Deutschland sicher im Netz

DSIN-RATGEBERREIHE
AUSGABE „DIGITALE GEWALT“



DIGITALE GEWALT

ERKENNEN UND HANDELN

Digitale Gewalt geht uns alle an – erfahre hier, wie du sie erkennst und wie du gegen sie aktiv werden kannst.

TELEKOM KAMPAGNE GEMEINSAM #GEGENHASSIMNETZ



Kampagnenspot „Was sich liebt …“ ansehen

Trigger-Warnung: Der Spot zeigt Szenen digitaler Gewalt.

Kampagnenspot ansehen: youtube.com/watch?v=-zqZ7EXvGX4

Dieser Ratgeber ist im Rahmen der Telekom-Kampagne „Was sich liebt…“ und ihrer Initiative **Gemeinsam #GegenHassImNetz** entstanden.

EINSTIEG

Digitale Gewalt erkennen und handeln

Das Internet verbindet uns. Wir tauschen uns aus, finden Gleichgesinnte, spielen gemeinsam online und mischen uns in gesellschaftliche Debatten ein. So bietet das Netz vielen Menschen die Chance, mitzureden und Gesellschaft mitzugestalten. Damit das so bleibt, muss es ein sicherer Ort für alle sein.

Leider nutzen manche Menschen die Freiheiten des Internets aus, um anderen zu schaden. Sie beleidigen, bedrohen, überwachen oder stellen andere bloß. Das passiert im Klassenchat genauso wie beim Gaming, im Teamchat auf der Arbeit oder unter einem ganz normalen Social-Media-Post. Digitale Gewalt kann also uns alle treffen.

Egal, ob du selbst betroffen bist, dir Sorgen um jemanden machst oder einfach mehr wissen möchtest: Dieser DsiN-Ratgeber zeigt dir, welche Formen digitaler Gewalt es gibt, wie du sie erkennst, dich davor schützt und was du dagegen tun kannst.

INHALT

Was beschäftigt dich?

KAPITEL 1
Was ist digitale Gewalt und wer ist betroffen? →

KAPITEL 2
„Ich werde online beschimpft oder bedroht.“
Angriffe durch Worte →

KAPITEL 3
„Ich habe das Gefühl, dass jemand mein Handy überwacht.“
Kontrolle und Überwachung →

KAPITEL 4
„Fremde kennen meine Adresse oder meine Telefonnummer.“
Angriffe auf Privatsphäre und Identität →

KAPITEL 5
„Jemand droht, echte oder gefälschte Nacktbilder von mir zu veröffentlichen.“
Missbrauch von Bildern →

KAPITEL 6
Technik-Check →

KAPITEL 7
Was tun im Ernstfall? →

KAPITEL 8
Hilfe finden →

KAPITEL 1

Was ist … **digitale Gewalt?**

- … „bezeichnet Gewaltformen, die über das Internet oder digitale Technologien ausgeübt werden – z. B. durch Belästigung, Überwachung, Drohungen oder das Veröffentlichen intimer Inhalte.“ (UN Women Deutschland)
- … kann über technische Geräte wie Smartphones oder Ortungs-Tracker, über Programme wie Überwachungs-Apps und über soziale Medien oder Online-Plattformen ausgeübt werden.
- … verfolgt oft ein klares Ziel. Betroffene sollen eingeschüchtert, bloßgestellt, ausgegrenzt oder zu etwas gezwungen werden, das sie nicht wollen.
- … wird dadurch erleichtert, dass Täter:innen online anonym bleiben können und viele Kanäle zur Verfügung haben.
- … kann jede Person treffen. Oft werden Menschen aber angegriffen, weil sie einer bestimmten Gruppe zugeordnet werden oder eine bestimmte gesellschaftliche Rolle haben.
- … findet nicht nur zwischen Fremden statt, sondern häufig auch im direkten Umfeld.
- … ist niemals die Schuld der Betroffenen.

Online und offline

Digitale und analoge Gewalt hängen zusammen

Digitale Gewalt kann bestehende Gewalt im Alltag verstärken, sie kann aber auch aus dem Netz in die analoge Welt übergreifen. Besonders deutlich wird das im direkten Umfeld. Wer in einer Beziehung kontrolliert oder bedroht wird, erlebt das häufig auch über das Handy, etwa durch ständige Nachrichten, heimliche Ortung oder Druck über soziale Medien. Auch nach einer Trennung nutzen manche (Ex-)Partner:innen digitale Wege, um weiter Kontrolle auszuüben. Frauen sind davon besonders häufig betroffen.

