Datenmissbrauch und Kostenfallen

Kinder im Internet schützen

– 26.05.2026 –

Jessica Wawrzyniak
Referentin & Autorin für Medien, Bildung & Datenschutz
Erziehungs- und Medienwissenschaftlerin (M.A.)

Wovor schützen wir Kinder & Jugendliche im digitalen Raum?

Vor schlechten Einflüssen

Vor Gefahren für Leib und Seele

Cybermobbing, Hass und Gewalt

sexuelle Anmache (z.B. Cybergrooming/Stalking)

schädliches Umfeld (z.B. Radikalisierung)

Falschnachrichten und Desinformation

Abzocke (z.B. Kostenfallen, In-App-Käufe, Phishing)

Datenanalysen und Manipulation (z.B. Profiling, Werbung)

Gewaltdarstellungen (z.B. in Filmen/Spielen)

u.v.m.

Der Schutz von Daten hilft in allen Bereichen

Daten schützen – Wieso, weshalb, warum?

„Wieso sollte ich meine Daten schützen? Ich hab‘ doch nichts zu verbergen!“

6 Punkte

Besonderer Schutz von Kindern

Erwägungsgrund 38 der DSGVO:

„Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen."

- Heißt: Angebote, die explizit für Kinder sind, unterliegen besonderen Regeln.
- Aber: Kinder nutzen auch Angebote, die nicht explizit für Kinder sind.
- Einwilligung der Eltern nötig (bis zum Alter von 16 Jahren). Kaum Kontrollen.

Bild: Screenshot, Dr. Datenschutz 2025

„Ich hab’ doch nichts zu verbergen!“

Gute Gründe für den Schutz von Daten:

1. Der Schutz von Daten ist ein Grundrecht
2. Andere entscheiden, was wir zu verbergen haben
3. Unsere Persönlichkeit wird analyisiert/manipuliert
4. Unternehmen verdienen Geld mit Daten
5. Polizei und Strafverfolgungsbehörden werten Daten aus
6. Daten können Kriminellen in die Hände fallen

Datenschutz
ist immer
Menschenschutz!

