Digitale Räume sicher, respektvoll und barrierefrei nutzen

1



Praxisnaher Präsenz-Workshop | ca. 2 Stunden



Gemeinsam erarbeiten wir us einen Einstieg zum Thema digitale Awareness.



Was mach digitale Räume sicher, barrierrearm, respektvoll und stärkend?

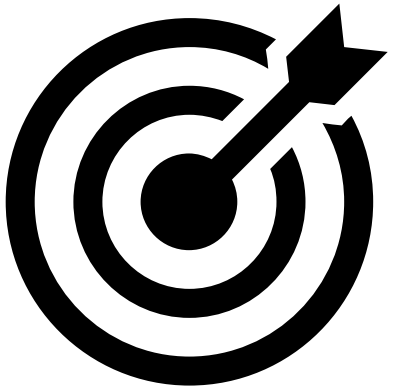


Für Organisationen, Verwaltung, Unternehmen, Interessenvertretungen und Privatpersonen



Moderatorin: Andrea Grassow

Ziel des Workshops



Orientierung, Sensibilisierung und erste Handlungssicherheit

Digitale Gewalt in ihren Formen besser erkennen

Auswirkungen auf Betroffene und Organisationen verstehen

Besonders gefährdete Gruppen in den Blick nehmen

Erste Handlungsmöglichkeiten kennenlernen

Prävention im privaten und organisationalen Alltag mitdenken

Wer ist heute angesprochen?



Der Workshop verbindet persönliche und organisationale Perspektiven

Privatpersonen: Was kann ich für mich selbst tun?

Organisationen: Welche Strukturen brauchen wir?

Verwaltung und Unternehmen: Wie entstehen sichere digitale Räume?

Personal- und Betriebsräte, SBV, Peervertretungen: Wie unterstützen wir Betroffene?

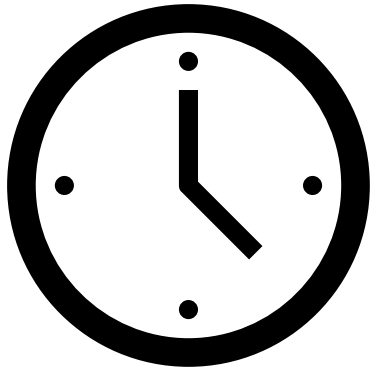
Führungskräfte und Fachkräfte: Wie schaffen wir klare Zuständigkeiten?

Workshoprahmen



Damit ein sicherer Austausch möglich ist
Niemand muss persönliche Erfahrungen teilen.
Erfahrungen werden nicht bewertet oder infrage gestellt.
Betroffenenperspektiven sind Expertise.
Wir sprechen respektvoll und vertraulich.
Es geht um Lernen, Schutz und Veränderung – nicht um Schuldzuweisung.

Ablauf in ca. 2 Stunden



Vom gemeinsamen Verständnis zum ersten Handlungsschritt

Ankommen und Einstieg

Grundlagen: Was ist digitale Gewalt?

Zehn Formen digitaler Gewalt

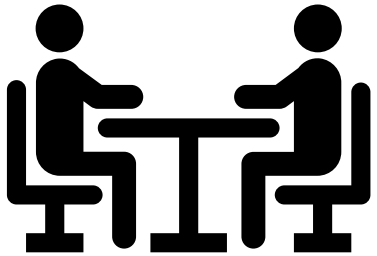
Besonders betroffene Gruppen

Fallwerkstatt mit Praxisbeispielen

Handlungsmöglichkeiten, Prävention und Unterstützung

Abschluss: Was nehme ich konkret mit?

Einstieg: Digitaler Alltag



Digitale Räume sind längst Teil unserer Lebenswelt

Arbeit, Bewerbung, Verwaltung und Beratung

Social Media, Messenger und Öffentlichkeitsarbeit

Banking, Mobilität, Gesundheit und Bildung

Digitale Räume können Teilhabe ermöglichen.