Umgekehrt bleibt auch Hass im Netz nicht immer online. Ein Shitstorm in den sozialen Medien kann dazu führen, dass Betroffene im Alltag, am Arbeitsplatz oder sogar zu Hause bedroht oder angegriffen werden. Das gilt besonders dann, wenn private Daten wie die Wohnadresse veröffentlicht wurden.

Online und offline gehen also ineinander über. Und weil Smartphone und Co. immer dabei sind, gibt es weder Feierabend noch einen sicheren Rückzugsort, an dem digitale Gewalt einfach endet.

Digitale Gewalt kann alle treffen

15 %

der Internetnutzer:innen waren schon selbst von Hass im Netz betroffen.

Quelle: „Lauter Hass, leiser Rückzug“

76 %

der erwachsenen Gamer:innen wurden beim Online-Spielen schon belästigt.

Quelle: ADL, „Hate is No Game 2023“ (USA)

35 %

der Schüler:innen in Klassenchats haben dort schon Belastendes gesehen, meist Beleidigungen.

Quelle: WDR / infratest dimap

60 %

der Internetnutzer:innen haben schon mitbekommen, wie Politiker:innen im Netz angegriffen oder herabgewürdigt werden. Damit ist die Politik die am häufigsten betroffene Gruppe.

Quelle: „Lauter Hass, leiser Rückzug“

Frauen sind häufiger und schwerer betroffen

Jede 5. Frau

hat in den letzten fünf Jahren digitale Gewalt erlebt und jeder 7. Mann.

Quelle: BKA, LeSuBiA

45,9 %

der Frauen haben online schon unerwünschte sexualisierte Nachrichten bekommen.

Quelle: Deutscher Frauenrat, 2026

Fast jede 3.

junge Frau hat erlebt, dass intime Bilder von ihr ohne Einwilligung verbreitet wurden.

Quelle: Deutscher Frauenrat, 2026

21 %

der jungen Frauen waren schon selbst Ziel sexualisierter Deepfakes.

Quelle: Deutscher Frauenrat, 2026

73 %

der Frauen mit Gewalterfahrung im digitalen Raum ändern danach ihr Online-Verhalten.

Quelle: Deutscher Frauenrat, 2026

Mehr als 2×

so viele Frauen wie 2020 wurden 2024 von (Ex-)Partner:innen über das Internet bedroht, gestalkt oder genötigt. Die Dunkelziffer ist deutlich höher.

Quelle: BKA, Lagebild Häusliche Gewalt 2024, S. 34

KAPITEL 2

Angriffe durch Worte

„Ich werde online beschimpft oder bedroht.“



Was ist … **Hatespeech?**

- … bezeichnet abwertende oder feindliche Aussagen, die Menschen aufgrund ihrer Zugehörigkeit zu einer bestimmten Gruppe herabsetzen.
- … greift Menschen zum Beispiel aufgrund ihres Geschlechts, ihrer Herkunft, Hautfarbe, Religion, sexuellen Orientierung, geschlechtlichen Identität, einer Behinderung oder ihres Alters an.
- … trifft Frauen oft in sexualisierter Form, etwa durch Kommentare über Körper und Aussehen oder durch Vergewaltigungsdrohungen.
- … soll Menschen einschüchtern und ausgrenzen und verletzt ihre Würde und ihre Rechte.
- … kann strafbar sein, etwa als Beleidigung, Bedrohung oder Volksverhetzung. Plattformen müssen gemeldete rechtswidrige Inhalte prüfen und entfernen.

Was ist … **Cybermobbing?**

- … bezeichnet wiederholte Beleidigungen, Bedrohungen, Bloßstellungen oder gezielte Ausgrenzung einer Person über Messenger, soziale Netzwerke, Gaming-Plattformen oder Gruppenchats in Schule und Job.
- … richtet sich gezielt gegen eine bestimmte Person, kann sich aber mit Hatespeech überschneiden, etwa wenn das Mobbing rassistisch oder sexistisch ist.
- … geht oft von Menschen aus dem eigenen Umfeld aus, etwa aus Schule, Arbeit oder Freundeskreis. Mitlesende können die Angriffe durch Liken oder Teilen noch verstärken.

DsiN-Tipps

Reagieren und melden

- **Beweise sichern:** Sichere Inhalte als Erstes, auch wenn du nicht sicher bist, ob sie strafbar sind. Kommentare und Posts können schnell verändert oder gelöscht werden. Wie du Beweise rechtssicher festhältst, erfährst du hier. → **Was tun im Ernstfall?**
- **Auf der Plattform melden:** Wähle beim Melden die Option „als rechtswidrig melden“ oder ähnlich. Nur dann muss die Plattform deine Meldung nach dem Digital Services Act prüfen und dir mitteilen, wie sie entschieden hat.
- **Meldestellen nutzen:** Melde den Inhalt zusätzlich bei einer Meldestelle. Dort hilft man dir auch einzuschätzen, ob er strafbar ist. → **Meldestellen**
- **Hass keinen Raum geben:** Blockiere Accounts und lösche oder verberge Hasskommentare unter deinen Beiträgen, nachdem du Beweise gesichert hast.

