Leitfaden zur Medienkompetenz

Diese Zusammenstellung an Informationen ist aus dem Projekt „Medienkompetenz“ des MGF entstanden.

1. Allgemeines zur Internetnutzung

a. Cyberkriminalität
- Kriminalität im Internet, die auch genauso bestraft wird wie „normale“ Kriminalität
- 87.000 Fälle im Jahr 2021, also keine Randerscheinung
- Social engineering: Manipulation von Usern durch Fake E-Mails, Accounts
- Cyber-Spionage durch Smart Speaker wie Alexa und Siri u.a.: Datenmissbrauch

b. Datenschutz
- Zur Info: Ca. 75% der Apps auf unseren Smartphones greifen auf unsere Daten zu.
- AGB lesen, obwohl sie sehr lang sind und es langweilig ist.
- Evtl. auf Installation der App verzichten

c. Urheberrecht
- Das Recht auf das eigene Bild: Vor dem Hochladen Einverständnis holen!
- Unbedingt Quellenangabe bei Fotos aus dem Internet (lizenzfrei?)!
- Aktuelle Kinofilme sind urheberrechtsgeschützt.
- Ein Verstoß stellt eine Straftat dar.

d. Hasskommentare
- Täter verstecken sich hinter Anonymität: ungehemmt und verletzend
- Standort kann aber ausfindig gemacht werden.
- Wenn man betroffen ist, sich mit anderen austauschen und Account dem Anbieter melden.
- Evtl. Anzeige erstatten.

e. Erst denken, dann klicken
- Seriosität der Internetseite überprüfen.
- Vorgegebene Links nicht unbedacht anklicken.
- Beim Posten von Bildern überlegen, ob ich gegen kein Recht verstoße und ob ich wirklich will, dass das gesehen wird. (Frage: Will ich das im echten Leben auch zeigen? Will ich das meinen Eltern zeigen?)
- Beim Download auf Quelle achten und „Neben-Downloads“ verhindern.

(Quelle: https://www.klicksafe.de/materialien/felix-michels-alias-tomatolix-so-wirst-du-zum-internet-profi, zuletzt aufgerufen am 25.07.2022)

2. Regeln für den Klassenchat

- Sinn: Hilfestellung bei Krankheit, Hausaufgaben oder wenn man etwas nicht verstanden hat.
- Auf diese Funktion beschränken!
  Das bedeutet:
  - Keine Nachrichten während des Unterrichts!
  - Nicht rund um die Uhr senden!
  - Keine Hausaufgabenlösungen (bringt nichts!)!
  - Keine Privatnachrichten!
  - Kein Spam von Stickern, Videos, Bildern, Links oder Nachrichten!
  - Keine Kettenbriefe weiterleiten!
  - Keine Beleidigungen!

3. Social Media: Welche Fotos lade ich hoch?

- Hintergrund: Was kann man erkennen?
- Sich nur so zeigen, wie man sich auch in der Öffentlichkeit zeigen würde.
- Wer kann das Foto sehen?
  Achtung: Auch beim Privat-Account kann Missbrauch betrieben werden: Anbieter hat evtl. Nutzungsrechte an Bild (AGBs gelesen?). Auch kann der Post von anderen weitergeleitet werden (Privatsphäreeinstellungen!).
- Kann das Bild negative Folgen in der Zukunft für mich haben (z.B. bei der Jobsuche)?
- Habe ich die Rechte an dem Bild abgeklärt?
- Was ist mit Hashtags und Kommentaren dazu?

4. Wie schütze ich mich vor Gefahren?

a. Challenges: NICHT ALLE sind harmlos!
   - Sie sind meist harmlos und können Spaß machen.
   - Aber: Es muss ein Gefahrenbewusstsein vorhanden sein (z.B. Würge- oder Luftanhalten-Challenges haben zu mehreren Todesfällen geführt!)

b. Bloßstellung durch Sexting
   - Definition: „Sexting ist ein Kofferwort, bestehend aus den Wörtern „Sex“ und „Texting“. Es beschreibt das Versenden und Empfangen selbstproduzierter, freizügiger Aufnahmen via Computer oder Smartphone. Unter Jugendlichen sind auch die Begriffe "Pics" oder "Nudes" gebräuchlich.“
     (Quelle: https://www.klicksafe.de/sexting#c50421, zuletzt aufgerufen am 25.07.2022)
   - Nicht die Person, die sich fotografiert, trägt Schuld, sondern die, die es missbraucht.
     Dennoch: Man sollte sich vorab gut überlegen, ob man ein solches Foto digital verschickt. Kann man der Person absolut vertrauen? Was ist, wenn die Beziehung beendet wird und Gefühle evtl. verletzt worden sind?
   - Hat der Anbieter der App ein Recht an meinem Bild (s. AGBs!)?
   - Das Bild/Video wird evtl. ohne mein Wissen weitergeleitet!

