



#DigitaleVorbilder
Familien gehen online.

Zwischen Sensibilisierung und Handlungskompetenz: Ein Praxisprojekt zur digitalen Befähigung von Familien





#DigitaleVorbilder

Familien gehen online.

Ein Gemeinschaftsprojekt
der Datenschutzaufsichtsbehörden aus
Mecklenburg-Vorpommern und Hamburg.



“

*(...) Jede Aufsichtsbehörde [muss] in ihrem Hoheitsgebiet die Öffentlichkeit für die Risiken (...) und Rechte (...) sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei **spezifische Maßnahmen für Kinder**.*

(Art. 57 Abs. 1 lit. b DSGVO)

54%

der 6- bis 13-jährigen
Internetnutzenden sind
täglich online (KIM-Studie
2024)

71%

der Eltern geben an, **keine
Sicherheitseinstellungen**
an Geräten vorzunehmen
(KIM-Studie 2024)

77 %

der Eltern sorgen sich um
Onlinesicherheit ihrer Kinder
(Jugendmedienschutzindex
2022)

Agenda

- 1 #DigitaleVorbilder
- 2 Vorstellung der Zielgruppe
- 3 Unsere Angebote
- 4 Risikonarrative
- 5 Abschluss

Unser Team



Antje Kaiser

Projektleitung
Mecklenburg-Vorpommern



Alina Schömig

Projektleitung
Hamburg



Christina Münster

Projektkoordinatorin
Mecklenburg-Vorpommern



Lydia Roth

Projektkoordinatorin
Hamburg



Ermutigung statt Verunsicherung

Wir möchten Familien ...



Ziel # 1

Hilfestellungen zum Schutz
ihrer Privatsphäre
aufzeigen



Ziel # 2

Ermutigen das eigene
Mediennutzungsverhalten
zu hinterfragen.

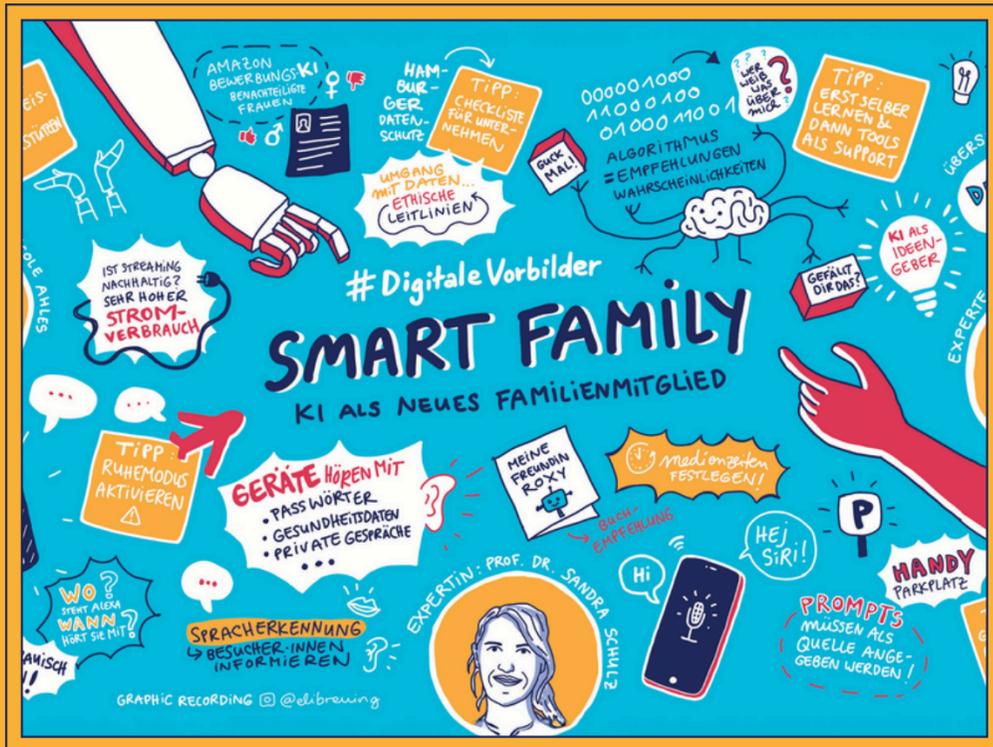


Ziel # 3

Für die digitale Lebenswelt
ihrer Kinder begeistern.