GUT ZU WISSEN

Was nicht strafbar ist, kann trotzdem verletzen

Nicht jeder Angriff im Netz ist strafbar, manche Kommentare sind sogar bewusst knapp unter dieser Grenze formuliert. Verletzend sind sie trotzdem, vor allem weil sie oft öffentlich stehen bleiben und sich schnell verbreiten. Wie sehr das belastet, zeigt eine bundesweite Studie: Zwei Drittel der Menschen, die persönlich mit Hasskommentaren angegriffen wurden, berichten von psychischen Folgen wie Stress, Angst, einem angeschlagenen Selbstbild oder depressiven Symptomen. Quelle: IDZ Jena, „#Hass im Netz“, 2019

Digitale Gewalt hinterlässt echte Spuren, deshalb sind deine Gefühle berechtigt und du musst damit nicht allein bleiben. Beratungsstellen unterstützen dich, auch wenn keine Straftat vorliegt. → **Hilfe finden**

Was kann ich tun?

Gegen Hass im Netz kannst du etwas tun, selbst wenn du nicht direkt betroffen bist. Wichtig ist nur, dass du dich dabei nicht selbst gefährdest.

Gegenrede

Mit Gegenrede (engl. Counterspeech) widersprichst du Hasskommentaren öffentlich und zeigst, dass Hass nicht die Mehrheitsmeinung ist. Laut einer Studie wirkt es am besten, Mitgefühl für die Angegriffenen zu wecken, etwa mit **„Für viele Menschen ist es sehr verletzend, so etwas zu lesen."** Wer so angesprochen wurde, schrieb danach rund ein Drittel weniger Hasskommentare. Quelle: ETH Zürich, Hangartner u. a., 2021

Wenn du nicht weißt, wie du antworten sollst, hilft dir ModSupport, ein kostenloses KI-Tool der Amadeu Antonio Stiftung, mit konkreten Vorschlägen für den Umgang mit Hass in Kommentarspalten.

Digitale Zivilcourage

Digitale Zivilcourage heißt, dich schützend vor Betroffene zu stellen. Dabei geht es vor allem darum, die angegriffene Person zu stärken und andere Mitlesende zu mobilisieren. Schon ein kurzer Kommentar wie **„Ich stehe hinter dir"** zeigt der Person, dass sie nicht allein ist, und ermutigt andere, sich anzuschließen. Wie das konkret geht, kannst du bei LOVE-Storm lernen und üben.

Deine Sicherheit geht vor

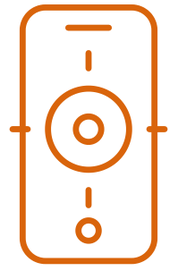
Deine eigene Sicherheit geht dabei immer vor. Wenn eine Diskussion eskaliert oder du selbst zur Zielscheibe wirst, zieh dich zurück, sichere Beweise und melde die Inhalte.

Bei Trollen und Bots lohnt sich eine Diskussion meist nicht, Melden reicht dann völlig.

KAPITEL 3

Kontrolle und Überwachung

„Ich habe das Gefühl, dass jemand mein Handy überwacht.“



Was ist … **Cyberstalking?**

… bezeichnet das wiederholte und hartnäckige Verfolgen, Belästigen oder Überwachen einer Person mit digitalen Mitteln (auch Onlinestalking).

… wird auf ganz unterschiedliche Weise begangen. Häufig genutzt werden zum Beispiel Informationen aus sozialen Netzwerken, Fake-Profile zur Kontaktaufnahme, heimliche Ortung oder Spionage-Apps auf dem Smartphone.

… geht häufig von (Ex-)Partner:innen aus und dreht sich um Macht und Kontrolle.

… trifft vor allem Frauen.

… ist in Deutschland als Nachstellung strafbar.

Was ist … **Stalkerware?**

… bezeichnet Apps oder Programme, die heimlich auf einem Gerät installiert werden und unbemerkt im Hintergrund laufen.

… kann nahezu alles überwachen, von Nachrichten, Anrufen und Fotos über den Browserverlauf bis zum Standort. Manche Programme greifen sogar auf Kamera oder Mikrofon zu.

… ist im Internet leicht zu kaufen und vor allem auf Android-Smartphones schnell installiert. Dafür reicht meist schon ein kurzer Zugriff auf das Gerät, etwa durch (Ex-)Partner:innen.