- Wenn es in die falschen Hände gerät, kann es zu Erpressung, Bloßstellung und Mobbing führen!

c. Missbrauch durch Pädophilie bei Cybergrooming
   - Definiton:
     „Cybergrooming bezeichnet die Anbahnung von sexueller Gewalt gegen Minderjährige im Internet. Das englische Wort „Grooming" bedeutet „Striegeln" und steht metaphorisch für das subtile Annähern von Täter*innen an Kinder und Jugendliche. Cybergrooming ist gekennzeichnet von bestimmten Täter*innen-Strategien, die sich oft ähneln. Ihnen allen liegt zugrunde, dass die Unbedarftheit, die Vertrauensseligkeit und das mangelnde Risikobewusstsein von Kindern und Jugendlichen ausgenutzt wird. Oft versuchen die Täter*innen ein Vertrauens- oder Abhängigkeitsverhältnis herzustellen, um ihre Opfer manipulieren und kontrollieren zu können."
     (Quelle: https://www.klicksafe.de/cybergrooming, zuletzt aufgerufen am 26.07.2022)
   - Achtung! Vorsicht ist in den folgenden Situationen geboten:
     - Jemand will sich offline mit dir treffen.
     - Jemand will wissen, wo du wohnst (Auch deine IP-Adresse kann abgegriffen werden, indem du Links anklickst. Damit kann er/sie deinen Standort ausfindig machen, sogenannte IP-Grabber.)
     - Jemand stellt dir sehr persönliche Fragen.
     - Jemand möchte Fotos von dir (später auch freizügige).
     - Jemand bittet dich, deine Web-Cam anzustellen.
     - Jemand fragt dich nach deiner Telefonnummer oder will in einen privaten Chat wechseln.
     - Jemand bittet dich, nichts anderen zu erzählen.
     - Jemand bietet dir Geschenke an.

5. Umgang mit Fake News und Verschwörungstheorien

- Definition: gezielt eingesetzte Fehlinformationen durch Manipulation von Tatsachen bis hin zu kompletten Falschmeldungen
- Zweck: Man will damit andere von seiner eigenen Position durch Manipulation beeinflussen, um so Stimmung für oder gegen bestimmte Themen, Personen, Gruppen oder Organisationen zu machen.
- Gefahr: Diese Fehlinformationen werden dazu eingesetzt, um politische Entscheidungen zu manipulieren, um gesellschaftliche Gruppen wie z.B. Asylbewerber schlecht zu machen und damit auszugrenzen, um Verschwörungstheorien zu verbreiten.
- Formen der Manipulation:
  - Bilder werden zusammengeschnitten, um Straftaten schlimmer darzustellen oder Personen in einem schlechten Licht erscheinen zu lassen.
  - Falsche „Zitate" werden Menschen zugeordnet, z.B. berühmten Persönlichkeiten, um überzeugender zu wirken.
  - Bilder werden durch Bildbearbeitungsprogramme verändert oder mit falschen Bildunterschriften versehen, um den Ruf von Personen zu beschädigen.
  - *Deep Fake*: Programme (KI) werden eingesetzt, um in Videos Gesichtsbewegungen auf andere Personen zu übertragen und ihnen so Worte in den Mund zu legen, die sie nie gesagt haben.

- *Filterblasen*: Informationen werden auf mein Profil zugeschnitten und mir werden basierend auf meinem Standort, meinem Klickverhalten und meiner Suchhistorie gefilterte Informationen angeboten. „Also sieht die Person nur bestimmte, vielleicht ähnliche Angebote, Texte oder Webseiten zu einem Thema. Es ist wie in einer kleinen Blase. Andere Angebote, Texte oder Webseiten werden dieser Person also gar nicht angezeigt. Texte mit anderer Meinung sieht diese Person dann auch nicht."

  (Quelle: https://www.bpb.de/kurz-knapp/lexika/lexikon-in-einfacher-sprache/303050/filterblase/, zuletzt aufgerufen am 26.07.2022)
- Die Wirkung von *Echokammern*: „Eine Echokammer beschreibt das Phänomen, dass der Großteil der Menschen dazu neigt, sich mit Gleichgesinnten zu umgeben, um sich gegenseitig in einem geschlossenen Raum in der eigenen Position zu verstärken. Dies geschieht dadurch, dass Überzeugungen durch Kommunikation und Wiederholung im geschlossenen Raum vertieft und gefestigt werden."

  (Quelle: https://norbert-pohlmann.com/glossar-cyber-sicherheit/echokammer/, zuletzt aufgerufen am 26.07.2022.)
- Fake News verbreiten sich rasend schnell durch Likes, Kommentare oder die Teilen-Funktion und manipulieren so Menschenmengen in Windeseile.
-

<u>Wie kann ich Fakten checken, was kann ich tun, um nicht auf Fake News hereinzufallen?</u>

a. <u>Überschriften und Fotos</u>
   - Super reißerische Überschriften, die oftmals wenig mit dem Text zu tun haben.
   - Veränderte oder nicht aktuelle Fotos oder Fotos, die überhaupt nichts damit zu tun haben.

b. <u>Quelle</u>
   - Sind Quellen angegeben (Link)? Erscheint die Quelle seriös? Quelle nachverfolgen!

c. <u>Fakten checken</u>
   - Auf anderen Internetseiten checken, ob diese Meldung auch irgendwo auftaucht.
   - Gibt es auch Meldungen in seriösen Zeitungen dazu?

d. <u>Hinweisen</u>
   - Wenn du eine Nachricht als Fake News entlarvst, weise den/die Verfasser:in respektvoll darauf hin, damit die Nachricht gelöscht und so die Verbreitung verhindert werden kann.

e. <u>Melden</u>
   - Im Extremfall sollte ein Post auch gemeldet werden, z.B. wenn Gefahr droht oder es sich um Hetze und Hass handelt, die sich zu einer Gefahr für eine Person oder einen Personenkreis entwickeln können. Falschmeldungen und Verschwörungserzählungen müssen so nicht stehen bleiben.