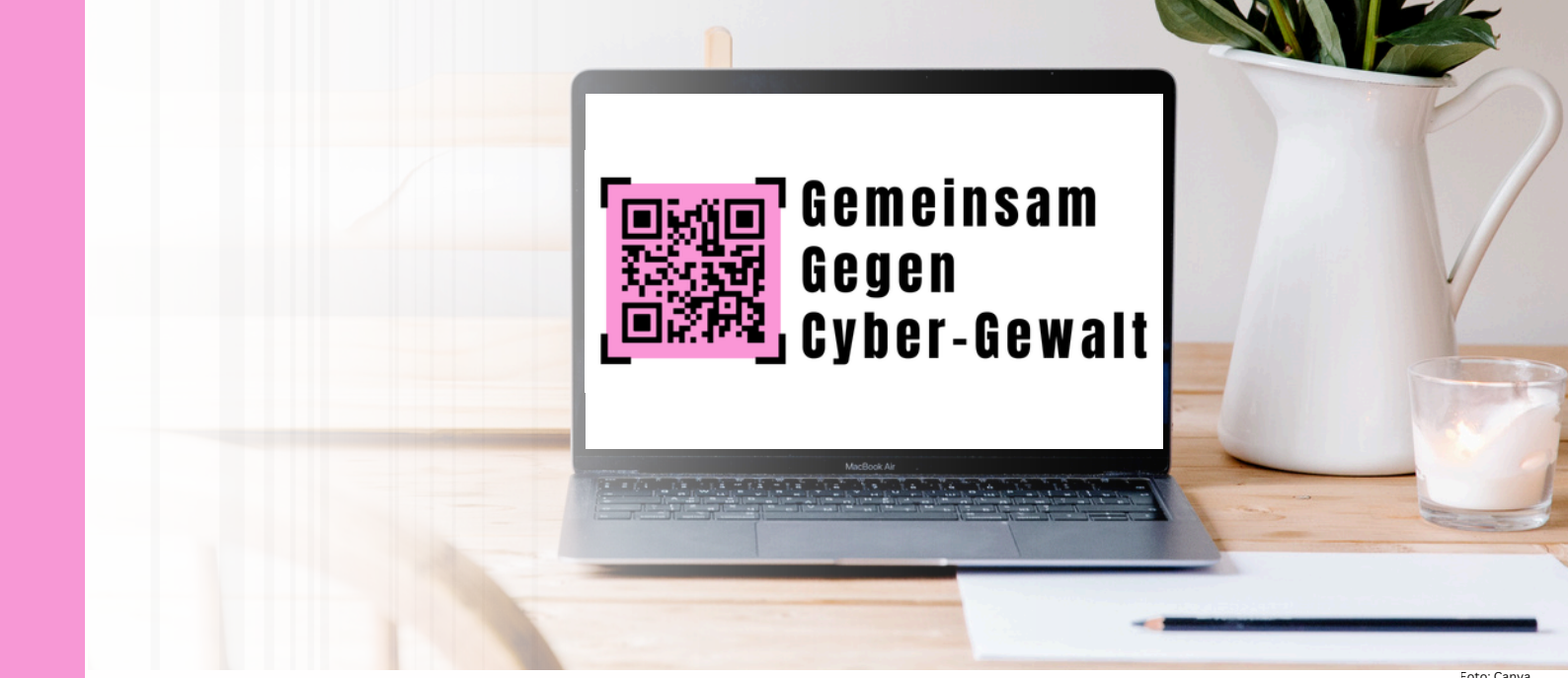


Foto: Canva

#GemeinsamGegenCybergewalt ist ein Projekt des Frauenservice Graz in Zusammenarbeit mit dem Dachverband Frauen- und Mädchenberatung.

Frauen und Mädchen im digitalen Raum stärken!

Cyber-Gewalt ist auch geschlechtsspezifische Gewalt - jede 3. Frau erfährt mindestens ein Mal im Jahr digitale Gewalt (vgl. Weisser Ring 2018). Ein Großteil der Gewalt findet durch Personen aus dem persönlichen Nahraum, wie dem eigenen Partner oder (Ex-)Partner, statt (vgl. EIGE 2017).

Das Projekt #GemeinsamGegenCybergewalt stärkt Frauen und Mädchen in ihren digitalen Kompetenzen und ihrer Selbstwirksamkeit im Netz. Ein weiterer Fokus liegt auf der Stärkung der Beratungskompetenz zum Thema Cyber-Gewalt. Denn immer häufiger melden sich Frauen und Mädchen aufgrund von Gewalterfahrungen im Internet bei Frauen- und Mädchenberatungsstellen.

Unterstützung in der Beratung

Digitale Entwicklungen sind sehr schnelllebig und Cyber-Gewalt ist besonders komplex: Sie variiert in ihrer Form, dem Medium und den Betroffenen. Doch es gibt Strategien und Techniken, um sich gegen Cyber-Gewalt zu wappnen und die eigene Selbstwirksamkeit im Netz zu steigern.

Im Rahmen des Projekts werden Factsheets erstellt, die wichtige Informationen und Hinweise für die Beratung bei Cyber-Gewalt liefern und so die Beratungskompetenzen weiter stärken.

Wichtiger Hinweis:

Die Informationen dienen zur Kompetenz- und Wissenserweiterung von Berater*innen zu Cyber-Gewalt und bedeuten für Betroffene Sicherheit und Schutz. Uns ist wichtig darauf hinzuweisen, dass unsere Factsheets auch potenzielles Täterwissen enthalten. Wir bitten daher um eine verantwortungsvolle Verwendung und Weitergabe.

Gemeinsam Gegen Cyber-Gewalt

Basiswissen Cyber-Gewalt

unterschiedliche Formen von Cyber-Gewalt

Formen & Auswirkungen | Anzeichen in der Beratung

Unser Alltag digitalisiert sich immer mehr. 91 % der Österreicher*innen ab 14 Jahren sind online. Momentan liegt die tägliche Internetnutzung bei 5 Stunden und 22 Minuten (vgl. Statista 2024). Technik, Medien und Soziale Netzwerke werden zunehmend Teil von Gewalthandlungen und fließen in Gewaltdynamiken mit ein. Jede 3. Frau ist in Österreich von häuslicher oder sexualisierter Gewalt betroffen. 1 von 10 Frauen hat schon Cyber-Gewalt in einer Beziehung erlebt. Besonders betroffen sind Frauen und Mädchen im Alter von 15-29 Jahren. Die Täter sind den meisten Betroffenen bekannt (vgl. EIGE 2017). Die noch immer weit verbreitete Unterscheidung zwischen "online" und "realer" Gewalt ist irreführend: Cyber-Gewalt und Partnerschaftsgewalt treten immer häufiger gemeinsam auf. Für Betroffene hat Cyber-Gewalt reale Folgen.

▷▷▷ Was ist Cyber-Gewalt?

Cyber-Gewalt* ist ein Sammelbegriff für verschiedene Formen von Gewalt gegen Frauen und Mädchen.
Bei Cyber-Gewalt versucht die gewaltausübende Person (meist der Freund oder Ex-Mann) über das Internet Macht und Kontrolle auf die betroffene Frau oder das betroffene Mädchen auszuüben.
Ziel dieser Gewalt ist es immer, der Betroffenen Schaden zuzufügen und dadurch eine Abhängigkeit herzustellen.

Formen von Cyber-Gewalt

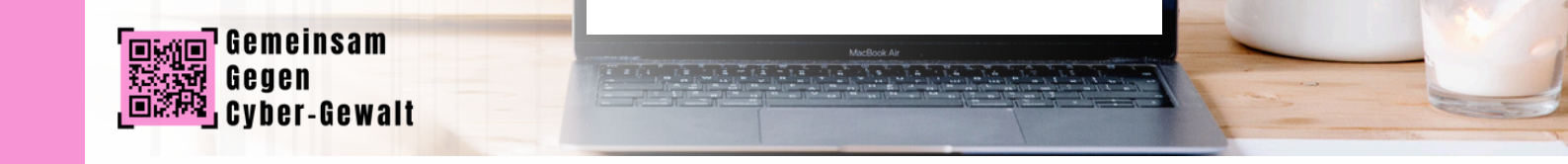
Die Erfahrung der Frauen- und Mädchenberatungsstellen des Netzwerks zeigt eine steigende Zahl an Beratungsanfragen zu Cyber-Gewalt. Oft können Betroffene nicht benennen, dass sie von Cyber-Gewalt betroffen sind. Sie berichten von einem komischen oder seltsamen Gefühl, dass sie (online) verfolgt werden oder der Gewalttäter zu viel über sie weiß. Es ist deshalb wichtig als Berater*in sensibel für das Thema zu sein und gezielt nach etwaigen Erfahrungen von digitaler Gewalt zu fragen. Betroffene wenden sich immer öfter mit folgenden Erfahrungen von Cyber-Gewalt an Frauen- und Mädchenberatungsstellen:

Stalking	Eine Frau wird über die Sozialen Netzwerke oder Cloud-Dienste verfolgt, dazu kann auch sogenannte Stalkerware auf dem Smartphone der Frau installiert werden.
Bildbasierte digitale Gewalt	Nach der Trennung verbreitet der Ex-Partner Fotos oder Filme einer Frau, ohne ihre Zustimmung im Internet und lädt sie auf pornographischen Plattformen hoch.
Identitätsdieb-stahl	Der Ex-Partner geht ohne Einverständnis der Frau mit ihrer Kreditkarte in einem Onlineshop sehr teure elektronische Geräte einkaufen und lässt sie auf den Kosten für die Geräte sitzen.