Angst- und Bedrohungsnarrative zeigen geringe Wirkung – wirksamer sind Erzählungen, die Ermutigung und Selbstwirksamkeit betonen.





Zielgruppe: Familien



Eltern als Schlüssel für die Medienerziehung der Kinder.

Von der Theorie....

Eltern als Vorbilder

- Modell- oder Beobachtungslernen (u.a. Bandura, (1999))
- Eltern als Vorbilder und Gate Keeper (Daum, M. M., & Gampe, A. (2016))

Generelle Annahmen

- Hoher elterlicher Einfluss auf das Lernen der Kinder (Livingstone, S., Blum-Ross, A., (2020))
- Heterogenität der Familienstruktur (Jurczyk, K., & Klinkhardt, H., (2014))

... zur Praxis:

Nur durch bewusstes und reflektiertes Verhalten können Eltern als Vorbilder im digitalen Raum wirken.



Medienaktionstage

Mecklenburg-Vorpommern & Hamburg

- ~ 400 Besucher:innen
- Programm für Eltern: Info-Stände, Kurzvorträge, Podium, Austausch mit Expert:innen
- Programm für Kinder: Klettern, Basteln, Gaming, Podcast-Studio

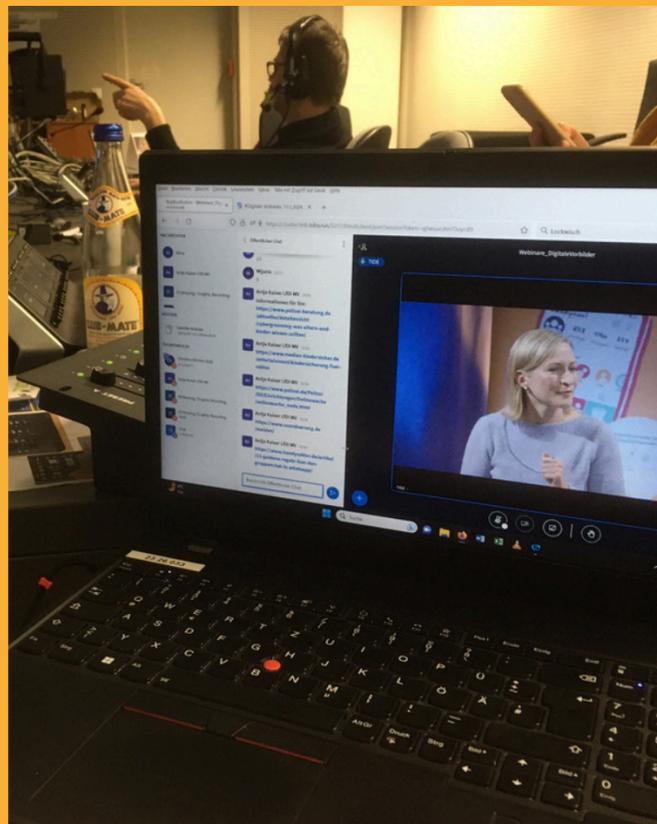




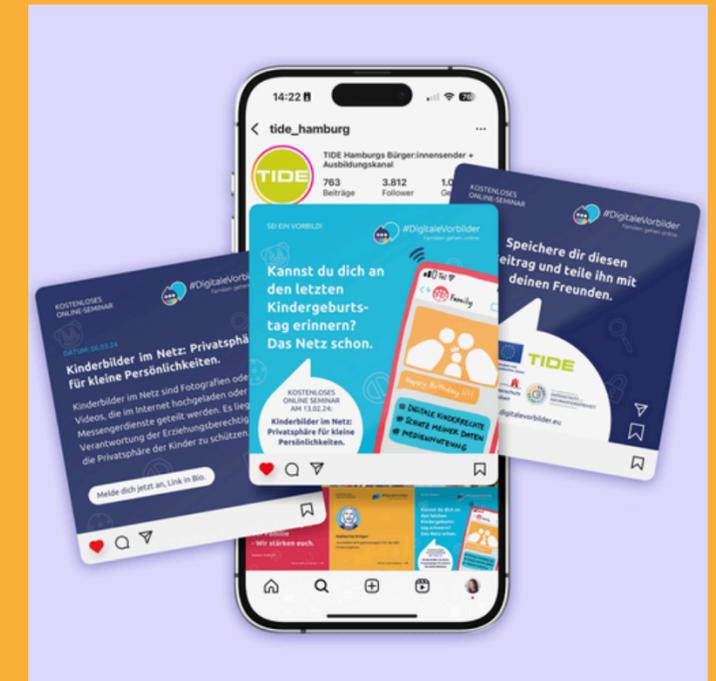
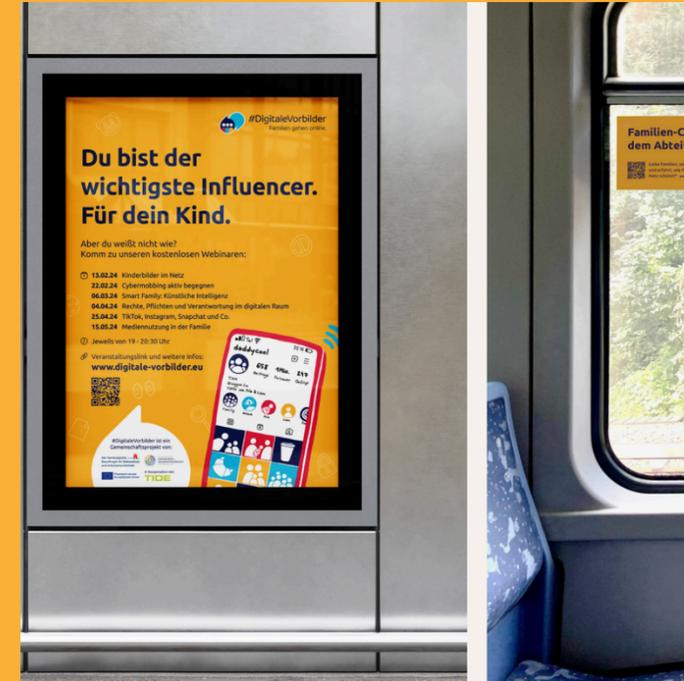
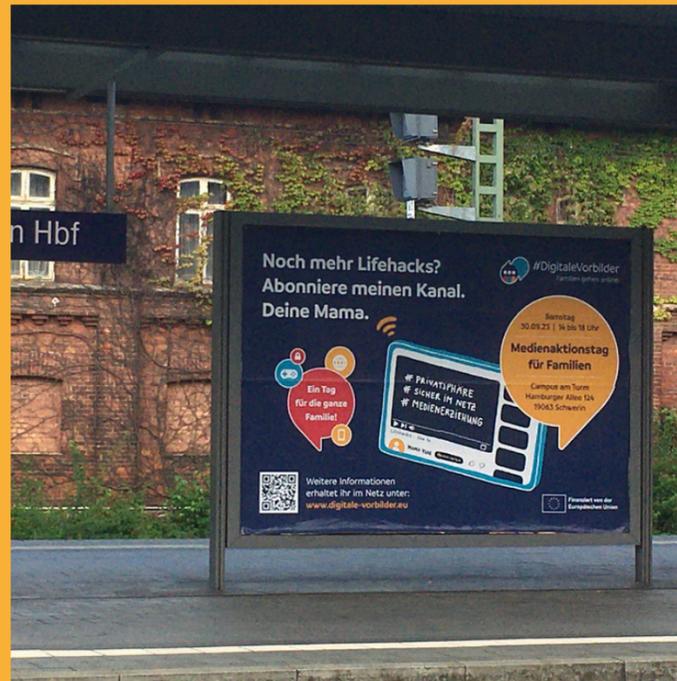
Webinare

aufgezeichnet im Bürger:innensender TIDE

- + 1000 Besucher:innen
- Input mit Moderation und Expert:innen
- Teilnehmende hatten die Möglichkeit Fragen ins Studio zu stellen
- Themen: Gaming, Smarte Datendiebe, Kinderbilder, Datenschutzmythen, Cybermobbing, "TikTok, Insta, Snapchat & Co.", Mediennutzung in der Familie, Wahlbeeinflussung, ...