Bild: Tumisu, Pixabay License

Einfalltor: Staatliche Überwachung

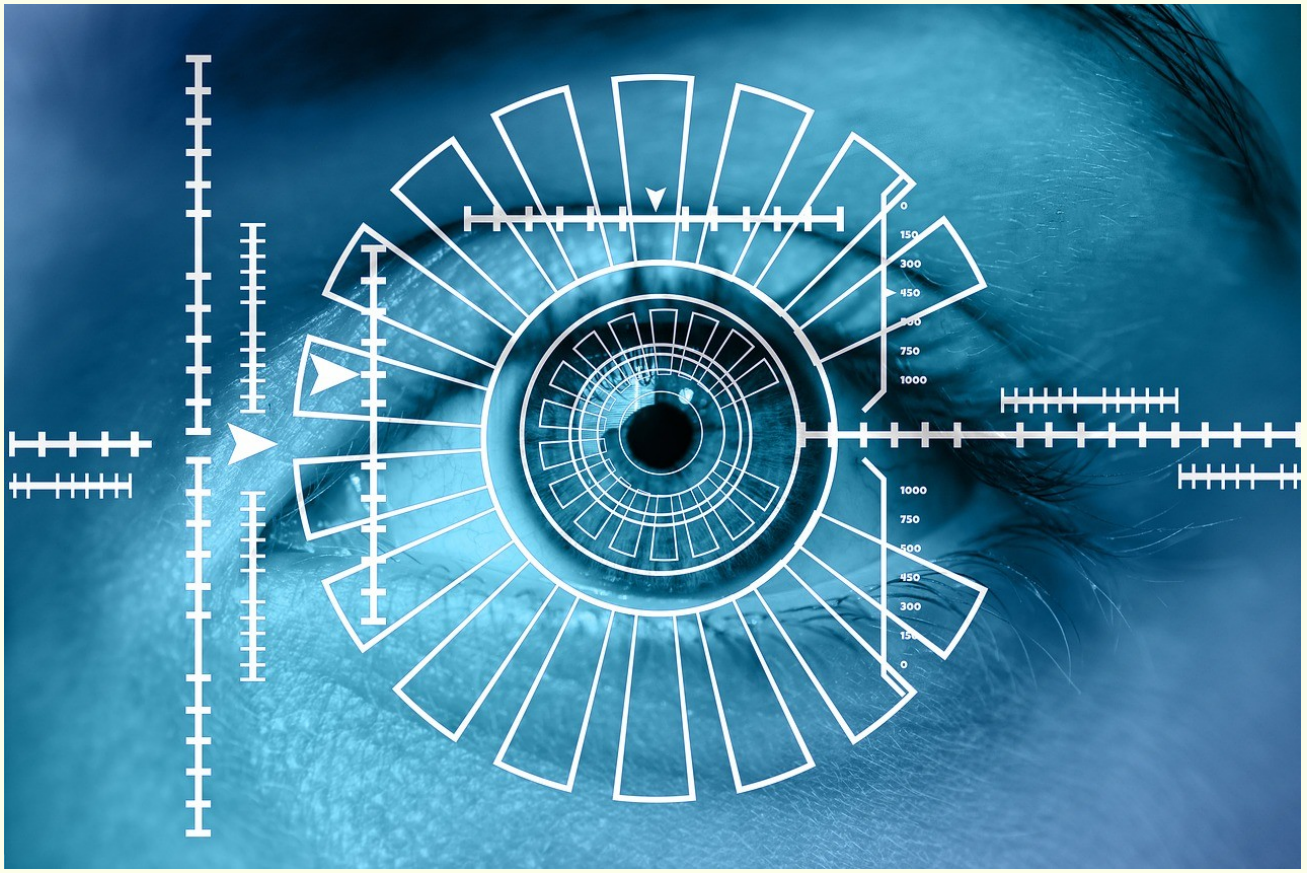


Bild: Gerd Altmann, Pixaybay License

Umstrittene (anlasslose) Überwachung

Anlasslose Massenüberwachung

EU-Datenschutzbeauftragter gegen wahlloses Scannen bei freiwilliger Chatkontrolle

Der europäische Datenschutzbeauftragte verlangt wirksame Schutzmaßnahmen gegen das wahllose massenhafte Scannen bei der freiwilligen Chatkontrolle. Die Ausnahmeerlaubnis für Konzerne wie Meta, Google oder Microsoft dürfe sonst nicht nochmals verlängert werden.

von Constanze 6

Gesetzentwurf

Vorratsdatenspeicherung deutlich länger als drei Monate

Die geplante Vorratsdatenspeicherung von IP-Adressen steht in der Kritik. Die großen Internetanbieter weisen darauf hin, dass die Pläne der Justizministerin zu vielen Monaten Speicherzwang führen würden und daher rechtswidrig sind. Doch schon die eigentlich geplanten drei Monate Speicherpflicht sind mit nichts begründet.

von Constanze 12

Baden-Württemberg

Grüne geben Polizeidaten für Palantir frei

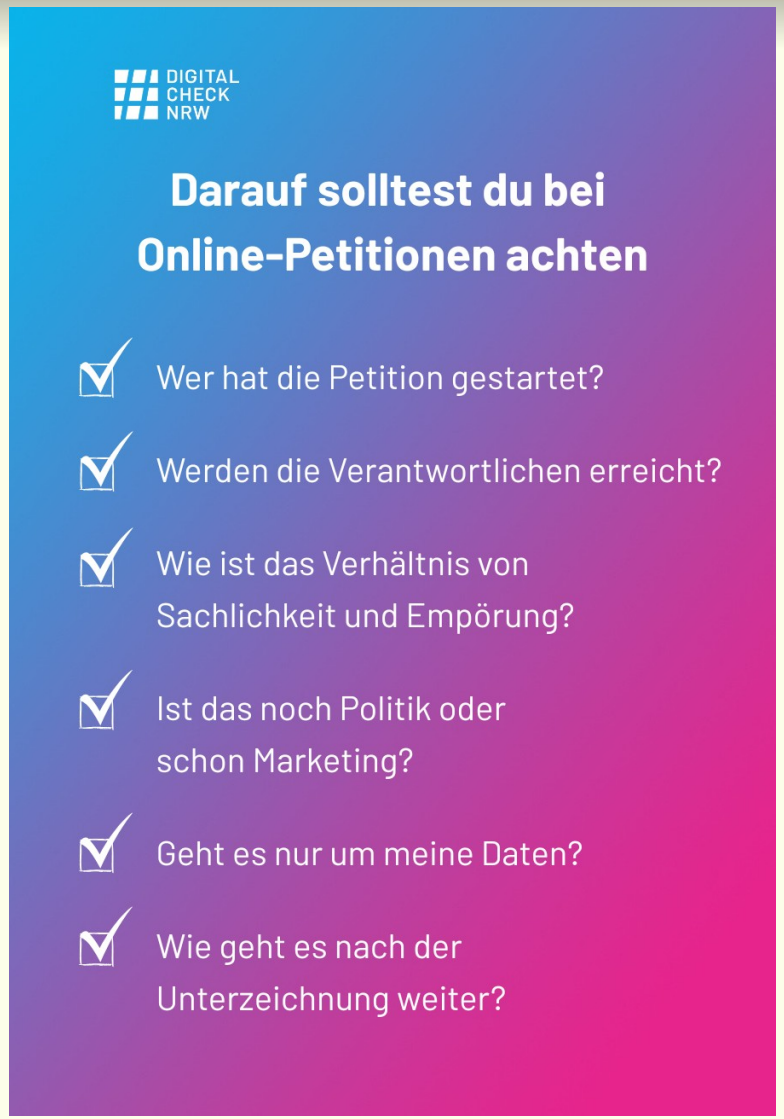
Die grün-schwarze Regierung in Stuttgart winkt die automatisierte polizeiliche Datenanalyse und damit den Einsatz von Software von Palantir durch. Die Grünen machten das nach einem politischen Kuhhandel zu einem Nationalpark möglich. Eine „Experimentierklausel" im Gesetz gibt außerdem polizeiliche Datenschätze für kommerzielle Unternehmen frei.

