Praxisbeispiel Elternabend: Interaktives Schaubild „Was verrät mein Post über mich?“

Das folgende Praxisbeispiel veranschaulicht, wie leicht sich persönliche Daten und private Informationen aus Social-Media-Posts herauslesen lassen. Das Schaubild zeigt einen beispielhaften Social-Media-Post, der viele Gegenstände/Elemente enthält, die Rückschlüsse auf die abgebildete Person zulassen. Mithilfe des interaktiven Schaubilds werden Eltern für den Umgang mit persönlichen Daten und Informationen in Beiträgen auf Social-Media-Angeboten sensibilisiert. Eltern sollen sich über eigene Erfahrungen austauschen und miteinander diskutieren.

Technische Vorbereitung

Material

- Interaktives Schaubild „Was verrät mein Post über mich?“ (Online- oder Offline-Version)
- Leistungsfähiger Laptop oder Computer mit einem gängigen Internet-Browser
- Beamer mit Leinwand oder Smartboard für die Präsentation

Nutzung mit Internetverbindung (Online-Version)

- **Schaubild „Was verrät mein Post über mich?“**

Nutzung ohne Internetverbindung (Download der Offline-Version)

- **Für Windows: Schaubild „Was verrät mein Post über mich?“**
  - Schaubild_Social_Media_Post.zip-Datei herunterladen
  - Schaubild_Social_Media_Poste.zip-Datei entpacken
  - Schaubild_Social_Media_Post.exe starten
- **Für MacOS: Schaubild „Was verrät mein Post über mich?“**
  - Schaubild_Social_Media_Post.dmg-Datei herunterladen
  - Schaubild_Social_Media_Post.dmg-Datei entpacken
  - App bzw. Programm direkt starten oder in Mac-Apps hinzufügen

Inhaltliche Vorbereitung und Einsatz des interaktiven Schaubilds

Hintergrundinformationen zur inhaltlichen Vorbereitung finden Sie in den Dokumenten **„Was sind persönliche Daten?“**, **„Warum ist Selbstdatenschutz wichtig?“**, **„Daten verbergen und schützen“** sowie **„Persönliche Daten und Selbstdatenschutz“** im Bereich „Social Media: Privatsphäre und Selbstdatenschutz“.

Halten Sie das interaktive Schaubild „Was verrät mein Post über mich?“ in der Online- oder Offline-Version bereit, z. B. zur Ansicht über einen Bildschirm/Beamer.

Möglicher Ablauf

- Öffnen Sie das interaktive Schaubild in der 100%-Ansicht.

- Beginnen Sie mit Impulsfragen an die Eltern: „Welche persönlichen Daten kennen Sie?“ (bzw. „Was versteht man unter dem Begriff „persönliche Daten“ und welche sind damit gemeint?“), „Welche Informationen im Bild können Aufschluss über die gezeigte Person geben?“. Bei Klick auf den Info-Button links oben werden in einem Pop-Up die Fragen angezeigt. Sammeln Sie erste Ideen und Antworten der Anwesenden.

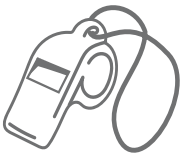
- Suchen Sie nun gemeinsam mit den Eltern nach Informationen, die auf dem Foto zu finden sind. Lassen Sie die Eltern erklären, warum z. B. ein bestimmter Gegenstand Informationen über die gezeigte Person preisgeben kann. Klicken Sie nacheinander auf die gefundenen Elemente. Sobald ein Element angeklickt wurde, wird es per Zoom hervorgehoben. Bei erneutem Klicken verschwindet der gezoomte Ausschnitt und das Element bleibt im Post „markiert“. Durch die optische Hervorhebung aller Gegenstände und Elemente im Bild wird abschließend auf einen Blick deutlich, wie viele Informationen und persönliche Daten ein einziger Social-Media-Post über eine Person preisgeben kann.