Das ist nur ein kleiner Auszug der vielseitigen Arten von Cyber-Gewalt. Alle Formen von Cyber-Gewalt haben direkte psychische oder auch physische Auswirkungen auf Betroffene, besonders bei Partnerschaftsgewalt, in Trennungssituationen und bei Stalking.

*Im deutschsprachigen Raum und der Fachliteratur wird der der Begriff digitale Gewalt bzw. geschlechtsspezifische digitale Gewalt verwendet.

DFMB Dachverband Frauen- und Mädchenberatung
FRAUEN* SERVICE BERATUNG BILDUNG FORSCHUNG
Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts

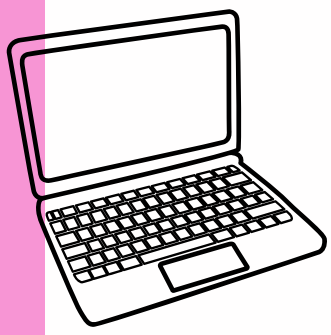


Gemeinsam Gegen Cyber-Gewalt

Sicherheitstipps für Klient*innen: Passwortsicherheit

Sichere Passwörter | Passwörter erstellen und verwalten | Stärkste Passwörter

Ein Passwort ist die erste und wichtigste Sicherheitshürde in der digitalen Welt. Ein sicheres Passwort verhindert, dass eine gewaltausübende Person (meist der (Ex-)Freund oder Ehemann) die Benutzerkonten in Sozialen Netzwerken oder E-Mail-Konten einer betroffenen Frau einsehen kann. Ein sicheres Passwort hat mindestens 16 Zeichen. Es enthält Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Wichtig ist, dass es sich nicht aus dem eigenen Namen, einer nahestehenden Person oder einem Geburtsdatum ableiten lässt. Jedes Konto muss ein anderes Passwort haben, das regelmäßig (min. 1 Mal im Jahr) geändert wird.



Passwort-Chaos? So behält man den Überblick!

Es gibt spezielle Programme, die bei der sicheren Verwaltung von Passwörtern helfen: Sogenannte Passwort-Manager funktionieren auf Computern und Smartphones. Sie speichern alle verschiedenen Passwörter sicher hinter einem Haupt-Passwort (Master-Passwort), das mindestens 20 Zeichen lang sein sollte. So muss man sich nur noch ein einziges Passwort merken. Bekannte, kostenfreie und sehr gute Passwort-Manager sind für Windows, Linux und MacOS: KeePassXC, für Android: KeePassDX und für iOS: KeePassium.

Ein guter Tipp für sichere Passwörter ist es, einen Satz zu nehmen, den man sich leicht merken kann. Zum Beispiel: "Heute werde ich mit viel Freude Eis und Schokolade essen." Aus den Anfangsbuchstaben jedes Wortes ergibt sich mit der Kombination von einem Sonderzeichen „!" und einer Jahreszahl ein sicheres Passwort: HwimvFEuSe!2025. Diese Sätze können für jedes Konto angepasst werden. Für Facebook gilt beispielsweise: HwimvFEuSe!2025 und für das E-Mail Konto: "Morgen werde ich mit vielen netten Menschen Pizza und Pasta essen." = MwimvnMPuPe?2026.

Auch **"Phishing"** (Wortkreation aus dem Englischen: Passwort fischen) kann Gefahren bergen. Dazu werden Betrugs-E-Mails an Frauen und Mädchen geschickt - etwa mit der Aufforderung einen Seiteninhalt anzuklicken, Passwörter zurückzusetzen oder einen Inhalt herunterzuladen. Danach geschieht zunächst nichts Sichtbares für die Betroffene, aber wenn sie beispielsweise ihr Facebook-Benutzerkonto öffnet, könnte sie zu einer gefälschten Internetseite geführt werden. Wenn sie auf dieser Seite ihre Zugangsdaten eingibt, können diese eingesehen und ohne ihr Einverständnis weiterverwendet werden.

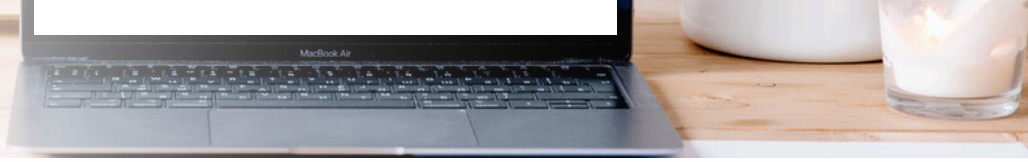
Achtung: Ein Passwort ist einfach zu hacken, wenn man entsprechende Sicherheitstipps nicht beachtet. Auch wenn man in öffentlichen WLAN-Netzwerken einsteigt (bspw. in der ÖBB oder in der Bibliothek) können Passwörter leichter von unbefugten Person ausgelesen werden.

Die 2 wichtigsten und sichersten Passwörter sind:

1) für den digitalen Passwortmanager und
2) für die persönliche E-Mail-Adresse

Zentral ist ein eigenes E-Mail-Postfach, auf das niemand sonst Zugriff hat, da praktisch jeder Online-Dienst zur weiteren Kommunikation (wie die Zurücksetzung des Passworts) die Angabe einer E-Mail-Adresse verlangt. Frauen/Mädchen, die von Gewalt betroffen sind, müssen deshalb eventuell eine neue E-Mail-Adresse einrichten und diese bei allen vorhandenen Online-Konten und Diensten der Frau / des Mädchens ändern.

DFMB Dachverband Frauen- und Mädchenberatung
FRAUEN* SERVICE BERATUNG BILDUNG FORSCHUNG
Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



Betroffene unterstützen

Checkliste: Erste Hilfe bei Cyber-Gewalt

Smartphone | Bestandsaufnahme & Sicherheitspraxis | E-Mail-Sicherheit

1. Schritt: Bestandsaufnahme

Um gute Erste Hilfe in der Beratung zu leisten, muss geklärt werden, ob die gewaltausübende Person (wie (Ex)-Partner) Zugriff auf die persönlichen elektronischen Geräte wie das Smartphone, Fitnessarmband, den Router oder Rechner der betroffenen Frau hatte. Wenn ja, sollten diese Geräte auf „Freigaben" geprüft werden. Fitnessarmbänder sollten nicht mehr getragen werden. Auch die elektronischen Geräte und "smarte Spielzeuge" der Kinder (z.B. sprachgesteuerte Spielzeuge und Gegenstände, die mit einer App verbunden sind) sollten gesichtet und überprüft werden.

Wenn die Betroffene mit dem Gewalttäter zusammengewohnt hat oder er smarte Elektronikgeräte im Haushalt installiert hat, müssen außerdem SmartHome-Geräte (z.B. smarte Türöffner, Jalousien oder Heizungssysteme) überprüft und möglichst der Internet-Router zurückgesetzt werden.

Fragen für die (telefonische) Erstberatung bei Cyber-Gewalt

Orientierungsfragen für das psychosoziale Erstgespräch oder eine erste telefonische Beratung bei Cybergewalt

1. Wer ist in Ihrer Beziehung für technische Dinge zuständig?
2. Unterstützt Ihr Partner Sie bei Fragen rund um Handy oder Computer?
   (Bei beendeter Beziehung: Hat Ihr Ex-Partner dabei unterstützt?)
3. Wer hat das Smartphone nach dem ersten Einschalten eingerichtet?
4. Wer installiert Apps und/oder nimmt Einstellungen am Handy vor?