Sie können aber auch Barrieren, Unsicherheit und Gewalt verstärken.

Impulsfrage



Reflexion im Dialog

Stellen Sie sich vor: Sie öffnen morgens Ihr Smartphone.

Sie haben 127 neue Nachrichten.

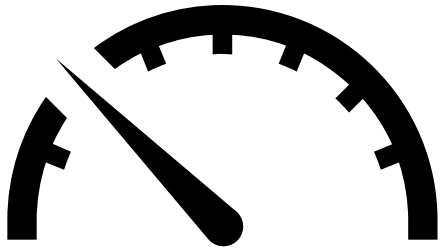
Ein Beitrag über Sie wird geteilt, kommentiert und bewertet.

Was wäre Ihr erster Gedanke?

Was würden Sie als Erstes tun?

Stimmungsbarometer

8



0 = Ich fühle mich im digitalen Raum überhaupt nicht sicher.

10 = Ich fühle mich sehr sicher.

Teilnehmende stellen sich auf der Linie auf.

Kurze Nachfrage: Was gibt Sicherheit? Was verunsichert?

Was ist digitale Gewalt?



Digitale Gewalt umfasst Übergriffe, Herabwürdigung, Kontrolle, Bedrohung oder Schädigung mit digitalen Mitteln.

Sie kann über Messenger, soziale Netzwerke, E-Mail, Apps, Plattformen oder Foren stattfinden.

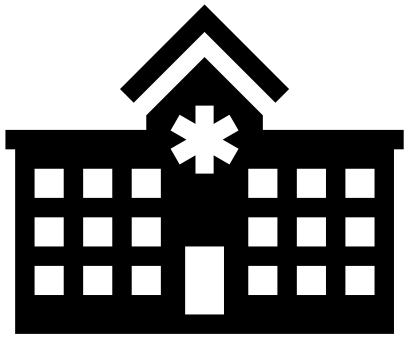
Sie kann einzelne Personen, Gruppen oder ganze Organisationen treffen.

Digitale Gewalt wirkt häufig über den Bildschirm hinaus in Alltag, Arbeit, Gesundheit und Teilhabe.

Was ist das Besondere an digitaler Gewalt?

Digitale Dynamiken können Belastungen verstärken
Hohe Reichweite: Inhalte verbreiten sich sehr schnell.
Dauerhaftigkeit: Beiträge, Bilder oder Screenshots bleiben oft verfügbar.
Anonymität: Täterinnen und Täter treten häufig unter falschen Profilen auf.
Rund-um-die-Uhr-Belastung: Betroffene können schwer abschalten.
Verknüpfung mit analoger Gewalt: Online-Angriffe können reale Folgen haben.

Digitale Gewalt betrifft auch Organisationen



Nicht nur Einzelpersonen sind betroffen

Hassmails, Drohungen oder Shitstorms können Teams verunsichern.

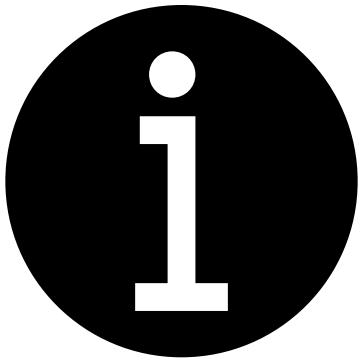
Fake-Profile können Vertrauen in eine Organisation beschädigen.

Datenschutzvorfälle können Betroffene zusätzlich gefährden.

Kommentarspalten können zu unsicheren Räumen werden.

Unklare Zuständigkeiten führen im Ernstfall zu Verzögerungen.