Was haben wir gemacht?



Du bist der wichtigste Influencer. Für Dein Kind.

Familien-Chat mit dem Abteil teilen?

Kannst Du Dich an den letzten Kindergeburtstag erinnern? Das Netz schon.

Materialien



Graphic Recordings & Info-Karten

DIE GRÖßTEN DATENSCHUTZMYTHEN

– Argumentationshilfen für den Alltag

Wir leben in einer Welt ständig verfügbarer Informationen, die dank des Internets von jedem Ort aus abrufbar sind. Damit wir diese Informationen, Apps und Anwendungen nutzen können, braucht es meist eine Anmeldung oder Registrierung. Auf diese Weise sind unsere Daten schnell in alle Welt gestreut. Wer im Netz diese Informationen und Daten sehen kann, ist uns oft nicht bewusst. Einen Überblick über unsere Datenspuren zu behalten, fällt schwer. Im Falle eines Datenlecks kann dies unüberschaubaren Schaden verursachen.

MYTHOS 1: ICH HABE NICHTS ZU VERBERGEN UND MUSS MICH NICHT UM DATENSCHUTZ KÜMMERN.

Falsch! Der Missbrauch von Daten, die freiwillig oder unbeabsichtigt im Netz landen, kann großen persönlichen Schaden verursachen. Es ist schwer zu überblicken, welche Konsequenzen mangelnder Datenschutz nach sich ziehen kann, da die Gefahr abstrakt wirkt. Es ist daher hilfreich, die Risiken zu kennen und einschätzen zu können.

Mögliche Folgen von Datenmissbrauch

1. Verlust der Privatsphäre, bspw. durch Standortverfolgung, Preisgabe von persönlichen Informationen, Abhörfunktionen oder unverschlüsselte Chats
2. Profilbildung durch eingegebene Daten und Verbindung von Daten unterschiedlicher Quellen, um passgenaue Inhalte und Werbung anzuzeigen
3. Verlust des Grundrechts auf freie Entfaltung der Persönlichkeit durch das Gefühl der Überwachung oder Bewertung
4. Intransparente Datenübermittlung, z.B. an Werbefirmen, Geheimdienste
5. Manipulation von Kauf- oder gar Wahlentscheidungen durch Tracking und personalisierte Werbung
6. Identitätsdiebstahl oder -betrug, indem Kriminelle mit fremden Namen

4.2 Die größten Datenschutzmythen



Wusstest du, dass ...

du ein Recht darauf hast, dass deine Daten von Firmen gelöscht und korrigiert werden?

#DigitaleVorbilder
Familien gehen online.

Ein Smartphone displaying a social media profile for 'daddycool' is shown.

QR-Code: Noch mehr nützliche Infos oder praktische Tipps rund um das Thema Datenschutz? Dann scann' den QR-Code und klick dich durch unsere Videos, Podcasts, Graphic Recordings uvm.

Unsere Broschüre -
mehrsprachig & barrierefrei



Broschüre

MYTHOS 1: ICH HABE NICHTS ZU VERBERGEN UND MUSS MICH NICHT UM DATENSCHUTZ KÜMMERN.

Falsch! Der **Missbrauch von Daten**, die freiwillig oder unbeabsichtigt im Netz landen, kann großen persönlichen Schaden verursachen.

Es ist schwer zu überblicken, welche Konsequenzen mangelnder Datenschutz nach sich ziehen kann, da die Gefahr abstrakt wirkt. Es ist daher hilfreich, die **Risiken** zu kennen und einschätzen zu können.