Achtung: Wenn der Gewalttäter über Wissen aus dem Bereich der Informations- und Kommunikationstechnologien verfügt, besteht ein erhöhtes Sicherheitsrisiko für die Betroffene. Dieses sollte in der Beratung gezielt abgefragt werden, relevant sind dabei evtl. sein Job, sein Hobby oder auch seine Interessen.

2. Schritt: Sicherheitsbasis schaffen

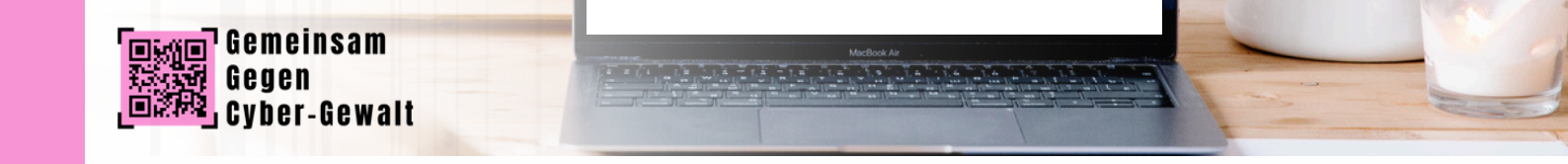
Um sich einen Überblick zu verschaffen, ist es notwendig, systematisch alle vorhandenen Online-Konten (E-Mail-Adressen, Social Media-Konten, Online-Dienste oder Online-Dating-Accounts) aufzulisten und zu vermerken, welche E-Mail-Adressen und/oder Handynummern die betroffene Frau bzw. ihre Kinder dafür verwenden. Als erstes ist es wichtig, bei allen alten E-Mail-Adressen die Passwörter zu ändern – ggf. auch bei jenen der Kinder. Deutlich sicherer ist hierbei eine sogenannte Zwei-Faktor-Authentifikation – also ein zweistufiges Anmeldeverfahren.

Achtung: Zentral für weitere Schritte ist ein eigenes E-Mail-Postfach, auf das niemand sonst Zugriff hat, da praktisch jeder Online-Dienst zur weiteren Kommunikation die Angabe einer E-Mail-Adresse verlangt. Es muss daher evtl. eine neue E-Mail-Adresse eingerichtet werden und diese als Kontakt in den vorhandenen Online-Konten und Diensten geändert werden. Anschließend sollten alle weiteren Passwörter geändert werden: Vom heimischen WLAN über den Internet-Router bis hin zu Social Media Accounts und Diensten wie Netflix oder Online-Einkaufsdiensten. Das benötigt Zeit. Damit die Betroffene online handlungsfähig bleibt, ist es wichtig, sie mit dem privaten Modus von Internet-Browsern vertraut zu machen. Der private Modus macht es möglich, den eigenen, aber auch fremde Rechner zu nutzen, ohne Spuren zu hinterlassen und. Wenn nicht ausgeschlossen werden kann, dass der Gewalttäter heimlich mitliest, bzw. smarte Geräte überwacht, sollte auf das Speichern von sensiblen Daten auf den Geräten verzichtet werden.

3. Schritt: Beweissicherung

Berater*innen sollten Betroffene von Cyber-Gewalt dabei unterstützen Beweise genau zu dokumentieren. Wie bei häuslicher oder sexualisierter Gewalt möchten Betroffene zunächst oft keine polizeiliche Anzeige erstatten oder juristisch gegen die Gewalt vorgehen. Es ist wichtig die Beweise dennoch zu sichern, falls die Betroffene ihre Meinung dazu ändert. (vgl. Factsheet #4 Beweissicherung und den Fachbuchartikel: Digitale Erste Hilfe und Sicherheitsprinzipien für Berater*innen bei digitaler Gewalt von Bauer & Hansen (2021))

DFMB Dachverband Frauen- und Mädchenberatung
FRAUEN* SERVICE BERATUNG BILDUNG FORSCHUNG
Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



Gemeinsam Gegen Cyber-Gewalt

Unterstützung bei Cyber-Gewalt

I Beweise sichern

Netzbeweis.at

Sicherheitseinstellungen in Sozialen Netzwerken überprüfen

Die Beweissicherung bei Cyber-Gewalt ist sehr wichtig und kann umfangreich sein. Für die betroffene Frau empfiehlt es sich, dass sie ein (digitales) Gewalttagebuch führt, in dem sie genau erfasst, wann, welcher Übergriff geschehen ist. Festgehalten werden sollte auch, ob/welche Zeug*innen etwas beobachten konnten und welche psychische oder physische Reaktion der Angriff bei der betroffenen Frau ausgelöst hat. Jeder Eintrag sollte mit Beweismaterial wie Screenshots, Ausdrucken, Fotos oder abgespeicherten Sprachnachrichten untermauert werden. Beweismaterial kann als Hinweise oder als Zusatz bei der Polizei zur Anzeige gebracht und zur Verfügung gestellt werden.*

Achtung: Die Beweismittel (E-Mails, Nachrichten oder Sprachnachrichten) sollen nicht an andere Personen weitergeleitet werden, das kann diese verfälschen. Bei E-Mails empfiehlt es sich den „Header" anzeigen zu lassen. Dies kann nach dem Öffnen der E-Mail an einem Computer unter den Einstellungen „Header", „Kopfzeile" oder „Original anzeigen" eingestellt werden. Der „Header" bietet der Polizei wichtige Meta-Daten für die Strafermittlung.

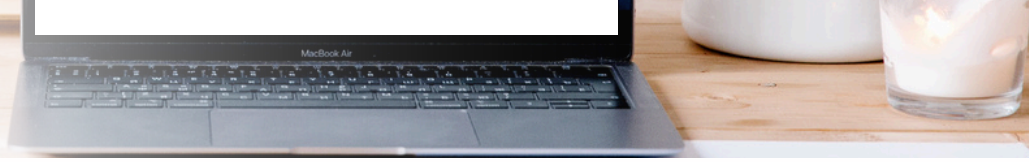
Wenn die Beweise gesichert sind, sollte unverzüglich gemeinsam mit der betroffenen Frau / dem betroffenen Mädchen Kontakt mit den Seitenbetreiber*innen aufgenommen werden, um unerwünschte Informationen (Posts, Fotos, Nachrichten, Daten) von der Internetseite oder aus sozialen Netzwerken zu löschen.

Personenbezogene Daten, Fotos und Videos können aus der Google-Suche oberflächig gelöscht werden. Google hat dafür ein eigenes Antragsformular zur Entfernung personenbezogener Daten, das ihr unter folgendem Link findet: https://bit.ly/2HgYW8p

Die Initiative netzbeweis.com bietet verschiedene Möglichkeiten zur Beweissicherung von digitalen Vorfällen von Cyber-Gewalt und ist kostenfrei für die Betroffenen zugänglich.

*In Deutschland gibt es bereits die Möglichkeit, dass Betroffene von Cyber-Gewalt eine polizeiliche Anzeige online einbringen können. Der Erstkontakt mit der Polizei ist in solchen Fällen online. Danach wird die Frau zur Erfassung der Aussage vorgeladen.

DFMB Dachverband Frauen- und Mädchenberatung
FRAUEN* SERVICE BERATUNG BILDUNG FORSCHUNG
Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



Basiswissen Cyber-Gewalt

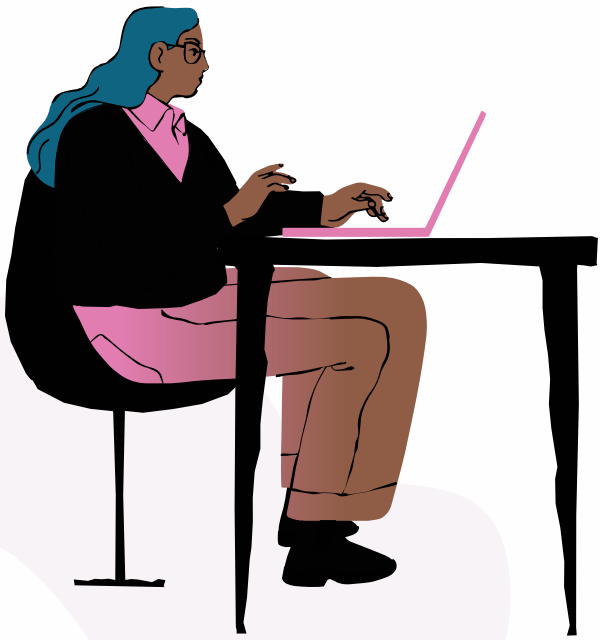
unterschiedliche Formen von Cyber-Gewalt

