WEISSER RING

Wir helfen Kriminalitätsopfern.

Über die vielfältigen Formen von digitaler Gewalt und wie Sie sich schützen können

Unbegrenzte Möglichkeiten. Leider auch für Kriminelle

Smartphone, Computer und Co. gehören heute fest zu unserem Leben dazu. Viele Bereiche des Alltags hat die Digitalisierung verändert, durchdrungen und beschleunigt. Und sie wird mit großen technischen Schritten weitergehen, KI ist hier ein Stichwort. Die vielen positiven Aspekte des Internets haben auch ihre Schattenseiten.

Alles, was uns im echten Leben bewegt, schlägt ebenso hohe Wellen im Netz. Seien es das aktuelle Weltgeschehen, Kriege, die aufgeheizte Stimmung, die Spaltung und die zunehmende Verrohung der Gesellschaft. Das Internet wird zu einem Nährboden für Betrug, Gewalt, Hass und Hetze.

Viele digitale Räume. Viele unterschiedliche Tatorte

Vielleicht ist es hilfreich, nicht von dem einen Internet zu sprechen, sondern von digitalen Räumen. Social-Media-Plattformen wären dann beispielsweise ein großer digitaler Raum, in dem man sich online bewegt. Und den wir zusammen mitgestalten können. Was es dazu braucht, sind Regeln und ein klarer gesellschaftlicher Konsens, damit digitale Gewalterfahrungen nicht zur Normalität werden. Schließlich möchte niemand sein Kind online gehen lassen mit dem Wissen, dass es dort Gewalt erlebt. Weil in jedem digitalen Raum eigene Gefahren und trickreiche Cyberkriminelle lauern, kommt der Prävention eine besondere Rolle zu.

Aufklären, denn Wissen ist der beste Schutz

Mit dieser Broschüre möchten wir Sie über digitale Gewalt, ihre Formen und die damit verbundenen Gefahren im Internet aufklären. Wir zeigen Ihnen, wie Cyberkriminelle vorgehen, welche Schwachstellen sie ausnutzen und geben Ihnen jede Menge Wissen als Rüstzeug an die Hand. Dazu gehört auch, wie Sie sich schützen können und was Sie im Ernstfall tun können, wenn Sie von digitaler Gewalt betroffen sind.

Meilensteine der Digitalisierung

1984	Erste E-Mail in Deutschland verschickt
1991	Offizieller Start des World Wide Web
1996	Das erste internetfähige Smartphone
1997	Google Suchmaschine geht online
2002	Erste Handys mit Digitalkamera
2004	Facebook gegründet, Start der Social-Media-Ära
2005	YouTube startet
2007	Einführung des iPhones
2009	Gründung von WhatsApp
2022	ChatGPT und KI-Anwendungen erobern den Markt

Digitale Gewalt – ein weites Feld

Der Begriff digitale Gewalt ist in Fachkreisen bereits geläufig, der breiten Öffentlichkeit eher unbekannt. Digitale Gewalt ist ein Oberbegriff, der ein breites Spektrum an verschiedenen kriminellen Handlungen im Internet umfasst. Dazu gehören z. B. Cybermobbing, Messenger-Betrug oder Romance Scamming. Was all diese Delikte vereint, sie werden im digitalen Raum und/oder mithilfe von technischen Kommunikationsmitteln wie z. B. E-Mail oder SMS begangen und haben für die Betroffenen schwerwiegende Folgen. Mitunter dringt die digitale Aggression tief in das Leben der Opfer ein*. Zur digitalen Gewalt werden Desinformation oder Cybercrime-Delikte wie Online-Betrug nicht direkt dazugezählt. Allerdings werden die letztgenannten Delikte häufig für digitale Gewalt genutzt, um z. B. durch Desinformation eine Person zu schädigen und zu mobben. Eine trennscharfe Abgrenzung ist daher nicht leicht.

* vgl. Merz, Zeitschrift für Medienpädagogik, 2020/01, Wie analog ist digitale Gewalt?, S. 8

Zahlen, Fakten, Studien: Es kann jeden Internet-User treffen

In Deutschland nutzen 95 % der Bevölkerung das Internet.** Eine Studie*** konnte aufzeigen, dass fast jede zweite Person schon einmal online beleidigt wurde. 29 % der Befragten erhielten ungewollt Nacktbilder. Ein Bundeslagebild**** liefert weitere Zahlen zur digitalen Gewalt im Jahr 2023. Über 62 % der Opfer sind weiblich, betroffen waren über 17.100 Frauen. Auch Männer wurden angegriffen und wurden z. B. Opfer von Sextortion, die Erpressung mit sexuellem Bildmaterial.

** ARD/ZDF Medienstudie 2024 *** Studie „Lauter Hass – leiser Rückzug. Wie Hass im Netz den demokratischen Diskurs bedroht“ 2024
**** Bundeslagebild: „Geschlechtsspezisch gegen Frauen gerichtete Straftaten 2023“, BKA

Neben Hass und Hetze werden vielfältige Formen der Belästigung wie Cyberstalking oder bildbasierte Gewalt, zu denen beispielsweise Rachepornos gehören, zum weiten Feld der digitalen Gewalt gezählt.

Ganz gleich, ob das Verbrechen im Internet oder in der realen Welt stattfindet, Straftat bleibt Straftat. Im digitalen Raum ist sie jedoch schwerwiegender. Da das Netz nichts vergisst, bleiben die Inhalte mitunter jahrzehntelang abrufbar.

Gewalt, die hin- und herspringt

Digitale Gewalt kann zu analoger werden und umgekehrt, oft finden beide Formen sogar gleichzeitig statt. Die Dynamik ist nicht zu kontrollieren. Es wird beobachtet, dass sich zum Beispiel Partnerschaftsgewalt und sexualisierte Gewalt immer stärker digitalisieren und ihre analoge Form nicht mehr allein auftritt. So können verbale Anfeindungen im Netz zu echten Übergriffen vor der eigenen Haustür werden, wie es etwa bei Hass- und Hetzedelikten der Fall sein kann.
Wiederum können sich z. B. Nachstellungen beim Stalking aus der realen Welt in den digitalen Raum ausbreiten und zu Cyberstalking werden.

Merkmale von digitaler Gewalt

- zahlreiche Gewaltformen, die teilweise ineinander übergehen und sich schwer voneinander abgrenzen lassen
- sie ist meist zeit- und ortsunabhängig, Betroffene leiden rund um die Uhr
- kann in den analogen Raum übergehen und sich sogar in körperliche und sexuelle Gewalt wandeln oder diese verstärken
- oft großes Publikum
- es ist unüberschaubar, wohin sich Inhalte im Netz verbreiten, diese Inhalte sind schwer zu löschen und schnell zu kopieren, strafbare Handlungen können sich wiederholen

Über die digitalen Angreifer

Die Täter fühlen sich in der Anonymität des Internets sicher und haben eine große Distanz zum Opfer. Dadurch sinkt wiederum die Hemmschwelle, Straftaten zu begehen. Hinzu kommt: Die Täter nehmen sich im Netz als Teil einer gesellschaftlichen Mehrheit bzw. unter Gleichgesinnten wahr und handeln entsprechend ihrer Filterblase.

Bei einigen Straftaten wie dem Cyberstalking kann der Täter dem Opfer auch bekannt sein. Bei Betrugsdelikten sind die Täter häufig in Banden organisiert, die aus dem Ausland agieren.