Die zehn Formen im Überblick



Ein gemeinsamer Wortschatz für die Fallarbeit

Cybermobbing | Cyberstalking | Hate Speech

Doxing | Deepfakes | Identitätsdiebstahl

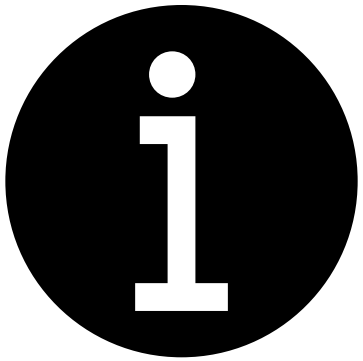
Phishing | Sextortion

Unerlaubte Bild- und Videoverbreitung

Digitale Bedrohung und Einschüchterung

1 | Cybermobbing

13



Wiederholtes Herabwürdigen und Ausgrenzen

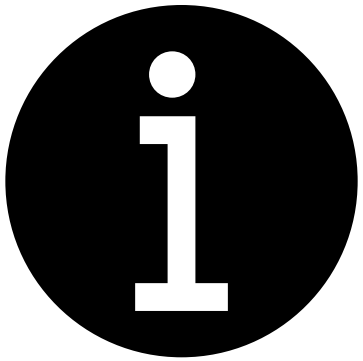
Eine Person wird über digitale Kanäle wiederholt beleidigt, verspottet, bloßgestellt oder ausgeschlossen.

Typische Orte: Gruppenchats, soziale Netzwerke, Kommentarspalten, Schul- oder Arbeitsplattformen.

Beispiel: Ein peinliches Foto wird in einer Gruppe geteilt und mit beleidigenden Kommentaren versehen.

Erste Reaktion: nicht allein lassen, Inhalte sichern, Plattform melden, Vertrauensperson einbeziehen.

2 | Cyberstalking



Digitale Nachstellung und Kontrolle

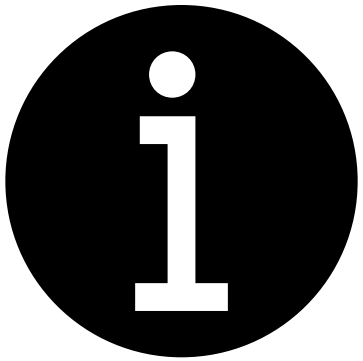
Eine Person wird wiederholt gegen ihren Willen kontaktiert, beobachtet, verfolgt oder kontrolliert.

Beispiele: neue Accounts nach Blockierungen, ständige Nachrichten, Standortkontrolle, Kontaktaufnahme über Dritte.

Betroffene verändern oft ihr Verhalten: Nummer wechseln, Profile löschen, Rückzug aus Öffentlichkeit.

Erste Reaktion: Kontakt nicht fortsetzen, dokumentieren, Konten schützen, Unterstützung holen.

3 | Hate Speech



Abwertung, Diskriminierung und Hass im digitalen Raum

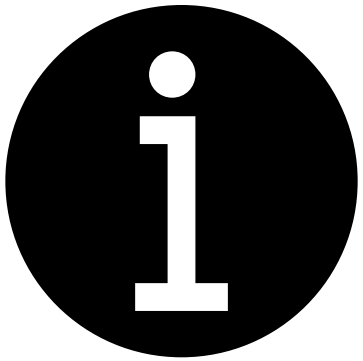
Menschen oder Gruppen werden abgewertet, beleidigt, entmenschlicht oder bedroht.

Angriffe beziehen sich häufig auf Geschlecht, Behinderung, Herkunft, Religion, Alter, sexuelle Identität oder politische Haltung.

Beispiel: Unter einem Beitrag einer Organisation erscheinen ableistische oder frauenfeindliche Kommentare.

Erste Reaktion: dokumentieren, moderieren, klare Grenzen setzen, Betroffene schützen.

4 | Doxing



Private Daten werden ohne Zustimmung veröffentlicht

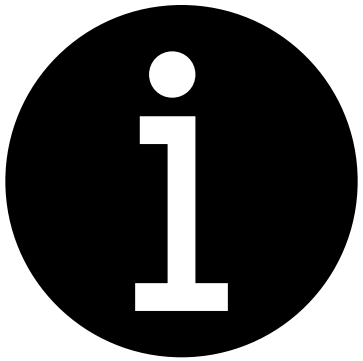
Persönliche Daten werden gesammelt und veröffentlicht, um Druck, Angst oder Angriffe auszulösen.