Standortüberwachung | GPS-Tracker | Cloud-Dienste

Cloud-Dienste überprüfen

Die häufigste Ortungsart ist die Ortung via Cloud-Dienste (wie Google Drive oder iCloud). Standortdaten können über eine Cloud geteilt werden, was es der Gewalt ausübenden Person ermöglichen kann, den Standort der Frau / des Mädchens zu orten. Über Cloud-Dienste lassen sich Smartphones und andere elektronische Geräte auf den Meter genau orten und so der Aufenthaltsort der Frau / des Mädchens herausfinden. Bei Google Drive geht dies über die Funktion „Find My Mobile" und bei der iCloud „Wo ist?".
Die Ortung via Cloud funktioniert nur, wenn Standortdienste aktiviert sind und diese mit anderen geteilt werden oder wenn ein Dienst wie "Find My iPhone" (für Apple-Geräte) oder "Find My Device" (für Android-Geräte) verwendet wird, um ein verlorenes Gerät wiederfinden zu können. Diese Einstellungen können auch ohne Wissen der Betroffenen aktiviert sein. Es ist deshalb wichtig, die Sicherheitseinstellungen am Smartphone zu überprüfen und sicherzustellen, dass die Standortdaten nicht geteilt werden.

Es kann passieren, dass ein Gewalttäter kleine Geräte wie einen "AirTag", "Tile" oder GPS-Tracker z.B. am Auto, in einer Tasche der Betroffenen oder im Spielzeug der Kinder versteckt hat. Der Täter kann sich mithilfe seines eigenen Smartphones mit den kleinen Geräten koppeln und so jederzeit den Aufenthaltsort der Betroffenen ausfindig machen. AirTags oder Tile, die eigentlich dafür gedacht sind, die eigenen Geräte bei Verlust wiederzufinden, können so missbräuchlich verwendent werden. Wenn ein Täter den neuen Wohnort oder andere Aufenthaltsorte der Betroffenen immer wieder ausfindig macht, könnte ein (Bluetooth)-Tracker dahinterstecken.



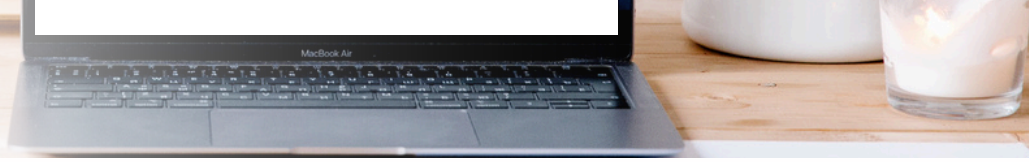
Achtung: Die Funktion "Standortdaten" sollte ausgeschaltet sein und die Geräte durch sichere Passwörter (vgl. Factsheet #2) und eine Zwei-Faktor-Authentifikation geschützt sein.

Achtung: Es kann vorkommen, dass betroffene Frauen / Mädchen ihre Smartphones bei Verlust aus der Ferne sperren lassen wollen. Das ist auch ohne Cloud-Dienste der Geräte möglich und funktioniert mit der IMEI (Mobile Equipment Identidy) Nummer des Smartphones. Um die IMEI abzurufen, muss man einfach die Nummer

*#06#

anrufen. Dadurch lässt sich eine einzigartige Nummer einsehen, die man aufschreiben kann und mit der das Smartphone bei Verlust durch den/die Netzbetreiber*innen bzw. die Polizei gesperrt werden kann.

DFMB
Dachverband Frauen- und Mädchenberatung
FRAUEN* SERVICE
BERATUNG BILDUNG FORSCHUNG
Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



Basiswissen Cyber-Gewalt

| Cyber-Gewalt gegen Frauen & Mädchen mit Behinderungen

Teilen von Passwörtern mit Betreuungspersonen | Social Media & Computerspiele

Für viele Frauen und Mädchen mit Behinderungen ist das Internet ein wichtiger Ort, um sich mit anderen zu vernetzen oder auszutauschen. Frauen und Mädchen mit Behinderungen sind eine besonders vulnerable Gruppe, wenn es um Cyber-Gewalt geht. Sie sind verschiedenen Formen von Gewalt und Diskriminierung im digitalen Raum ausgesetzt, was bereits bestehende Herausforderungen verstärkt. Oft sind die Gewalttäter aus dem nahen Umfeld der Frauen und Mädchen mit Behinderungen oder sind betreuende Personen mit denen Passwörter geteilt werden.

Mädchen und Frauen mit Behinderungen, die sich im Internet äußern oder online sind, werden oft mit sexualisierter Gewalt bedroht, sie werden sexuell belästigt, beleidigt und gestalkt. Das kann beispielsweise über Social Media sein oder auch bei online Computerspielen.

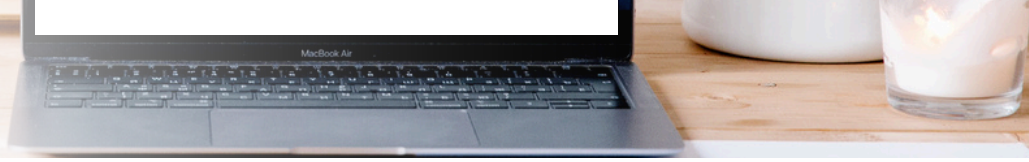
Im Netz wirken Machtverhältnisse. Auch das Netz bildet unsere u.a. sexistische und ableistische Gesellschaft ab.
Darüber hinaus haben Frauen und Mädchen mit Behinderungen nie barrierefreie Zugänge zum Internet oder einen nur eingeschränkten Zugang zu Websites oder Apps und zu Informationen.

Für die Beratung oder Gruppenangebote gilt, proaktiv Cyber-Gewalt anzusprechen, da viele Frauen und Mädchen mit und ohne Behinderungen noch nicht genau benennen können, dass sie Gewalt erfahren haben.

Der deutsche bff, Bundesverband Frauenberatungsstellen und Frauennotrufe, hat Informationen zu Cyber-Gewalt in Leichter Sprache verfasst - hier zum Nachlesen:

Frauen gegen Gewalt - Digitale Gewalt (https://www.frauen-gegen-gewalt.de/de/leichte-sprache/das-ist-gewalt/digitale-gewalt.html)

DFMB Dachverband Frauen- und Mädchenberatung
FRAUEN* SERVICE BERATUNG BILDUNG FORSCHUNG
Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



Basiswissen Cyber-Gewalt

| Stalkerware: “Ich weiß, wo du bist!”

Per E-Mail/Nachricht/physischen Zugriff | Anti-Diebstahl-Apps | Via Cloud

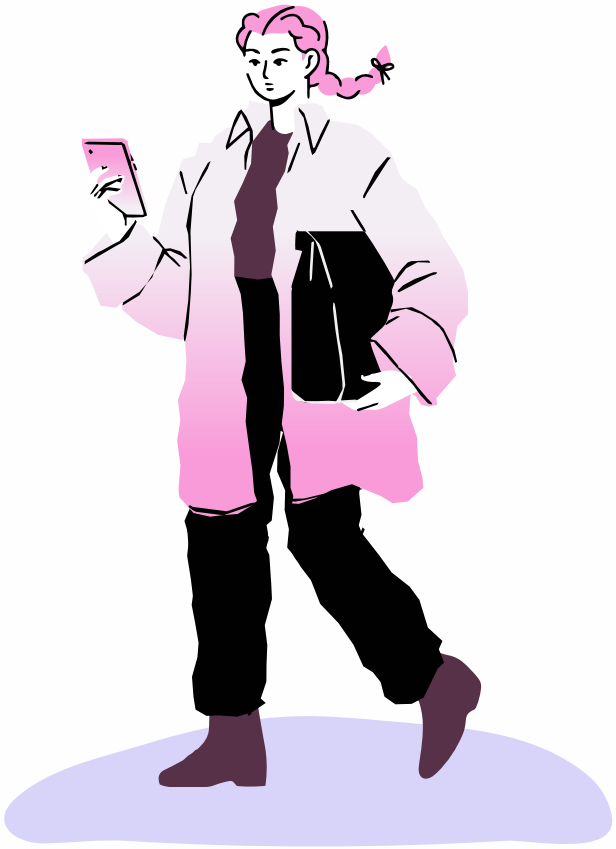
Es gibt 3 Möglichkeiten, wie eine Stalkerware (auch genannt Spionage Software, Spy Apps) auf das Smartphone oder den Computer der betroffenen Frau gelangt:

- Stalkerware kann durch E-Mail- oder Nachrichten Anhänge unabsichtlich heruntergeladen werden, weil die Software beispielsweise als Katzenbild oder wichtiges Dokument getarnt war. Auch Anti-Diebstahl Software, die auf den ersten Blick als etwas „gutes und praktisches“ wirkt, kann als Stalkerware missbraucht werden.