Digitale Gewalt hat viele Ausprägungen

Beziehung und Partnerschaft

CYBERSTALKING

Worum geht's: Digitales Nachstellen, Demütigen und Ausspionieren, um das Opfer zu kontrollieren
Weiterlesen: ab Seite 10
So schützen Sie sich: ab Seite 30

ROMANCE SCAMMING

Worum geht's: Vortäuschung großer Gefühle und einer Beziehung, um große Geldsummen abzuzocken, kurz: Heiratsschwindler 2.0
Weiterlesen: ab Seite 13
So schützen Sie sich: ab Seite 30

Sexuelles und Intimes

SEXTORTION

Worum geht's: Erpressung mit sexuellem Bildmaterial
Weiterlesen: ab Seite 14
So schützen Sie sich: ab Seite 31

DICKPICS

Worum geht's: Männliche Genitalbilder, die ungefragt verschickt werden
Weiterlesen: ab Seite 14
So schützen Sie sich: ab Seite 31

RACHEPORNOS

Worum geht's: Bloßstellen und Demütigen des Ex-Partners durch das Veröffentlichen von sexuellem Bildmaterial
Weiterlesen: ab Seite 16
So schützen Sie sich: ab Seite 31

DEEPNUDES (DEEPFAKES)

Worum geht's: Mit KI erzeugte Nacktbilder oder Pornos
Weiterlesen: ab Seite 16
So schützen Sie sich: ab Seite 31

CYBERGROOMING

Worum geht's: Gezielte Kontaktaufnahme für das Anbahnen von sexuellem Missbrauch von Kindern bzw. Jugendlichen
Weiterlesen: ab Seite 17
So schützen Sie sich: ab Seite 31

Manipulieren, Spalten und Ausgrenzen

CYBERMOBBING

Worum geht's: Bloßstellen und Fertigmachen auf allen Kanälen
Weiterlesen: ab Seite 18
So schützen Sie sich: ab Seite 32

DEEPFAKES

Worum geht's: Verbreiten von Falschinformationen und Propaganda mithilfe von mit KI gefälschten Videos und Fotos
Weiterlesen: ab Seite 18
So schützen Sie sich: ab Seite 32

HASS & HETZE

Worum geht's: Einschüchtern und Angst machen sowie Abwertung, Ausgrenzung und Diffamierung von bestimmten Gruppen
Weiterlesen: ab Seite 19
So schützen Sie sich: ab Seite 32

DESINFORMATION

Worum geht's: Das Verbreiten von Falsch- und Fehlinformationen
Weiterlesen: ab Seite 19
So schützen Sie sich: ab Seite 32

Kapital- und Betrugsdelikte

PHISHING

Worum geht's: Das Abfischen von Passwörtern und sensiblen Daten für Betrugszwecke
Weiterlesen: ab Seite 21
So schützen Sie sich: ab Seite 33

IDENTITÄTSDIEBSTAHL

Worum geht's: Digitale Identität und Accounts von Fremden geklaut, übernommen und zweckentfremdet
Weiterlesen: ab Seite 24
So schützen Sie sich: ab Seite 33

MESSENGER-BETRUG

Worum geht's: Gefälschte Nachrichten, um kleinere Geldsummen zu erbeuten
Weiterlesen: ab Seite 24
So schützen Sie sich: ab Seite 33

Cyberstalking: nachgestellt mit digitalen Mitteln

CYBERSTALKING

Wenn aus der großen Liebe ein realer Albtraum wird. Über 16 % der 2023 bei der Polizei registrierten Opfer* litten unter Partnerschaftsgewalt. Diese Gewaltform kann sowohl während als auch nach einer Beziehung auftreten. Cyberstalking, also das penetrante Nachstellen, Bedrohen und Belästigen im digitalen Raum, gehört auch dazu. Überdurchschnittlich oft sind Frauen davon betroffen, die unter ihrem aktuellen oder ehemaligen Ehe- bzw. Lebenspartner leiden. Die eingesetzten Mittel beim Cyberstalking sind vielfältig, um den Partner zu kontrollieren und auszuspionieren. Um die Aktivität und die Bewegung zu überwachen, werden beispielsweise smarte Bluetooth-Tracker zur Ortung eingesetzt und dem Opfer heimlich untergeschoben, z. B. ein AirTag von Apple oder eine Variante für Android-Geräte wie z. B. ein SmartTag von Samsung. Die Tracker in der Größe einer 2-Euro-Münze wurden eigentlich konzipiert, um Verlorenes wiederzufinden. Da Ex-Partner meist die Passwörter und Zugangsdaten vom Handy oder den Social-Media-Accounts kennen, können auch diese Daten missbräuchlich verwendet werden. Beim Stalking geht es immer um Macht und Kontrolle über das Opfer.

* Häusliche Gewalt, Bundeslagebild 2023, BKA

Schwer zu greifen: Zahlen & Fakten

Das Bundeskriminalamt (BKA) hat für das Jahr 2023 über 1.800 Stalkingfälle in Partnerschaften registriert, die mit dem Tatmittel Internet begangen wurden und nennt als Beispiele E-Mails und Chats. Hinzuzurechnen sind noch über 2.200 Fälle von Bedrohungen, die ebenfalls mit dem Tatmittel Internet verübt wurden. Die Grenzen zwischen analogem und digitalem Stalking lassen sich nur schwer ziehen, denn das Opfer wird auf allen möglichen Wegen drangsaliert. Die tatsächlichen Opferzahlen liegen nach Expertenmeinung deutlich höher. Fakt ist: Die Fälle von Cyberstalking nehmen zu.

Wenn man die Kontrolle verliert

Er war unter ihrem Fahrradsattel versteckt. Niemals wäre Verena Z.* auf die Idee gekommen, dass ihr Ex-Partner sie mit einem kleinen Bluetooth-Tracker ausspionierte und deshalb genau wusste, wann sie im Fitnessstudio trainierte. Mehrmals hatte er ihr nach dem Sportkurs aufgelauert und sie massiv bedrängt. Die 35-Jährige war extrem verängstigt und litt unter Panikattacken. Kurz nach ihrer Trennung hatte das Cyberstalking angefangen. Schon während der Beziehung hatte ihr Ex-Partner heimlich eine Spyware-App auf ihrem Smartphone installiert und sie kontrolliert. Rückhalt fand Verena Z. beim WEISSEN RING. Die Opferhelferin war nicht nur eine große emotionale Stütze für sie, sondern half auch bei der Suche nach einer neuen Wohnung. Seit Verena Z. den Bluetooth-Tracker gefunden hat, sind die Vorfälle weniger geworden.

* Name von der Redaktion geändert

Stalking macht krank

Das penetrante Belästigen, auch über das Internet, setzt den Betroffenen massiv zu. Es schränkt die Lebensqualität und den Alltag ein, beschneidet die Privatsphäre und führt zu Ohnmachtsgefühlen. Betroffene können nicht nur körperlich krank werden, sondern auch psychisch leiden und traumatisiert werden.

Tipp: Das eigene Handy, Passwörter und Accounts sind Privatangelegenheit. Achten Sie auch in einer Beziehung auf Ihre Privatsphäre. Die gleichen Passwörter zu benutzen oder diese untereinander zu teilen, ist kein Vertrauensbeweis.

Die häufigsten Strategien der Cyberstalker

- Heimliches Installieren von Stalkerware auf dem Smartphone oder Computer des Opfers, um Informationen zu sammeln und Betroffene zu überwachen. Diese Programme können Chat-Nachrichten, SMS und den Standort der Person an den Täter übermitteln.
- Ortung und Überwachung der Betroffenen durch z. B. Bluetooth-Tracker und auch durch ehemals gemeinsam benutzte Cloud-Dienste
- Warenbestellung im Namen der Betroffenen
- Nutzung von Social Media, um die Betroffenen bloßzustellen und zu denunzieren
- Permanente Kontaktaufnahme und Belästigung, z. B. auf dem Handy, per E-Mail und über Social Media
- Überwachung und Zugriff auf den Home-WLAN-Router sowie auf E-Mails durch Kenntnis der Passwörter
- Kontrolle der Social-Media-Kontakte, wenn die Zugangsdaten bekannt sind
- Identitätsdiebstahl, z. B. Hacken des Social-Media-Accounts und Posten von Nachrichten im Namen der betroffenen Person

Romance Scamming: große Gefühle vorgetäuscht und ausgenutzt

ROMANCE SCAMMING

Diese Online-Betrüger bzw. Heiratsschwindler 2.0 versprechen die große Liebe. Am Ende haben sie es nur auf das Geld abgesehen. Sowohl Frauen als auch Männer fallen dem Romance Scamming zum Opfer.