… muss nicht immer eine spezielle Spionage-App sein. Auch ganz normale Apps, etwa zum Wiederfinden eines verlorenen Handys, lassen sich zum Ausspionieren missbrauchen.

… ist strafbar, wenn sie ohne Zustimmung installiert wird. Davon zu unterscheiden sind Kinderschutz-Apps, die offen und im Einvernehmen genutzt werden.

DsiN-Tipps

Überwachung erkennen und beenden

- **Auf Anzeichen achten:** Ein Akku, der sich auffällig schnell leert, hoher Datenverbrauch, unbekannte Apps oder eine Person, die mehr über dich weiß, als sie eigentlich kann, können Hinweise auf Stalkerware sein.
- **Nicht vorschnell löschen:** Wird Stalkerware entfernt, bemerkt die überwachende Person das oft, und wichtige Beweise gehen verloren. Hol dir zuerst Beratung und nutze für die Kommunikation ein anderes Gerät. → **Hilfe finden**
- **Gerät prüfen:** Im Technik-Check zeigen wir dir Schritt für Schritt, wie du dein Smartphone und deine Konten überprüfst und absicherst. → **Technik-Check**

ACHTUNG

Ortungs-Tracker wie AirTags erkennen

Kleine Bluetooth-Tracker wie AirTags lassen sich leicht in Taschen, Jacken oder im Auto verstecken, um jemanden zu verfolgen. Um sie aufzuspüren, haben iPhone und Android eingebaute Funktionen, die dich entweder automatisch warnen oder die du über die Suche in den Einstellungen findest. Außerdem kannst du die kostenlose Anti-Tracking-App AirGuard nutzen, die dich warnt, wenn dir ein Tracker folgt.

Falls dein Handy womöglich selbst überwacht wird, bitte am besten eine Vertrauensperson, mit ihrem Gerät gemeinsam mit dir zu suchen. Findest du einen Tracker, dokumentiere den Fund und hol dir Beratung oder informiere die Polizei, bevor du ihn entfernst.

GUT ZU WISSEN

Digitale Partnerschaftsgewalt

Geteilte Passwörter oder Standortfreigaben wirken in Beziehungen oft harmlos, können aber zur digitalen Kontrolle genutzt werden, besonders nach einer Trennung. Fachleute sprechen dann von digitaler Partnerschaftsgewalt, wenn Partner:innen oder Ex-Partner:innen digitale Mittel nutzen, um zu überwachen, unter Druck zu setzen oder einzuschüchtern. Freigaben kannst du allerdings jederzeit beenden. → **Technik-Check**

KAPITEL 4

Angriffe auf Privatsphäre und Identität

„Fremde kennen meine Adresse oder meine Telefonnummer.“



Was ist … **Doxing?**

- … bezeichnet das Sammeln und Veröffentlichen persönlicher Daten im Netz, etwa Wohnadresse, Telefonnummer, Ausweisscans oder Bankdaten.
- … trifft häufig Menschen, die öffentlich sichtbar sind, etwa Politiker:innen, Journalist:innen oder Aktivist:innen, kann aber jede Person treffen.
- … passiert meist über soziale Netzwerke oder anonyme Upload-Seiten.
- … kann dazu führen, dass Betroffene auch offline bedroht werden, zum Beispiel vor der eigenen Haustür.
- … erleichtert Identitätsdiebstahl.

Was ist … **Identitätsdiebstahl?**

- … bezeichnet den Missbrauch persönlicher Daten wie Name, Fotos, Adresse oder Zugangsdaten, um sich als eine andere Person auszugeben.
- … zeigt sich oft in Fake-Profilen, über die in deinem Namen Nachrichten verschickt, Inhalte gepostet oder andere Menschen kontaktiert werden.
- … wird gezielt eingesetzt, um Betroffene bloßzustellen, ihrem Ruf zu schaden, sie zu bedrohen oder zu erpressen.
- … kann auch dazu dienen, in fremdem Namen Waren zu bestellen.
- … wird durch schlecht gesicherte Konten erleichtert, aber auch durch Daten, die bereits im Netz kursieren, etwa nach Doxing.
- … bleibt oft lange unbemerkt, bis Bekannte auf seltsame Nachrichten hinweisen oder unerwartete Rechnungen eintreffen.