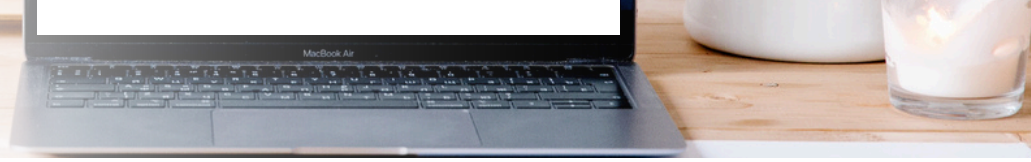
- Die gewaltausübende Person hatte einmal direkten Zugriff auf das elektronische Gerät der betroffenen Frau und hat in dieser Zeit Stalkerware installiert.

- Die gewaltausübende Person hat zu Cloud-Diensten der betroffenen Frau Zugang und die Stalkerware funktioniert über diesen Dienst.

Achtung: Sollte die betroffene Frau davon berichten, dass die gewaltausübende Person viele Informationen und Aufenthaltsorte von ihr kennt, könnte das ein Indiz für die Existenz von Spionage Software auf ihrem Handy sein. Durch das ständige Abfangen und Auslesen der Daten der Frau werden die Geräte langsamer als gewohnt und der Akku ist schneller leer. Das Zurücksetzen bzw. das Neuaufsetzen von Geräten kann eine wirkungsvolle Strategie sein, um sich der Software zu entledigen. Trotzdem wird nicht jede Software damit nachhaltig gelöscht. Im Zweifelsfall sollten IT-Spezialist*innen hinzugezogen bzw. die Geräte ausgetauscht und die Passwörter geändert werden.



Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



Basiswissen Cyber-Gewalt

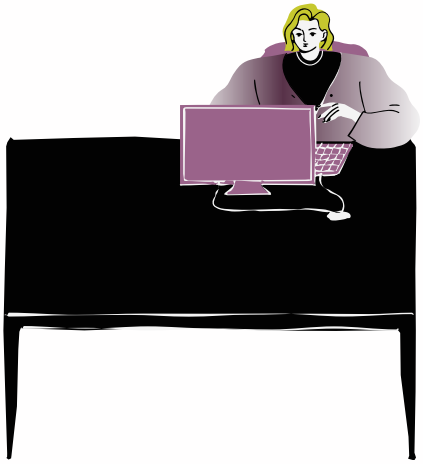
| Social Media

Was ist bei Facebook zu beachten?

Sicherheitseinstellungen in Sozialen Netzwerken überprüfen

Facebook ist ein beliebtes Soziales Netzwerk in Österreich und ist in den letzten Jahren wegen des Datenschutzes unter berechtigter Kritik gestanden. Nun wurden einige Sicherheits- und Privatsphäreeinstellungen für die Nutzer*innen nachgebessert.

Achtung: Diese Facebook-Seite (https://about.meta.com/actions/safety) bietet aufschlussreiche Informationen für betroffene Frauen und steht in verschiedenen Sprachen zur Verfügung. Grundsätzlich lässt sich festhalten, dass die Privatsphäre- und Sicherheitseinstellungen von Facebook bei einer Erstanmeldung sehr offen sind. Immer wenn neue Nutzungsbedingungen von Soziale Netzwerken wie Facebook gelten oder Updates erfolgen, sollten nochmals alle Sicherheitseinstellungen überprüft werden. Es kann sein, dass neue Funktionen hinzugekommen sind, die eine gewaltbetroffene Frau gefährden könnten, oder dass vorgenommene Einstellungen rückgängig gemacht worden sind.



Unter „Einstellungen und Privatsphäre“ auf Facebook lassen sich interessante Funktionen für die betroffene Frau konfigurieren:

- „Hier bist du aktuell angemeldet“ unter dieser Funktion im „Aktivitätenprotokoll“ lässt sich einsehen, wo und mit welchem Gerät das Facebook Profil angemeldet ist. So kann die betroffene Frau feststellen, ob sich ein Unbefugter Zugang zu ihrem Profil verschafft hat und ihre Kommunikation mitlesen kann.
- Achtung: Sollte festgestellt werden, dass ein Unbefugter an einem bestimmten Gerät angemeldet ist, ist es möglich, diese Funktion anzuklicken und sich „sofort abzumelden“. Danach sollte die betroffene Frau so schnell wie möglich ihre Passwörter ändern und eine Zwei-Faktor Authentifikation einstellen (vgl. Factsheet #2).
- Unter „Einstellungen und Privatsphäre“ und dem Überpunkt „Kontenübersicht“ unter „Passwörter ändern“ und „Zweistufige Authentifizierung“ lassen sich die Passwörter einfach ändern.
- „Login-Warnungen“ Wenn diese Funktion aktiviert ist, erhält die betroffene Frau eine E-Mail oder SMS mit einem Warnhinweis, wenn eine unbefugte Person versucht, sich von einem anderen Internetbrowser oder Gerät als gewöhnlich in dem Benutzerkonto der Frau anzumelden.
- Unter „Einstellungen“ und „Deine Informationen und Berechtigungen“ können alle Informationen und Daten der Frau per Mail abgerufen werden. Diese Datensammlung enthält u.a. alle Nachrichten (teilweise auch gelöschte) sowie alle Posts sowie Fotos. Diese Funktion eignet sich als hervorragendes Mittel zur Sicherung von Beweisen.

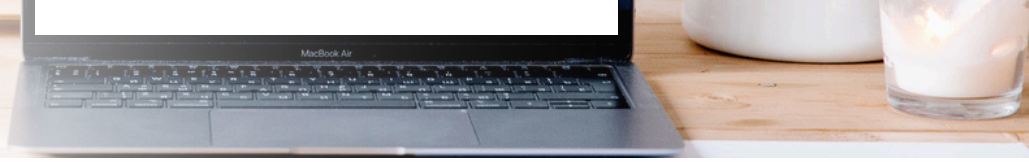
Achtung: In der Beratung sollte geklärt werden, mit wem die betroffene Frau in ihren Sozialen Netzwerken „befreundet“ ist. Sind ihre Facebook „Freunde“ auch ihre Freund*innen aus ihrem realen Leben oder gibt es darunter Personen, die Kontakt mit der gewaltausübenden Person haben? Unter „Einstellungen“ und „Privatsphäre-Einstellungen“ sollte beachtet werden, dass alle möglichen Funktionen von „Öffentlich“ auf „Freunde“ gestellt sind.

Achtung: Auch mit den Kindern der betroffenen Frau sollte über Freundschaften in Sozialen Netzwerken gesprochen werden. Wenn das Facebook Profil der betroffenen Frau gehäckt wurde, kann dies unter www.facebook.com/hacked gemeldet werden. Das Profil kann vorrübergehend gesperrt bzw. ein neues Passwort vergeben werden.

DFMB
Dachverband Frauen- und Mädchenberatung

FRAUEN* SERVICE
BERATUNG BILDUNG FORSCHUNG

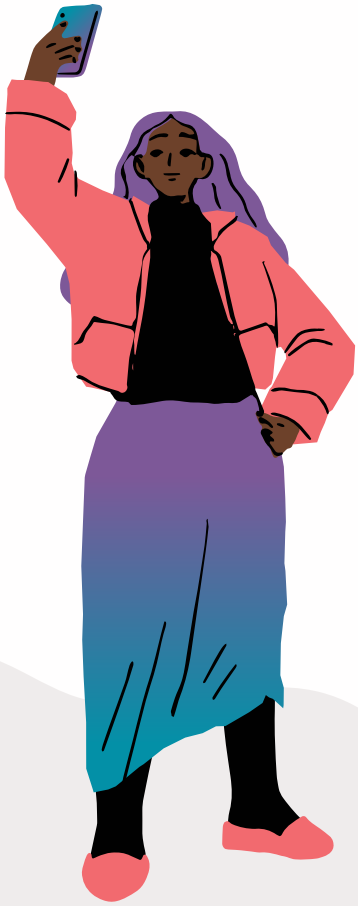
Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