von Constanze 17

Vorgeschobene Argumente: 1. Terrorismusbekämpfung, 2. Schutz von Kindern

Quelle: https://netzpolitik.org/tag/massenueberwachung/ (25.05.2026)

(Online-)Aktivismus



Petitionen unterschreiben? – Ja, bitte!
Aber **mit Vorsicht**!

Weitere Infos: https://www.digitalcheck.nrw/digital-weiterwissen/uebersicht/artikel/demokratie-online-so-kannst-du-dich-angemessen-beteiligen

Einfalltore für Datensammler

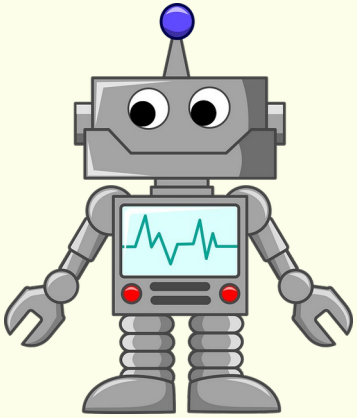
(kommerzielle Überwachung)

Durch Apps & Websites:

z.B. Accounts, AGB, Tracking

Durch das Kinderzimmer:

„Smarte“ Spielzeuge, Apps, usw.



Durch Ängste der Eltern:

Kinderuhren, Tracker am Handgelenk

Durch die Schule:

Da muss jedes Kind hin (Geräte & Programme)

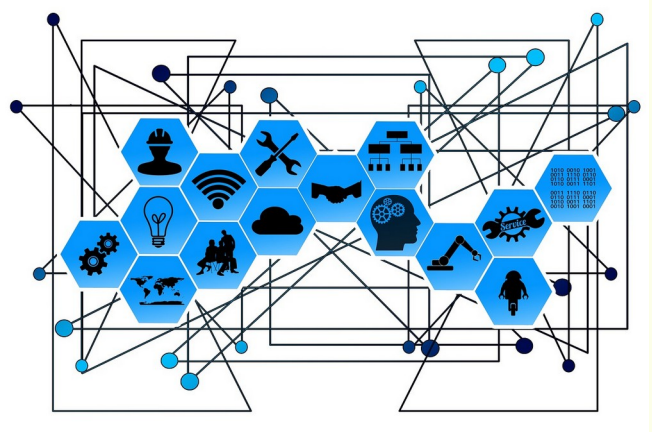
Datensammeln durch Tracking

- durch **Tracking**

  GPS, öffentliches WLAN, Hotspots,...