DsiN-Tipps

Eigene Daten finden und schützen

- **Eigene Daten finden:** Such regelmäßig nach deinem Namen und deiner Adresse. Mit einer umgekehrten Bildersuche findest du heraus, wo deine Fotos im Netz auftauchen.
- **Daten entfernen lassen:** Nach der Datenschutzgrundverordnung hast du das Recht, Webseitenbetreiber um die Löschung deiner persönlichen Daten zu bitten. Bei Suchmaschinen wie Google kannst du außerdem über ein Formular beantragen, dass entsprechende Treffer entfernt werden.
- **Fake-Profile melden:** Sichere Beweise und melde das Profil bei der Plattform, meist über die Option „Identitätsdiebstahl“ oder ähnlich. Informiere außerdem Freund:innen und Familie, damit sie nicht auf Nachrichten in deinem Namen reagieren.
- **Konten absichern:** Prüf mit dem Identity Leak Checker des Hasso-Plattner-Instituts, ob deine Zugangsdaten bei einem Datenleck aufgetaucht sind. Mit starken Passwörtern und Zwei-Faktor-Authentifizierung erschwerst du, dass jemand deine Konten übernimmt. → **Technik-Check**

GUT ZU WISSEN

Auskunftssperre im Melderegister

In Deutschland lässt sich deine Privatadresse in vielen Fällen über das Melderegister erfragen. Wurdest du bereits bedroht oder hast digitale Gewalt erlebt, kannst du bei deiner Meldebehörde eine Auskunftssperre beantragen, damit deine Adresse nicht mehr einfach herausgegeben wird.

Der Antrag ist formlos schriftlich oder persönlich möglich, wobei du begründen solltest, warum dir durch die Auskunft eine Gefahr droht. Die Sperre gilt in der Regel zwei Jahre und kann danach verlängert werden. Da das Verfahren nicht immer einfach ist, kann es sich lohnen, eine Beratungsstelle um Unterstützung zu bitten. → **Hilfe finden**

KAPITEL 5

Missbrauch von Bildern

„Jemand droht, echte oder gefälschte Nacktbilder von mir zu veröffentlichen.“



Was ist … **bildbasierte Gewalt?**

- … bezeichnet das Aufnehmen, Verbreiten oder Androhen der Verbreitung intimer Fotos oder Videos ohne Zustimmung der abgebildeten Person.
- … umfasst zum Beispiel heimliche Aufnahmen, das Weiterleiten privater Nacktbilder an Freund:innen, Familie oder ins Netz und das ungefragte Zusenden sexueller Bilder, etwa sogenannter Dickpics.
- … kann auch mit künstlich erzeugten Bildern passieren, die echt wirken.
- … trifft besonders häufig Frauen, Jugendliche und junge Erwachsene und findet oft in (Ex-)Partnerschaften statt, wo Täter:innen damit Kontrolle ausüben wollen.
- … ist in vielen Fällen strafbar, zum Beispiel wenn Bilder ohne Zustimmung veröffentlicht werden.

Was ist … **Sextortion?**

- … bezeichnet sexuelle Erpressung mit intimen Bildern oder Videos und setzt sich aus den englischen Wörtern „sex“ und „extortion“ (Erpressung) zusammen.
- … beginnt oft mit einer scheinbar netten Bekanntschaft über soziale Netzwerke oder Dating-Apps, die Interesse signalisiert und dann um Nacktbilder oder sexuelle Handlungen im Videochat bittet.
- … endet meist mit der Drohung, die Aufnahmen an Freund:innen und Familie zu schicken oder im Netz zu veröffentlichen, wenn kein Geld gezahlt wird. Wer zahlt, bekommt oft weitere Forderungen.
- … kommt außerdem als massenhaft verschickte Spam-Mail vor, in der behauptet wird, es gebe Sexvideos von dir.
- … trifft überwiegend Männer, aber auch Frauen.

DsiN-Tipps

Bilder stoppen, Erpressung abwehren

- **Nicht zahlen:** Geh nicht auf Forderungen ein und brich den Kontakt ab, denn wer einmal zahlt, wird meist weiter erpresst.
- **Beweise sichern:** Sichere Chatverläufe, Profile und Forderungen, bevor du den Kontakt blockierst, und erstatte Anzeige bei der Polizei. → **Was tun im Ernstfall?**
- **Verbreitung verhindern:** Mit kostenlosen Diensten wie StopNCII oder Take It Down kannst du intime Bilder sperren lassen, ohne sie hochladen zu müssen. Auf deinem Gerät wird nur ein digitaler Fingerabdruck erstellt, mit dem teilnehmende Plattformen die Bilder erkennen und blockieren.
- **Dickpics anzeigen:** Ungefragt zugeschickte Nacktbilder sind strafbar. Mit dem kostenlosen Tool Dickstinction bereitest du in wenigen Schritten eine Anzeige vor, die du anschließend bei der Online-Wache hochladen oder bei der Polizei abgeben kannst.
- **Hilfe holen:** Du bist nicht schuld, wenn jemand deine Bilder missbraucht. Beratungsstellen unterstützen dich vertraulich.
  → **Hilfe finden**

NEUE GEFAHR

Deepfakes

Deepfakes sind Bilder, Videos oder Tonaufnahmen, die mithilfe von künstlicher Intelligenz erstellt oder verändert werden und täuschend echt wirken. Häufig werden sie genutzt, um sexualisierte Darstellungen realer Personen zu erzeugen, wovon vor allem Frauen betroffen sind.