(Daten-)Sicherheit in der Beratung

| Sichere Kommunikation für die Beratung

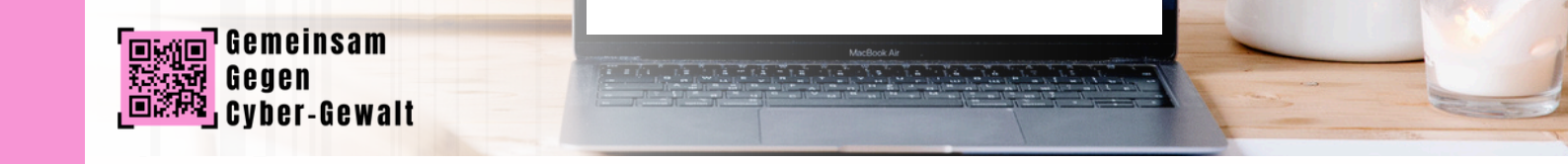
Messenger sicher nutzen | Signal, Threema



Verschlüsselte Messaging-Apps sind wichtig für die sichere Kommunikation mit Klientinnen und der Arbeit einer Frauen- und Mädchenberatungsstelle. Dazu sollten Messaging-Apps verwendet werden, die eine Ende-zu-Ende-Verschlüsselung anbieten, wie z.B. Signal oder Threema. Dadurch werden die Nachrichten während der Übertragung und auch auf den Servern der Dienstanbieter*innen verschlüsselt. Die Apps sind außerdem Open Source, damit der Quellcode und besonders die richtige Implementierung der Verschlüsselung von unabhängigen Stellen laufend kontrolliert werden kann.

Achtung: Auch wenn Whatsapp eine Ende-zu-Ende-Verschlüsselung hat, gehört es zu Facebook (Meta) und das Programm weist starke Sicherheitsmängel auf. Keine sensiblen Daten und Fotos von Klientinnen über Whatsapp teilen.

Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



(Daten-)Sicherheit in der Beratung

| Datenlecks vermeiden: Speicherung von sensiblen Daten

Nuudel statt Doodle | Cryptpad statt Google Drive | Sichere Browser & Suchmaschinen

Um Datenlecks zu vermeiden und sensible Daten sicher zu speichern, gibt es einige bewährte Methoden, wie Verschlüsselung von Daten, das Einrichten einer Zugriffskontrolle (Smartphone Code) und upgedatete elektronische Geräte, um von großen internationalen Firmen abzusehen.

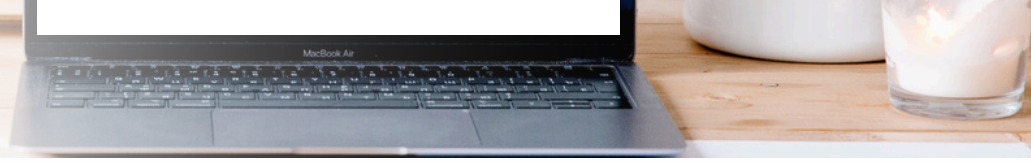
Keine sensiblen Daten auf den Geräten speichern und Sicherheitskopie der Daten erstellen

Falls sich die gewaltausübende Person doch Zugriff zu dem Smartphone verschafft hat, kann sie alle abgespeicherten sensiblen Daten der Frau einsehen. Der Speicherung von abfotografierten Dokumenten der betroffenen Frau (wie beispielsweise: Krankenkassenkarten, Briefe mit Termin bei Behörden oder Gerichten) oder der Pässe der Kinder ist immer abzuraten.

Achtung: In der Beratung sollte gemeinsam mit der Frau geklärt werden, wo sie ihre sensiblen Daten speichern möchte und wie sie eine Sicherheitskopie ihrer Daten (mögliche Beweise) erstellen kann. Möglichkeiten sind österreichische oder europäische Cloud-Dienste (wie Nextcloud) oder externe Festplatten (wie bspw. USB-Speichersticks).

Achtung: Für die Beratung sollte unbedingt mit datensparsamen Tools zum Schutz der Klient*innen und der Mitarbeiter*innen gearbeitet werden. Auch wenn Google (Docs) und Doodle einfach bedienbare Anwendungen sind – datensparsam sind sie auf keinen Fall. Datensparsame Alternativen: Suchmaschine duckduckgo, Terminfindungstool mit nuudel, CryptPad.fr

Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



#GemeinsamGegenCybergewalt

| Was es braucht, um gegen Cyber-Gewalt vorzugehen

Wie geht es weiter? | Handlungsspielräume | Wissensvermittlung | Kooperationen | Forderungen

Cyber-Gewalt ist Alltag für Frauen und Mädchen in Österreich. Unsere Einschätzung ist, dass eine klare Abgrenzung zwischen häuslicher und sexualisierter und digitaler Gewalt in ein paar Jahren keinen Sinn mehr machen wird – weil alle geschlechtsspezifischen Gewaltformen digitale Komponenten haben.
Wir vom Dachverband Frauen- und Mädchenberatung kritisieren in diesem Zusammenhang die nach wie vor oft vorgenommene Trennung zwischen „online" und „realer" Gewalt: Digitale Gewalt hat reale Auswirkungen auf die Betroffenen. Es ist wichtig, jede Gewalterfahrung ernst zu nehmen, Betroffenen keine Schuld zu geben sowie Beratung und Prävention zu stärken. Die Istanbul Konvention gilt auch für den digitalen Raum!
Frauen- und Mädchenberatungsstellen müssen Cyber-Gewalt und die Lücken in der Unterstützungs- und Interventionsmöglichkeiten für Betroffene in ihre Gremienarbeit und Austauschtreffen mit Politik, Verwaltung und Polizei einbringen.

Jetzt stellt sich die Frage **Was muss Politik & Gesellschaft tun, um Cyber-Gewalt nachhaltig zu bekämpfen?**

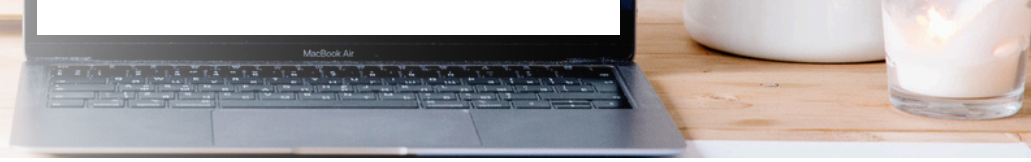
Handlungsbedarfe aus Sicht des Dachverbands

Vorhandene Expertisen stärken und erweitern

- Hilfreich in der Beratung gewaltbetroffener Frauen wäre momentan vor allem ein Unterstützungssystem der Frauen- und Mädchenberatungsstellen, das sicher finanziert und so ausgestattet ist, dass die Beratungsstellen mit der Digitalisierung Schritt halten können und neben der eigentlichen Beratung auch Kapazitäten für Präventionsangebote und Öffentlichkeitsarbeit haben. Die Berater*innen aus Beratungsstellen und Frauenhäusern setzen sich einem hohen Risiko aus, selbst zum Ziel von (digitalen) Angriffen zu werden.

- Deswegen empfehlen wir die Verpflichtung zu Fortbildungen für alle relevanten Berufsgruppen umzusetzen: Anwält*innen, Polizei, Strafverfolgungsbehörden und Richter*innen. Das technische Wissen und Medienkompetenzen müssen regelmäßig aktualisiert und in die bestehende Expertise zum Umgang mit geschlechtsspezifischer Gewalt integriert oder bei verlässlichen externen Expert*innen abgerufen werden können.

Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



#GemeinsamGegenCybergewalt

| Was es braucht, um gegen Cyber-Gewalt vorzugehen

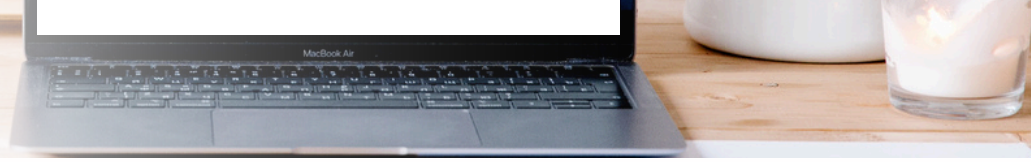
- Eine große Zahl von Berater*innen wird im aktuellen Netzwerk-Projekt „Gemeinsam gegen Cyber-Gewalt“ zu Beratung bei Cyber-Gewalt geschult. Es gibt sehr viele Anfragen zu dem Thema. Es kristallisiert sich außerdem zunehmend der Bedarf an IT-Expertise für besonders komplexe oder umfangreiche Fälle von Cyber-Gewalt heraus, z.B. in Form von Technikkompetenzzentren für geschlechtsspezifische Cyber-Gewalt. Diese sollten für das professionelle Unterstützungssystem und Betroffene ansprechbar sein, um Gefährdungen zu analysieren. Gleichzeitig sollten diese gewaltbetroffene Frauen dabei unterstützen ihre Geräte und Accounts zu sichern und gerichtsfeste Beweise festzuhalten.
- Zudem brauchen Frauen- und Mädchenberatungsstellen zusätzliche finanzielle Mittel für das Hinzuziehen von IT-Fachpersonen und die Absicherung der eigenen technischen Ausstattung und digitalen Infrastruktur.