  Browserfingerabdruck:

  - Surfen auf Websites (Cookies)
  - Nutzung von Suchmaschinen
  - Geräteinformationen



- durch **Fremdzugriff**

  Zugriff über AGB, App-Berechtigungen, Tracking, usw. sind **KEIN** Fremdzugriff, wenn wir sie erlaubt haben

Webseiten selbst prüfen

Webbkoll

(webbkoll.dataskydd.net)

Bilder: Screenshots, webbkoll, 24.03.25

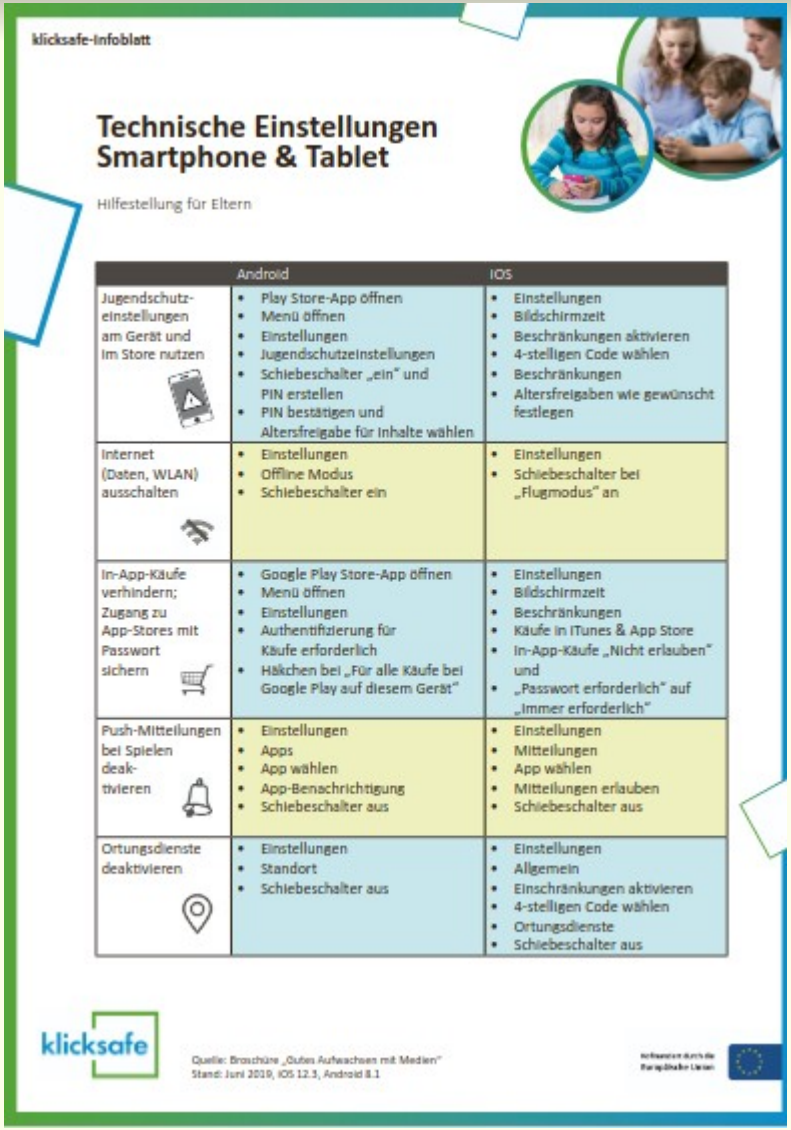
Apps selbst prüfen

Exodus Privacy (Android) | Tracker Control (iOS)

