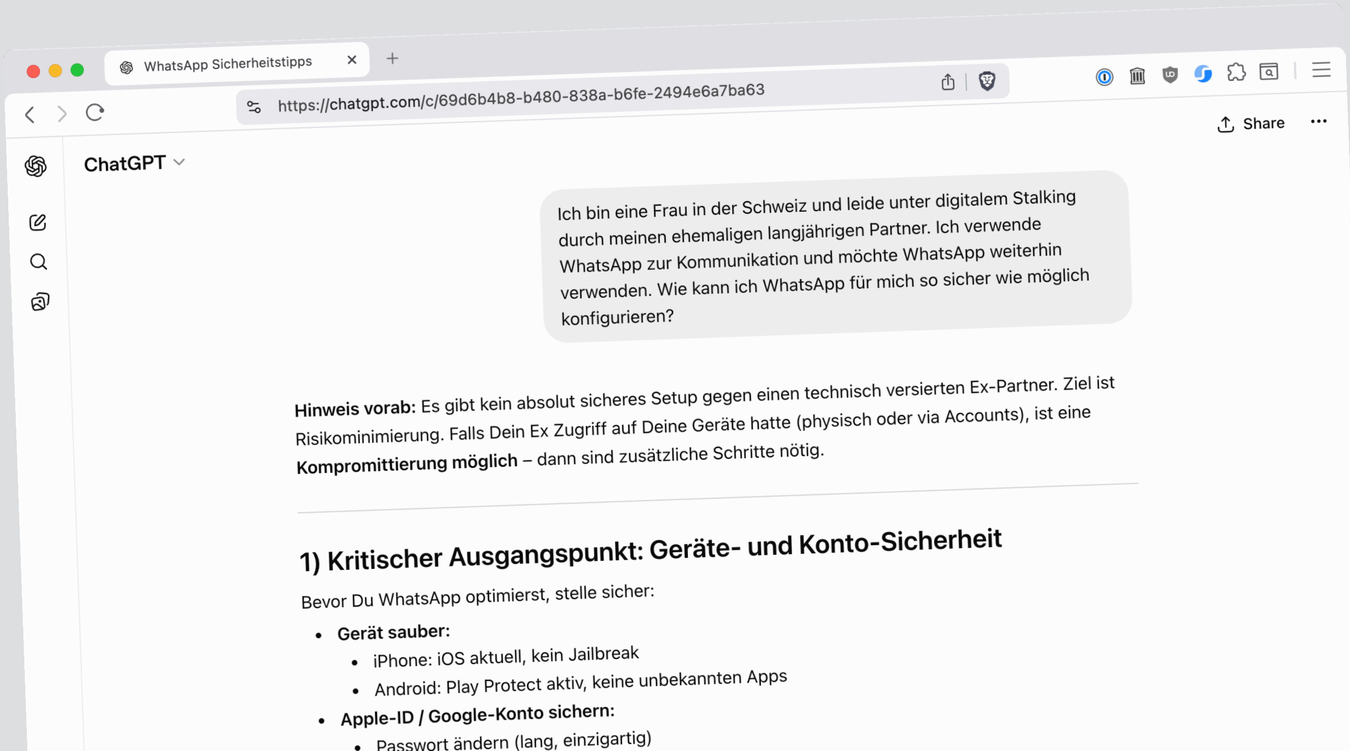
Grundlegende Frage: Wer hat wie und wo Zugriff auf mein «digitales Leben»?

Insbesondere: Smartphone? Cloud-Dienste? Social-Media-Plattformen?

- **Im Alltag:** Präventive Massnahmen zum eigenen Datenschutz
- **Im Ernstfall:** Verschärfte Massnahmen bis «Going dark» und Absicherung der Kommunikation – auch mit anwaltlicher Unterstützung

Alles in allem: Fleissarbeit, die sich lohnt!

(Und allenfalls kann KI helfen …)



martinsteiger.ch 🙏