



Cyber-Grooming

Digitale Dienste und Inhalte sind in der heutigen Zeit allgegenwärtig. Durch die zunehmende Anzahl verfügbarer Internetinhalte steigen auch die Risiken und Gefahren, welche die Nutzung von digitalen Medien mit sich bringen.

Die Anzahl an Kindern und Jugendlichen, die bereits im Grundschulalter ein Smartphone besitzen und somit ungehinderten Zugriff auf die Internetwelt haben, steigen rasant.

Die Sorge vieler Eltern, wer alles mit dem eigenen Kind Kontakt aufnehmen kann, ist berechtigt. Durch den ungefilterten Zugang zur Online-Welt können Kinder und Jugendliche sehr leicht, auch ungewollt, mit Pornographie oder Gewaltvideos konfrontiert werden, was für Kinder eine sexuelle Grenzverletzung darstellt.

Die selbstverständliche Verfügbarkeit von Smartphone und Internet hat auch Auswirkungen auf das Sozialverhalten von Kindern und Jugendlichen. Immer mehr jüngere Menschen verschicken freizügige oder intime Fotos oder stellen diese auf ihren Social Media-Profilen ein. Dadurch ist es für Pädokriminelle leichter geworden, sexuelle Kontakte zu Kindern anzubahnen.

Jeder Betroffene sollte sich direkt an die Polizei wenden und Anzeige erstatten!

Unter Cyber-Grooming versteht man das gezielte Ansprechen von Kindern im Internet mit dem Ziel der Anbahnung sexueller Kontakte.

Hier versuchen Erwachsene über soziale Netzwerke, Chat-Foren oder Online-Communitys gezielt mit Kindern und Jugendlichen in Kontakt zu treten. Die Täter geben sich gegenüber Kindern oder Jugendlichen als gleichaltrig aus, um so zunächst das Vertrauen der arglosen Minderjährigen zu gewinnen und sie dann im weiteren Verlauf zu manipulieren. Häufig werden hierzu Fake-Accounts oder Avatare benutzt, um so gleichaltrige Kommunikationspartner zu simulieren. Oft können die Täter die Minderjährigen dazu überreden, ihnen freizügige Selbstporträts oder Videos zuzusenden (Sexting) oder eine Kommunikation mit sexuellen Inhalt zu starten. Hierbei ist das Ziel, sexuellen Missbrauch online oder bei realen Treffen (Blind-Dates) anzubahnen.

Es wird grob zwischen zwei Tätertypen unterschieden: dem Blackmailer-Typ und dem Good-Friends-Typ.

Der **Blackmailer-Typ** ist offensiv und versucht direkt sexuell motivierten Kontakt zu Minderjährigen aufzubauen. Hier wird meistens direkt nach Cybersex gefragt. Wird sexuell enthaltenes Bild- oder Videomaterial erlangt, so wird dies, wenn das Opfer die Kommunikation beenden möchte, in erpresserischer Weise als Druckmittel gegen die Minderjährigen eingesetzt, um sie zu weiteren Handlungen zu bewegen.

Der **Good-Friends-Typ** plant langfristig und sucht sein potentiell Opfer gezielt aus. Zunächst baut der Täter ein harmloses Kommunikationsverhältnis auf, um langfristig das Vertrauen des Opfers zu gewinnen. Die Minderjährigen werden dabei nach Geschlecht des Avatars bzw. Nutzernamens ausgewählt. Gerade die unbedachten privaten Informationen in Profileinstellungen von Kindern dienen als Informationsquelle für die Kriminellen.

Cyber-Grooming gegenüber Kindern ist unter den Voraussetzungen des § 176 (Sexueller Missbrauch von Kindern) Abs. 4 Nr. 3 und 4 Strafgesetzbuch (StGB) strafbar und kann eine Freiheitsstrafe von drei Monaten bis zu fünf Jahren nach sich ziehen.

Bereits vorbereitende Handlungen vor einer potentiellen Kindesmisshandlung sowie das Anfertigen von kinderpornografischen Schriften und Bildern ist strafbar. Auch der Besitz und Erwerb sowie der versuchte Erwerb von Posing-Bildern und textliche Schilderungen sexueller Missbrauchshandlungen an Kindern die anderen Nutzern zugänglich gemacht werden, ist unter Strafe gestellt.



Um sich vor Cyber-Grooming zu schützen, sollten einige einfache Verhaltensregeln beachtet werden.

In den Sozialen Medien sowie allgemein im Internet sollten Privatsphäre-Einstellungen der einzelnen Dienste verwendet werden. Es ist wichtig, nicht zu viele oder unnötige Informationen von sich preis zu geben.