Mögliche Folgen von Datenmissbrauch

1. **Verlust der Privatsphäre**, bspw. durch Standortverfolgung, Preisgabe von persönlichen Informationen, Abhörfunktionen oder unverschlüsselte Chats

4.2 Die größten Datenschutzmythen



2. **Profilbildung** durch eingegebene Daten und Verbindung von Daten unterschiedlicher Quellen, um passgenaue Inhalte und Werbung anzuzeigen
3. **Verlust des Grundrechts auf freie Entfaltung der Persönlichkeit** durch das Gefühl der Überwachung oder Bewertung
4. **Intransparente Datenübermittlung**, z.B. an Werbefirmen, Geheimdienste
5. **Manipulation von Kauf- oder gar Wahlentscheidungen** durch Tracking und personalisierte Werbung
6. **Identitätsdiebstahl oder -betrug**, indem Kriminelle mit fremden Namen

MYTHOS 4: MEIN SMARTPHONE HÖRT MIT.



Vermutlich nicht! Es gibt das Gerücht, dass Smartphones Gespräche mithören, um gezielte Werbung anzuzeigen.

Diese Gründe sprechen dagegen

1. Smartphone-Apps benötigen eine **ausdrückliche Erlaubnis**, um das Mikrofon nutzen zu dürfen.
2. Betriebssysteme ab Android 12 und iOS 14 lassen einen unbemerkten Zugriff auf Mikrofon und Kamera durch im Hintergrund laufende Apps nicht mehr zu. Sie informieren mithilfe eines **Privacy Indicators** darüber, wenn eine App das Mikrofon oder die Kamera benutzt.
3. Würde das Smartphone tatsächlich dauerhaft mithören und Gespräche übermitteln, müsste dies am Stromverbrauch und dem **verbrauchten Datenvolumen** zu erkennen sein.

Warum uns trotzdem personalisierte Werbung angezeigt wird

1. Werbeanzeigen basieren auf dem **Onlineverhalten des Nutzenden**. Suchanfragen, Browserverlauf und andere

3. Tatsächlich gibt es eine **KI-basierte Technologie** namens „**Active Listening**“. Sie ermöglicht es Werbefirmen, Gespräche in Echtzeit auszuwerten, um in Kombination mit anderen Verhaltensdaten der Person zielgerichtet Werbung auszuspielen. Ob diese in Deutschland verbotene Technologie in der Vergangenheit jedoch angewandt wurde, ist zum jetzigen Zeitpunkt nicht bewiesen.⁴

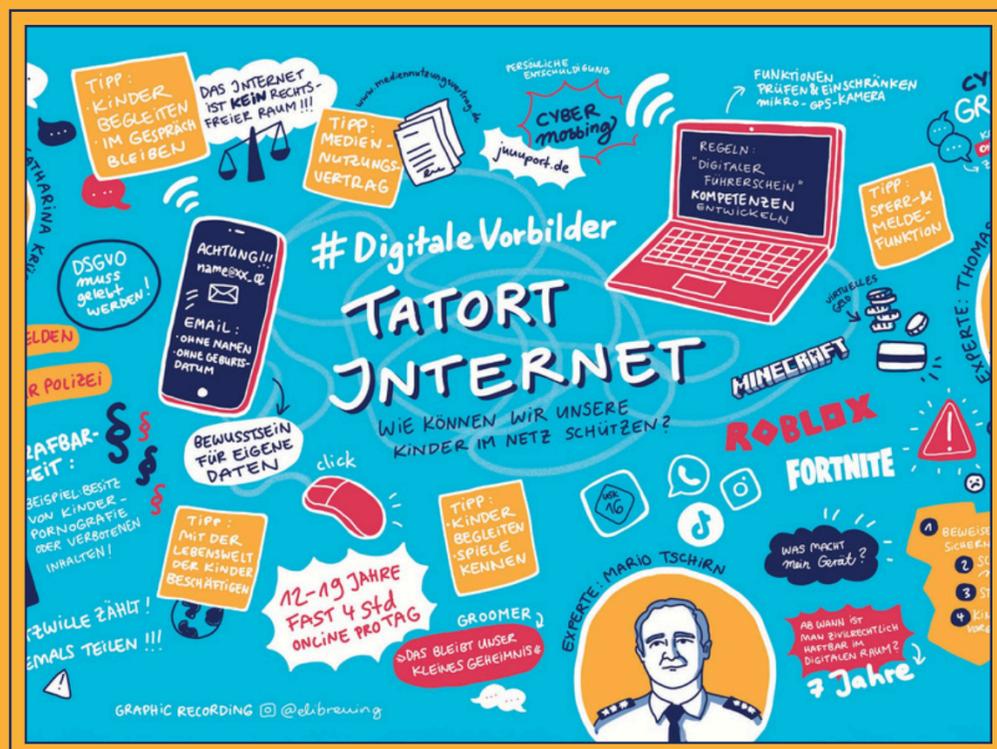


Wer nichts zu verbergen hat, hat auch nichts zu befürchten, oder?





