

Schützen und sicher Agieren

Technische Voraussetzungen

- Smartphones der Schüler*innen, ggf. Internetverbindung

Unterrichtsskizze in Schritten

- **Einstieg:** Um die persönlichen Erfahrungen der Schüler*innen zu aktivieren und ihnen die Bedeutung des Themas bewusst zu machen, startet die Lehrkraft mit einer Blitzlichtrunde zu der Frage „Wem vertraust du deine Geheimnisse an?“. Nachdem sich alle geäußert haben, sollte besprochen werden, auf welchen Kommunikationswegen (analog / digital) Privates bzw. Geheimnisse weitergegeben werden.
- **Am eigenen Beispiel recherchieren:** Unter der Fragestellung „Was weiß dein Smartphone über dich?“ führen die Schüler*innen in Einzelarbeit anschließend eine Recherche mit dem eigenen Gerät durch und listen auf, welche Apps sie nutzen und welche persönlichen Daten sie darin preisgeben. Sie überprüfen also zum einen, was sie selbst eingegeben haben, zum anderen reflektieren sie, welche Daten bei der Nutzung der App entstehen, die dann verarbeitet werden.
- **Die Vielfalt gespeicherter Daten begreifen:** Um die Dimension der möglichen Datenspeicherung von Nachrichten mit sehr persönlichen Inhalten via Messenger bis hin zur Speicherung von Gesundheitsdaten zu begreifen, werden die Ergebnisse der Schüler*innen im Plenum gesammelt. Dazu eignet sich beispielsweise eine tabellarische Übersicht nach Art der preisgegebenen Informationen, unter denen die genutzten Apps gelistet werden.

Beispiel

| | |
|----------------------------------|---|
| alle Apps mit Anmeldung | allgemeine Profilinformationen, meist Name, Geburtsdatum, E-Mail-Adresse, Anschrift |
| Browser/Suchmaschinen | Browserverlauf, Suchbegriffe |
| Messenger-Apps/soziale Netzwerke | zusätzliche persönliche Profilinformationen und hochgeladene Bilder, Beziehungen & Interaktionen, Nachrichtenverläufe |
| Fitness-Apps | Bewegungsdaten (z. B. Schrittzähler), weitere Gesundheitsdaten wie Herzfrequenz (bei Verknüpfung mit Smartwatch) |
| Shopping-Apps | angesehene und bestellte Produkte, Zahlungsinformationen |

- **Die Folgen möglichen Missbrauchs simulieren:** Die so erhobenen Informationen dienen als Grundlage für eine Simulation: Die Schüler*innen entwerfen gemeinsam mit Teampartner*innen ein Worst-Case-Szenario: In diesem Szenario wird ein Handy gestohlen, auf dem die genannten Apps installiert und die entsprechenden Daten gesammelt sind. Dem Dieb gelingt es, die Codesperre zu knacken und an die Daten zu kommen. Die Schüler*innen erläutern, welche Schäden dem Smartphone-Besitzer im Hinblick auf seine Reputation und seine Finanzen entstehen können.

Beispiel

- Posten von Spammessages/unangemessenen Inhalten in den Social-Media-Profilen
- Nutzung der Bankdaten für Bestellungen
- Diskreditierung der Person durch Weitergabe privater Informationen über die installierten Messengerdienste

- *Maßnahmen für Datensicherheit sammeln:* Anschließend werden notwendige Maßnahmen definiert, um sowohl das Smartphone als auch die persönlichen Accounts vor einem solchen Missbrauch zu schützen. Je nach Altersstufe können die Schüler*innen diese Informationen auch selbst recherchieren.

Beispiel

Schlagworte:

- Vergabe von sicheren Passwörtern
- keine Preisgabe von Zugangsdaten
- Zwei-Faktor-Authentifizierung
- Hinterlegung weiterer Kontaktdaten zur Sicherung des Kontos

- *Sicherungsmaßnahmen ausprobieren und anwenden:* Da auch diese Sicherungsmaßnahmen der Übung bedürfen, sollten altersgemäße Anwendungsbereiche gefunden werden. Jüngere Schüler*innen können die Vergabe sicherer Passwörter anhand gängiger Kriterien einüben, ältere Schüler*innen können nach dem Grad an Datensicherheit der von ihnen genutzten Plattformen recherchieren und alternative Anbieter*innen für ähnliche Funktionen vorstellen.
- *Das eigene Verhalten reflektieren und Handlungsanweisungen für die Zukunft ableiten:* Zum Abschluss bietet es sich an, zu reflektieren, welche Informationen für die Schüler*innen neu waren und ob bzw. wie sich ihr Blick auf die Preisgabe von Daten verändert hat. Eine nachhaltige Wirkung kann erzielt werden, wenn sich die Schüler*innen selbst Vorsätze für eine Verbesserung der Sicherheit ihrer Daten überlegen. Diese können dann zu einem späteren Zeitpunkt erneut aufgegriffen und reflektiert werden.