reports.exodus-privacy.eu.org/de/
ios.trackercontrol.org

Bilder: Screenshots, Exodus Privacy, 2021

Weitere Tipps gegen Tracking



klicksafe-Infoblatt

Technische Einstellungen Smartphone & Tablet

Hilfestellung für Eltern

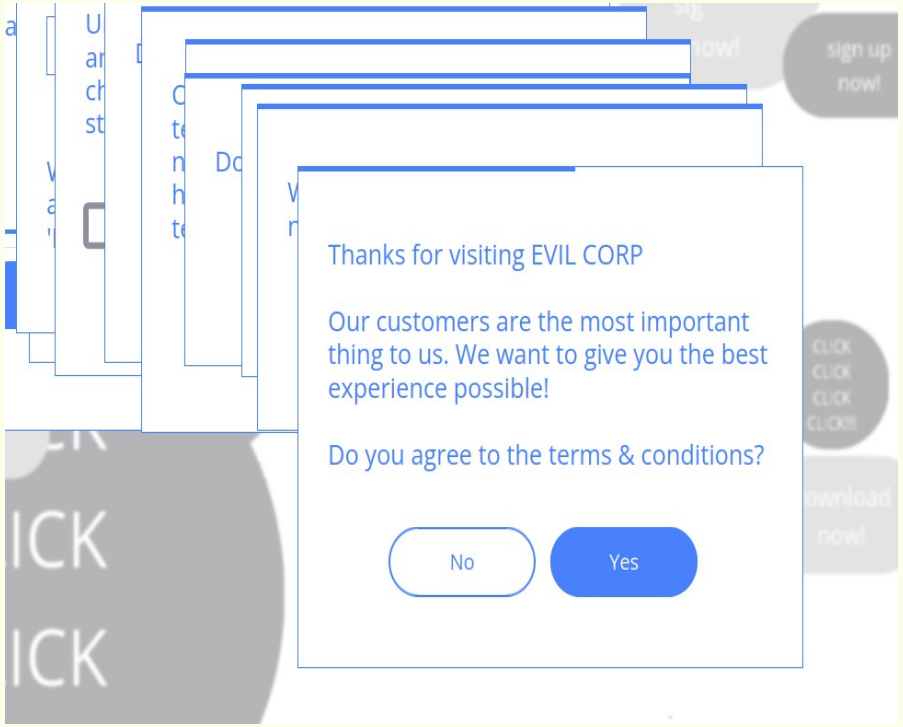
	Android	IOS
Jugendschutz-einstellungen am Gerät und im Store nutzen	• Play Store-App öffnen • Menü öffnen • Einstellungen • Jugendschutzeinstellungen • Schiebeschalter „ein“ und PIN erstellen • PIN bestätigen und Altersfreigabe für Inhalte wählen	• Einstellungen • Bildschirmzeit • Beschränkungen aktivieren • 4-stelligen Code wählen • Beschränkungen • Altersfreigaben wie gewünscht festlegen
Internet (Daten, WLAN) ausschalten	• Einstellungen • Offline Modus • Schiebeschalter ein	• Einstellungen • Schiebeschalter bei „Flugmodus“ an
In-App-Käufe verhindern; Zugang zu App-Stores mit Passwort sichern	• Google Play Store-App öffnen • Menü öffnen • Einstellungen • Authentifizierung für Käufe erforderlich • Häkchen bei „Für alle Käufe bei Google Play auf diesem Gerät“	• Einstellungen • Bildschirmzeit • Beschränkungen • Käufe in iTunes & App Store • In-App-Käufe „Nicht erlauben“ und • „Passwort erforderlich“ auf „Immer erforderlich“
Push-Mitteilungen bei Spielen deak-tivieren	• Einstellungen • Apps • App wählen • App-Benachrichtigung • Schiebeschalter aus	• Einstellungen • Mitteilungen • App wählen • Mitteilungen erlauben • Schiebeschalter aus
Ortungsdienste deaktivieren	• Einstellungen • Standort • Schiebeschalter aus	• Einstellungen • Allgemein • Einschränkungen aktivieren • 4-stelligen Code wählen • Ortungsdienste • Schiebeschalter aus

klicksafe

Quelle: Broschüre „Guten Aufwachsen mit Medien“
Stand: Juni 2019, iOS 12.3, Android 8.1

https://www.klicksafe.de/materialien/technische-einstellungen-smartphone-tablet

Cookie-Banner-Spiel



https://termsandconditions.game/

Bild: Screenshot, termsandconditions 2023

Gute Gründe gegen das Sammeln von Daten an Schulen

Stadt Speyer

Hackerangriff auf Schul-IT in Speyer – Untersuchungen dauern an

Auf die schulinternen Server der allgemeinbildenden Schulen und der Berufsbildenden Schule in Speyer hat es in der vergangenen Woche einen...

20.01.2025

BR

Cyberattacke: Hacker verschlüsseln Schul-Daten

Hacker haben die Daten von sieben weiterführenden Schulen im Landkreis Kitzingen teilweise verschlüsselt. Die Schulen können aktuell nicht...

28.10.2024

Das Recht auf informationelle Selbstbestimmung macht keine Ausnahmen für Schulen

Ist alles gut, was aus der Schule kommt?

- Großkonzerne wittern ihre Chance: Wirtschaftliche Interessen:
  Geld + Daten = **Geld + Geld**.

- Die Algorithmen („Erfolgsrezepte“) bleiben geheim. Wissen und Handwerk werden nicht geteilt.

