

# Allgemeines

- [Hausdurchsuchung](#)
- [Checkliste Sicherer Umgang mit Technik](#)
- [Staatstrojaner in Deutschland](#)

# Hausdurchsuchung

Hier geht es um den Technikaspekt von Hausdurchsuchungen. Für den juristischen Teil gibt es eine eigene Seite im [Legal Wiki](#).

Laptop und andere Technik hausdurchsuchbar machen hat 2 Säulen:

1. Daten vor fremden Augen sichern
2. arbeitsfähig bleiben

## Daten vor fremden Augen sichern

### Allgemein

Alle angebotenen Betriebssystemupdates schnellstmöglich installieren.

## Gerätespeicher verschlüsseln

- [Android verschlüsseln](#)
- iOS: ist von Haus aus verschlüsselt
- [Windows verschlüsseln mit Bitlocker](#)
- [macOS verschlüsseln](#)

## Messenger

Verhindern, dass Team Blau sich Signal und Telegram mit eurer Nummer installieren kann:

- bei [Signal eine PIN einrichten](#)
- bei Telegram ein Passwort einrichten, denn Telegram synchronisiert alle Inhalte auf das Handy der Polizei, indass sie die Ersatzsimkarte vom Provider einlegen.

Sollte dein Handy ohne Telegram-Passwort beschlagnahmt werden, keine Panik. Dann

kannst du dein Telegram-Konto mittels <https://my.telegram.org/auth?to=delete> löschen.

PIN und Passwort solltest du in deinem [Passwortmanager](#) abspeichern.

# nach Hausdurchsuchung arbeitsfähig bleiben

Die folgenden Schritte solltet ihr jetzt durchdenken, damit ihr nach einer Hausdurchsuchung arbeitsfähig bleibt.

- SIM-Karte nachbestellen: prüft vorher, ob ihr eine Hotline oder eine Onlinemöglichkeit findet, um bei eurem Mobilfunkanbieter eine SIM-Karte nachzubestellen.  
Die Lieferzeiten sind sehr unterschiedlich: Beim klimafreundlichen Anbieter WEtell geht das z.B. innerhalb eines Werktages; bei ALDI TALK dauert es 8 Werktage.  
Wenn ihr die Handynummer behaltet, dann sperrt ihr die Polizei aus [Signal](#) aus.
- Zugriff auf Passwörter behalten: [Passwortmanager-Bitwarden](#)
- verschlüsseltes Backup bei fernen Verwandten oder Nicht-LG-Freunden aufbewahren. Eine sichere Verschlüsselung für Backups von:
  - Laptops: z.B. `restic`.
  - iOS: auf einem Mac oder einem Windows-Computer mit iTunes herstellen. Wichtig: Backup mit Passwort sichern, damit es vollständig ist.
  - Android: bitte ergänzen, wie das genau geht.
- Habt ihr irgendwo eine 2-Faktor-Authentifizierung (2FA) aktiviert? Dann überlegt, ob ihr da noch rankommt, wenn die Technik von zu Hause verschwunden ist.

## Skillshare-Video



## Tipps für's Smartphone

1. Ihr könnt im Telefon Notfall-Kontakte hinterlegen. Die könnt ihr anrufen, ohne das Handy entsperren zu müssen. Da könnt ihr z. B. die Nummer vom EA hinterlegen oder von Menschen, die bei euch im Haus wohnen. Anleitung:

<https://www.chip.de/news/Notfallinfos-auf-dem-Sperrbildschirm-Das-kann-im-Ernstfall-Ihr->

[Leben-retten 184234487.html](#) Es ist jedoch unrealistisch, dass die Polizei bei einer Hausdurchsuchung erlaubt, dass ihr euer eigenes Telefon berührt.

2. Wir haben die Erfahrung gemacht, dass die Polizei beschlagnahmte Smartphones in den Flugmodus setzt. Sie haben manchmal auch spezielle Beutel mit Powerbank, um das Telefon angeschaltet, aber funklos zu halten. Damit kann sie verhindern, dass das Gerät nicht aus der Ferne gelöscht wird.

- auf Android:

In den Quick Settings könnt ihr den Flugmodus aktivieren bzw mobile Daten ausschalten. Prüfe, ob das auch aus dem Sperrbildschirm heraus geht, ohne die PIN eingeben zu müssen. Wenn die PIN nicht eingegeben werden muss, kannst du Flugmodus/'mobile Daten ausschalten' aus dem Quick Menü entfernen.

Um die Fernlöschung zu testen [hier](#) einloggen

[Hier](#) könnt ihr euch mal anschauen, wie das dann aussieht.