Übertragbarkeit auf andere Fächer

Diese Unterrichtseinheit ist insbesondere für gesellschaftswissenschaftliche Fächer geeignet, gerade der Politikunterricht oder auch Religion / Ethik bieten Anknüpfungspunkte. Auch ein Exkurs im Mathematikunterricht ist jedoch denkbar (Stochastik / Dauer des Hackens von Passwörtern über die Anzahl der möglichen Kombinationen).

Privatsphäre in digitalen Umgebungen durch geeignete Maßnahmen schützen

Handlungsanleitungen für den Schutz der Privatsphäre in verschiedenen sozialen Netzwerken erarbeiten

Klasse
5-10

Von Kristina Wahl

Mögliches Ziel / Kurzbeschreibung

Die Schüler*innen reflektieren, welchen Personenkreisen sie durch die Nutzung von sozialen Netzwerken Zugriff auf Teilbereiche ihrer Privatsphäre ermöglichen. Sie setzen sich anhand ausgewählter Beispiele mit Maßnahmen zur Verhinderung des Zugriffs Unbefugter auseinander.

Technische Voraussetzungen

- Smartphones der Schüler*innen
- Messenger-App (für das Beispiel wurde WhatsApp gewählt)

Unterrichtsskizze in Schritten

- **Einstieg:** Für den Einstieg eignet sich eine einfache Übung, bei der die meisten Schüler*innen aufgrund der hohen Verbreitung des Messengerdienstes WhatsApp aktiv mitwirken können: In Partner*innenarbeit analysieren die Schüler*innen gegenseitig, was auf ihren Profilbildern zu sehen ist und welche privaten Informationen sie dadurch preisgeben (z. B. Familie / Freunde, Zuhause, Hobbys etc.).
- **Sammlung:** Die Schüler*innen stellen in einer Gesprächsrunde das Profilbild des Gegenübers aus der Partnerarbeitsphase vor, indem sie das Abgebildete beschreiben. Anhand der Beschreibungen werden die Profilbilder auf einer Achse nach dem Grad des Einblicks in die Privatsphäre sortiert.
- **Problematisierung:** Um die Schüler*innen dazu anzuleiten, ihre Privatsphäre-Einstellungen zu überprüfen, eignet sich eine Gegenüberstellung der Fragen „Wer sollte / darf dein Profilbild sehen?“ vs. „Wer kann dein Profilbild sehen?“.
- **Überprüfung der Einstellungen:** Um die Antwort auf die zweite Frage zu verifizieren und darüber hinaus feststellen zu können, welche weiteren Privatsphäre-Einstellungen bei der Nutzung des Messengerdienstes vorgenommen werden können, suchen die Schüler*innen nach den entsprechenden Optionen (Einstellungen > Account > Datenschutz).
- **Beurteilung:** Die Schüler*innen beurteilen, welche Einstellungen besonders geeignet sind, um die Messengerdienste als soziale Netzwerke zur Interaktion zu nutzen und dennoch nicht zu viel preiszugeben. Sie entwickeln eine kurze Liste von Tipps, die an andere weitergegeben werden können, z. B. als Plakat / Flyer.

Beispiel

Tipps für die WhatsApp-Nutzung:

- Profilbild wählen, das nicht die Schüler*innen selbst zeigt
- persönliche Infos (zuletzt online, Profilbild, Info) nur für Kontakte sichtbar machen
- Status nur für ausgewählte Kontakte sichtbar machen
- Live-Standort nicht teilen
- Lesebestätigungen ausschalten
- ungewollte Kontakte blockieren

- **Übertragung auf andere Apps:** Um die Vorgehensweise auf andere Apps zu übertragen, werden im Plenum die sozialen Netzwerke zusammengetragen, welche für die Schüler*innen relevant sind.

Pro Kleingruppe wird nun eines der Netzwerke untersucht, um die Einstellungen für WhatsApp zu übertragen.

