ONLINEWELT

MODUL
INTERNET, PRIVATSPHÄRE UND DATENSCHUTZ

Ziele

- Die SchülerInnen kennen und definieren die Begriffe Privatsphäre und Datenschutz.
- Die SchülerInnen verstehen, dass Privatsphäre und Datenschutz als Geschäftsmodelle genutzt werden.
- Die SchülerInnen können ein sicheres Kennwort erstellen.
- Die SchülerInnen kennen weitere Möglichkeiten, um Zugangsbarrieren zu persönlichen Daten aufzubauen.
- Die SchülerInnen reflektieren ihren Umgang mit persönlichen Daten im Internet.

Wissen für PädagogInnen

Das Internet ist seit Beginn (ca. 1991) als soziales Medium konzipiert. Schon die ersten Webseiten waren Foren zur gegenseitigen Unterstützung. Digitalisierung und soziale Medien haben damit in den letzten 30 Jahren auch das Konzept von Privatsphäre und Datenschutz massiv verschoben. In den 2000er Jahren wurde es mit Web 2.0 für jede Person – z.B. über Facebook - möglich, das Internet mit Informationen zu füllen (Zuboff, 2019).

Informationen, die vor 20 Jahren noch als sehr persönlich oder vielleicht sogar intim galten, sind in der Zwischenzeit problemlos online abrufbar geworden. Für viele Jugendliche ist die Definition von privat: „das, was Eltern nicht wissen dürfen". Große Unternehmen wie Microsoft, Facebook oder Google haben diese neue Definition von Privatsphäre bewusst mitgeprägt und nutzen die geteilten Daten als zentrales Geschäftsmodell. Wenn UserInnen Daten mit diesen Plattformen teilen, werden diese bis ins kleinste Detail ausgewertet – unabhängig davon, ob diese Daten öffentlich abrufbar sind oder nicht. Google liest beispielsweise alle Google-Emails automatisiert mit, Microsoft wertet jedes Skype-Telefonat automatisch zu Werbezwecken aus (Zuboff, 2019).

Die Privatsphäre der meisten Menschen ist aufgebaut wie eine Zwiebel. Am äußeren Rand befinden sich Informationen, die alle wissen dürfen, wie z.B. den Namen oder die berufliche Email-Adresse. Im Innersten befinden sich sehr intime Informationen wie Kontostand oder auch Gesundheitsdaten. Dazwischen befinden sich jedoch zahlreiche Informationen, die mehr oder wenig öffentlich sind oder mit FreundInnen geteilt werden.

In einem Zeitalter, in dem auch persönliche Informationen als digitale Daten abgelegt sind, wird Datenschutz zunehmend wichtiger. Datenschutz bedeutet für AnbieterInnen, dass Daten vor Zugriffen durch Fremde oder nicht autorisierte Personen geschützt sind. Hierzu werden sogenannte kryptographische Verfahren verwendet, die Daten so verschlüsseln, dass sie nur durch die EigentümerIn entschlüsselt werden können. Bei einem möglichen Datendiebstahl werden nur nicht verwendbare Daten gestohlen. Für Einzelpersonen bedeutet dies, dass ich auf eigenen und auf mir anvertraute Daten achtgeben muss. Ich bin somit nicht nur für meine Daten verantwortlich, sondern auch für Daten von anderen – beispielsweise persönliche Informationen wie Telefonnummer oder auch für Fotos (Bundesministerium für Digitalisierung und Wirtschaftsstandort).

Um Datenschutz sicherzustellen ist es wichtig, Zugangsbarrieren z.B. durch ein Passwort zu aktivieren. Ein sicheres Passwort besteht aus zumindest 12 Zeichen, Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern und ist nicht als Wort im Wörterbuch auffindbar. Moderne Smartphones unterstützen auch den Fingerabdruck oder einen Gesichtsscan als Zugangsbarriere. Beide Methoden gelten als relativ sicher. Immer häufiger wird im Internet auch die sogenannte Zwei-Faktoren-Authentifizierung genutzt, z.B. bei Telebanking. Hier braucht es immer eine zweite Zugangsbarriere, etwa einen Code, der per SMS auf ein Smartphone gesandt wird, um bestimmte Informationen aufzurufen. Alle großen Unternehmen unterstützen inzwischen diese Zwei-Faktoren-Authentifizierung. Potenzielle DatendiebInnen müssten also sowohl das Passwort als auch das entsperrte Smartphone besitzen, um beispielsweise eine Überweisung tätigen zu können (Bundesministerium für Digitalisierung und Wirtschaftsstandort).