Beispiele: Adresse, Telefonnummer, Arbeitsplatz, private Fotos, familiäre Informationen.

Besonders riskant für öffentlich engagierte Personen, Beratungsstellen, Aktivistinnen und Betroffene.

Erste Reaktion: Daten sichern, Löschung verlangen, Risiken einschätzen, Schutzmaßnahmen prüfen.

5 | Deepfakes



Manipulierte Bilder, Stimmen oder Videos

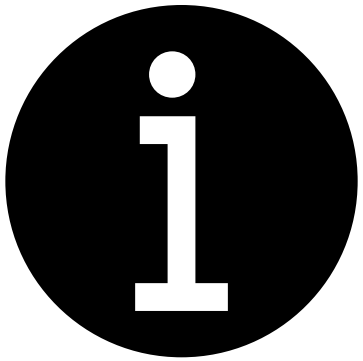
Mit digitalen Werkzeugen oder KI werden Inhalte erzeugt, die täuschend echt wirken.

Eine Person scheint etwas zu sagen oder zu tun, was nie passiert ist.

Deepfakes können für Rufschädigung, Betrug, sexualisierte Gewalt oder politische Manipulation eingesetzt werden.

Erste Reaktion: nicht weiterverbreiten, Originale sichern, Plattform melden, kommunikativ vorsichtig handeln.

6 | Identitätsdiebstahl



Jemand tritt digital unter fremdem Namen auf

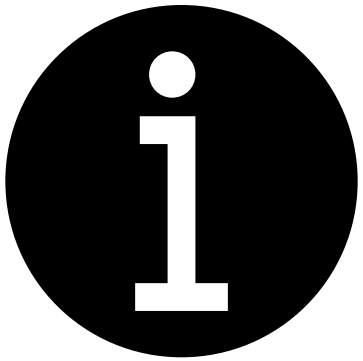
Fotos, Namen, Daten oder Accounts werden missbraucht, um sich als andere Person auszugeben.

Beispiele: Fake-Profil, Nachrichten im Namen einer Person, Spendenaufrufe über falsche Accounts.

Folgen: Vertrauensverlust, finanzielle Schäden, Rufschädigung, hohe Belastung für Betroffene.

Erste Reaktion: Profil melden, Umfeld informieren, Zugänge sichern, Belege sammeln.

7 | Phishing



Täuschung, um Daten oder Zugänge zu erhalten

Gefälschte Nachrichten oder Webseiten sollen Menschen zur Preisgabe von Passwörtern oder Daten bewegen.

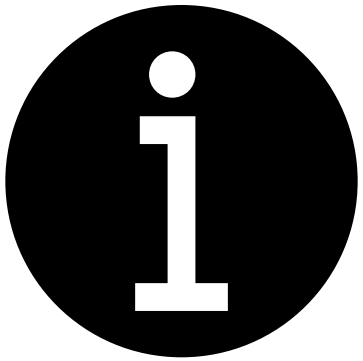
Typische Mittel: Zeitdruck, Autorität, Angst, angebliche Rechnungen, falsche Login-Seiten.

Beispiel: Eine E-Mail wirkt wie eine interne Nachricht und fordert zur schnellen Passwortbestätigung auf.

Erste Reaktion: nicht klicken, Absender prüfen, IT/Ansprechperson informieren, Passwort ändern wenn nötig.