Profilbilder und private Informationen verraten sehr viel über eine Person. Auch Selfies oder Likes zu bestimmten Themen nutzen Kriminelle, um sich potentielle Opfer zu suchen. Bei der Verwendung von Endgeräten mit Webcam ist es ratsam, diese zu deaktivieren oder mit einem Sticker zu überkleben. Ein gesundes Misstrauen gegenüber Fremden sollte ebenfalls angebracht sein, da sich hinter einem Profil nicht immer die Person verbirgt, für die sie sich ausgibt.

Kinder und Jugendliche sollten daher keine Fotos, Videos und persönliche Daten an fremde Personen weiterleiten und auch keine Verabredungen mit Unbekannten treffen, ohne sich den Eltern anzuvertrauen.

Des Weiteren sollte man sich weder vom Partner oder Partnerin und schon gar nicht von Fremden unter Druck setzen lassen. Hier ist es ratsam, unangenehme Dialoge im Internet einfach abubrechen.

Es ist deshalb ratsam, dass Eltern sich mit dem Internet, seinen Möglichkeiten und Gefahren auseinandersetzen und die Kinder und Jugendlichen bei den ersten Schritten im Internet und dem Smartphone/Laptop begleiten.

Starke Passwörter verwenden

Stark ist ein Passwort, wenn es aus mindestens neun Zeichen unter Nutzung von Klein- und Großbuchstaben, Ziffern und Sonderzeichen besteht. Bitte keine Namen, Geburtsdaten oder Passwörter aus dem Wörterbuch verwenden und auf keinen Fall an Dritte weiter geben. Es wird empfohlen, für verschiedene Onlinezugänge auch unterschiedliche Nutzernamen und Passwörter zu verwenden. Diese Passwörter sollten auch an geeigneten Stellen und vor Dritten geschützt aufbewahrt werden. Optimal ist auch die Verwendung eines Passwortmanagers mit Schlüsselbundfunktion. Verwenden Sie keine Passwörter, die in der Vergangenheit schon einmal benutzt wurden und vermeiden Sie die „Passwort merken“-Funktion von Anwendungen im Browser und in Applikationen (Apps). Bevorzugt werden sollten auch Dienste, welche die Zwei-Faktor-Authentifizierung unterstützen.

Privatsphäre schützen

Richtige Sicherheitseinstellungen auf den Endgeräten sowie in den Sozialen Medien reduzieren das Risiko, zu viele Informationen von sich selbst preiszugeben. Ein sorgfältiger Umgang mit seinen Profildaten und Bildern ist unerlässlich.
=> Seien Sie sparsam mit der Weitergabe Ihrer persönlichen Daten!
[Profilbild, personenbezogene Daten, Freunde-Einstellungen, öffentliche-Daten, Selfies, Likes]

Misstrauisch sein

Bei Anfragen von Unbekannten immer misstrauisch sein! Cyberkriminelle verstecken sich in erster Linie hinter anonymen, gefälschten und unseriösen Profilen. Aus diesem Grund sollte jede Kontaktanfrage immer kritisch hinterfragt und keine sensiblen Daten herausgegeben werden. Auch E-Mails von Unbekannten sollten weder geöffnet, noch sollten Anhänge und Links in keinsten Weise angeklickt werden. Hier verbirgt sich oftmals Schadsoftware, mit der Absicht Passwörter zu erbeuten, um weitere, kriminelle Handlungen durchzuführen. Oftmals lassen sich Betrüger auch durch die unkorrekte Schreibweise der E-Mailabsenderadresse, deren Inhalt, falsche Umlaute, kryptische Buchstaben oder anhand der Linkadresse erkennen. Eine sichere Website erkennt man am „s“ (secure) in der Kopfadresse bei <https://...>

Wenn man Opfer von Cybercrime geworden ist, stehen einem die gleichen umfangreichen Hilfs- und Unterstützungsangebote zur Verfügung, wie den Opfern von Straftaten in der realen Welt.

Bei akuter Bedrohung, wählen Sie 110! Die Polizei wird alles Erforderliche tun, um Sie zu schützen.

- Zeigen Sie die Straftat bei der Polizei an (Strafanzeige ist bei jeder Polizeidienststelle möglich)
- Existierendes Datenmaterial, wie z. B. E-Mails, Chat-Verläufe in Messenger-Diensten, digitale Fotos oder Videos sind wichtige Beweismittel, die Sie bis zum ersten Kontakt mit der Polizei bestenfalls komplett unverändert lassen.
- Bringen Sie das gesicherte Beweismaterial am besten gleich zur Anzeigenerstattung mit. Das ist wichtig für die weiteren Ermittlungen, um den Verlust von Spuren im Netz zu vermeiden.
- Kinder können sich beim Kinder- und Jugendtelefon 0800 111 0333 Nummer gegen Kummer, anonym und kostenlos erreichbar montags – samstags 14.00 - 20.00 Uhr, Hilfe und Unterstützung holen.