- auf iOS:

In der Einstellungen-App auf „Face/Touch ID & Code“ gehen und das „Kontrollzentrum“ abschalten. Dann lässt sich das Telefon nicht mehr in den Flugmodus stellen.

Die Fernlöschung lässt sich nach der Beschlagnahme über [iCloud.com](#) » „Wo ist?“ aktivieren. Da Apple zum Einloggen bei [iCloud.com](#) einen 2. Faktor verlangt ist es praktisch, einen Notfall-Kontakt zu hinterlegen, der dann die SMS bekommt, wenn euer Handy bei der Polizei ist.

3. Es ist auch schon vorgekommen, dass mit Hilfe abgenommener Fingerabdrücke ein [Smartphone entsperrt](#) wurde.
4. Einige Menschen empfehlen, kein Face-ID zum Entsperren des Telefons zu nutzen. Face-ID ist automatisch ausgeschaltet, wenn ihr das Telefon ausschaltet. Außerdem ist es aus, wenn ihr die Seitentaste und eine der Lautstärketasten zwei Sekunden lang gedrückt haltet. Ausschalten ist eine gute Routine vor dem Einschlafen. Sonst hält euch die Polizei das Gerät vor's Gesicht und es ist entsperrt. Das klappt allerdings nicht, wenn ihr die Augen geschlossen haltet (Aufmerksamkeitsprüfung für Face ID).

## E-Mails

Wenn deutsche Mailanbieter wie GMX, [Web.de](#) oder [Posteo](#) einen korrekten Gerichtsbeschluss zur Herausgabe von Daten bekommen, dann werden sie deine Mails herausgeben. Typischerweise ist das keine Liveüberwachung, sondern eine Herausgabe zu einem fixen Zeitpunkt oder die Beschlagnahme des Kontos.

Das kannst du mit folgenden Strategien verhindern - eine davon reicht:

- Anbieter außerhalb der EU, der nicht mit Deutschland zusammenarbeitet.
- Mails mit [PGP-Verschlüsselung](#) empfangen und senden (für einzelne Mails einfach, flächendeckend unmöglich)
- zu einem Provider gehen, der Mails aus technischer Sicht nicht herausgeben kann:
  - ProtonMail: [proton.me/legal/transparency](https://proton.me/legal/transparency)
  - LG-Mailadressen, die auf @letztegeneration.org enden (nur für AGs, WiGs und interne Gruppen; nicht für Personen)

# Google-Account

Bedenke auch: wo liegt dein Google-Konto? Bekommst du da Mails wie „Ihnen wurde das Google Doc Xyz freigegeben“? Falls ja, kann die Polizei das Dokument von Google bekommen, falls sie deine Mails lesen können. Es ist auch bereits vorgekommen, dass die StA Google per Gerichtsbeschluss gezwungen hat, ein von LG genutztes Konto zu sichern und zu schließen. Das bedeutet, dass auf einen Schlag alle Google-Dokumente unzugänglich werden, die diesem Konto gehören. Google-Konten lassen sich auch für Mailadressen anlegen, die bei einem Mailprovider liegen, der keine Mails an die Polizei rausgibt - siehe [oben](#).

Die IT-AG empfiehlt, statt Google Docs unsere Nextcloud zu nutzen. Die findet ihr unter [cloud.raz-ev.org/apps/files/](https://cloud.raz-ev.org/apps/files/)

Hilfe dazu gibt es [hier im Wiki](#).

*TODO: Trage hier ein gutes Beispiel ein, wenn du eines hast.*



# Checkliste Sicherer Umgang mit Technik

## Hausdurchsuchungen & sicherer Umgang mit Technik

Neben den Checklisten findest du unten auch eine Liste mit hilfreichen Links.

### Checkliste: Hausdurchsuchung

Spieler es mal durch: Angenommen die Polizei schaut morgen vorbei und nimmt dir deine Geräte weg. Wie gut bist du vorbereitet? Falls du noch nicht alles abhaken kannst: Schau dich hier im Wiki um!