8 | Sextortion

20



Erpressung mit intimen Bildern oder Informationen

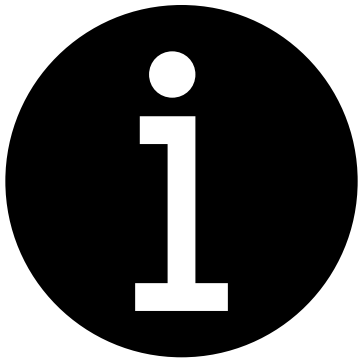
Intime Bilder, Videos oder private Informationen werden genutzt oder angedroht, um Druck auszuüben.

Forderungen können Geld, weitere Bilder, Kontakt oder bestimmtes Verhalten sein.

Scham und Angst führen häufig dazu, dass Betroffene lange allein bleiben.

Erste Reaktion: nicht zahlen, nicht weiterverhandeln, Beweise sichern, vertrauliche Hilfe holen.

9 | Unerlaubte Bild- und Videoverbreitung



Aufnahmen werden ohne Einwilligung weitergegeben

Fotos oder Videos werden aufgenommen, geteilt oder veröffentlicht, ohne dass die betroffene Person zustimmt.

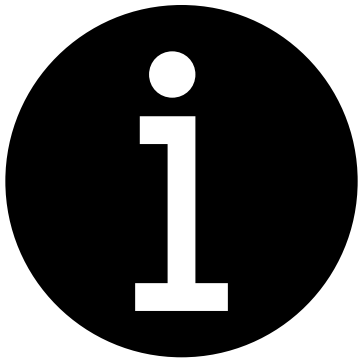
Das betrifft private Bilder, intime Aufnahmen, Veranstaltungfotos oder Mitschnitte aus digitalen Treffen.

Auch ursprünglich freiwillig geteilte Bilder dürfen nicht beliebig weiterverbreitet werden.

Erste Reaktion: Löschung verlangen, Plattform melden, Belege sichern, Unterstützung einbeziehen.

10 | Digitale Bedrohung und Einschüchterung

22



Angst erzeugen und Teilhabe verhindern

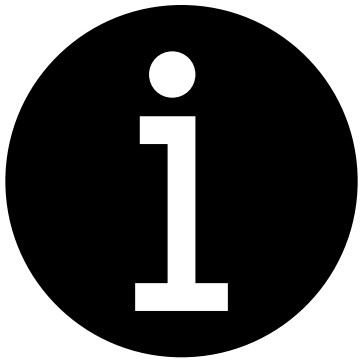
Drohungen, Einschüchterungen oder koordinierte Angriffe sollen Menschen mundtot machen oder verdrängen.

Betroffene ziehen sich aus Debatten, Ehrenamt, Öffentlichkeit, Arbeit oder digitalen Räumen zurück.

Beispiel: Nach einem öffentlichen Beitrag erhält eine Person Drohungen gegen sich oder ihre Familie.

Erste Reaktion: Gefährdung ernst nehmen, dokumentieren, Unterstützung und zuständige Stellen einbeziehen.

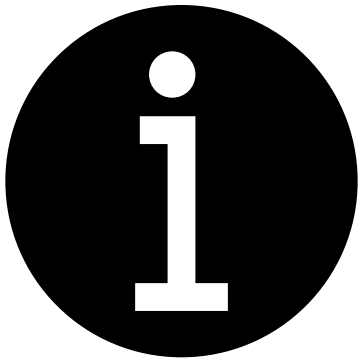
Besonders betroffene Gruppen



Digitale Gewalt trifft nicht alle gleich

- Menschen mit Behinderungen
- Frauen – insbesondere Frauen mit Behinderungen
- Kinder und Jugendliche
- Seniorinnen und Senioren
- Menschen in Abhängigkeitsverhältnissen oder mit geringen Unterstützungszugängen
- Öffentlich sichtbare Personen, Ehrenamtliche, Peervertretungen und Interessenvertretungen

Menschen mit Behinderungen



Digitale Teilhabe kann Schutz brauchen

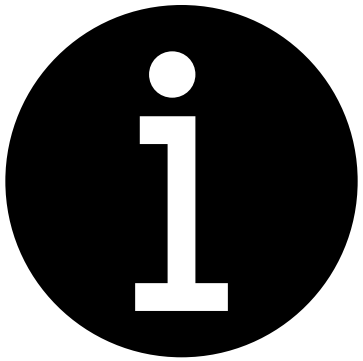
Digitale Angebote können Selbstbestimmung und Beteiligung ermöglichen.

