

Digitaler Selbstschutz für Frauen

Prüfplan zur Aufdeckung von Smartphone-Überwachung, Stalkerware, GPS-Trackern & rechtliche Schutzschritte

♥ 1. Du bildest dir das nicht ein – Vertraue deinem Instinkt

Stalking und digitale Überwachung beginnen meist schleichend: Der Ex-Partner taucht an Orten auf, an denen er nicht sein dürfte, kennt private Chatnachrichten oder reagiert auf Dinge, die du nur Freundinnen erzählt hast. Täter nutzen Verwirrung (*Gaslighting*), um Betroffene an der eigenen Wahrnehmung zweifeln zu lassen. **Vertraue deinem Bauchgefühl.** Mit diesem Leitfaden überprüfst du alle Einfallstore systematisch und sicherst dir deine Freiheit und Privatsphäre zurück.

☰ 2. Die 10 digitalen Einfallstore: Prüfliste zum Abhaken



1. WhatsApp Web / Verknüpfte Messenger-Geräte

SEHR HÄUFIG

Gefahr: Einmalig den QR-Code gescannt – und der Täter liest auf seinem PC jeden deiner Chats unbemerkt live mit.

So überprüfst du es: WhatsApp öffnen → *Einstellungen* → *Verknüpfte Geräte*. Alle unbekannten Computer/Browser sofort auf „Abmelden“ tippen!



2. Stalkerware & getarnte Spionage-Apps

KRITISCH

Gefahr: Heimlich installierte Spy-Apps (z. B. mSpy) greifen GPS-Standorte, Tastenanschläge und Kamera-/Mikrofondaten ab.

So überprüfst du es: Android: *Einstellungen* → *Sicherheit* → *Geräteadministrator-Apps* (nach verdächtigen Namen wie „Battery Health“, „System Update“ suchen). iPhone: Unbekannte Konfigurationsprofile unter *Profile & Geräteverwaltung* löschen.



3. Physische Tracker (Apple AirTags, SmartTags)

PHYSISCH

Gefahr: Versteckte Tracker im Auto (Radkasten, Handschuhfach, Kofferraum), in Handtaschen oder Jacken.

So überprüfst du es: iPhone warnt automatisch (*„AirTag bewegt sich mit dir“*). Auf Android die kostenlose Apple-App „Tracker-Erkennung“ oder AirGuard nutzen. Bei Fund: Batterie herausdrehen und für die Polizei aufbewahren.



4. Dauerhafte Standortfreigaben (Google Maps & Apple „Wo ist?“)

UNAUFFÄLLIG

Gefahr: Einmal heimlich aktiviert, sendet dein Handy 24/7 den Live-Standort, ohne dass ein Warnsymbol aufpoppt.

So überprüfst du es: Google Maps: Profilbild oben rechts → *Standortfreigabe* prüfen. iPhone: „Wo ist?“-App → *Personen* kontrollieren und unberechtigte Freigaben sofort stoppen.



5. Connected Cars & Fahrzeughersteller-Apps (VW, BMW, Audi, Mercedes)

NEUER TREND

Gefahr: Täter ist in der Auto-App als Hauptnutzer hinterlegt, sieht GPS-Parkorte, Fahrtrouten und kann Türen fernentriegeln.

So überprüfst du es: Im Infotainment-System des Autos auf *Nutzer / Profile* gehen. Alle fremden Nutzer löschen, Auto auf Werkseinstellungen zurücksetzen und beim Vertragshändler alte App-Bindungen löschen lassen.



6. Smart Home, Smart Locks (Nuki) & Kameras

WOHNUNG

Gefahr: Täter behält digitale Schlüssel für das Nuki-Türschloss oder lauscht über Alexa Drop-In mit.

So überprüfst du es: Nuki-App öffnen und fremde Berechtigungen entziehen. WLAN-Router-Passwort zwingend neu setzen. Smarte Lautsprecher und Kameras auf Werkseinstellungen zurücksetzen.