- ☐ Ich nutze nur noch verschlüsselte Geräte (Laptop, Handy, Tablet, externe Festplatten)
- ☐ Ich habe Sachen aus der Wohnung geschafft, die die Polizei nicht mitnehmen soll (muss auch nicht LG related sein, z. B. externe Festplatten mit Familienfotos oder alte Tagebücher)
- ☐ Ich mache regelmäßig Backups
  - ☐ Meine Backups sind verschlüsselt
  - ☐ Meine Backups sind an einem sicheren Ort (nicht zu Hause)
  - ☐ Meine Backups enthalten alles wichtige (Passwörter, Signal-Account, Browser-Historie/Lesezeichen, Kontakte, Dokumente)
- ☐ Ich kann auch nach der Hausdurchsuchung auf meine Passwörter zugreifen (denke auch an Zwei-Faktor-Authentifizierung)
- ☐ Ich kann auch nach der Hausdurchsuchung auf meine E-Mails zugreifen (um im Notfall Passwörter zurücksetzen zu können)
- ☐ Ich kann auch nach der Hausdurchsuchung auf Kalender, Kontakte und Arbeitsdokumente (iCloud) zugreifen
- ☐ Ich kann auch nach der Hausdurchsuchung auf Social Media zugreifen
- ☐ Ich kann jederzeit mit LG/meiner AG Kontakt aufnehmen (EA-Nummer an der Wand/im Kopf)
- ☐ Ich weiß, wie ich an Ersatzgeräte komme, um arbeitsfähig zu bleiben
- ☐ Ich habe meine Mitbewohner\*innen vorbereitet und teile diese Informationen mit ihnen
- ☐ Ich weiß, dass ich für all das selbst verantwortlich bin und bei Fragen jederzeit Hilfe von der IT AG bekomme
- ☐ Optional: Ich kann mein Smartphone aus der Ferne löschen

Wir haben die Erfahrung gemacht, dass die Polizei alles an elektronischen Geräten mitnimmt, was sie findet. Wenn sich der Beschluss gegen euch richtet habt ihr darauf keinen Einfluss. Aber wenn sich die Durchsuchung nicht gegen euch richtet (ihr seid Beziehungsmensch/Mitbewohner\*in, bzw betrifft das eure Mitbewohner\*innen), dann beschwert euch lautstark/wehement, dass eure Sachen nicht mitgenommen werden.

Bei den bisherigen Durchsuchungen war es dann oft so, dass sich die Polizei die Geräte vor Ort angeschaut und geprüft hat, ob da relevante Infos (genauer: Sachen von LG oder ein entsprechender Benutzer-Account) vorhanden sind und entscheidet dann vor Ort. Mit unterschiedlichem Ausgang:

- Menschen durften ihre Technik behalten
- die Festplatte wurde vor Ort gespiegelt (kopiert), dafür wurde sie nicht mitgenommen
- Festplatte/Laptop wird trotzdem mitgenommen

Wichtig dabei: Die Menschen mussten dabei ihre Geräte (Handy/Laptop) entschlüsseln/entsperren. Das ist natürlich gefährlich. Deshalb müsst ihr euch **vorher** fragen, wie wichtig euch die jeweilige Hardware ist und wie sensibel die Daten darauf sind (Disclaimer: all eure privaten Daten sind schützenswert!).

Bei den letzten Hausdurchsuchungen wurden die Menschen vorher überwacht und dort durchsucht, wo sich die Menschen zu der Zeit aufgehalten haben. Es ist also nicht unwahrscheinlich, dass ihr bei einer Durchsuchung gerade mit anderen LG-Menschen zusammen seid.

Macht euch auch bewusst, dass eine Hausdurchsuchung eine absolute Stresssituation ist. Menschen (gar nicht von LG) wurden von der Polizei unter Druck gesetzt und haben Passwörter herausgegeben/eingegeben.

## Genereller Umgang mit Technik

- ☐ Ich nutze nur noch verschlüsselte Geräte (Laptop, Handy, Tablet, externe Festplatten)
- ☐ Mir ist bewusst, dass die Polizei eventuell meine Telefongespräche abhört
- ☐ Mir ist bewusst, dass die Polizei eventuell meine E-Mails/SMS mitliest
- ☐ Ich bevorzuge die LG-Nextcloud gegenüber Google-Dokumenten
  - ☐ Bedenke, dass die Polizei auch die E-Mails bekommt mit: "dir wurde ein Google Dokument geteilt" - damit kann die Polizei zu Google gehen
- ☐ Ich bevorzuge Signal gegenüber unverschlüsselter Kommunikation (Telefon/SMS), da Signal nicht einfach abgehört werden kann
- ☐ je älter mein Handy ist (bezogen auf: bekommt es noch Updates?), desto unsicherer ist es. Ich bevorzuge dann lieber meinen Laptop für die LG-Arbeit
- ☐ Ich nutze lieber Dokumente im Browser, als dass ich sie herunterlade
- ☐ Ich nutzte PGP-Verschlüsselung für meine E-Mail-Kommunikation (mindestens für die Kommunikation mit dem Legal-Team)
- ☐ mein Handy ist mit einer sicheren PIN/Passwort gesichert