Barrieren erschweren aber Melden, Beschweren, Verstehen oder Beweissicherung.

Ableistische Angriffe nutzen Behinderung, Hilfebedarf oder Sprache gezielt zur Herabwürdigung.

Unterstützung muss barrierearm, verständlich, erreichbar und vertraulich sein.

Frauen – insbesondere Frauen mit Behinderungen



Mehrfachbetroffenheiten ernst nehmen

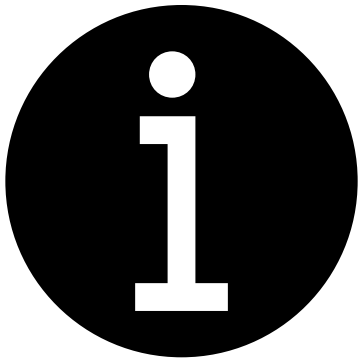
Digitale Gewalt kann geschlechtsspezifisch, sexualisiert und diskriminierend auftreten.

Frauen mit Behinderungen können mehrere Formen von Abwertung gleichzeitig erleben.

Scham, Angst und fehlende barrierearme Angebote erschweren Hilfewege.

Unterstützung braucht Vertraulichkeit, Selbstbestimmung und Schutz vor weiterer Beschämung.

Kinder und Jugendliche



Digitale Räume sind soziale Räume

Gruppenchats, Plattformen und soziale Netzwerke sind Teil von Freundschaft, Schule und Identität.

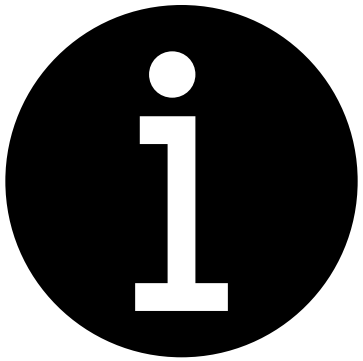
Cybermobbing, Bildweitergabe und Gruppendruck können sehr schnell eskalieren.

Betroffene brauchen Erwachsene, die zuhören, unterstützen und nicht sofort den digitalen Zugang entziehen.

Prävention: Medienkompetenz, klare Regeln, Vertrauenspersonen und niedrigschwellige Hilfewege.

Seniorinnen und Senioren

27



Sicherheit ohne Bevormundung

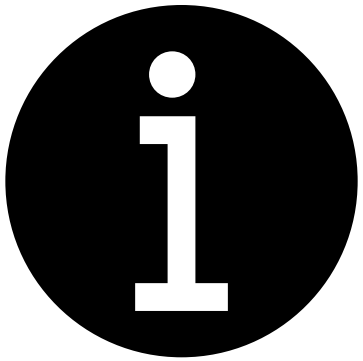
Digitale Angebote können Wege sparen und Selbstständigkeit stärken.

Unverständliche Prozesse, Zeitdruck oder täuschend echte Nachrichten können verunsichern.

Phishing, Betrug und Identitätsmissbrauch nutzen oft Vertrauen oder Unsicherheit aus.

Prävention: verständlich erklären, gemeinsam prüfen, Ansprechpersonen schaffen, nicht beschämen.

