Rheinland-Pfalz
POLIZEIPRÄSIDIUM MAINZ

CYBERSTALKING

AUSPRÄGUNGEN, RECHTE HANDLUNGSMÖGLICHKEITEN

CYBERSTALKING - DEFINITION

Rheinland-Pfalz
POLIZEIPRÄSIDIUM MAINZ

„Cyberstalking“ ist Stalking durch E-Mails, Beiträge und Nachrichten über Messenger, Chats oder andere soziale Netzwerke und digitale Medien oder Techniken

CYBERSTALKING – ZWEI VARIANTEN

RheinlandPfalz
POLIZEIPRÄSIDIUM MAINZ

Cyberstalking ohne Vorbeziehung besteht meist aus:

- Beharrliche Kontaktaufnahme via digitaler Medien
- Identitätsdiebstahl (Bestellung von Waren, Erstellung von Profilen in Kontaktbörsen etc)

Cyberstalking zw. (Ex-) Partner*innen ist meist:

- „Klassisches“ Stalking mithilfe digitaler Medien und Techniken
- Erfolgt meist durch Handlungen der Kontrolle + Überwachung (z.B. Spyware+Tracking-Apps)

CYBERSTALKING - AUSPRÄGUNGEN

- Wiederholt unerwünschte **Kontaktaufnahme** per Mail
- Verbreitung von personenbezogenen Daten („**Doxing**“), Lügen, intimen bzw. kompromittierenden Details oder Fotos im Internet
- **Bestellungen** im Internet auf Namen der betroffenen Person (Waren nicht annehmen!!!)
- **„Identitätsdiebstahl**“ z.B. durch Anmeldung in Kontaktbörsen oder in sozialen Netzwerken unter dem Namen des Opfers
- Handlungen der **Kontrolle + Überwachung** durch technische Hilfsmittel (Spyware, Kameras, Tracking-Apps)

STALKING MIT TRACKINGAPPS

- Überwachung des Standortes + Lesen von SMS und Messenger-Apps können mitgelesen werden
- Zugriff auf Fotos und auf die Kamera in Echtzeit
- Browserverlauf, Dateien, Kalender und Kontakte können abgerufen werden
- Sind legal und oft kostenlos im App-Store erhältlich
- Dienen vordergründig der Überwachung der eigenen Kinder oder dem Diebstahlschutz
- Installation bedingt kein technisches Know-How
- **ABER** – der Täter braucht physischen Zugriff zur Installation

STALKING MIT TRACKINGAPPS

- Beispiele für solche Apps:

Mobile Tracker Free // Cerberus // mSpy //

FlexiSpy //

iSpyoo // TheTruthSpy

SONSTIGE TECHNISCHEN STALKINGMITTEL

RheinlandPfalz
POLIZEIPRÄSIDIUM MAINZ

- „Datenklau“ via spezieller Ladekabel
- „**Cartracker**“: Kosten ca. 50€ inkl. starkem Magnet; Batterien halten bis zu 6 Monate; GPS-Sender überträgt Standort über Mobilfunk/Bluetooth
- GPS-Sender in Schlüsselanhängern etc.
- WhatsApp-Synchronisation via QR-Code-Scan unter **web.whatsapp.com** mit einem Computer
- **Alexa/Google Echo** etc. zeichnen bei vorher definierten Schlüsselwörtern Unterhaltungen

RECHTLICHE INTERVENTION

- **Strafanzeige** bei der Polizei (§ 238 StGB Nachstellung / Stalking)
- Erwirkung einer **Verfügung nach dem Gewaltschutzgesetz**
- Anwaltlichen Beistand hinsichtlich zivilrechtlicher Schritte (z.B. **Schmerzensgeld / Schadensersatz**)
- Gem. § 10 Nr. 2 Telemediengesetz unerwünschte Inhalte im Internet vom Dienstanbieter löschen lassen (Dienstanbietersuche über **www.denic.de**)