Das englische Wort romance bedeutet Romanze bzw. Liebesgeschichte und scamming betrügen. Es ist eine weitverbreitete Masche, um potenzielle Opfer im Internet auf Datingplattformen oder in sozialen Netzwerken zu umgarnen, sie in eine emotionale Abhängigkeit zu bringen und abzuzocken. Genaue Zahlen oder Statistiken, wie häufig diese Masche eingesetzt wird, sind nicht vorhanden. Doch die Dunkelziffer ist hoch. Die finanziellen Schäden der Betrogenen liegen im vier- bis fünfstelligen Bereich. Diese bleiben nicht nur mit einem leer geräumten Konto zurück, sondern sind zutiefst gekränkt und schämen sich, weil sie auf einen Online-Betrüger hereingefallen sind.

Das raffinierte Vorgehen der Scammer

Es fängt harmlos mit einer netten Kontaktanfrage auf Social Media an. Über eine gewisse Zeit wird der Kontakt intensiviert und eine innige Beziehung zum Opfer aufgebaut. Fast täglich wird über digitale Kanäle miteinander kommuniziert. Der Scammer erschleicht sich einen wichtigen Platz im Alltag und im Herzen des Betroffenen. Kurz bevor ein reales Treffen stattfinden soll, wird eine plötzliche Notsituation vorgetäuscht, für die dringend Geld benötigt wird. Das kann ein Unfall, ein Überfall, eine OP etc. sein. Die Geldsumme soll meist per Bargeldtransfer (z. B. mit Western Union oder MoneyGram) ins Ausland geschickt werden.

Sextortion: Erpressung mit sexuellen Aufnahmen

SEXTORTION

Diese Art der Erpressung geht unter die Gürtellinie, größtenteils Männer fallen ihr zum Opfer. Laut BSI gehört Sextortion zu den Top-3-Bedrohungen im Jahr 2023*. Der Begriff ist eine Wortkreation aus den englischen Begriffen sex und extortion, was für Erpressung steht. Es beginnt meist damit, dass der Betroffene eine fremde Person über die sozialen Medien wie Facebook, Snapchat oder Instagram kennenlernt. Man kommt locker ins Gespräch und das fremde Gegenüber signalisiert Interesse mit eindeutigen Sprüchen und reizvollen Fotos. Die Betrüger treiben es so weit, dass sie ihr Opfer dazu bringen, sich mit der eigenen Webcam nackt zu fotografieren, ebenfalls anzügliche Posen einzunehmen und sexuelle Handlungen an sich vorzunehmen. Am Ende steht die Drohung, die Aufnahmen im Netz zu veröffentlichen bzw. an Freunde und Familie zu schicken, wenn die Betroffenen nicht eine hohe Geldsumme zahlen. Meist wird erst eine kleinere dreistellige Summe gefordert. Wird diese bezahlt, fordern die Täter mehr.

* Lage der IT-Sicherheit in Deutschland 2023 im Überblick, BSI

Dickpics: eklig und strafbar

DICKPICS

Einfach unangenehm anzuschauen, für viele eklig und vor allem übergriffig. Die Rede ist von Penisbildern, die immer häufiger und unaufgefordert an Frauen und auch an Männer geschickt werden. Dickpics ist eine Wortkreation aus dem englischen Wort dick für Schwanz und pic als Abkürzung für picture und diese Art von Bildern zählen zu bildbasierter Gewalt. Ob als Direktnachricht oder im Chatverlauf: Die meisten Betroffenen fühlen sich von den männlichen Genitalbildern belästigt oder verängstigt. Auch Vulvabilder sind im Umlauf. Solche Aufnahmen zu verschicken ist strafbar und kann mit einer Freiheitsstrafe von bis zu einem Jahr oder einer Geldstrafe geahndet werden.

Hemmungslos schamlos

Der Name Claire23 hat sich fest in Matteo M.s* Kopf eingebrannt. Die junge Frau mit den dunklen lockigen Haaren hatte ihn auf einer Social-Media-Plattform angeschrieben und fand sein Lachen auf dem Profilbild so sympathisch. Der Student fühlte sich geschmeichelt. Schnell wurde die Kommunikation anzüglicher und sie begann, ihm Nacktaufnahmen von sich zu schicken. Nur kurz danach wechselten sie zur Videotelefonie und auch Matteo M. begann, sich nackt vor der Webkamera zu zeigen. Und phantasierte von mehr. Es wurde zu intim zwischen den beiden, um es hier zu beschreiben. Dann endete es abrupt. Claire23 schrieb: „2.000 Euro und die Aufnahme bleibt unter uns. Ansonsten schicke ich sie an deine Familie und Freunde.“ Matteo M. ist trotz übergroßer Scham nicht auf die Forderung eingegangen. Stattdessen hat er sich an das Opfer-Telefon des WEISSEN RINGS gewandt und Unterstützung erhalten.

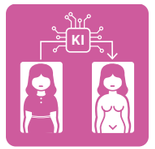
* Name von der Redaktion geändert

Rachepornos: eine nachträgliche Demütigung

RACHEPORNOS

Eigentlich waren sie nicht für die Augen der Öffentlichkeit gedacht. Die Rede ist von intimen Aufnahmen und auch Fotos, die in einer Partnerschaft entstanden sind. Rachepornos, auf Englisch revenge porn, werden vom frustrierten Ex-Partner bzw. der Ex-Partnerin nach einer Trennung im Internet auf speziellen Rachepornoseiten veröffentlicht und zeigen den Betroffenen nackt oder während sexueller Handlungen. Meist sind Frauen die Zur-Schau-Gestellten. Von der Veröffentlichung der Videos und Fotos wissen die Opfer entweder nichts oder es wird gegen ihren Willen gemacht. Als wäre es nicht schon schlimm genug: Oft werden unter den Videos der echte Name, persönliche Daten oder das Social-Media-Profil der betroffenen Frau mitveröffentlicht. Die Folgen für die Abgebildeten sind nachhaltig und können massive Auswirkungen auf das Ansehen, den Arbeitsplatz und das eigene Umfeld haben. Auch schädigt es die psychische Gesundheit.

Deepnudes: ungewollt zur Pornodarstellerin gemacht



DEEPNUDES

Die KI-Software dafür ist für jeden zugänglich und einfach zu bedienen. Ein einziges alltägliches Foto bzw. eine harmlose Videosequenz genügt und die spezialisierte KI kann Nacktfotos oder einen Porno daraus generieren. Rasend schnell verbreiten sich diese gefälschten Nacktaufnahmen im Netz, die fast täuschend echt aussehen und sich nur schwer wieder löschen lassen. Hauptbetroffene sind auch hier Frauen. Deepnudes leitet sich vom englischen Wort deepfakes ab und nude steht für nackt – gefälschte Nacktaufnahmen, KI-generiert.