Auswirkungen digitaler Gewalt



Betroffene erleben häufig mehr als einen einzelnen Vorfall

Psychisch: Angst, Stress, Schlafstörungen, Scham, Kontrollverlust

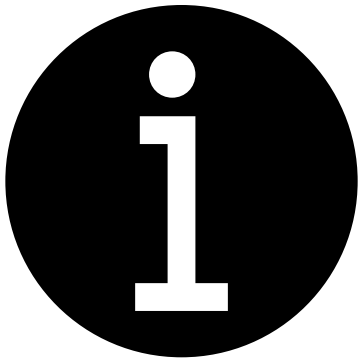
Sozial: Rückzug, Isolation, Vertrauensverlust, Konflikte

Beruflich/ehrenamtlich: Arbeitsausfall, Rückzug aus Rollen, weniger Sichtbarkeit

Gesundheitlich: Erschöpfung, Belastungsreaktionen

Gesellschaftlich: weniger Beteiligung, weniger Vielfalt, weniger demokratische Teilhabe

Übung: Barriere, Risiko oder Schutzfaktor?



Kurze analoge Raumpositionierung

Eine Aussage wird vorgelesen.

Links im Raum: Das erhöht Risiko.

Rechts im Raum: Das schützt oder ermöglicht Teilhabe.

Mitte: Kommt darauf an.

Nachfrage: Was müsste verändert werden, damit daraus ein Schutzfaktor wird?

Fallwerkstatt: Gemeinsame Analyse



Für Organisationen und Privatpersonen nutzbar

Jede Gruppe bearbeitet einen Praxisfall.

Analyse: Was passiert hier?

Betroffenenperspektive: Was braucht die Person jetzt?

Organisationsperspektive: Wer muss handeln?

Prävention: Was kann künftig vorbereitet werden?

Vorstellung: 3 Minuten Ergebnis pro Gruppe

Arbeitsfragen für jede Fallgruppe



Welche Form(en) digitaler Gewalt erkennen wir?

→ Wer ist unmittelbar und mittelbar betroffen?

↓

Welche Risiken entstehen kurzfristig?

→ Welche ersten Schritte sind sinnvoll?

↓

Welche Unterstützung ist notwendig?

→ Welche präventiven Maßnahmen wären künftig hilfreich?

Sofort handeln: Erste Orientierung



Keine Panik – Schritt für Schritt vorgehen

1. Sicherheit: Besteht eine akute Gefahr?

2. Stabilisierung: Betroffene ernst nehmen und unterstützen.

3. Sicherung: Inhalte, Links, Namen, Datum und Kontext dokumentieren.

4. Zuständigkeit: interne oder externe Ansprechpersonen klären.

5. Nächster Schritt: gemeinsam entscheiden, was jetzt sinnvoll ist.

Beweise und Informationen sichern



Praktisch, ruhig und nachvollziehbar

Screenshots mit Datum, Uhrzeit, Nutzername und Kontext sichern.

Links und Profilinformationen dokumentieren.

Nachrichten nicht vorschnell löschen.

Dokumente geschützt aufbewahren.

Nur notwendige Personen einbeziehen.

Bei Unsicherheit fachliche Unterstützung holen.

Was Betroffene häufig brauchen



- **Unterstützung beginnt mit Haltung**
- Glauben und ernst nehmen
- Keine Schuldzuweisung
- Schutz vor weiterer Bloßstellung
- Mitbestimmung über die nächsten Schritte
- Barrierearme und verständliche Informationen
- Begleitung zu Beratungs-, Beschwerde- oder Unterstützungsstellen

Was Organisationen vorbereiten können



Prävention ist Organisationsentwicklung

Klare Ansprechpersonen benennen

Meldewege sichtbar und niedrigschwellig gestalten

Regeln für Social Media, Messenger, Fotos und digitale Veranstaltungen vereinbaren