TECHNISCHE + PRAKTISCHE TIPPS

RheinlandPfalz
POLIZEIPRÄSIDIUM MAINZ

- Spyware benötigt **Akku und Datenvolumen** - aufmerksam werden, wenn beides außergewöhnlich schnell sinkt!
- Unbekannte Apps löschen
- Berechtigungsverwaltung der Apps checken (**Welche Apps haben Zugriff auf Mikro oder Kamera?**)
- **Keine automatischen Log-Ins** auf passwortgeschützten Seiten
- **Deaktivierung der Standort** / Bluetooth / Internetverbindung bei Nichtnutzung
- Bei Spyware Handy auf **Werkseinstellungen** zurücksetzen

TECHNISCHE + PRAKTISCHE TIPPS

RheinlandPfalz
POLIZEIPRÄSIDIUM MAINZ

- Regelmäßig **Sicherheitseinstellungen** des Smartphones prüfen
- Versehen Sie ihr Handy mit einer automatischen **Bildschirmsperre / PIN-Sperre**
- Verhindern Sie Einblicke auf Ihr Display z.B. mit spezieller **Sichtschutzfolie**
- Sichtschutzblenden für **Webcam an PC + Smart-TV** nutzen; nur bei Eigenbedarf entfernen

WICHTIGSTE HANDLUNGSHINWEISE

Rheinland-Pfalz
POLIZEIPRÄSIDIUM MAINZ

Geräte nach Möglichkeit nicht aus der Hand geben!!! (Vor allem nicht an Fremde oder Expartner*innen)

Eignen Sie sich Kompetenzen über Nutzung und Wartung der eigenen Geräte an **(„Digitale Empowerment“**)

ALLGEMEINE HANDLUNGSHINWEISE

RheinlandPfalz
POLIZEIPRÄSIDIUM MAINZ

- Sorgsamer Umgang mit persönlichen Daten
- Nutzen Sie **sichere Passwörter**
- Nutzen Sie in sozialen Netzwerken/Datingportalen neutrale „**Nicknames“** und seperate E-Mail-Adressen
- Überprüfen Sie Ihre Geräte auf **Weiterleitungs-/Benachrichtigungsfunktionen**
- Lassen Sie Ihre Daten nicht von Ihrem Partner / Partnerin kontrollieren
- Kündigen Sie zeitnah nach einer Trennung die **Partnerverträge**
- Überprüfen Sie von Zeit zu Zeit Ihre Daten im Internet (**Was ist über mich im Netz gespeichert?)**

WAS TUN, WENN SIE OPFER GEWORDEN SIND

RheinlandPfalz
POLIZEIPRÄSIDIUM MAINZ

- Nachrichten speichern / ausdrucken // **Screenshots** von Chatverläufen fertigen
- **Dokumentation** der einzelnen Ereignisse
- **Passwörter überall ändern**
- Sperrfunktionen nutzen
- **Neue Accounts eröffnen** und die alten nicht mehr nutzen (z.B. bei Amazon, Netflix, PayPal, Online-Banking)
- Betreiber der Plattformen informieren – die Nachrichten zu löschen (**Betreibersuche über www.denic.de**)
- Über juristische Möglichkeiten und Hilfsangebote informieren

LINKS

Polizeiliche Kriminalprävention des Bundes und der Länder:
https://www.polizei-beratung.de/opferinformationen/stalking/

Bundesverband der Frauenberatungsstellen und Frauennotrufe in Deutschland:
www.aktiv-gegen-digitale-gewalt.de

Das Infoportal für sichere Handynutzung:
www.mobilsicher.de

LINKS

Bundesamt für Sicherheit in der Informationstechnik:
www.bsi.bund.de/verbraucherinnen-und-verbraucher

Das Infoportal für sichere Handynutzung:
www.mobilsicher.de

Coalition Against Stalkerware:
www.stopstalkerware.org