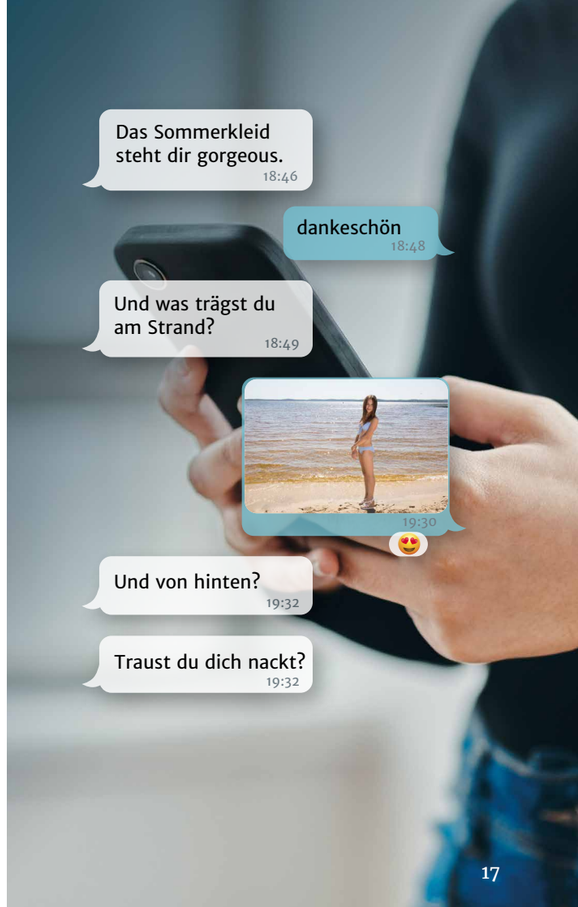
Cybergrooming: perverse Anmache mit Hintergedanken

CYBERGROOMING

Es passiert auf beliebten Social-Media-Plattformen wie TikTok oder Snapchat, auf YouTube oder Twitch, in Videospielen oder in Chats. Ältere Personen, meist Männer, geben sich als Gleichaltrige aus und versuchen, zu Kindern und Jugendlichen Kontakt aufzunehmen, um sie sexuell zu belästigen oder zu missbrauchen. Cybergrooming beschreibt die gezielte Anbahnung sexueller Kontakte mit Minderjährigen.

Erschreckend: Laut einer Umfrage* wurden bereits 16 % der Kinder und Jugendlichen in Deutschland von einer erwachsenen Person online kontaktiert und von dieser nach einem realen Treffen gefragt. Es beginnt harmlos mit einem netten Gespräch. Dann drängen sie darauf, Fotos oder Videos zu schicken und wollen sich mit ihrem jungen Opfer treffen.

* Umfrage von der Landesanstalt für Medien NRW 2024 zum Cybergrooming



Cybermobbing: Fertigmachen auf allen digitalen Kanälen

CYBERMOBBING

Nahezu unbegrenzte Möglichkeiten zum Mobben haben sich mit den digitalen Medien aufgetan. Betroffen sind laut einer Studie* größtenteils Kinder und Jugendliche zwischen 7 und 20 Jahren, die unter dem öffentlichen Belästigen, Bloßstellen, Beleidigen und Fertigmachen im Internet leiden. Cybermobbing geht mit klassischem Mobbing Hand in Hand – und schwappt zwischen offline und online hin und her.

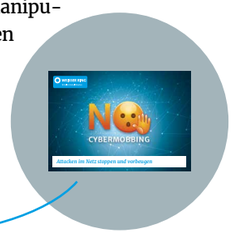
Die Zahl der Cybermobbingopfer ist alarmierend hoch. Über 18 % der Schülerinnen und Schüler aus der Studie haben angegeben, mindestens einmal im Internet attackiert worden zu sein. Das sind hochgerechnet auf Deutschland etwa 2 Millionen Betroffene. Zu den beliebtesten Lästerplattformen gehören WhatsApp, Instagram, TikTok und Snapchat**.

* Cyberlife Studie V 2024 ** JIM-Studie 2024

Die Künstliche Intelligenz mobbt mit

DEEPFAKES

Mithilfe von KI-basierten Computerprogrammen oder Face-Swap-Apps können ohne großen Aufwand gefälschte Videos, Bilder oder sogar Tonaufnahmen von Personen erzeugt werden. Diese manipulierten Aufnahmen werden als Deepfakes bezeichnet und werden gezielt zum Herabsetzen eines Mobbingopfers eingesetzt. Das ist pure bildbasierte digitale Gewalt. Sie können Dinge zeigen, die so nicht passiert sind. Sie verletzen, erniedrigen, verbreiten Unwahrheiten und können sogar Leben ruinieren. Dabei fällt es zunehmend schwerer, die Fälschungen zu erkennen, da die Technik immer besser und leichter zugänglich wird.



Für alle, die tiefer einsteigen möchten:
weisser-ring.de/mobbing

Hass & Hetze: vergiftetes Klima

HASS & HETZE

Hass ist wie ein unsichtbares Gift, das in zahlreichen digitalen Räumen anzutreffen ist - in den sozialen Medien, in Messengerdiensten, auf Videoportalen, in Chatrooms, Kommentarspalten, Foren, Blogs etc. Die abwertenden, menschenverachtenden Inhalte richten sich meist gegen vermeintlich Schwächere und Minderheiten, beispielsweise gegen Frauen, Homosexuelle und Migranten. Mithilfe von Sprache und Texten, Bildern und Videos werden andere Personen attackiert und abgewertet. Im schlimmsten Fall wird sogar zu Gewalt aufgerufen.

Mit Mut und Zivilcourage gegen den Hass

Die Mehrheit reagiert mit Schweigen auf die Hassattacken im Netz und klickt einfach weiter. Dadurch wird die Meinung der Wenigen lauter, was letztendlich die Hassvertreter bestärkt. Die wirksamsten Mittel sind: Zivilcourage zeigen und Hasskommentare melden und löschen lassen.

Für alle, die mehr erfahren wollen:
weisser-ring.de/hassundhetze

Desinformation & Deepfakes: Manipulation, Lügen und angebliche Experten

DESINFORMATION

Welcher Information im Netz kann man trauen? Was ist Propaganda? Und was sind Falschinformationen? Gerade Social-Media-Plattformen werden dazu benutzt, diese massenhaft zu verbreiten. Um die aktuelle Nachrichtenlage bzw. Informationen richtig einzuordnen, fehlt neben dem Wissen oft die Zeit für eine eigene Recherche. Daher: Seriöse Quellen nutzen, Quellen prüfen und Falsch- bzw. Fehlinformationen melden, sind wichtige Schritte gegen Desinformation. Auch sogenannte Faktenchecker wie z. B. *mimikama.org* oder *correctiv.org* helfen dabei, Informationen besser einzuordnen.

Online-Betrugsmaschen: grenzenlos kriminell

Die Zahlen der Polizei zeichnen ein eindeutiges Bild. Straftaten, die mit dem „Tatmittel Internet“ begangen wurden, steigen weiter an und lagen im Jahr 2022 bei über 398.000 Fällen*. Knapp ein Drittel davon machte Waren- und Warenkreditbetrug aus mit über 128.000 Fällen. Computerbetrug lag bei über 64.000 Fällen. Unter den Betrugsmaschen werden viele Delikte gebündelt wie Fake Shops, Onlinebetrug, Angriffe mit Schadsoftware, Phishing und Identitätsdiebstahl. Das BSI zählt die letzten beiden Delikte zu den Top-3-Bedrohungen** 2023.

* Polizeiliche Kriminalstatistik 2023 ** Lage der IT-Sicherheit in Deutschland 2023 im Überblick, BSI

Der Faktor Mensch: wenn Schwächen ausgenutzt werden

Beim Social Engineering geht es um Handlungen, die das Ziel haben, Menschen zu beeinflussen und zu manipulieren. Der Mensch, als ein Faktor in der Sicherheitskette, wird als Schwachstelle gesehen. Schamlos ausgenutzt werden menschliche Eigenschaften wie Hilfsbereitschaft, Höflichkeit, Anerkennung, Respekt vor Autoritätspersonen, Vertrauen und auch Leichtgläubigkeit. Da ein Großteil der menschlichen Handlungen unbewusst und intuitiv abläuft, wird nicht viel darüber nachgedacht, warum man so reagiert. Und genau hier setzen die Cyberkriminellen an. Sie täuschen z. B. vorsätzlich eine andere Identität vor, damit das Opfer sensible Daten von sich preisgibt. Das Opfer glaubt erst mal, dass z. B. ein echter Polizist anruft.