Kommentarbereiche moderieren

Beschäftigte, Ehrenamtliche und Verantwortliche sensibilisieren

Vorfälle dokumentieren und daraus lernen

Rolle von Personalvertretung, Betriebsrat und SBV



Brücken bauen, unterstützen, Strukturen verbessern

Betroffene begleiten und Orientierung geben

Auf barrierearme, sichere Meldewege hinwirken

Schutzbedarfe im Arbeitsumfeld sichtbar machen

Prävention in Dienstvereinbarungen, Leitlinien oder Schulungen anregen

Führung, Personalbereich, Datenschutz, IT und Gleichstellung vernetzen

Rolle von Peervertretung und Selbstvertretung



Erfahrungswissen als Ressource

Betroffenenperspektiven sichtbar machen

Vertrauensvolle Erstorientierung geben

Barrieren in digitalen Räumen benennen

Organisationen auf Ausschlussrisiken hinweisen

Gemeinsam mit Betroffenen Lösungen entwickeln, statt über sie zu entscheiden

Unterstützungswege



Niemand muss einen Vorfall allein bearbeiten

Interne Ansprechpersonen: Leitung, Personal, Interessenvertretungen, Datenschutz, IT

Peer- und Selbstvertretungsstrukturen

Fachberatungsstellen und Opferunterstützung

Plattform-Meldewege

Datenschutzaufsicht bei Datenschutzvorfällen

Polizei oder zuständige Stellen bei Bedrohung, Stalking, Erpressung oder akuter Gefahr

Prävention für Privatpersonen



- **Kleine Schritte können viel bewirken**
- Privatsphäre-Einstellungen regelmäßig prüfen
- Starke Passwörter und Mehr-Faktor-Authentifizierung nutzen
- Standortfreigaben und gemeinsame Konten kontrollieren
- Persönliche Daten bewusst veröffentlichen
- Blockieren, Melden und Hilfeholen als legitime Schutzmaßnahmen verstehen

Prävention für Organisationen



- **Sichere digitale Kultur gestalten**
- Digitale Gewalt als Risiko in Schutz- und Präventionskonzepte aufnehmen
- Verantwortlichkeiten und Eskalationswege festlegen
- Barrierearme Informationen und Beschwerdewege bereitstellen
- Social-Media- und Foto-Prozesse verbindlich regeln
- Regelmäßig Schulungen und Reflexionsräume anbieten
- Nach Vorfällen auswerten: Was verbessern wir?

Erste Maßnahmenplanung



Welche digitalen Räume nutzen wir?

Wo können Menschen ausgeschlossen, bedroht oder beschämt werden?

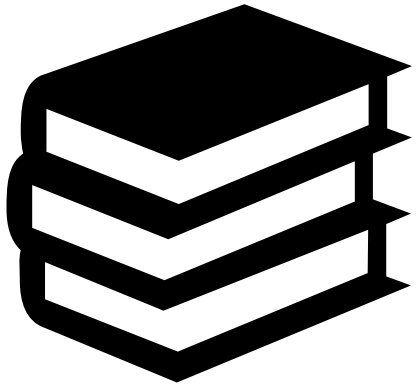
Wer wäre im Ernstfall zuständig?

Wie erfahren Betroffene von Unterstützung?

Welche Regel oder Checkliste fehlt uns noch?

Was ist ein realistischer erster Schritt in den nächsten vier Wochen?

Fünf Leitgedanken zum Mitnehmen



Ein Kompass für digitale Sicherheit

ERKENNEN: digitale Gewalt nicht verharmlosen

ZUHÖREN: Betroffene ernst nehmen

SCHÜTZEN: Sicherheit und Selbstbestimmung stärken

HANDELN: Zuständigkeiten und Unterstützung nutzen

VORBEUGEN: aus Risiken und Vorfällen lernen

Abschlussfrage

43



Transfer in den Alltag

Was nehme ich aus dem Workshop mit?

Was möchte ich in meinem privaten oder beruflichen digitalen Alltag genauer prüfen?

Welche Maßnahme kann ich sofort umsetzen?

Welche Frage bleibt offen?

Wer sollte in meiner Organisation ebenfalls über dieses Thema sprechen?

Vielen Dank für den Austausch



Digitale Gewalt erkennen • Betroffene stärken • Prävention gemeinsam gestalten

Kontakt:

Andrea Grassow,
grassow@selbstvertretung-thueringen.de