7. 1-Cent-Überweisungs-Stalking (§ 238 StGB)

PSYCHISCHER DRUCK

Gefahr: Nach Blockierung nutzt der Täter 0,01 € Banküberweisungen, um Nachrichten und Drohungen im Verwendungszweck zu senden.

So handelst du: Niemals Geld zurücküberweisen! Kontoauszüge als PDF sichern. Dies ist ein glasklarer Nachweis beharrlicher Nachstellung nach § 238 StGB für Anzeige und Gericht.



8. KI-Deepfakes, intime Bildmanipulationen & Erpressung

STRAFBAR

Gefahr: Der Täter erpresst mit gefälschten Nacktbildern oder droht mit Weiterleitung an Arbeitgeber oder Familie.

So handelst du: Kein Geld zahlen, nicht erpressen lassen. Drohnachrichten sichern. Strafanzeige nach § 201a Abs. 3 & § 238 StGB erstatten und [StopNCII.org](https://stopncii.org) zur Sperrung nutzen.



9. Geteilte Cloud-Accounts & E-Mail-Weiterleitungen

DATENABFLUSS

Gefahr: Gemeinsame Apple IDs synchronisieren Fotos und Notizen. Heimliche Weiterleitungsregeln im Mailkonto leiten alle Mails an den Täter weiter.

So überprüfst du es: Im Webmail (z. B. GMX, Gmail) unter *Filter & Weiterleitung* nachsehen. Passwörter für Apple ID und E-Mail nur über ein fremdes, sicheres Gerät ändern.



10. Browser-Verläufe & sensible Recherchen

PRIVATSPHÄRE

Gefahr: Über synchronisierte Google-/Safari-Konten sieht der Täter deine Suchen nach Wohnungen, Anwälten oder Frauenhäusern.

So schützt du dich: Sensible Suchen nur im Inkognito-Modus oder an einem unüberwachten Drittgerät (z. B. bei einer Freundin) durchführen.



3. Die 4 goldenen Schutzschild-Handlungsregeln

1. Keine voreilige Konfrontation

Lösche verdächtige Apps nicht überstürzt. Sichere erst Screenshots mit Datum und Uhrzeit. Wenn der Täter merkt, dass du Bescheid weißt, löscht er Beweise oder eskaliert.

2. Der 2-Geräte-Grundsatz

Ändere Passwörter (Mail, Apple ID, Bank) **nur über ein sicheres fremdes Gerät** (z. B. PC einer Freundin). Ein überwacht Smartphone liest neue Passwörter sofort mit.

3. Rechtliche Schutzanordnung (GewSchG)

Beantrage beim Amtsgericht eine einstweilige Verfügung nach **§ 1 Gewaltschutzgesetz (GewSchG)** (Kontakt-, Näherungs- und Betretungsverbot). Geht ohne Anwalt bei der Rechtsantragstelle!

4. Die Kunst des Stehenlassens (Kap. 23)

Konsequenter Kontaktabbruch (Null-Reaktion). Jede Reaktion – selbst ein wütendes „Lass mich in Ruhe!“ – belohnt den Täter und bestätigt ihm, dass er dich erreicht. Lass ihn ins Leere laufen.



4. Offizielle Hilfs- und Notrufnummern

Hilfetelefon „Gewalt gegen Frauen“

116 016

Kostenlos, anonym, 24/7 in 18 Sprachen erreichbar. Fachberatung bei Cyberstalking und Nachstellung.

Weisser Ring e. V. (Opferhilfe)

116 006

Opferberatung, Begleitung zu Behörden und finanzielle Soforthilfe für Rechtsberatung & Schlössertausch.

HateAid (Digitale Gewalt)

hateaid.org

Rechtsberatung und emotionale Unterstützung bei digitaler Belästigung, Erpressung und Deepfakes.

Polizeinotruf (Akute Gefahr)

110

Bei unmittelbarer Verfolgung oder Bedrohung vor der Wohnung sofort 110 anrufen.