- Im Schaubild finden sich acht anklickbare Gegenstände/Elemente, die Rückschlüsse auf persönliche Daten zulassen:
  - **Pokal mit Vereinsname:** Ein Gegenstand wie ein Pokal kann Aufschluss darüber geben, was die Person in ihrer Freizeit macht – z. B. in einem Sportverein einen bestimmten Sport betreiben.
  - **Bekanntes Gebäude/bekannter Straßenname einer bestimmten Stadt:** Eindrücke einer Stadt, z. B. im Bildhintergrund, oder der Blick durch ein Fenster können Aufschluss über den (exakten) Wohnort der Person geben.
  - **Tablettenverpackung:** Eine liegen gelassene Verpackung eines Medikaments kann Rückschlüsse über den Gesundheitszustand oder mögliche Erkrankungen der Person zulassen.

- **T-Shirt mit personalisiertem Aufdruck:** Ein Kleidungsstück kann durch einen (personalisierten) Aufdruck Informationen preisgeben, z. B. über Jahr und Ort des Schulabschlusses oder eine Vereinsmitgliedschaft.
- **Geldbeutel mit verschiedenen Karten:** Ein offener Geldbeutel kann nicht nur den realen Namen einer Person, z. B. über den Personalausweis, sondern ggf. auch weitere sensible Daten wie Konto-, Kreditkarten-, Personalausweis- oder Versichertennummer preisgeben.
- **Foto im Bild von anderen Personen:** Wenn auf Social-Media-Posts Fotos zu sehen sind, die andere Personen zeigen, kann sichtbar werden, mit wem eine Person befreundet oder verwandt ist.
- **Bildunterschrift/-beschreibung:** Die Bildunterschrift eines Beitrags gibt möglicherweise persönliche Daten und andere Informationen preis, z. B. wenn hier Namen, (Wohn-)Ort oder Zeitangaben geteilt werden.
- **Kommentare von anderen Personen in der Kommentarspalte:** Durch Kommentare anderer Nutzerinnen und Nutzer werden möglicherweise weitere Informationen preisgegeben, wenn diese sich auf die Inhalte eines Fotos oder Beitrags beziehen.

- Beginnen Sie eine offene Gesprächsrunde und regen Sie einen persönlichen Austausch der Eltern an. Mögliche Diskussionsfragen:
  - Welche Bilder posten Sie selbst auf Social-Media-Angeboten? Welche Bilder posten Ihre Kinder auf Social-Media-Angeboten (sofern sie diese nutzen)? Besteht ein Unterschied (z. B. ob nur Fotos von Reisen, Landschaften, Gebäuden oder auch von sich selbst und anderen Personen gepostet werden)?
  - Haben Sie mit Ihrem Kind Regeln aufgestellt, was es posten darf und was nicht?
  - Fanden Sie schon ein mal ein Bild oder einen Post einer Ihnen bekannten Person zu persönlich? Wenn ja, warum?
  - Welche Probleme können sich durch die Preisgabe persönlicher Daten ergeben?

- Besprechen Sie mögliche Handlungsoptionen und Tipps für den eigenen Alltag. Anregung bieten die beiliegenden **„Handlungstipps"**. Die Tipps finden Eltern auch im Bereich „Social Media: Privatsphäre und Selbstdatenschutz".



Handlungstipps

Wert von persönlichen und privaten Daten besprechen und klare Regeln vereinbaren

Erklären Sie Ihrem Kind den Wert von privaten Daten. Besprechen Sie gemeinsam, dass Daten auch missbraucht werden können, z. B. für unerwünschte Werbung und Spam, für Belästigung und Mobbing oder sogar Identitätsdiebstahl. Um Missbrauch zu vermeiden, können gemeinsame Regeln helfen, z. B. welche Daten geteilt werden oder welche Personen sie sehen dürfen. Machen Sie Ihrem Kind deutlich, dass es personenbezogene und persönliche Daten nicht ohne Rücksprache mit Ihnen herausgeben sollte.

