Warum ist Selbstdaten-schutz wichtig?

Preisgabe von Daten thematisieren

Viele Angebote im Internet, z. B. Social-Media-Angebote, ermöglichen es, sich selbst darzustellen, mit anderen auszutauschen und sich zu vernetzen. Wer die Angebote nutzen will, gibt persönliche Daten preis. Schon bei der Anmeldung werden viele Daten abgefragt. Auch bei eigenen Beiträgen im Profil wollen Nutzerinnen und Nutzer, oft möglichst viele verschiedene Dinge von sich und dem eigenen Leben zeigen, um interessant zu wirken. Daher geben sie oft persönliche Daten preis, die man in einem persönlichen Gespräch oder einer anderen Alltagssituation eher vertraulich behandeln würde. Der Zwiespalt zwischen Selbstdarstellung und Schutz der Privatsphäre ist für viele Kinder und Jugendlichen eine Herausforderung. Negative Konsequenzen, wenn Fremde auf ihre Daten zugreifen, sind ihnen oft nicht bewusst. Daher sollten Eltern sowohl beim eigenen Umgang mit Social-Media-Angeboten auf ihren Datenschutz achten und gleichermaßen auch ihre Kinder für das Thema sensibilisieren.

Persönliche Daten – ein gutes Geschäft

Persönliche Daten sind wie Gold für die Betreiber von Social-Media-Angeboten. Marktdatenhändler, Internet-Tracking-Unternehmen und die Werbewirtschaft freuen sich über wertvolle Daten der einzelnen Nutzerinnen und Nutzer, wie Wohnort, Hobbys, Nutzungsgewohnheiten und vieles mehr. Der Verkauf der Daten bringt den Anbietern viel Geld. Ein Indiz, dass eigene Daten verkauft wurden, ist etwa eine plötzliche Flut von Werbesendungen oder Spam-Mails. Eltern sollten sich daher die Datenschutzerklärung und die Allgemeinen Geschäftsbedingungen (AGB) der Angebote genau anschauen. Besonders die Anbieter vieler Apps von Spielen und Social-Media-Angeboten stehen hier in der Kritik. Dort müssen die Nutzerinnen und Nutzer oft in die Weitergabe ihrer Daten einwilligen, sonst können sie das Angebot nicht nutzen.

Missbrauch von Daten vorbeugen

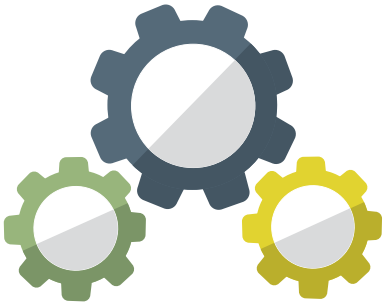
Nicht (ausreichend) geschützte Daten können durch Fremde gestohlen und missbraucht werden. Doch auch mit den richtigen Privatsphäre-Einstellungen können Daten gestohlen werden, z. B. wenn sich Hacker durch Sicherheitslücken auf der Plattform Zugriff verschaffen. Eine weitere Form des Datenmissbrauchs ist der Identitätsdiebstahl, etwa in Form von Fake-Profilen oder Online-Bestellungen im eigenen Namen bzw. dem Diebstahl von Bezahl- und Kontodaten. Eltern sollten Ihre Kinder für diese Gefahr sensibilisieren und Handlungsmöglichkeiten besprechen, wie das Sichern von Beweisen in Form von Screenshots und der Möglichkeit, Datenmissbrauch bei der Verbraucherzentrale oder sogar der Polizei zu melden.

Sind gelöschte Daten wirklich weg?

Digitale Daten lassen sich sehr schnell weiterleiten, vervielfältigen und verbreiten. Sind sie erstmal online, kann man sie nicht mehr zurückholen: Das Internet vergisst nichts. Online gestellte Daten können auch nach Jahren wieder auftauchen, obwohl man sie eigentlich gelöscht hat. So können dann auch zukünftige Arbeitgeberinnen und Arbeitgeber oder neue Partnerinnen und Partner diese Daten abrufen. Auch wenn man den Datenschutz ernst nimmt, kann man nie sicher sein, dass Fotos und Informationen der eigenen Person nicht trotzdem irgendwo im Internet herumgeistern – z. B. eingestellt durch Freundinnen oder Freunde. Zum Schutz der Privatsphäre sollte man also grundsätzlich sparsam mit seinen Daten sein. Man sollte sich in jeder Situation fragen, was man wirklich von sich preisgeben möchte und ob es notwendig ist.

Wie lassen sich eigene Daten am besten schützen?

Der beste Schutz von Daten ist es, sie gar nicht erst zu veröffentlichen. Auf jeden Fall sollte man gerade mit persönlichen Daten wie Name, Adresse, Geburtstag oder Telefonnummer sparsam umgehen und sie nicht einfach so herausgeben. Fragt ein Angebot zu viele dieser Daten ab, sollte man sich überlegen, ob man es wirklich nutzen möchte. Manchmal gibt es auch datensparsame Alternativen. Generell gilt: Weniger ist mehr. Daten, die nicht online stehen, können auch nicht so leicht missbraucht werden.



Tipp

Privatsphäre-Einstellungen sollten unbedingt vorgenommen und regelmäßig überprüft und aktualisiert werden. Eine der wichtigsten Datenschutzfunktionen bei Social-Media-Angeboten ist die Sichtbarkeit. Eigene Daten sollten nicht öffentlich, sondern nur für ausgewählte Kontakte („Freunde“) sichtbar sein. Eine weitere Möglichkeit ist es, Zugriffsrechte von Apps einzuschränken. So kann geprüft werden, auf welche Daten eine App zugreifen kann und ob sie den Zugriff wirklich benötigt.

Weitere Informationen zum Thema Datenschutz sowie konkrete Tipps für technische Einstellungen finden Sie in der Broschüre **„Selbstdatenschutz! Tipps, Tricks und Klicks“** der Bayerischen Landeszentrale für neue Medien (BLM).

Quellenangabe

Der Text ist Bestandteil der bereits bestehenden Unterrichtseinheit „Liken, posten, teilen“ des Medienführerscheins Bayern für den Bereich der sonderpädagogischen Förderung. Die Unterrichtseinheit ist verfügbar unter: **www.medienfuehrerschein.bayern.** Die Entwicklung wurde gefördert durch die Bayerische Staatskanzlei.