Strafverfolgung und Justiz

Die Strafverfolgung Cyber-Gewalt steckt – trotz gesetzlicher Nachbesserungen in den letzten Jahren – in den Kinderschuhen. Viele Betroffene, aber auch Täter, haben das Gefühl, dass das Internet ein rechtsfreier Raum ist. Das erhöht die Gewaltbereitschaft bei den Tätern. Gründe für mangelnde Strafverfolgung sind fehlende spezifische Kenntnisse zu digitalen Phänomenen sowie mangelnde Kapazitäten bei den Strafverfolgungsbehörden. Zusätzlich wird den Betroffenen häufig eine Mitschuld an der erlebten Gewalt zugeschrieben, was die Anzeigebereitschaft verringert. Immer wieder berichten Betroffene von Cyber-Gewalt außerdem, dass sie bei der Polizei auf eine große Ratlosigkeit im Umgang mit digitaler Technik gestoßen sind, z.B. bei Fragen der Sicherung von Beweisen, die sich auf Smartphones befinden.

- Wir empfehlen, dass die Ermittlungs- und Strafverfolgungsbehörden mehr IT-forensische Kapazitäten aufbauen, ihre technische Ausstattung und Medienbildung verbessert werden, damit die Verfolgung bei Cyber-Gewalt nicht bereits an der Beweissicherung scheitert.
- Seit vielen Jahren gibt es in Österreich bei Polizei und teils auch Justiz Einheiten, die auf häusliche Gewalt oder Sexualstraftaten spezialisiert sind. Diese sind bestenfalls sensibilisiert im Umgang mit Betroffenen geschlechtsspezifischer Gewalt, kennen sich aber nur eingeschränkt mit der neu hinzugekommenen digitalen Komponente dieser Gewalt in Beziehungen aus. Daneben gibt es Einheiten, die in den letzten Jahren speziell zur Bekämpfung von Cybercrime-Delikten eingerichtet wurden. In diesen Einheiten befindet sich wichtiges Fachwissen über IT-Anwendungen und die Möglichkeiten der digitalen Technik, dort werden aber keine Fälle geschlechtsspezifischer Cyber-Gewalt bearbeitet, sondern beispielsweise digitale Angriffe auf Wirtschaftsunternehmen.
- Wir empfehlen dringend, dass diejenigen Personen bei Polizei und Justiz, die mit Fällen geschlechtsspezifischer Gewalt befasst sind, zur digitalen Komponente dieser Gewalt fortgebildet werden müssen und bei Bedarf das Wissen der Kolleg*innen aus den Abteilungen Cybercrime hinzuziehen können.

DFMB
Dachverband Frauen- und Mädchenberatung
FRAUEN* SERVICE
BERATUNG BILDUNG FORSCHUNG
Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



#GemeinsamGegenCybergewalt

| Was es braucht, um gegen Cyber-Gewalt vorzugehen

Forschung

Die Datenlage zu Cyber-Gewalt gegen Frauen ist nach wie vor unzureichend. Umfassende Daten wären notwendig, um evidenzbasierte Maßnahmen zu setzen.

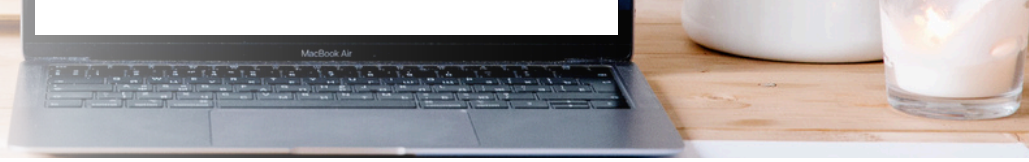
- Wir empfehlen deshalb, mehr aussagekräftige Studien über Ausprägung geschlechtsspezifischer Cyber-Gewalt durchzuführen, um Ausmaß und digitale Formen von Partnerschaftsgewalt, Stalking und sexualisierter Gewalt zu erfassen.
- Jegliche Prävalenzstudie zu Gewalt gegen Frauen sollte dringend auch digitale Aspekte geschlechtsspezifischer Gewalt detailliert und regelmäßig abfragen.
- Es lässt sich bereits jetzt sagen, dass die Anzahl geeigneter Tatmittel und Verbreitungswege mit der Digitalisierung weiterwachsen. Internationale Forschungsergebnisse weisen schon jetzt durchaus auf eine Zunahme einzelner Formen geschlechtsspezifischer Cyber-Gewalt hin, beispielsweise bildbasierter digitaler Gewalt in Form von Deep Fakes (insbesondere die Bildmanipulation von pornografischem Material). Um Strategien gegen diese Formen der Gewalt zu entwickeln und zu finanzieren, benötigt es aussagekräftige Zahlen zur Verbreitung. Ein regelmäßiges Monitoring der Entwicklungen unterschiedlicher Gewaltformen ließe sich ggf. durch die Einrichtung von Meldestellen erreichen, bei der Betroffene ihre Fälle auch unabhängig von einer Anzeige melden können.

Öffentlichkeitsarbeit

Eine größere Sichtbarkeit des Themas Cyber-Gewalt ist notwendig und hat in der Vergangenheit bereits auch konkrete Wirkung gezeigt.

- Viele Betroffene erfahren über Cyber-Gewalt über Social Media: Es ist wichtig, dass Betroffenen die Unterstützung suchen, eine professionelle Beratung in Form von Frauen- und Mädchenberatungsstellen zur Verfügung steht. Aber nicht nur Kampagnenarbeit muss geleistet werden – es braucht finanzielle Ressourcen für die Beratungsstellen, um zeitintensive Beratungen bei (Cyber-)Gewalt für Betroffene anzubieten.

Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



#GemeinsamGegenCybergewalt

| Was es braucht, um gegen Cyber-Gewalt vorzugehen

Verantwortung von Plattformbetreiber*innen und Internetfirmen

- Es braucht an den Interessen Gewaltbetroffener orientierte Handlungsempfehlungen, wie Entwickler*innen und Hersteller*innen von Hard- und Software mehr Verantwortung für gewaltschutzrelevante Sicherheitsstandards ihrer Produkte übernehmen können.
- Wir empfehlen, die Pflicht zu funktionierenden Meldewegen in sozialen Netzwerken, bei Seitenbetreiber*innen, Anbieter*innen von Online-Diensten sowie Software- und Produktentwickler*innen, wenn mit ihrem Produkt (bspw. Stalkerware, Ortungsdienste oder Heimweg-Apps) Cyber-Gewalt und damit verbunden, andauernde Kontrolle über eine Person ausgeübt werden kann.
- Für den Vertrieb von Produkten und Software, die es einer gewaltausübenden Person ermöglichen, Cyber-Gewalt und andauernde Überwachung elektronischer Geräte unerkannt auszuüben, empfehlen wir eine Pflicht zur Kennzeichnung. So wären beispielsweise eine Information beim Herunterladen von Apps, dass mit dieser App auch strafbare Handlungen ausgeübt werden können, sowie eine regelmäßige Informationsbenachrichtigung an die Nutzer*innen der Endgeräte sinnvoll.

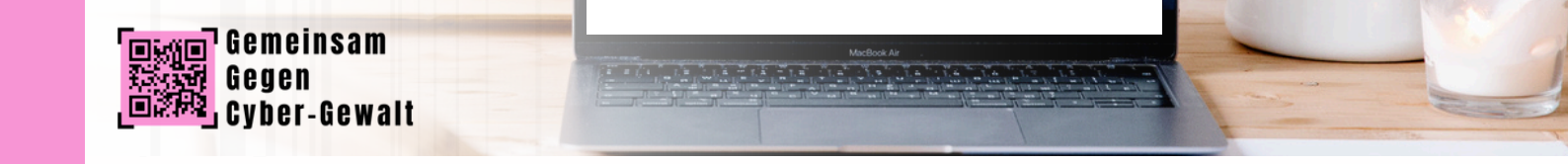
Wie sich zeigt gibt es viele Stellschrauben, an denen gearbeitet und nachjustiert werden muss.

