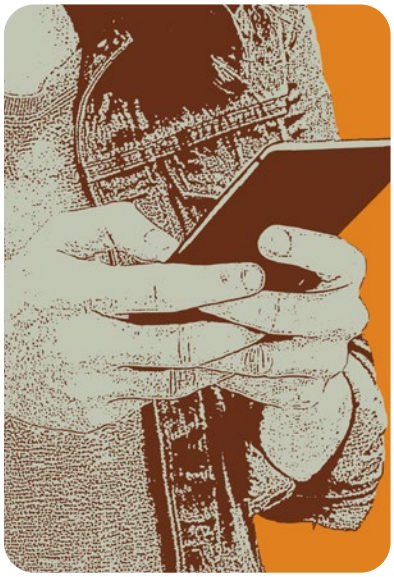
Stalking im digitalen Raum

Informationen und Hinweise für Fachpersonen



Digitales Stalking bezeichnet den Einsatz digitaler Mittel – Standortdienste, gemeinsame Accounts, Spionage-Software, Social Media oder vernetzte Geräte – um eine Person zu überwachen, zu kontrollieren oder einzuschüchtern. Es tritt häufig gemeinsam mit physischem Stalking oder häuslicher Gewalt auf und eskaliert oft schrittweise.

Dieses Dokument dient als **Leitfaden für Empfehlungen erster Massnahmen bei einem vermuteten Fall von digitalem Stalking.** Es ersetzt weder eine forensische Untersuchung noch eine juristische Beratung.

Wichtig: Technische Entwicklungen verändern sich laufend; neue Funktionen, Geräte oder Apps können jederzeit weitere Überwachungsmöglichkeiten schaffen.

Verdacht abklären

Warnindikatoren

Die folgenden Handlungen stellen einzeln keinen Beweis für digitales Stalking dar. Treffen jedoch mehrere gleichzeitig zu, ist eine Überwachung wahrscheinlich.

Die mutmassliche Tatperson:

- → erscheint wiederholt am selben Ort wie die betroffene Person, ohne plausible Erklärung;
- → kennt eine neue, nicht mitgeteilte Telefonnummer unmittelbar nach deren Vergabe;
- → reagiert gezielt auf Bewegungen ausserhalb der Wohnung;
- → weiss, wann die betroffene Person zu Hause ist oder das Haus verlässt;
- → verlangt Screenshots als «Beweis» des Standorts der betroffenen Person.

Zusätzlich ist folgendes typisch für eine Überwachung durch Spionage-Software[1].

Die mutmassliche Tatperson:

- → kennt Chatinhalte wortwörtlich;
- → kennt Details aus Gesprächen oder Nachrichten, an denen sie nicht beteiligt war, oder
- → reagiert sofort auf neue Kontakte.

Das elektronische Gerät[2]:

- → weist einen ungewöhnlich hohen Akku- oder Datenverbrauch auf;
- → wird auch ohne aktive Nutzung warm oder
- → enthält unbekannte Apps mit erweiterten Berechtigungen (z. B. Zugriff auf Standort, Mikrofon, Nachrichten, Hilfefunktionen).

1 Wie gelangt Spionage-Software auf ein Gerät? Zugriff auf ein entsperrtes Gerät, Geschenk, von der mutmasslichen Tatperson vorgenommene Konfiguration, Reparatur oder Updates.

2 Unter *elektronische Geräte* verstehen wir insbesondere: Smartphone, Tablet, Laptop, PC, Smartwatch, Kopfhörer, Smart-Home (Kameras, Türklingeln, Schlösser, Thermostate, Assistenten, Saugroboter, usw.), Vernetzte Auto-Apps, Konsolen, Smart-TV, E-Reader

Risikoanalyse – Fragen an die betroffene Person

Diese Fragen helfen, mögliche Angriffspunkte zu ermitteln, bevor Massnahmen ergriffen werden müssen.

Gerätezugang

- → Kennt die mutmassliche Tatperson den Entsperrcode des Smartphones oder anderer elektronischer Geräte?
- → Hat sie das betroffene Gerät gekauft, eingerichtet, repariert oder geschenkt?
- → Auf wen ist die SIM-Karte des Smartphones registriert?

Kontenzugang

- → Hat die mutmassliche Tatperson Zugriff auf E-Mail-Konten?
- → Kennt sie die Zugangsdaten zu Apps?
- → Bestehen gemeinsame Google-, Apple- oder Microsoft-Konten?
- → Besteht eine Familienfreigabe?
- → Hat die mutmassliche Tatperson elterliche Rechte oder Zugriff auf das Smartphone oder auf andere elektronische (Kinder-)Geräte? Werden die für Kinder bestimmten Geräte gemeinsam genutzt (z. B. Smartwatch mit GPS, App zur Kindersicherung, Spielkonsole)?

Technische Kompetenz

- → Verfügt die mutmassliche Tatperson über technische Kenntnisse (z. B. im IT-Bereich tätig)?



Bei erhöhtem Risiko oder Notfall

- → Betroffene Geräte ausschalten und in eine signaldichte Hülle (Faraday-Bag) legen. Kein Einschalten im Haus bzw. dort, wo die betroffene Person Zuflucht gefunden hat.
- → Umleitung der Kommunikation auf ein anderes, unbelastetes Gerät – mit neuer Telefonnummer, neuer SIM-Karte und ohne Verknüpfung zu weiteren elektronischen Geräten.
- → Neue Konten[3] (inkl. Social Media) mit sicheren Passwörtern einrichten.
- → Nicht auf Werkseinstellungen zurücksetzen, bevor digitale Spuren von möglicher elektronischer Überwachung gesichert werden können.



Massnahmen mit der betroffenen Person ergreifen

Ist ein Gerätewechsel nicht möglich, können bestimmte Massnahmen (die selbstständig oder unter Anleitung ergriffen werden) dazu beitragen, eine mögliche Überwachung zu erkennen und die betroffene Person vor weiteren Überwachungen zu schützen.

- → Siehe Dokumente **«Informationen und Hinweise zum eigenen Schutz»** und **«Checkliste – Zugänge und Sicherheitseinstellungen prüfen»**

3 Unter *Konten und Cloud* verstehen wir insbesondere: E-Mail, Social Media, Messenger (inkl. WhatsApp Web), Apple-ID/iCloud, Google-Konto, Microsoft/Dropbox, Banking, Mobilfunkanbieter, SBB-Mobile und andere Reise-App, Online-Shops, Streaming, Gaming-Konten, Lieferdienste (Uber Eats, usw.), Bonusprogramme (Cumulus, Supercard, usw.), Apps mit Abonnement, usw.

SKPPSC Schweizerische Kriminalprävention
Ihre POLIZEI
Votre POLICE
La vostra POLIZIA