Mit vollem Kalkül

Die Täter gehen hochprofessionell vor. Sie springen auf aktuelle Themen auf und sind geschult darin, Menschen auszutricksen und ihre Ängste zu triggern (z. B. Angst vor Krieg, Angst vor hohen Energiepreisen, vor Ansteckung bei Corona). Auch nutzen sie alle neuen technischen Optionen und passen sich wie ein Chamäleon an neue Gegebenheiten an.

Phishing: dreister Datenklau

PHISHING

Über 93 % aller Internetnutzer haben Angst davor, Opfer von Internetkriminalität zu werden, so eine Umfrage*. Am häufigsten wurde die Sorge angegeben, dass das Smartphone oder der Computer von Schadsoftware wie Viren befallen wird. Mehr als die Hälfte, 55 %, fürchtet sich vor einem Diebstahl von Passwörtern. Das bringt uns direkt zum Thema Phishing, das zu den am meisten auftretenden Internetdelikten gehört. Phishing, eine englische Wortkreation aus password und fishing, bedeutet so viel wie Fischen nach Passwörtern. Mit dem Abfischen von sensiblen Informationen wie Bank- oder Adressdaten, TANs, PINs, Kreditkartennummern können Cyberkriminelle einen hohen finanziellen Schaden verursachen oder schlimmstenfalls sogar Identitätsdiebstahl begehen. Um ihre Opfer zu ködern, verschicken sie täuschend echt aussehende E-Mails bzw. Links von Websites im Namen von Banken, Versandhäusern und Unternehmen.

Im Jahr 2024 wurden laut BSI knapp die Hälfte** aller Phishing-E-Mails dazu verwendet, um Authentisierungsdaten von Banken und Sparkassen zu erbeuten. Neben dieser bekannten Masche gab es eine neue Entwicklung. Die Angreifer verschickten 52 % dieser Mails im Namen von bekannten Streamingdiensten. Ihr Ziel: an sensible Nutzerdaten der Accountinhaber wie etwa Kreditkartennummern zu kommen. Dabei spielen die Täter auf Zeit. Im Schnitt erfolgt erst nach fünf Tagen eine missbräuchliche Transaktion mit den Daten. Weitere Tricks: Druck machen, manipulieren und zum Handeln zwingen.

* Bitkom Research, Umfrage „Wodurch fühlen Sie sich im Internet bedroht?“, Zeitraum KW 37 bis 42 / 2023

** Lage der IT-Sicherheit in Deutschland 2024 im Überblick, BSI

Schmerzhaft: um Tausende Euro betrogen

„Bitte aktualisieren Sie Ihre Daten, sonst müssen wir Ihr Konto deaktivieren.“ Ugur O.* wurde nicht misstrauisch, als er diese Mail von seiner Bank las, die einen Link enthielt. Alles stimmte: Das Logo, die Farben und sogar der Bankname kamen in der Webadresse vor. Er klickte auf den Link und gab auf einer professionell gestalteten Website in einem Formular seine Kontonummer, seine PIN und noch weitere persönliche Daten ein. Ein großer Fehler, wie sich ein paar Tage später herausstellte. Unbekannte hatten mehrere Tausend Euro von seinem Konto abgebucht und mit seiner Bankverbindung zahlreiche Bestellungen getätigt.

* Name von der Redaktion geändert

Tipp: Nehmen Sie die E-Mail-Adresse des Absenders genau unter die Lupe. Sie verrät die Betrüger etwa durch Phantasienamen oder fehlerhafte Rechtschreibung.

Weitere Datenklau-Varianten:

Smishing: Hier geht es um den Betrug per SMS. Vor allem von angeblichen Paketdiensten oder Logistikdienstleistern werden diese SMS verschickt, die die Empfänger auf eine nachgeahmte, professionell aussehende Website weiterleiten. Gezielt abgefischt werden Adress- und Kontodaten oder Zugangsdaten zum Onlineshop.

Quishing: Statt einem Link führt ein QR-Code auf eine gefälschte Website, auf der das Opfer seine Daten eingeben soll.

Fake Shops: Guter Preis, professionell wirkender Onlineshop, aber meist nur mit Vorkasse. Fake Shops ziehen alle Register, um Verbraucher zu täuschen. Neben dem finanziellen Schaden erbeuten sie auch Konto- und Adressdaten.

Schadsoftware: Als Schadsoftware versteht man bspw. Viren, Trojaner oder Ransomware. Diese schleust sich unbemerkt ins System ein und löst schädliche Aktionen aus, wie Daten verschlüsseln, Passwörter oder sensible Daten ausspionieren, Inhalte oder Kontaktdaten verschicken etc.

Die Originaladressen lauten:
deutschepost.de und **dhl.de**

Identitätsdiebstahl: Das bin ich nicht

IDENTITÄTS-DIEBSTAHL

Wenn ein Fremder sich Zugang zu Ihren Online-Accounts verschafft hat, in Ihrem Namen beispielsweise Online-Überweisungen tätigt, E-Mails schreibt, Waren bestellt oder auf Social Media Beiträge postet, dann spricht man von Identitätsdiebstahl. Der Datenklau und -missbrauch ist hierbei so umfangreich, dass die ganze digitale Identität geklaut wird und man mit allen Daten zum Opfer wird. Oft geht dieser Identitätsdiebstahl Hand in Hand mit Phishing, bei dem wichtige Passwörter und Zugangsdaten im Vorfeld entwendet wurden. Ob Name, Adresse, Geburtstag, E-Mail-Adresse, Handynummer, Log-in-Daten und Kontodaten – auf diese persönlichen Daten haben es Cyberkriminelle besonders abgesehen.

Oft wird der Identitätsdiebstahl erst dann bemerkt, wenn der Schaden bereits entstanden ist. Neben finanziellen Verlusten kann es um Rufmord und die Schädigung von anderen Personen gehen. Auch können in Ihrem Namen Fakeprofile erstellt werden und neue Internetstraftaten begangen werden.

Messenger-Betrug: folgenschwere Nachrichten

MESSENGER-BETRUG

Sie gehören fest zum digitalen Alltag und fast jeder benutzt sie. Messengerdienste wie SMS, WhatsApp und Co erleichtern nicht nur die private Kommunikation, sondern sind auch bei Betrügern extrem beliebt. Wahllos verschicken die zum Teil in Banden organisierten Kriminellen ihre gefälschten Nachrichten an unzählige Handynummern, die beispielsweise von gekauften Listen aus dem Darknet stammen. Viele kleine Beträge lassen sich damit über die Masse erbeuten.
Laut der Polizei fordern die Täter meist Summen zwischen 1.000 und 3.000 Euro. Im Jahr 2022 ist dabei eine Schadenssumme von deutlich über 25 Millionen Euro entstanden, mehr als 50.000 Straftaten wurden registriert. Die Dunkelziffer liegt wahrscheinlich deutlich höher, denn aus Scham erstatten viele Opfer

keine Anzeige. Erschreckend: Die Täter kommunizieren so überzeugend, dass in nahezu jedem dritten Fall das eingeforderte Geld überwiesen wird.

Je nach Zielgruppe gibt es unterschiedliche Tricks. Der Sohn- bzw. Tochtertrick per WhatsApp funktioniert nach dem gleichen Muster wie der erfolgreiche Enkeltrick. Angeblich nahe Verwandte, wie z. B. das eigene Kind, geben vor, das Handy verloren zu haben. Ein paar belanglose Nachrichten später fordern sie dann einen Geldbetrag, weil sie in einer dringenden Notlage stecken. „Mein Rechner ist kaputtgegangen“ oder „Mein Onlinebanking ist gesperrt, könntest du mir bitte 1.000 Euro überweisen“ sind exemplarische Begründungen.

Tipp: Rufen Sie Ihr Kind bzw. den nahen Angehörigen einfach unter der alten Handynummer an, meist klärt sich der Betrug sofort auf. Überweisen Sie kein Geld.

