

Thema: **Datenschutz in sozialen Medien**

Kompetenzen:

- Die Schülerinnen und Schüler werden für das Thema Datenschutz in den sozialen Medien sensibilisiert.
- Sie machen sich bewusst, was mit ihren Daten passiert.
- Sie wissen, wie sie ihre Daten schützen können.

Vorgehen:

Einstieg:

Im Unterrichtsgespräch können die Fragen besprochen werden:

- In welchen sozialen Medien sind Sie vertreten?
- Welche kennen Sie darüber hinaus noch (ggf. Xing, LinkedIn, Tiktok, Instagram)?
- Warum nutzen Sie diese?
- Welche Daten müssen Sie bei der Anmeldung preisgeben?
- Welche Daten geben Sie durch Ihre fortlaufenden Aktivitäten preis?
- Können Sie sich vorstellen, was mit Ihren Daten passiert?

Anschließend lesen die Schüler/innen den Ratgeber „So schützen Sie Ihre Daten in den sozialen Medien“ (siehe Arbeitsauftrag) und notieren sich in Partnerarbeit Stichpunkte zu den angesprochenen Schwerpunkten.

Die Ergebnisse werden im Plenum zusammengetragen und diskutiert.

Arbeitsauftrag:

Lesen Sie den Ratgeber „So schützen Sie Ihre Daten in den sozialen Medien“ (<https://www.finanztip.de/social-media-datenschutz/>) und notieren Sie zusammen mit Ihrem Partner Stichpunkte zu den folgenden Schwerpunkten:

- Was passiert mit den gesammelten Daten?
- Worauf sollte man in den Nutzungsbedingungen achten?
- Wie kann man seine Daten schützen? Was empfiehlt Finanztip?
- Was ist eine Ende-zu-Ende-Verschlüsselung?
- Die Messenger-App Threema sendet Nachrichten verschlüsselt. Threema gilt als der Messenger, der die größtmögliche Anonymität bietet. Dennoch nutzen ihn wenige. Woran könnte das liegen?
- Wie kann man seine Konten vor externen Zugriffen schützen?

Lösung:

Arbeitsauftrag:

Lesen Sie den Ratgeber „So schützen Sie Ihre Daten in den sozialen Medien“ (<https://www.finanztip.de/social-media-datenschutz/>) und notieren Sie zusammen mit Ihrem Partner Stichpunkte zu den folgenden Schwerpunkten:

- Was passiert mit den gesammelten Daten?
*Die gesammelten Daten werden an Unternehmen verkauft.
Die Daten werden verwendet, um personalisierte Werbung auszuspielen, Empfehlungen auszusprechen, zum Beispiel für interessante Gruppen oder Seiten. Das bewirkt, dass der Nutzer weitere Daten von sich preisgibt.
Das Nutzerverhalten kann analysiert werden, was wiederum die Möglichkeit bietet, Vorhersagen über Trends und Muster zu machen.*
- Worauf sollte man in den Nutzungsbedingungen achten?
*Da die Nutzungsbedingungen in der Regel sehr umfangreich und nicht leicht zu verstehen sind, sollte der Nutzer zumindest nach diesen Begriffen Ausschau halten:
Nutzungsrechte und Lizenzen - Welche Rechte hat das Netzwerk an meinen Inhalten? Wie umfassend sind sie?
Pflichten - Welche Pflichten gehe ich als Nutzer ein?
Daten und Datenschutz - Wie werden Daten von erhoben? An welche Dienste werden sie weitergeleitet? Wie werden sie verwendet?
Beendigung der Mitgliedschaft – Kann ich meine Mitgliedschaft beenden? Wie kann ich kündigen?
Vertragspartner - Mit wem schließe ich den Vertrag?*

- Wie kann man seine Daten schützen? Was empfiehlt Finanztip?
Der beste Schutz ist natürlich, die sozialen Medien nicht zu nutzen. Da dies für viele nicht vorstellbar oder machbar ist, kann man zumindest sparsam mit seinen Daten umgehen.

Das heißt: wenig Persönliches weitergeben, evtl. ein Pseudonym und eine private E-Mail-Adresse verwenden, keine Angabe des Standortes, keine Fotos, Informationen über Angehörige, ein Symbolfoto als Profilbild, ein anderes Geburtsdatum, wenn möglich Freunde in Listen oder Kreisen zu verwalten
- Was ist eine Ende-zu-Ende-Verschlüsselung? Was zeichnet sie aus?
Die Unterhaltung wird auf dem Handy verschlüsselt und erst beim Empfänger wieder entschlüsselt. Diese Übertragung ist besonders sicher, denn eine Auswertung der Informationen kann nicht erfolgen.
- Die Messenger-App Threema sendet Nachrichten verschlüsselt. Threema gilt als der Messenger, der die größtmögliche Anonymität bietet. Dennoch nutzen ihn wenige. Woran könnte das liegen?
Individuelle Antworten der Schüler, evtl. könnten Argumente kommen, wie: Meine Familie, meine Freunde und Bekannten nutzen WhatsApp. Auch die benutzen inzwischen eine Ende-zu-Ende Verschlüsselung.
Threema ist kostenpflichtig.
Anonymität ist mir nicht wichtig; mir ist es egal, was mit meinen Daten passiert.
- Wie kann man seine Konten vor externen Zugriffen schützen?
ein sicheres Passwort verwenden; an jedem Computer ausloggen, den man nicht ausschließlich allein benutzen.

FINANZTIP

Hilfreich – inzwischen nutzen auch Social-Media-Anbieter immer häufiger eine Zwei-Faktor-Authentifizierung (zum ersten Faktor – dem Passwort – kommt ein weiterer Faktor hinzu, zum Beispiel die Identifizierung durch das Handy oder eine zusätzliche Sicherheitsfrage)

Eine Authentifizierung durch das Handy ist nicht ratsam, da der Anbieter so weitere Daten über sammeln kann.