Einen eigenen Straftatbestand gibt es dafür bisher nicht. Wer gefälschte Inhalte verbreitet, kann sich aber schon heute strafbar machen, etwa wegen Verletzung des Rechts am eigenen Bild. Die Bundesregierung hat im Oktober 2026 einen Gesetzentwurf auf den Weg gebracht, der sexualisierte Deepfakes ausdrücklich unter Strafe stellen soll.

KAPITEL 6

Technik-Check: Geräte und Konten absichern

ACHTUNG

Erst sichern, dann handeln

Wenn du vermutest, dass dein Handy oder deine Konten überwacht werden, lösch nichts vorschnell und setz dein Gerät nicht einfach zurück, denn die überwachende Person kann das bemerken und wichtige Beweise gehen verloren. Nutze für die Suche nach Hilfe und zum Ändern von Passwörtern möglichst ein anderes, sicheres Gerät und hol dir Unterstützung bei einer Beratungsstelle. → **Hilfe finden**

Ob jemand dein Handy überwacht, deine Konten nutzt oder über Freigaben mitliest, lässt sich oft mit wenigen Handgriffen überprüfen. Die folgenden Checklisten helfen dir dabei, Schritt für Schritt herauszufinden, wo du nachschauen solltest und wie du dich schützen kannst.

Stalkerware erkennen

- [ ] Schau in den Einstellungen nach, welche Apps besonders viel Akku oder Datenvolumen verbrauchen, und prüfe, ob darunter Apps sind, die du eigentlich gar nicht nutzt.
- [ ] Achte darauf, ob sich dein Gerät von selbst ein- und ausschaltet oder sich Einstellungen verändert haben.
- [ ] Geh deine installierten Apps durch und halte Ausschau nach solchen mit uneingeschränkten Rechten, etwa für Standort, Mikrofon oder Kamera.
- [ ] Führe einen Sicherheits-Scan mit einer zuverlässigen Sicherheitssoftware durch.

Angemeldete Geräte prüfen

- [ ] Öffne in deinem Google-Konto oder deiner Apple-ID die Liste der verbundenen Geräte und entferne alle, die du nicht kennst oder nicht mehr nutzt.
- [ ] Schau bei WhatsApp und anderen Messengern unter „Verknüpfte Geräte“ nach, ob deine Chats noch auf einem anderen Gerät oder im Browser geöffnet sind.
- [ ] Kontrolliere in deinen sozialen Netzwerken die aktiven Sitzungen und melde fremde Geräte ab.
- [ ] Wirf einen Blick in die Einstellungen deines E-Mail-Postfachs, um sicherzugehen, dass dort keine Weiterleitungen eingerichtet sind, von denen du nichts weißt.

Privatsphäre einstellen

- [ ] Stell deine Profile so ein, dass nur Menschen deine Inhalte sehen, mit denen du befreundet bist.
- [ ] Nimm nur Kontaktanfragen von Personen an, die du auch außerhalb des Internets kennst und denen du vertraust.
- [ ] Lege fest, wer dich kontaktieren, markieren oder deine Beiträge kommentieren darf.
- [ ] Prüfe, ob deine Telefonnummer oder dein Wohnort öffentlich sichtbar sind, und schalte Standortangaben in Beiträgen und Apps aus, damit niemand sehen kann, wo du dich gerade aufhältst.

Technik-Check (Fortsetzung)

Freigaben und geteilte Konten prüfen

- [ ] Sieh nach, mit wem du deinen Standort teilst, etwa über die Ortungsfunktionen von Apple oder Google, und beende Freigaben, die du nicht mehr möchtest.
- [ ] Kontrolliere, ob deine Fotoalben oder Cloud-Ordner noch für andere sichtbar sind.
- [ ] Prüfe, ob du Teil einer Familienfreigabe bist oder ob auf deinem Gerät eine Kinderschutz-App eingerichtet ist, von der du nichts weißt.
- [ ] Finde heraus, wer bei gemeinsam genutzten Konten, etwa für Streaming-Dienste oder Onlineshops, noch angemeldet ist, und ändere die Zugangsdaten, wenn du sie mit dieser Person nicht mehr teilen möchtest.