# Umgang mit Signal

- ☐ Ich habe eine PIN hinterlegt (Registration Lock/Registrierungssperre), damit bei der Neu-Einrichtung des Accounts eine PIN eingegeben werden muss - der Empfang einer SMS reicht dann nicht mehr aus
- ☐ Wenn mein Handy beschlagnahmt wird, lasse ich meine SIM-Karte vom Provider sperren, bestelle mir eine neue SIM-Karte und nutze die bisherige Nummer weiter. Damit kann die Polizei nicht einfach ungemerkt meinen Signal-Account nutzen
- ☐ Ich nutze im LG-Kontext 'Disappearing Messages' (verschwindende Nachrichten)
  - ☐ Ich nutze 'Disappearing Messages' automatisch für alle neuen Chats (lässt sich einstellen)
- ☐ Ich nutze Signal auch auf dem Laptop, um im Falle eines gestohlen/defekten/beschlagnahmten Gerätes weiter arbeitsfähig zu bleiben
- ☐ Android: Es kann noch eine zweite PIN (Bildschirmsperre/Screen lock) in der App hinterlegt werden, die eingegeben werden muss, um die Signal-App auf dem Handy zu öffnen
- ☐ in Signal (und anderen Messengern) mal nach linked devices (verknüpften Geräten) schauen. Die Polizei nutzt das Feature im Rahmen der Telekommunikationsüberwachung, um Messenger abzuhören ([Quelle](#), 2021)

## Ich melde mich bei der IT AG, wenn

- ☐ ich technische Fragen/Probleme habe
- ☐ ich E-Mails mit Links bekomme, auf die ich drauf klicken soll (gerne weiterleiten)
- ☐ ich in meiner Akte/anderweitig mitbekomme, dass ich überwacht werde ([TKÜ/Quellen-TKÜ](#))
- ☐ meine Akte forensische Berichte enthält (über analysierte/gehackte Telefone/Laptops)
- ☐ ich beschlagnahmte Geräte von der Polizei zurück bekommst (vorallem Laptops!)

## Kontakt

- [it-support@letztegeneration.org](mailto:it-support@letztegeneration.org) (gerne auch [PGP verschlüsselt](#))

## Links

- Verschlüsselung:

[Allgemeines zum Thema Verschlüsselung](#)

[Windows verschlüsseln mit Bitlocker](#)

[Windows verschlüsseln mit Veracrypt](#)



## [Android verschlüsseln](#)

## [MacOS verschlüsseln](#)

## [PGP-Verschlüsselung einrichten](#)

- Signal:
  - [Signal sicher benutzen](#)
  - [Signal auf dem Laptop nutzen](#)
  - [Mehrere Signal-Accounts auf dem Handy nutzen](#)
- Generelles:
  - [Auf eine Hausdurchsuchung vorbereiten](#)
  - [Bitwarden Passwort-Manager](#)
  - [Nextcloud](#)
- externe Ressourcen
  - [Vortrag \(mit LG-Bezug\): Staatliche Überwachung: Erfahrungen und Beispiele aus der Praxis](#)
  - [Checkliste mit konkreten Vorschlägen zur Verbesserung deiner Smartphone-Sicherheit](#)
  - [Webseite von esc-it \(Kollektiv, das IT-Sicherheitstrainings für Aktivist\\*innen gibt\)](#)

# Staatstrojaner in Deutschland

# Staatstrojaner in Deutschland

2011 hat der CCC (Chaos Computer Club) einen deutschen Staatstrojaner aufgedeckt. Auf dieser Seite findet ihr Vorträge vom CCC mit einer gesellschaftlichen, rechtlichen und technischen Einordnung.

1. Aufdeckung, Analyse und Bewertung: [28c3: Der Staatstrojaner, \(Youtube, aus 2011\)](#).
2. Ein Jahr später: Was ist seitdem passiert: [29c3 staatstrojaner \(Youtube, aus 2012\)](#).
3. Stand 2023: Über den Gesetzesvorschlag der Ampel zur Einschränkung von Staatstrojanern: [Staatstrojaner für bereits begangene Straftaten \(Youtube, Camp 2023\)](#)
4. Statistiken zum Einsatz von Staatstrojanern: [Staatliche Überwachung: Erfahrungen und Beispiele aus der Praxis \(2024\)](#)

## Artikel

- Um einen aktuellen Überblick (Oktober 2023) zum Thema Staatstrojaner zu bekommen: <https://netzpolitik.org/2023/gesetzentwurf-polizei-soll-staatstrojaner-etwas-seltener-nutzen-duerfen/>
- Pressemitteilung vom CCC zum neuen Gesetzesentwurf: <https://www.ccc.de/en/updates/2023/schon-wieder-staatstrojaner-vorm-verfassungsgericht>
- Aktuelle Infos rund um Staatstrojaner findet ihr auch bei [Netzpolitik](#)