Über AGB und Altersfreigaben von Social-Media-Angeboten informieren

Beim ersten Anmelden in Social-Media-Angeboten ist es wichtig, sich mit den Allgemeinen Geschäftsbedingungen (AGB) zu beschäftigen. Die wichtigsten Punkte sollten Sie mit Ihrem Kind besprechen. Erkundigen Sie sich z. B. vorab, ab welchem Alter das jeweilige Social-Media-Angebot genutzt werden darf. Viele Angebote geben ein Mindestalter vor. AGB sind jedoch in der Regel nicht sehr nutzerfreundlich aufbereitet – sehr lang, kompliziert geschrieben und schwer verständlich. In der **„Linkliste: Weiterführende Informationsangebote“** finden Sie für verschiedene Social-Media-Angebote die „Nutzungsbedingungen kurzgefasst“ von handysektor. Dort sind die wichtigsten Punkte übersichtlich aufbereitet. Die Betreiber können die AGB auch ändern. Daher kann es helfen, regelmäßig nachzusehen. Besprechen Sie mit Ihrem Kind, dass es Sie informiert, wenn der Anbieter auf AGB-Änderungen hinweist.

Möglichst wenig Daten preisgeben

Wer sich ein Profil in Social-Media-Angeboten anlegt, gibt in der Regel viele persönliche Daten an. Dabei ist es wichtig, nur die nötigsten Angaben zu machen. Angaben, die wirklich notwendig sind, sind mit einem „*“ gekennzeichnet. Vor allem persönliche Daten wie Nachname, Adresse, Geburtsdatum und Telefonnummer sollte man nur angeben, wenn sie für die Nutzung des Profils gebraucht werden. Auch der gewählte Nickname sollte keine Hinweise auf das Alter oder den Nachnamen enthalten.
Tipps, wie sich persönliche Daten verhüllen lassen, finden Sie im Bereich „Privatsphäre und Selbstdatenschutz“ in der **„Checkliste: Daten verbergen und schützen“**.

Alternative Angebote wählen

Fragt ein Angebot zu viele persönliche Daten ab, können Sie gemeinsam mit Ihrem Kind überlegen, ob es das Angebot wirklich nutzen muss. Manchmal finden sich zu bestimmten Angeboten auch datensparsame Alternativen. Ganz allgemein gilt bei der Preisgabe der eigenen Daten die Faustregel: Weniger ist mehr. Daten, die nicht online stehen, können nicht so leicht missbraucht werden.

Zugriffsrechte von Apps beschränken

Bei der Installation und, je nach Betriebssystem, auch danach können Sie die Zugriffsrechte von Apps einschränken, z. B. das Taggen von Fotos mit GPS-Daten. Generell ist es sinnvoll, vor der Installation zu prüfen, auf welche Daten eine App zugreift und ob sie diese Zugriffsrechte wirklich benötigt. Falls eine App zu viele Zugriffsrechte fordert, können Sie überlegen, ob die App wirklich genutzt werden soll.

Privatsphäre-Einstellungen von Angeboten nutzen und regelmäßig überprüfen

Die meisten Social-Media-Angebote haben eigene Privatsphäre-Einstellungen. Z. B. kann man seine Daten vor der Öffentlichkeit verbergen und nur für ausgewählte Personen (den „Freunden“) sichtbar machen. Diese Einstellungen können bei der Weiterentwicklung eines Angebotes aber verändert werden, ohne dass die Nutzerinnen bzw. Nutzer informiert oder um ihre Einwilligung gebeten werden. Daher ist es wichtig, die Einstellungen regelmäßig zu überprüfen und bei Bedarf neu anzupassen. Privatsphäre-Einstellungen bieten zwar keinen 100-prozentigen Schutz vor Datenmissbrauch, doch das Risiko wird eingedämmt. Die Privatsphäre-Leitfäden von **saferinternet.at** u. a. für Snapchat, TikTok oder Instagram zeigen in Schritt-für-Schritt-Anleitungen, wie Sie mögliche Sicherheitseinstellungen vornehmen können.

Datenmissbrauch melden

Sind Sie oder Ihr Kind einem Datenmissbrauch zum Opfer gefallen, können Sie das beim jeweiligen Anbieter melden und dagegen vorgehen. Dafür sollten Sie Beweise sichern, z. B. mittels eines Screenshots. Bei Datenmissbrauch können Sie sich z. B. an die **Verbraucherzentrale** wenden. In schweren Fällen wie Identitätsdiebstal sollte Anzeige bei der **Polizei** gestellt werden.