Fotos sicher teilen

- [ ] Schalte in den Einstellungen den Standortzugriff für deine Kamera-App aus, damit beim Fotografieren keine Ortsdaten mehr gespeichert werden.
- [ ] Entferne beim Teilen die Standortinformationen aus bereits gespeicherten Fotos, viele Smartphones bieten dafür eine eigene Option an.
- [ ] Verzichte darauf, Beiträge in sozialen Netzwerken mit einem Ort zu markieren, der anzeigt, wo ein Bild entstanden ist.
- [ ] Achte auf den Hintergrund deiner Fotos, denn schon Hausnummern, Straßenschilder oder die Aussicht aus dem Fenster können deinen Wohnort verraten.
- [ ] Teile Fotos von unterwegs lieber erst später, wenn du den Ort schon wieder verlassen hast.

Konten absichern

- [ ] Schütze dein Smartphone mit einem sicheren Code und gib ihn an niemanden weiter, auch nicht an Partner:innen.
- [ ] Nutze für jedes Konto ein eigenes, starkes Passwort, das sich nicht aus öffentlich bekannten Informationen wie Geburtstagen oder Namen erraten lässt. Ein Passwortmanager hilft dir, den Überblick zu behalten.
- [ ] Prüfe mit dem Identity Leak Checker des Hasso-Plattner-Instituts, ob deine Zugangsdaten bei einem Datenleck aufgetaucht sind, und ändere betroffene Passwörter.
- [ ] Richte überall, wo es möglich ist, eine Zwei-Faktor-Authentifizierung ein.
- [ ] Kontrolliere die hinterlegten Wiederherstellungsdaten wie Telefonnummer oder zweite E-Mail-Adresse, damit nur du dein Konto zurücksetzen kannst.
- [ ] Halte Betriebssystem und Apps auf dem neuesten Stand.

Was tun im Ernstfall?

1 Beweise sichern

Ein rechtssicherer Screenshot muss viele Angaben enthalten, die ein einfacher Screenshot oft nicht abdeckt. Dafür kannst du zum Beispiel die kostenlose Browser-Erweiterung Atomshot für Chrome und Firefox nutzen, die jeden Screenshot automatisch mit Link sowie atomuhrgenauem Datum und Uhrzeit versieht. Auf deinen Screenshots sollte zu sehen sein:

- der Inhalt selbst
- der Zusammenhang, also zum Beispiel der ursprüngliche Beitrag
- das Profil der verfassenden Person
- Datum und Uhrzeit
- der Link zum Inhalt

Achtung: Mach keine Screenshots von kinder- oder jugendpornografischen Inhalten und leite sie nicht weiter, denn schon der Besitz kann strafbar sein. Wende dich in diesem Fall direkt an die Polizei.

HateAid hat für alle gängigen Plattformen Anleitungen zur rechtssicheren Beweissicherung.

2 Inhalte melden

- Melde den Inhalt bei der Plattform ausdrücklich als rechtswidrig. Nur dann muss sie deine Meldung nach dem Digital Services Act prüfen und dir antworten.
- Melde ihn zusätzlich bei einer Meldestelle. Dort hilft man dir auch einzuschätzen, ob er strafbar ist. → **Meldestellen**

3 Reagieren, blockieren, löschen

- Du musst nicht auf Angriffe antworten, kannst aber Freund:innen oder deine Community bitten, dich mit Gegenrede zu unterstützen.
- Blockiere Accounts, die dich angreifen.
- Lösche oder verberge Hasskommentare unter deinen Beiträgen, aber erst, wenn die Beweise gesichert sind.

4 Anzeige erstatten

- Erstatte Anzeige bei der Polizei. Das geht vor Ort oder online über die Online-Wache deines Bundeslandes.
- Hast du ungefragt ein Dickpic bekommen, hilft dir Dickstinction dabei, die Anzeige vorzubereiten.

5 Unterstützung holen

- Sprich mit Menschen, denen du vertraust.
- Hol dir Hilfe bei einer Beratungsstelle. Du musst das nicht allein durchstehen.
  → **Hilfe finden**

KAPITEL 8

Hilfe und Beratung

IM NOTFALL

Polizei

Bei akuter Gefahr sofort anrufen. Anzeige erstatten kannst du auch online über die Online-Wache deines Bundeslandes.

110

portal.onlinewache.polizei.de

FÜR FRAUEN

Hilfetelefon „Gewalt gegen Frauen“

Rund um die Uhr, kostenlos, anonym und in vielen Sprachen.

116 016

FÜR MÄNNER

Hilfetelefon „Gewalt an Männern“

Für Männer, die Gewalt erleben.

0800 1239900

FÜR ALLE

Weisser Ring

Für alle Opfer von Kriminalität.

116 006

DIGITALE GEWALT

HateAid

Beratung für Betroffene digitaler Gewalt.

hateaid.org

FÜR FRAUEN

bff: Frauen gegen Gewalt e. V.