Risikonarrative

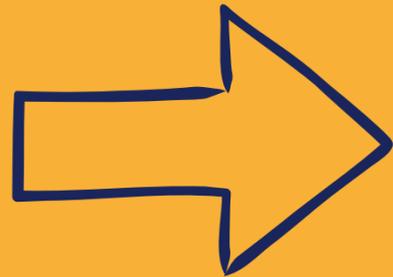


Wie lassen sich Risikonarrative so gestalten, dass sie Dringlichkeit vermitteln, keine Ohnmacht auszulösen, sondern zu Handeln motivieren?

Risikonarrative - Beispiele

Angst und Bedrohung

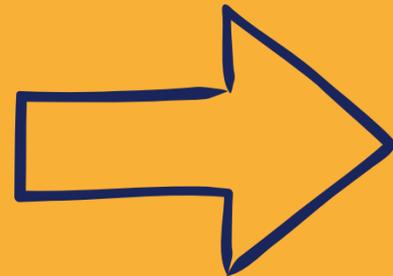
„Kinder sind
ausgeliefert“



„Eltern können aktiv
gestalten“

Empowerment / Verantwortungsframe

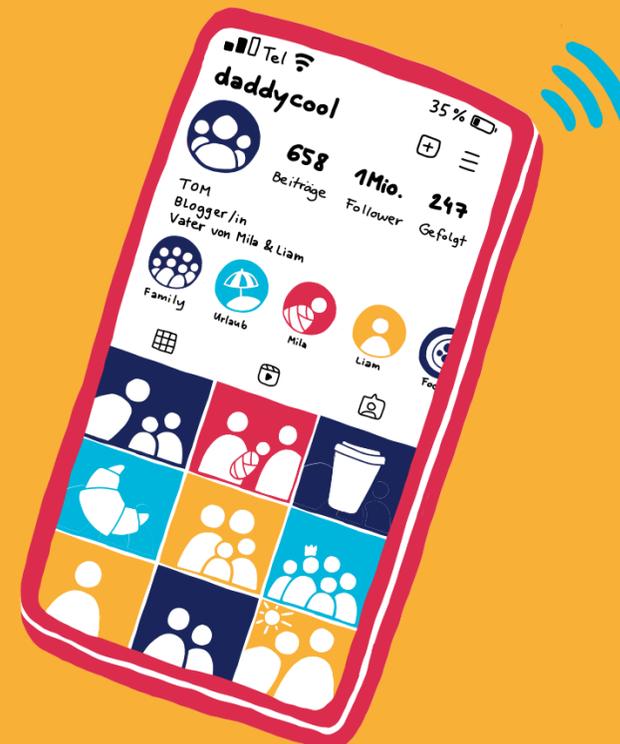
„Eltern verlieren
Kontrolle“



„Eltern als Vorbilder“



Abschluss



Was haben wir nach zwei Jahren Projektlaufzeit gelernt?

Unsere Learnings

Risikonarrative sind unvermeidbar.

Weniger Angst, mehr Selbstwirksamkeit.

Von Bedrohung zu Handlungsperspektive.





Vielen Dank.

Antje Kaiser

Referatsleiterin Presse, Kommunikation und Medienbildung
LfDI Mecklenburg Vorpommern
Kontakt: antje.kaiser@datenschutz-mv.de

Alina Schömig

Referentin Presse- und Öffentlichkeitsarbeit, Medienbildung
HmbBfDI
Kontakt: alina.schoemig@datenschutz.hamburg.de



Weitere Informationen
www.digitale-vorbilder.eu