Weitere Betrugsmaschen:

- **Gefälschte Anrufe** im Namen von Amazon, PayPal, Microsoft, der Polizei oder von Mitarbeitern internationaler Polizeibehörden wie Europol, FBI etc. Der Trick: Kriminelle täuschen überzeugend eine andere Identität vor und arbeiten sogar mit professionell klingenden Bandansagen und Weiterleitungen. Ziel ist es, ihr Opfer unter Druck zu setzen und zum schnellen Geldüberweisen zu bringen.

- **CEO-Fraud:** Der Täter gibt sich als vermeintlicher Vorgesetzter oder Chef aus und weist Mitarbeiter per E-Mail oder Telefon an, hohe Überweisungen zu veranlassen.

Sie haben es in der Hand: Lassen Sie digitale Gewalt nicht an sich ran

Wichtig: gute Passwörter
Es klingt so einfach: Wenn jeder Internetnutzer sichere Passwörter verwenden würde, dann könnten knapp 80 % der Straftaten im Internet verhindert werden. Die Realität sieht leider anders aus. Die Top 5 der am häufigsten benutzten Passwörter* lautete im Jahr 2022: password, 123456, 123456789, guest und qwerty.

* nordpass.com/de/most-common-passwords-list/

Um es den Kriminellen nicht so einfach zu machen, sollten Sie am besten eine Kombination aus Groß- und Kleinbuchstaben sowie Zahlen oder Sonderzeichen für ein sicheres Passwort benutzen. So wird es einmalig, lang und komplex. Denken Sie auch an Passworthygiene. Das heißt: Erneuern Sie Ihre Passwörter regelmäßig, also mindestens einmal im Jahr, schreiben Sie diese nicht auf und geben Sie diese nicht an Dritte weiter.

Ein Bodyguard fürs Internet: der Passwortmanager
Sehr empfehlenswert ist auch die Nutzung eines Passwortmanagers. Das ist ein spezielles Programm, das eigenständig oder browserbasiert erhältlich ist und Sie bei der Verwaltung sämtlicher komplexer Passwörter Ihrer Accounts und Postfächer unterstützt. Vorteil: Der Passwortmanager merkt sich alle Ihre unterschiedlichen Passwörter, kann Ihnen neue sichere Varianten vorschlagen und wird meist mit nur einem einzigen Hauptpasswort entschlüsselt.

Das sollten Sie nicht vergessen: Geben Sie auch Ihrem WLAN-Router ein neues und sicheres Passwort und tauschen Sie das anfangs zugewiesene einfach aus.

So bauen Sie sich ein sicheres Passwort:

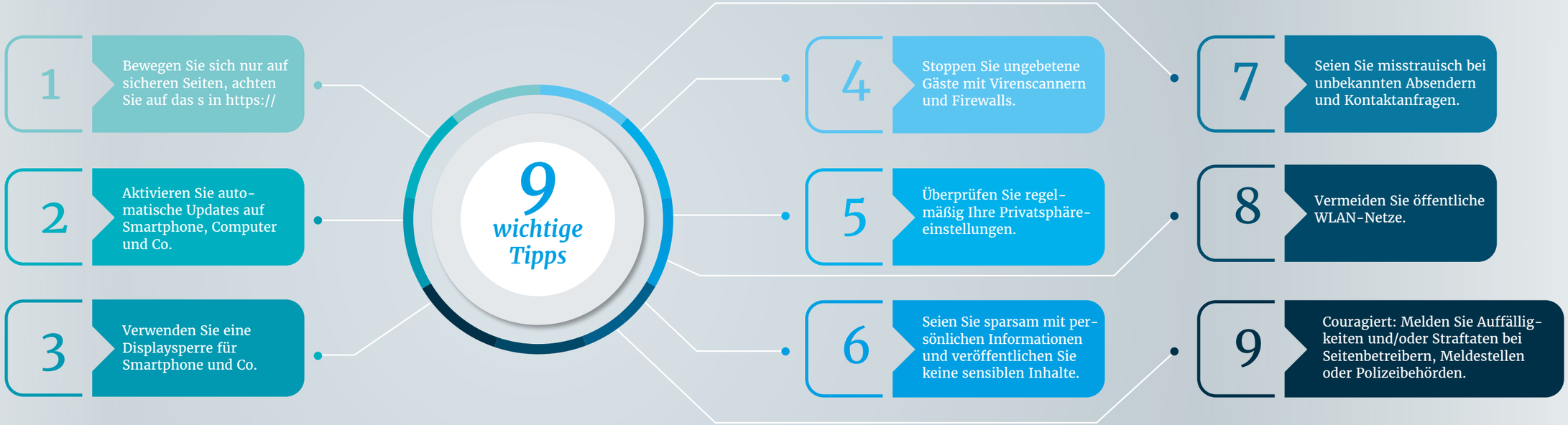
MeinblauerPapageitanzt7Stiefeldurch → MbPt7Sd
Für Instagram → InMbPt7Sdm

Benutzen Sie unterschiedliche Passwörter für verschiedene Anwendungen wie E-Mail-Programme, soziale Netzwerke, Messenger-Dienste und Onlinebanking.

Verwenden Sie, wenn möglich, die Zwei-Faktor-Authentisierung und melden Sie sich regelmäßig von der benutzten Anwendung ab, auch im Internetbrowser.

Neun Grundlagentipps, wie Sie sich sicher im Netz bewegen

Um sich im digitalen Raum vor potenziellen Gefahren zu schützen, müssen Sie selbst aktiv werden. Die gute Nachricht: Die Technik hilft Ihnen dabei. Mit dem Thema Sicherheit sind wir alle vertraut. Denken Sie nur an Ihre eigenen vier Wände, die Sie mit einem guten Türschloss sichern. Oder an Ihre Fenster, die Sie schließen, wenn Sie aus dem Haus gehen. Das sollte auch für Ihr digitales Leben gelten.



So schützen Sie sich vor digitaler Gewalt

CYBERSTALKING

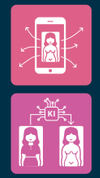
- Haben Sie Ihre mobilen Geräte im Blick. Geben Sie Ihr Smartphone nicht aus der Hand und nehmen Sie kein geschenktes Gerät an. Stalkerware kann in kürzester Zeit installiert werden oder ist bereits vorinstalliert.
- Auch wenn es schwerfällt: Richten Sie Ihr Smartphone am besten selbst ein. Im Internet gibt es auf den Herstellerseiten Erklärvideos dazu.
- Achten Sie auf sichere Passwörter, auch beim Router. Benutzen Sie sichere Bildschirmsperren für Ihre mobilen Geräte.

ROMANCE SCAMMING

- Seien Sie misstrauisch, wenn Sie jemand im Netz mit Komplimenten überhäuft.
- Nehmen Sie das Profil des Verehrers bzw. der Verehrerin im Netz genau unter die Lupe. Überprüfen Sie mit der umgekehrten Google-Bildersuche, ob geklaute Fotos verwendet wurden: *images.google.de*
- Fragen Sie gezielt nach. Bitten Sie um weitere persönliche Fotos und um Chats per Webcam.
- Teilen Sie mit der Bekanntschaft keine intimen Fotos und Videos, Sie könnten sich erpressbar machen.
- Lassen Sie sich nicht unter Druck setzen und überweisen Sie kein Geld.

VON DICKPICS ÜBER DEEPNUDES BIS SEXTORTION: BILDBASIERTE GEWALT

- Benutzen Sie ein Profilbild, auf dem Sie nur schwer zu erkennen sind, oder keines, wenn es geht. Auch ein geschlechtsneutraler Accountname oder ein Phantasiename ist hilfreich.
- Privatsphäreeinstellungen checken: Definieren Sie einen möglichst kleinen Personenkreis, der Sie über Social-Media-Plattformen oder Messenger-Dienste anschreiben darf.
- Lassen Sie sich nicht auf Chats mit Unbekannten ein und überprüfen Sie das Profil des „Betrügers“.
- Gehen Sie zur Polizei und erstatten Sie Anzeige, auch wenn es Ihnen unangenehm ist.