Schützen und sicher Agieren

Vorgehen darauf angewendet, indem die Kleingruppen die Privatsphäre-Optionen durchsuchen, die Möglichkeiten vergleichend gegenüberstellen und dann kritisch beurteilen.

- **Präsentation und Reflexion:** Die erarbeiteten Tipps werden der Lerngruppe vorgestellt, wobei die einzelnen Gruppen insbesondere auf app-spezifische Tipps eingehen. Diese können später der Schulgemeinschaft als Informationsmaterial zur Verfügung gestellt werden.

Beispiel

- Instagram (privates Profil, Teilen des Status über Listen, z. B. „enge Freunde“)
- Youtube (eigene Videos: auf Inhalt achten, z. B. Standort nicht erkennbar, keine persönlichen Informationen preisgeben; Funktion „nicht gelistet“ für Videos, die man nur mit Freund*innen teilen möchte)

Alternative Möglichkeiten

Aufgrund des Kontextes ist es zielführend, auch die Präsentationsmaterialien mit digitalen Medien zu erstellen. Um die Information breit zu streuen, wären übersichtliche und schnell zu erfassende Infografiken besser geeignet als Präsentationen mit mehreren Folien (als Tool eignet sich z. B. Canva). Eine zusammenfassende Grafik für mehrere Apps ist eine komplexere Aufgabe für höhere Klassenstufen.

Übertragbarkeit auf andere Fächer

Je nach Kontextualisierung ist die Unterrichtseinheit für den Deutschunterricht, gesellschaftswissenschaftliche Fächer oder den Informationsverarbeitungs- / Informatikunterricht geeignet.

Sicherheitseinstellungen ständig aktualisieren

Einen regelmäßigen Newsletter für die Klasse / Schule zum Thema „Safety first – Tipps für eure Sicherheitseinstellungen“ erstellen

Klasse
7–10

Von Julia Hastädt

Mögliches Ziel / Kurzbeschreibung

Die Schüler*innen verwenden eine Vielzahl an Online-Diensten und Apps, für die es einer Anmeldung, der Anlage eines oder mehrerer Passwörter bedarf und die in der Regel diverse Möglichkeiten an Sicherheitseinstellungen bieten. Diensteanbieter verkomplizieren es Nutzer*innen dabei jedoch häufig, Sicherheitseinstellungen bestmöglich aus Sicht der Anwender*innen einzurichten. Die Schüler*innen analysieren, welche Sicherheitseinstellungen es gibt, und beurteilen, wie sie diese – bezogen auf die von ihnen häufig verwendeten Dienste – möglichst unter Freigabe von so wenig Daten wie notwendig einrichten und regelmäßig aktualisieren können. Dazu erstellen sie einen Newsletter mit wertvollen Tipps, der in regelmäßigen Abständen z. B. über das schulische Lernmanagement-System verteilt werden kann.

Beispiel

Mögliche Themen wären:

- „Passwörter – darauf solltet ihr achten“
- „Ihr liebt Cookies? Wie bei Keksen kommt es auch online auf die Sorte an. Das solltet ihr beachten.“
- „Storys auf WhatsApp, Instagram und Co. – Bestimme deine Zielgruppe bewusst.“

Zunächst sollten die Schüler*innen sich einen Überblick verschaffen, was einen guten und interessanten Newsletter ausmacht und „Best-Practice-Beispiele“ für die inhaltliche und formale Gestaltung ihres eigenen Newsletters berücksichtigen. Dann geht es an die eigentliche Recherche, Formulierung der Texte und die Gestaltung. Es empfiehlt sich, dies zunächst in einem klassischen Textverarbeitungsprogramm wie Pages oder Word vorzunehmen.

- **Anwendung:** Je nach Anzahl der Gruppen sind einige Newsletter-Beiträge entstanden. Im Unterrichtsgespräch sollte nun geklärt werden, in welchem zeitlichen Abstand die Beiträge versendet werden und an wen (z. B. Parallelklasse, komplette Jahrgangsstufe, Schulgemeinschaft, ...). Wichtig wäre, dass die Schüler*innen selbst auch für das Lesen des Newsletters (z. B. auf dem Schulhof/ in den Pausen) werben und sich zugleich Feedback einfordern. Beim letzten Beitrag könnte ein Link zu einer Online-Befragung beigefügt werden, sodass die Schüler*innen ein anonymes und möglichst objektives Feedback erhalten.
- **Beurteilung / Reflexion:** Die Schüler*innen beurteilen auf Grundlage des Feedbacks aus der Anwendungsphase, inwieweit sie Sicherheitseinstellungen eine stärkere Bedeutung beimessen und ob sich ihr eigenes Verhalten diesbezüglich verändert hat. Im Unterrichtsgespräch kann dann diskutiert werden, ob der Newsletter regelmäßig fortgesetzt, nur bei Bedarf (z. B. neuen Features für Sicherheitseinstellungen) Anwendung findet oder eingestellt wird.