Frauenberatungsstellen in deiner Nähe finden.

frauen-gegen-gewalt.de

KINDER UND JUGENDLICHE

Nummer gegen Kummer

Für Kinder, Jugendliche und Eltern.

116 111

Elterntelefon:

0800 111 0 550

PSYCHISCHE KRISEN

Sozialpsychiatrischer Dienst

Unterstützung bei psychischen Krisen, in jedem Landkreis und jeder kreisfreien Stadt.

Such im Netz nach „Sozialpsychiatrischer Dienst“ und deinem Wohnort.

NUR RHEINLAND-PFALZ

SoliNet

Beratung und Informationen zu Hass und Gewalt im Netz.

0621 520 21 31

solinet@medienanstalt-rlp.de

solinet-rlp.de

KOMMUNALPOLITIK

Stark im Amt

Für Kommunalpolitiker:innen, die angefeindet werden.

0800 300 99 44

info@starkestelle.de

stark-im-amt.de

KOMMUNALPOLITIK

Starke Demokratie e. V.

Workshops, Beratung und Coaching für kommunalpolitisch Aktive zu Hass und Gewalt.

0151 70169966

kontakt@starkedemokratie.de

starkedemokratie.de

ALLE BUNDESLÄNDER

Mobile Beratung

Unterstützung bei Extremismus, Rassismus, Antisemitismus, Queerfeindlichkeit und Antifeminismus.

bundesverband-mobile-beratung.de

KAPITEL 8

Inhalte melden

BUNDESWEIT

REspect!

Meldestelle für Hass und Hetze im Netz.

respectimnetz.de

APP

MeldeHelden

App von HateAid und dem Hessischen Ministerium der Justiz, mit der du Hass im Netz direkt vom Smartphone aus meldest.

App Store **Google Play**

BUNDESWEIT

Internet-Beschwerdestelle

Meldung problematischer oder rechtswidriger Inhalte über ein Online-Formular, jede Meldung wird einzeln geprüft.

internet-beschwerdestelle.de

BUNDESWEIT

jugendschutz.net

Meldung von Verstößen gegen den Kinder- und Jugendmedienschutz.

jugendschutz.net

NUR NIEDERSACHSEN

Hass anzeigen

Meldestelle des Landes Niedersachsen.

hassanzeigen.de

NUR HESSEN

Hessen gegen Hetze

Meldestelle des Landes Hessen.

beratung-bei-hass.hessen.de

NUR BAYERN

Bayern gegen Hass

Initiative der bayerischen Justiz.

bayern-gegen-hass.de

Weitere Angebote von DsiN

APP

SiBa-App

Tagesaktuelle Sicherheitshinweise aufs Smartphone.

sicher-im-netz.de/siba

WEITERBILDUNG

DsiN-Digitalführerschein

Digitale Kompetenzen erwerben und zertifizieren lassen.

difue.de

RATGEBER

DsiN-Ratgeberreihe

Weitere Ausgaben zu Sicherheit im Netz.

sicher-im-netz.de/dsin-ratgeberreihe

Was ist …
die DsiN-Ratgeberreihe?

Die DsiN-Ratgeberreihe erklärt einfach und verständlich die wichtigsten Begriffe rund um Sicherheit im Internet – von Algorithmus bis Zwei-Faktor-Authentisierung. Mit unseren DsiN-Tipps erhältst du praktische Handlungsempfehlungen für souveränes Surfen im Alltag. In weiterführenden Links findest du umfassende Informationen zu den jeweiligen Themen sowie Kontakte zu Beratungs- und Hilfsangeboten. So hilft die DsiN-Ratgeberreihe, das Internet für dich, deine Familie und andere Menschen in deinem Umfeld sicherer zu machen.

Deutschland sicher im Netz

Weitere relevante Ausgaben

→ Belästigung im Netz – kompetent kontern (PDF)

→ Das digitale Ich – selbstbestimmt surfen (PDF)

→ Benutzerkonten sichern – einfach einloggen (PDF)

Zur Ratgeberreihe →

Mit freundlicher Unterstützung von:

Impressum

Deutschland sicher im Netz e.V.
Albrechtstr. 10 c, 10117 Berlin
Vollständiges Impressum

Datenschutz

Diese Seite setzt keine Cookies und lädt keine Tracking-Skripte. Für anonyme Besucherstatistiken werten wir die Zugriffsprotokolle unseres Servers mit Matomo aus, IP-Adressen werden dabei gekürzt. Alle Inhalte, auch die Schriften, werden von diesem Server geladen. Der eingebettete Kampagnenspot wird erst geladen, wenn du ihn abspielst. Datenschutzerklärung

Bei der Gestaltung dieser Webseite kam KI zum Einsatz.