RACHEPORNOS & DEEPNUDES

- Achten Sie besonders auf den Schutz von sensiblen Daten, zu denen intime Aufnahmen gehören. Geben Sie solche Dateien nicht sorglos weiter.
- Seit 2021 ist es strafbar, Rachepornos zu verschicken und wird dem Straftatbestand Cyberstalking zugeordnet. Wehren Sie sich, z. B. mit Unterstützung einer Meldestelle, juristisch und erstatten Sie Anzeige.

CYBERGROOMING

- Aufklärung und eine gute Eltern-Kind-Beziehung sind das A und O! Sprechen Sie mit Ihrem Kind über diese Masche und wie perfide die Täter vorgehen.
- Keine Kontaktanfragen von Fremden annehmen, am besten Nicknames benutzen.
- Stärken Sie Ihr Kind darin, in unangenehmen Situationen Nein zu sagen und sich Hilfe zu holen.

So schützen Sie sich vor digitaler Gewalt

CYBERMOBBING UND HASS & HETZE

- Schützen Sie Ihre Privatsphäre. Machen Sie sich nicht angreifbar und geben Sie nichts Persönliches oder Intimes preis. Stellen Sie in den jeweiligen Einstellungen ein, wer was von Ihnen lesen darf und wer nicht.
- Halten Sie Ihren Freundeskreis auf Social-Media-Plattformen eher klein. Am besten: Kennen Sie die mit Ihnen vernetzten Menschen auch persönlich. Prüfen Sie jede neue Freundschaftsanfrage.
- Bei Vorfällen: Suchen Sie sich Verbündete und nutzen Sie Meldemöglichkeiten und -plattformen.

DEEPFAKES UND DESINFORMATION

- Checken Sie die Quellen und überprüfen Sie deren Seriosität. Nutzen Sie Faktenchecker.
- Auf welcher Plattform wurde es erstmals veröffentlicht. Ist diese seriös? Wer spricht darüber?
- Werden Sie misstrauisch, wenn Inhalte zu reißerisch oder zu polarisierend sind.

PHISHING

- Eins vorweg: Kein Bankinstitut, keine Behörde oder Finanzdienstleister fordert Sie per E-Mail auf, vertrauliche Zugangsdaten wie Passwörter über einen Link zu ändern.
- Überprüfen Sie den Absender der E-Mail ganz genau. Schauen Sie auf die E-Mail-Adresse und die Browserzeile des Links. Diese wird sichtbar, wenn Sie mit der Maus darüber gehen. Bei geringsten Abweichungen skeptisch werden. Am besten die Originalinternetadresse selbst eingeben.
- Achten Sie auf sprachliche Ungenauigkeiten, z. B. die persönliche Anrede fehlt. Hat der Text der gefälschten E-Mail Zeichen- oder Rechtschreibfehler?
- Klicken Sie niemals auf den mitgeschickten Link bzw. öffnen Sie keine Anhänge im .exe- oder .scr-Format. Diese können Schadsoftware enthalten.

IDENTITÄTSDIEBSTAHL

- Nutzen Sie für jeden Account ein eigenes sicheres Passwort, verwalten Sie diese am besten mit einem Passwortmanager.

MESSENGER-BETRUG

- Seien Sie skeptisch, wenn Sie angeschrieben werden. Lassen Sie nicht Ihr Vertrauen ausnutzen. Stellen Sie z. B. Fangfragen mit persönlichen Details, die ein Fremder nicht wissen kann.
- Verifizieren Sie die Aussage der Nachricht. Rufen Sie die alte Nummer an.
- Einfach unpersönlich: Überprüfen Sie, ob der Absender einen Namen hat und ob die Anrede persönlich ist. Oft steht dort nur „Hallo Mama“ und „Hallo Papa“.

100 % Rückhalt und schnelle Hilfe für Betroffene

Wir vom WEISSEN RING helfen Menschen, die unter digitaler Gewalt leiden und unterstützen sie, aus ihrer misslichen Lage herauszukommen. Materielle Verluste sind meistens nicht die schwerwiegendsten Folgen. Vielmehr leiden Opfer unter physischen, psychischen und sozialen Beeinträchtigungen, die tiefgehende Einschnitte verursachen. Betroffene zweifeln an sich selbst, empfinden Scham und erleiden einen massiven Vertrauensverlust gegenüber den Mitmenschen und der Gesellschaft.

- Wir helfen den Opfern ganz individuell – durch emotionale und finanzielle Unterstützung. Betroffene können sich an eine unserer knapp 400 Außenstellen wenden, an das Opfer-Telefon oder unsere Online-beratung.

- Wir leisten Beistand, hören zu und zeigen Auswege auf.

- Wir begleiten Sie zu Gerichts- und Behördenterminen, klären über die dortigen Abläufe auf und stehen an Ihrer Seite.

- Wir vermitteln auch Hilfen von anderen Anlauf- und Beratungsstellen und sind gut vernetzt mit Fachleuten wie Rechtsanwälten und Psychologen.

100 %
RÜCKHALT FÜR BETROFFENE

Kann man Internet lernen? Alles über mehr Medienkompetenz

Richtigerweise müsste es Mediennutzungskompetenz heißen, denn der digitale Raum und seine Medien werden von den Internet-Usern auf vielfältige Art und Weise genutzt. Um Gefahren zu erkennen, ist es wichtig, über mögliche Risiken aufgeklärt zu sein und gerade Kinder und Jugendliche bei der Internetnutzung zu begleiten.

Außerdem geht es hier um Kenntnisse, wie man seine Privatsphäre schützt, wie man mit persönlichen Daten verantwortungsvoll im Netz umgeht und welche technischen Einstellungen man nutzen kann. Wie wichtig sichere Passwörter sind und wie man diese erstellen kann, haben wir Ihnen auf Seite 27 vorgestellt.

Machen Sie Ihren Digitalführerschein

Wer wirklich sicher im Netz und in den verschiedenen digitalen Räumen unterwegs sein möchte, der kann unter *difue.de* einen Digitalführerschein machen, ein Projekt von Deutschland sicher im Netz (DsiN). Dieser Führerschein kann sowohl für den privaten als auch für den beruflichen Gebrauch abgelegt werden. Je nach Vorwissen gibt es drei Level mit jeweils sechs Themenbereichen. Bundesweit einheitlich und nach erfolgreichem Abschluss mit Zertifikat.

Die Verbraucherzentrale Rheinland-Pfalz bietet kostenlose Lernmodule an unter dem Titel „Smart Surfer: Fit im digitalen Alltag“. Zu finden unter der gleichnamigen Adresse: *smart-surfer.net*

Aktiv werden und sich wehren: Meldestellen im Netz

Digitale Gewalt muss niemand hinnehmen. Ein erster wichtiger Schritt ist, die Straftat zu melden. Dafür gibt es zahlreiche Meldestellen und Beratungsangebote.

Kinder- und jugendgefährdende Inhalte

- *jugendschutz.net*
  Kompetenzzentrum von Bund und Ländern für den Schutz von Kindern und Jugendlichen im Internet
- *internet-beschwerdestelle.de*
  Beschwerde bei jugendgefährdenden oder volksverhetzenden Inhalten im Netz – Projekt der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter (FSM) e. V. und eco – Verband der Internetwirtschaft e. V.