Quellen

Bundesministerium für Digitalisierung und Wirtschaftsstandort. (2019). Konten und Passwörter. Download vom 08.01.2020, von *www.onlinesicherheit.gv.at/praevention/konten_und_passwoerter/249583.html*

Bundesministerium für Digitalisierung und Wirtschaftsstandort. (2019). Privatsphäre schützen. Download vom 08.01.2020, von *www.onlinesicherheit.gv.at/praevention/privatsphaere_schuetzen/250022.html*

Zuboff, S. (2018). Das Zeitalter des Überwachungskapitalismus. München: ABOD Verlag.

Fallbeispiele

Fallbeispiel für SchülerInnen der Unterstufe
Das Passwort eines Klassenkollegen wurde gestohlen. Da er sich das neue Kennwort für seinen Email-Account in der Schule lange nicht merken konnte, hat er es auf einen Zettel geschrieben und diesen in seinem Bankfach versteckt. Irgendjemand hat dies jedoch mitbekommen und sich mit seinem Account angemeldet. Den Account hat er dann dazu verwendet, um unpassende Emails an die Direktorin und den Klassenvorstand zu schicken. Dein Freund muss jetzt irgendwie beweisen, dass diese Emails nicht von ihm verschickt wurden. Nachdem sein Name als Absender aufscheint, könnte das ganz schön schwer werden. Wie könnt es deinem Freund gelingen, das zu beweisen? Wie hätte er sich vor diesem Missbrauch schützen können?

Fallbeispiel für SchülerInnen der Oberstufe
Deine Freundin teilt ihr ganzes Leben auf Instagram mit ihren Followern. Sie berichtet dort immer tagesaktuell von Streits mit ihren Eltern, in wen sie gerade verliebt ist oder wohin der nächste Familienurlaub geht. Nicht alle aus ihrer Schule sind davon begeistert und manchmal wissen SchulkollegInnen, die sie gar nicht wirklich kennt, eine ganze Menge von ihrem Leben. Am Gang wird sie in der Pause immer wieder auf ihre Erlebnisse angesprochen. Eines Tages steht plötzlich eine fremde Person vor der Schule und möchte mit ihr sprechen. Der Mann hat auf Instagram gesehen, in welche Schule deine Freundin geht und möchte sie jetzt nach dem Unterricht abfangen. Was könnte deine Freundin jetzt tun? Wie hätte sie diese Situation vermeiden können?

Reflexionsfragen für SchülerInnen

- Was bedeutet Privatsphäre?
- Was bedeutet Datenschutz?
- Welche Daten von dir sind privat? Was darf jede/r wissen?
- Welche Informationen solltest du auf sozialen Medien nicht teilen? Welche teilst du?
- Wie sieht ein sicheres Passwort aus? Warum sollte man Passwörter regelmäßig ändern?
- Warum sind persönliche Daten mittlerweile so viel wert? Wie können Unternehmen mit privaten Daten Geld verdienen?
- Wie beugt man den Missbrauch von persönlichen Daten vor?
- Warum können Probleme entstehen, wenn eine Person sehr viel von ihrem Leben auf sozialen Medien teilt?
- Was kann man bei Stalking unternehmen? Wer könnte unterstützen?

Material zu Partner-/Gruppen-/Einzelarbeit

www.feel-ok.at/de_AT/schule/themen/alle_arbeitsblaetter.cfm

Abschlussdiskussion mit der gesamten Klasse

Vertiefungsübungen

Vertiefungsübung für SchülerInnen der Unter- und Oberstufe
Die SchülerInnen werden in Gruppen aufgeteilt. Jede Gruppe sucht sich zu einem großen Internetdienst die AGBs bzw. die Datenschutzerklärung aus (Beispiele WhatsApp, Instagram, TikTok, Snapchat, YouTube). In den Datenschutzerklärungen können die SchülerInnen genau nachlesen, was die Unternehmen mit ihren Daten machen dürfen. Die Inhalte werden zusammengefasst, kurz präsentiert und diskutiert.

Weitere Informationen und Materialien zum Thema

Privatsphäre Leitfaden von Saferninternet.at
www.saferinternet.at/privatsphaere-leitfaeden

Klicksafe.de – Leitfäden für Instagram & Co
www.klicksafe.de/service/schule-und-unterricht/leitfaeden/?L=0