Alternative Möglichkeiten

Wenn Schüler*innen in der Klasse sind, die technisch versiert und im Umgang mit einem Content-Management-System vertraut sind, kann auch ein eigener Blog (z. B. mit WordPress) erstellt und ein „echter“ digitaler Newsletter eingerichtet werden. Der Blog könnte dann auf der Schulhomepage verlinkt werden.

Übertragbarkeit auf andere Fächer

Die Unterrichtseinheit ist auf viele Fächer übertragbar. Insbesondere bieten sich dafür der Deutsch-, Sozialkunde- sowie der Informatikunterricht an. Denkbar ist auch ein fächerübergreifendes Projekt, bei dem dann fachspezifische Apps und Online-Dienste mit Blick auf ihre Sicherheitseinstellungen genauer untersucht und für den Newsletter aufbereitet werden.

Schützen und sicher Agieren

Technische Voraussetzungen

- Smartphone / Table / Laptop / PC mit Internetanschluss pro Kleingruppe (max. 4 Personen)

Unterrichtsskizze in Schritten

- *Einstieg*: Als Einstieg teilt die Lehrkraft ein Video oder eine Nachricht mit den Schüler*innen und macht auf das Thema „Soziales Engagement“ aufmerksam.

Beispiel

Man kann z. B. ein Video über eine ehrenamtliche Tätigkeit oder über den Anstieg der CO₂-Emissionen einsetzen. Die Impulsfragen lauten: Welche sozialen Organisationen gibt es und welche Ziele haben sie? Wie können wir bedürftigen Menschen, Tieren oder der Natur helfen?

Die Schüler*innen können ihre Antworten an der Tafel oder mithilfe einer App wie z. B. Mentimeter (siehe alternative Möglichkeiten) sammeln.

- *Erarbeitung 1*: Die gesammelten Antworten werden Oberbegriffen zugeordnet und in Padlet (siehe alternative Möglichkeiten) den Arbeitsgruppen zugeteilt. Anschließend sammeln die Gruppen Informationen über soziale Organisationen und fassen kurz deren Tätigkeiten zusammen. Diese Informationen dienen als Grundlage und Einführung des Projektes.

Beispiel

Je nach Thema können folgende Oberbegriffe erstellt werden:

- Umweltschutz
- Tierschutz
- Menschenrechte
- Kindernot
- Krankheiten
- Jugendstiftungen

- *Sicherung 1 – Gruppenplanung*: Die Gruppen (Umweltschutz, Tierschutz, ...) erhalten ihre Aufgaben. Zuerst müssen sie einen Namen für ihre Gruppe finden (z. B. Gruppe „Umwelthelden“, Gruppe „Tierretter“, Gruppe „Menschenrechte-Ritter“ usw.) und die Aufgabenverteilung untereinander festlegen.

Beispiel

- Projektleiter*in: zuständig für die Umsetzungen des Projektes
 - Berater*in: zuständig für die Auswahl und Gestaltung der Inhalte
 - Expert*in: zuständig für die inhaltliche Aufbereitung
 - Designer*in: zuständig für die Darstellung von Videos, Bildern, Präsentationen
 - Redakteur*in: zuständig für die Kontrolle des Inhaltes und die sprachliche Korrektheit
- Mit diesen Titeln kann man auch gleichzeitig die Motivation steigern und somit das Verantwortungsgefühl erhöhen. Diese sollten auch schriftlich dargestellt werden, man kann ein „Über uns“-Plakat oder ein gemeinsames Padlet/Etherpad für die Gruppenarbeit erstellen.

- *Erarbeitung 2 – Projektidee festlegen*: Ziel des digitalen Projektes der Gruppen ist es, eine Idee für soziales Engagement mithilfe von digitalen Medien zu entwickeln. Die Schüler*innen besprechen gemeinsam die wichtigsten Punkte und legen eine Projektidee fest.