Anlaufstellen bei Online-Betrug und Diebstahl

- *bka.de*
  Die Onlinewachen der Landespolizei, hier können Online-Betrugsfälle oder Diebstahl (z. B. auf eBay Kleinanzeigen) gemeldet werden
- *verbraucherzentrale.de*
  Unter „Digitales“ findet man aktuelle Warnungen, viele Informationen, Sicherheitstipps, einen Phishingradar und einen Fake-Shop-Finder

Meldestellen für digitale Gewalt und Hass und Hetze

- *hateaid.org*
  Beratung und rechtliche Unterstützung bei digitaler Gewalt und Hass und Hetze plus Meldeformular für Onlineangriffe
- *hessengegenhetze.de*
  Die Meldestelle vom Hessischen Ministerium des Inneren und für Sport
- *meldestelle-respect.de*
  Jugendstiftung Baden-Württemberg im Demokratiezentrum
- *bayern-gegen-hass.de*
  Initiative der Bayerischen Staatsregierung

Kennen Sie Ihre Rechte und wehren Sie sich juristisch

Das Internet ist kein rechtsfreier Raum, auch hier gelten Regeln und Gesetze. Wenn es im World Wide Web wie im Straßenverkehr verbindliche Regeln für alle und z. B. Verkehrsschilder geben würde, wäre vieles einfacher. Aber: Rote Stoppschilder stehen auf den Datenautobahnen leider nicht. Dafür ziehen eine Reihe von Gesetzen rote Linien, die offline wie online gelten. Straftat bleibt Straftat, auch wenn sie im digitalen Raum begangen wird, und kann strafrechtlich und zivilrechtlich verfolgt werden. Onlinebeweise sichern ist deshalb das A und O, um erfolgreich gegen die Täter vorzugehen. Wie Sie rechtssichere Screenshots erstellen, erfahren Sie unter *hateaid.org/rechtssichere-screenshots/*

§ 130 StGB	# Volksverhetzung
§ 185 StGB	# Beleidigung
§ 186 StGB	# Üble Nachrede
§ 187 StGB	# Verleumdung
§ 201a StGB	# Unerlaubtes Veröffentlichen von Fotos
§ 238 StGB	# Nachstellung
§ 240 StGB	# Nötigung
§ 241 StGB	# Bedrohung
§ 253 StGB	# Erpressung

Cybergrooming:

§ 176 StGB	# Sex. Missbrauch von Kindern
§ 176a StGB	# Sex. Missbrauch ohne Körperkontakt
§ 176b StGB	# Vorbereitung eines sex. Missbrauchs

Wir alle füreinander

Auch die Zivilgesellschaft ist beim Thema digitale Gewalt gefragt. Neben mehr Zivilcourage kann jeder aktiv werden, Anzeige erstatten oder Inhalte melden. Das hilft zum einem der Polizei, die nicht die Ressourcen hat, alle digitalen Vergehen zu sichten und zu verfolgen. Zum anderen unterstützt es auch die Betroffenen selbst. Denn sie berichten, dass ihnen bei digitaler Gewalt am meisten geholfen hat, wenn andere Solidarität zeigen und die Ungerechtigkeit bzw. die Straftat gesehen wird.

Mehr WWWissen, weniger digitale Gewalt: unsere Seitenempfehlungen

bsi.bund.de/verbraucherinnen
Die offizielle Seite, wenn es um die digitale Sicherheit von Verbraucherinnen und Verbrauchern in Deutschland geht. Von aktuellen Warnmeldungen über zahlreiche Tipps für den digitalen Alltag bis hin zum Cybersicherheitsmonitor.

mobilsicher.de
Das Infoportal rund um das Handy. Großes Themenspektrum, nützliche App-Tests und einen App Store, der Apps listet, die nicht im Google Store erhältlich sind.

klicksafe.de
Fit fürs Internet und den digitalen Alltag. Dieses Informationsportal richtet sich an Eltern, Lehrkräfte und Multiplikatoren, die Kinder und Jugendliche dabei unterstützen, ihre Internetkompetenz auszubauen.

hateaid.org
Wer unter digitaler Gewalt, Angriffen oder Hass im Netz und deren Folgen leidet, erhält hier kompetente Beratung und rechtliche Unterstützung. Und zwar kostenlos. Betroffene können telefonisch, per Chat oder per E-Mail Kontakt aufnehmen.

silver-tipps.de
Digital sicher durchstarten: Alles, was man dazu braucht, findet man auf diesem Serviceportal. Es wurde eigens für ältere Onlinenutzer entwickelt und sorgt für mehr Klarheit im Umgang mit Internet, Smartphone und Co. Ein Highlight sind z. B. die kurzen Videos „Helga hilft“.

polizei-beratung.de
Zu den Gefahren im Internet gibt es auch auf der offiziellen Präventionsseite der Polizei umfangreiche Informationen und viele praktische und umsetzbare Tipps, wie man sich schützen kann. Plus: ein Sicherheitskompass.

Ob online oder offline: Jede Spende zählt

Auch beim Helfen brauchen wir alle Hilfe: Unterstützen Sie die Arbeit des WEISSEN RINGS mit einer Spende. Rund 3.000 ehrenamtliche Helferinnen und Helfer sind deutschlandweit für uns im Einsatz. Professionell kümmern sie sich z. B. um Opfer von digitaler Gewalt, leisten menschlichen Beistand und beraten. Neben der Opferhilfe engagieren wir uns außerdem im Bereich Präventions- und Aufklärungsarbeit, damit Gefahren frühzeitig erkannt und abgewehrt werden können. Das gilt für die reale Welt genauso wie für die digitale. Da sich unsere Arbeit aus Mitgliedsbeiträgen, Spenden, Nachlässen sowie Geldbußen finanziert, freuen wir uns über jeden Beitrag der uns beim Helfen hilft. Der WEISSE RING erhält keine staatlichen Mittel.

Jeder Betrag bewegt etwas

Mit **35 Euro** unterstützen Sie uns, einen Vortrag zum Thema „Wie man sich vor digitaler Gewalt schützen kann“ durchzuführen.

Mit **50 Euro** setzen Sie sich dafür ein, dass wir ein Präventionsprojekt vor Ort starten. Auch in Zusammenarbeit mit der Polizei.

Mit **75 Euro** helfen Sie uns, einen Infostand zu finanzieren, um auf das Thema digitale Gewalt aufmerksam zu machen.

Jetzt spenden: **spenden.weisser-ring.de**

Spendenkonto WEISSER RING
IBAN: DE42 5535 0010 0000 3434 34
BIC: MALADE51WOR
Rheinhessen Sparkasse

WEISSER RING e. V.
Bundesgeschäftsstelle • Weberstraße 16 • 55130 Mainz • Germany
info@weisser-ring.de • www.weisser-ring.de
www.facebook.com/weisserring
www.youtube.com/weisserringev

Seit 1976 an der Seite der Opfer

Bundesweit für Sie vor Ort, am Opfer-Telefon unter 116 006
und in der Onlineberatung auf www.weisser-ring.de

2. Auflage Dezember 2024
Artikelnummer: 1134 • Auflagenhöhe: 25.000

Bildnachweise:
Seite 1 (*istockphoto/BongkarnThanyakij*), Seite 3 (*istockphoto/VioletaStoimenova*),
Seite 8, 18, 32 Icon Deepfakes (*istockphoto/anttohoho*), Seite 11 (*istockphoto/Paolo Cordoni*),
Seite 12 (*istockphoto/Zbynek Pospisil*), Seite 13 (*istockphoto/Zozgurdonmaz*), Seite 15 (*istockphoto/Paolo Cordoni*),
Seite 17 (*istockphoto/Delmaine Donson, OceanProd*), Seite 20 (*istockphoto/xijian*), Seite 21 (*istockphoto/napong rattanaraktiya*),
Seite 22 (*istockphoto/Prostock-Studio*), Seite 23 (*istockphoto/Daria Kashurina*), Seite 25 (*istockphoto/Liubomyr Vorona*),
Seite 27 (*istockphoto/Thapana Onphalai*), Seite 35 (*Deutschland sicher im Netz e. V.*)

Die in dieser Broschüre geschilderten Vorfälle beruhen auf ähnlichen Begebenheiten.
Zum Schutz aller Beteiligten arbeiten wir mit fiktiven Namen.

Aus Gründen der besseren Lesbarkeit verzichten wir auf geschlechtsbezogene Formulierungen und verwenden nur die männliche Form, z. B. Täter. Wertfrei sind damit Frauen und Männer gemeint.