- Die Wechselkosten, um auf andere Systeme umzusteigen, sind viel zu hoch („Lock-in-Effekt“).

- Firmen haben ein Eigeninteresse, Kinder früh an ihre Produkte heranzuführen. Das bleibt hängen. Was aus der Schule kommt, muss gut sein.

Fälle Datenmissbrauch durch Smart Toys

Beispiele:

- **Sprechende Puppe „My Friend Cayla“**

  → 2017:ungesicherte Bluetooth-Verbindung: Fremde konnten im Kinderzimmer mithören und über das Mikro mit dem Kind sprechen. Vernichtung der Puppe Pflicht (Spionagewerkzeug).

- **Hackerangriff auf VTech**

  → 2015: Über 5 Millionen Nutzerkonten geklaut: Namen, Geschlecht, Geburtstdatum, Porträtfotos, Chatverläufe und Sprachnachrichten der Kinder. Außerdem: E-Mail-Adressen, Passwörter, IP-Adressen, Anschriften und die Download-Historie der Eltern.

- **Datensammlung der Toniebox**

  → 2024: Studien der Uni Basel belegen, dass sich durch das detaillierte Nutzungsverhalten die Entwicklung von Kindern nachvollziehen lässt. Ungesicherte Übertagung. Offline gespeicherte Daten werden vermutlich später online nachgeladen.

Quelle: My Friend Cayla: https://www.zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-bundesnetzagentur, Vtech: https://www.zeit.de/digital/datenschutz/2015-12/hacker-vteck-spielzeug-datensicherheit
Toniebox: https://www.heise.de/news/Studie-Smarte-Kinderspielzeuge-haben-oft-mangelhaften-Datenschutz-9847746.html

Digitales Kinderzimmer (Smart Toys)

- Erst überlegen, dann das Kleingedruckte lesen, dann kaufen
  - Mindestmaß an IT-Sicherheit bedenken
  - Seriöse Hersteller informieren darüber
- Wo immer möglich: Daten sparen
  - Geräte offline nutzen, falls möglich. Ansonsten: Zeitlich begrenzt freischalten
  - Account: Minimum an Daten eintragen
  - Speicherung von Audios, Fotos und Videos lokal (nicht in Clouds)
- Produkte aus der EU bevorzugen (DSGVO)

Tipp: Internetrecherche, z. B. bei Verbrauchenzentralen und Bundesnetzagentur

Kinder-Smartwatches

Computer Bild

Smartwatches für Kinder: Hacker haben einfaches Spiel!

Die Verbraucherschutzbehörde überprüfte zusammen mit dem IT-Unternehmen Mnemonic die Sicherheit von vier Smartwatches für Kinder. Konkret...

23.10.2017

CHIP

Alarmierende Sicherheitslücken: Hacker können über Spielzeug Kinder kontaktieren

Eltern sollten jetzt aufpassen, wenn es um Kinderspielzeug geht. Experten haben Sicherheitslücken entdeckt, die von Hackern ausgenutzt...

05.03.2024

Produktwarnungen

Sicherheit von Kinderprodukten: Jedes vierte Produkt für Kinder ist mangelhaft

Produkte für Kinder sind in Deutschland besonders unsicher. Die Stiftung Warentest hat ihre Tests von Kinderprodukten aus den Jahren 2017...

06.12.2018

„Der Schutzengel am Handgelenk!“

„Keine Chance für Entführer!“

„Beschützen Sie Ihr Kind!“

Sichere Passwörter

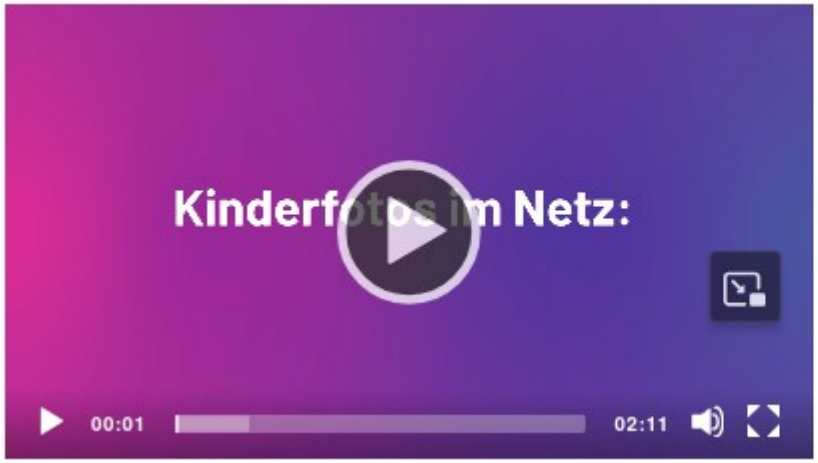
checkdeinpasswort.de

Bitte nur zum Üben mit Kindern nutzen und keine echten Passwörter eintragen!