Es braucht das Zusammenwirken auf unterschiedlichen Ebenen, damit Cyber-Gewalt nachhaltig entgegengetreten werden kann.

DFMB
Dachverband Frauen- und Mädchenberatung

FRAUEN* SERVICE
BERATUNG BILDUNG FORSCHUNG

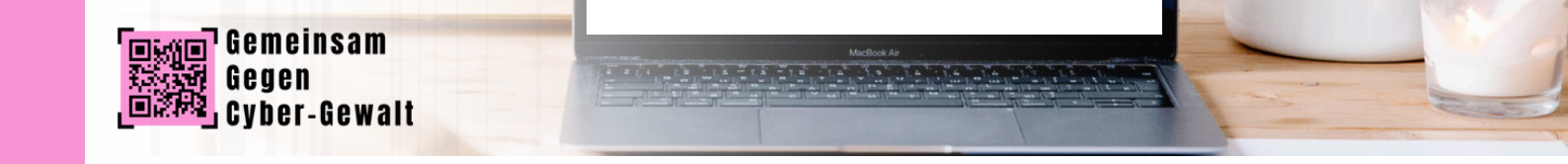
Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



Zusatzmaterial

Checkliste für Beratungsgespräche zu Cyber-Gewalt

Im Zuge des Projekts wurde eine Checkliste für den Beratungskontext bei Cyber-Gewalt entwickelt. Bei Interesse ist der Dachverband Frauen- und Mädchenberatung unter office@dfmb.at erreichbar.



Gemeinsam Gegen Cyber-Gewalt

Zusatzmaterial

(Daten-)sichere Programme & Werkzeuge

Alternativen zu herkömmlichen Programmen

cryptpad.fr anstelle von Google-Diensten (https://cryptpad.fr/)

Mithilfe dieser Software können Dokumente jeglicher Form datensicher, kostenfrei und online erstellt, abgerufen und miteinander geteilt werden.

nuudel anstelle von Doodle (https://nuudel.digitalcourage.de/)

Ein datensparsames Terminfindungs-Tool mit Sitz in Deutschland. Es werden nur Daten gespeichert, die auch eingegeben werden.

duckduckgo anstelle von Google-Suchmaschine (https://duckduckgo.com/)

Datensparsam und ohne Tracking der eigenen Suchanfragen.

f droid anstelle von Google Play und App Store (https://f-droid.org/de/)

Alternativer App-Store, um leichter auf Google oder Apple zu verzichten.

Signal oder Threema anstelle von Whatsapp und Telegram (https://signal.org/de/ und https://threema.ch/de)

Sichere Ende-zu-Ende-Verschlüsselung sowie Zusatzfunktionen, um Nachrichten dauerhaft zu löschen.

Digitale Selbstverteidigung für Betroffene und in der Beratung

netzwbeweis.com (https://www.netzbeweis.com/)

Unterstützung bei der digitalen Beweissicherung, kostenpflichtig

USB-Sticks zur Beweissicherung

Mit großem Speichervolumen in verschiedenen Geschäften zu erwerben

Alternatives Handy/Smartphone

Kaspersky tinycheck (https://tiny-check.com/#/)

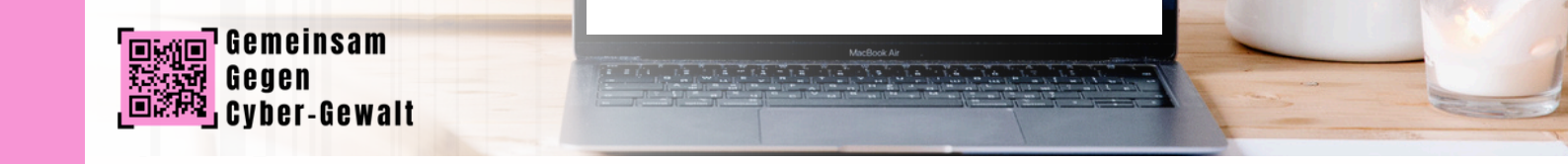
Erkennt Spyware/schädliche Software auf Endgeräten; zur Analyse der Daten wird allerdings eine IT-Person benötigt

DFMB Dachverband Frauen- und Mädchenberatung

FRAUEN* SERVICE BERATUNG BILDUNG FORSCHUNG

Bundeskanzleramt

Gefördert aus den Mitteln des Bundeskanzleramts



Zusatzmaterial

Hilfreiche Materialien & Literatur

bff & Prasad (2021) : Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung. Formen und Interventionsstrategien, Link: https://www.transcript-verlag.de/shopMedia/openaccess/pdf/oa9783839452813.pdf

Frauen* beraten Frauen* (2023): Ist das schon digitale Gewalt? Link: https://frauenberatenfrauen.at/publikation/handbuch-ist-das-schon-digitale-gewalt/

Digitalcourage & Leena Simon: Stalking, Hass, Kontrolle. Digitale Gewalt erkennen und benennen, Link: https://shop.digitalcourage.de/files/k_amp_m_978-3934636-34-7__Digitale_Gewalt__druck-n.pdf

bff & Beratungsstelle Frauennotruf Frankfurt (2024): Broschüre: Digitale Welten - Digitale Medien - Digitale Gewalt, Link: https://www.frauen-gegen-gewalt.de/de/digitale-gewalt-material/broschuere-digitale-welten-digitale-medien-digitale-gewalt.html

Melde- und Unterstützungseinrichtungen

Beratung und Meldestellen

Frauen- und Mädchenberatungsstellen des Netzwerks FMBS

ZARA GegenHassImNetz

Ban Hate - Meldung von Hasspostings/Hatecrime

Amadeu Antonio Stiftung: Antifeminismus melden

Unterstützung & Information

Saferinternet.at

mobilsicher.de

FairesNetz.at

Internet Ombudsstelle - Hass im Netz

epicenter academy - E learning

bff - Aktiv gegen digitale Gewalt

Anleitungen

Tech Safety - Ressources

Hateaid.org - Rechtssichere Screenshots (DE)

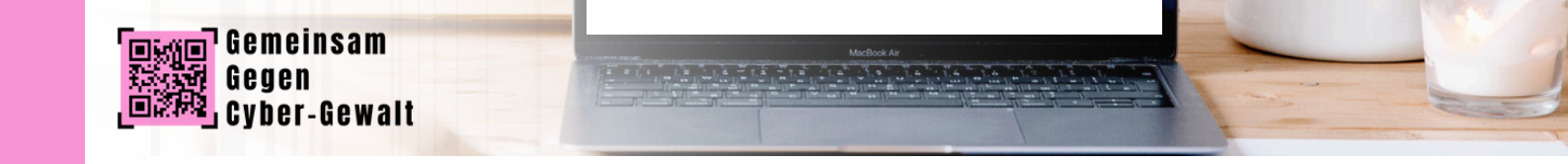
klicksafe - Materialien für den Umgang mit Kindern

haecksen

DFMB Dachverband Frauen- und Mädchenberatung

FRAUEN* SERVICE BERATUNG BILDUNG FORSCHUNG

Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts



Impressum

Herausgeber*in:
Dachverband Frauen- und Mädchenberatung
Stumpergasse 41-43/II/R3, 1060 Wien
https://dfmb.at
office@dfmb.at

Autorinnen:
Jenny-Kerstin Bauer, MA
Sophie Hansal, MA MA
Franziska Vesenmaier, MA

Layout:
Franziska Vesenmaier, MA

Das Booklet, bestehend aus 11 Factsheets und Zusatzmaterial, ist ein Produkt des Projekts #GemeinsamGegenCybergewalt. Die Factsheets sind für den Beratungskontext konzipiert und sollen Frauen- und Mädchenberater*innen sowie anderen Kolleg*innen aus dem Gewaltschutzbereich eine Unterstützung bei Cyber-Gewalt sein.

#GemeinsamGegenCybergewalt ist ein Projekt des Frauenservice Graz in Zusammenarbeit mit dem Dachverband Frauen- und Mädchenberatung von Herbst 2023 bis Dezember 2024. Das Projekt wird gefördert aus den Mitteln des Bundeskanzleramts.

DFMB
Dachverband Frauen- und Mädchenberatung

FRAUEN* SERVICE
BERATUNG BILDUNG FORSCHUNG

Bundeskanzleramt
Gefördert aus den Mitteln des Bundeskanzleramts