Bild: Screenshot, checkdeinpasswort.de

Kein Einfalltor, sondern offene Tür für Datenmissbrauch mit Sondereinladung

Kinderfotos im Netz



Kinderfotos im Netz – Darum ist Vorsicht wichtig!

Fotos und Videos von den eigenen Kindern zu machen gehört für viele Familien zum Alltag. Trotzdem ist es wichtig, einen Moment innezuhalten und vorm Hochladen in den WhatsApp-Status oder posten in Social Media bewusst zu überlegen: Was sind gute Gründe, um keine Bilder von Kindern ins Internet zu stellen. Im Video erfahrt ihr mehr.

https://www.digitalcheck.nrw/digital-weiterwissen/uebersicht/erklaervideos

Kostenfallen

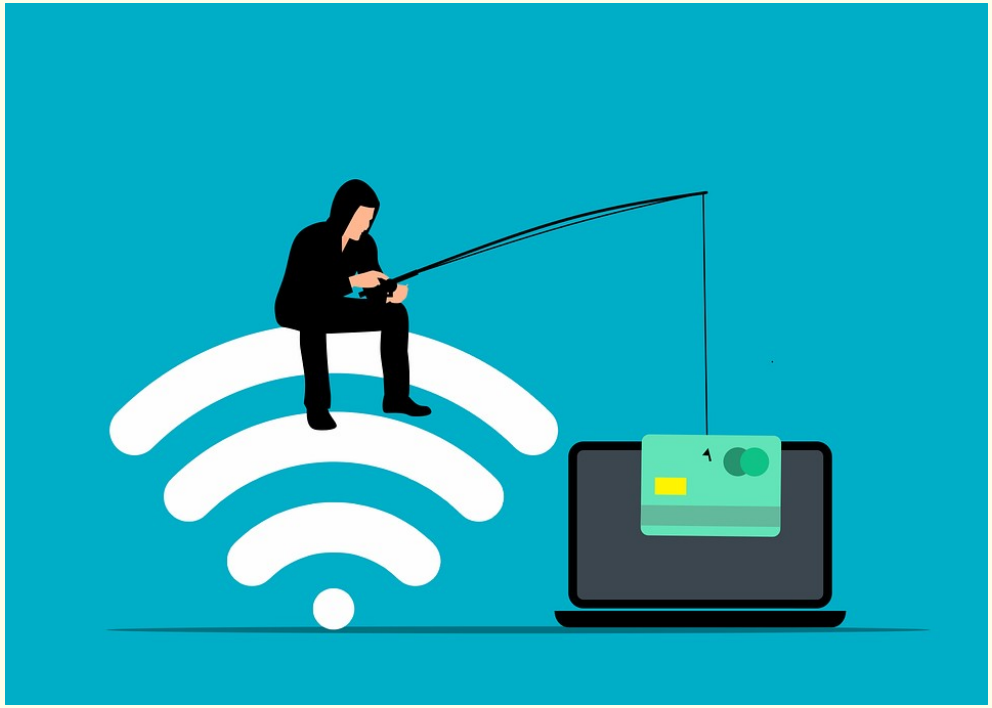
Was können Eltern tun?

- Technische Schutzmechanismen (Budgetlimits, Kinderkonten, Zwei-Faktor-Authentifizierung) sind keine Option, sondern eine Pflicht

  Anleitung für Einstellungen am Smartphone zu In-App-Käufen:
  https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/inappkaeufe-deaktivieren-bei-ios-und-android-so-gehts-13532

- Regelmäßige Kontrollen von Kaufbestätigungen und Abrechnungen wird als Mindestmaßnahme von Eltern erwartet
- Mündliche Absprachen mit Kindern reichen nicht aus, um die Haftung abzulehnen (auch nicht prüfbar)

Phishing erkennen

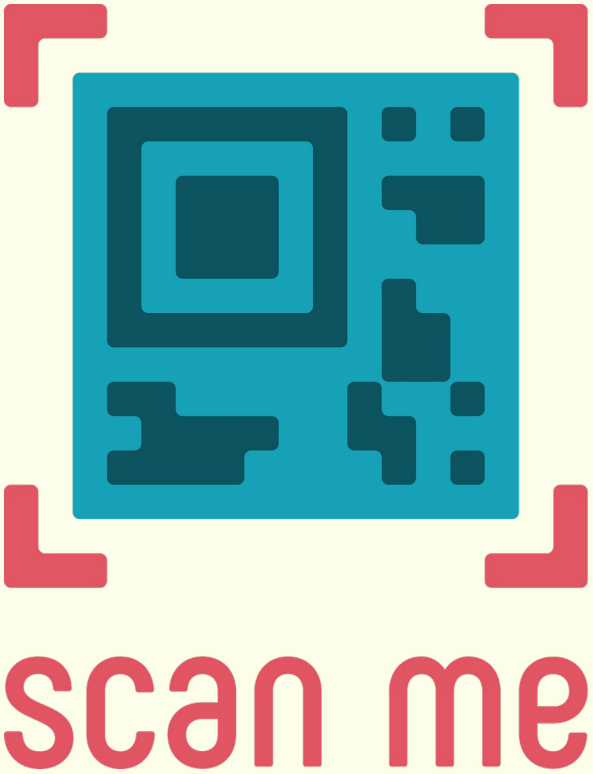


1. Von wem kommt die Mail?
2. Anrede korrekt?
3. Rechtschreibfehler?
4. Aufforderung, Daten einzugeben?
5. Wird Druck gemacht?

Gemeinsam mit Kindern üben:
Links prüfen, ohne sie anzuklicken!

QR-Codes prüfen

- Finden sich ÜBERALL
- Oft überklebt,
  ausgetauscht
- Schadcode oder
  Werbung integriert
- Erst den Link prüfen
  dann erst öffnen
- Qr-Code-Rader wie
  „Binary Eye“ nutzen.



Ratgeber: Screen Teens

Sie brauchen nicht jede einzelne App zu kennen und können nicht jeden einzelnen Fallstrick vorhersehen. Lassen Sie sich nicht beunruhigen, wenn die Medienerziehung der anderen spielerisch leicht aussieht – andere Eltern stehen vor denselben Herausforderungen wie Sie. Geben Sie Ihrem Kind Werte und Rüstzeug auf den Weg, die es online wie offline gebrauchen kann.

Jessica Wawrzyniak

KÖSEL

Screen Teens – Wie wir Jugendliche in die digitale Verantwortung begleiten

Und wie erreichen wir nun den besten Schutz?

- **Mitdenken**

  → Wo gebe ich Daten preis? Lohnt es sich wirklich, diese Daten bekannt zu geben?

- **Trainieren Sie Datenschutzeinstellungen immer gemeinsam**

  → Einstellungen am Gerät und in jeder einzelnen App. Damit werden keine Einsen und Nullen geschützt, sondern die Kinder selbst.

Bild: tanrica, Pixabay License

Gibt es noch Fragen?

Vielen Dank!

Kontakt:

Jessica Wawrzyniak

Mail:
medien.wawrzyniak@posteo.de

Website:
medien-wawrzyniak.info

Infos für Kinder, Jugendliche und Eltern

- www.juuuport.de
- www.handysektor.de
- www.klicksafe.de
- www.blinde-kuh.de
- www.buendnis-gegen-cybermobbing.de
- www.lizzynet.de

Weitere Literatur-Tipps:
https://www.medien-wawrzyniak.info/empfehlungsecke/

Zum Ausprobieren	Zum Lesen	Zum Spielen
(Websites & praktische Tools)	(Bücher, Broschüren & Unterrichtsmaterial)	(Aufklärende Quiz- & Browser-Spiele)

Meine Schwerpunkte

Eltern

Erziehung zur digitalen Mündigkeit unterstützen

Kontrollwahn & Überwachung von Kindern gegenlenken

Meine Schwerpunkte

Kinder

Datenschutz leicht verständlich vermitteln

gesellschaftliche, politische und wirtschaftliche Zusammenhänge erklären

Meine Schwerpunkte

Schulen
Wie kann guter Datenschutz aussehen?
Wer ist verantwortlich? Was ist zu tun?