Syllabus Nr. 6 – Schutz Ihrer Daten

Digitale Kompetenz: Risiken erkennen und verlässliche Online-Quellen nutzen

Unterrichtsvorschlag für die Fächer:

Politische Bildung, Informatik, Medienbildung, Wirtschaft, Gemeinschaftskunde, Sozialwissenschaften, Glück, Ethik, Betriebswirtschaftslehre

Zielgruppe	SuS in den ersten beiden Jahren der Sekundarstufe II
Themen	Verbraucherbewusstsein, digitale Ethik, Datenschutzverletzungen
Gruppengröße	Eine Schulklasse
Voraussetzungen und Vorkenntnisse	**Voraussetzungen für SuS:** • Grundkenntnisse über die Funktionsweise des Internets, von Suchmaschinen und sozialen Medien • Persönliche Erfahrung im täglichen Umgang mit Apps, sozialen Netzwerken und Online-Diensten • Grundlegendes Bewusstsein für die Bedeutung personenbezogener Daten (z. B. Name, Foto, Standort) und die möglichen Folgen ihrer Weitergabe **Vorzubereitende Materialien und Ressourcen:** • Zugang zu individuellen digitalen Endgeräten mit Internetverbindung (Tablets, Smartphones oder Laptops) • Vorbereitung digitaler oder gedruckter Formulare zum Erfassen und Reflektieren des eigenen digitalen Verhaltens • Arbeitsblätter mit konkreten Beispielen für „Dark Patterns“ (irreführende Gestaltungsmuster in digitalen Benutzeroberflächen) • Interaktives Whiteboard oder Beamer mit Audio
Lernziele aus dem DataPro-Curriculum	**C.1 Identitätsmanagement** **Sensibilisierung für Datennutzung**

	Regelmäßig hinterfragen, wie und wo man personenbezogene Daten verwendet und weitergibt, sowie welche Risiken damit verbunden sind. **C.2 Selbstschutz:** **Sichere Identifizierung** Digitale Identifizierung und Logins durch Methoden wie starke Passwörter und Zwei-Faktor-Authentifizierungen sicher durchführen. **Cybersicherheit** Standard-Sicherheitsmaßnahmen verwenden und anpassen, z. B. Passwortmanager abzustellen, verschiedene Passwörter für verschiedene digitale Dienste nutzen, Multi-Faktor-Authentifizierung, biometrische Schlüssel (Fingerabdruck, Iris etc.), regelmäßige Software-Updates und die Installation von Schutzsoftware (Virenscanner etc.). **Digitaler Diebstahlschutz** Sich über die üblichen Social-Engineering-Angriffe über verschiedene Kommunikationskanäle (Phishing, Smishing ...) und andere digitale Betrugsmaschen (z. B. Fakeshops) informieren, um den Diebstahl von (digitalen) Vermögenswerten zu verhindern. **C.4 Informationsquellenüberprüfung:** **Kritisch Sein** Regelmäßiges hinterfragen, wer oder was hinter Informationen im Internet, insbesondere in den sozialen Medien, steckt und welches Interesse hinter der Verbreitung von Fake News stecken könnte, z. B. Social Bots, Hassredner:innen, Echokammern (Filter Blasen). **Kritisch Bleiben** Sich bewusst machen, dass Fehlinformationen sehr überzeugend sein können, z. B. durch den Einsatz von Künstlicher Intelligenz, die auch anspruchsvolles Bildmaterial liefern kann. **Verzerrungen Erkennen** Sich bewusst machen, dass Informationen u.a. auf Grund ihrer Herkunft oder ihres Zwecks verzerrt sein können.

Weitere spezifische Lernziele	• Kritische Denkfähigkeiten entwickeln, um Online-Informationen zu bewerten • Fake News und unzuverlässige Quellen erkennen. • Irreführende Designmuster (Dark Patterns) erkennen und verstehen, wie sie Entscheidungen im Netz beeinflussen. • Strategien für bewussteres und weniger manipulierbares Surfen anwenden.
Dauer der Unterrichtseinheit	ca. 60 Minuten
Technische Anforderungen/ Hilfsmittel	• stabile Internetverbindung • ein Einzelgerät für jede:n SuS (Smartphone, Tablet oder Laptop) • Multimedia-Whiteboard oder Beamer mit Audio • Zugang zu digitalen Tools (z. B. Tools zur Verwaltung der Datenschutzeinstellungen in Browsern, Passwortüberprüfung, Websites zur Überprüfung von Datenlecks – z. B. „Have I Been Pwned“)
Schulungsmaterialien und Tools von DataPro	Chatbot „DataPro Assistent“ für praktische Übungen zur Datenschutzanalyse in den am häufigsten verwendeten Apps und zur Überprüfung digitaler Schnittstellen, Links und Quellen. Spiel „Entlarve die Nachrichten!“ (Interacty), um Informationen und Quellen auf ihre Zuverlässigkeit zu prüfen. Mini-Arbeitsheft „News Detective – Mini Anti Fake News Guide“ [auf Englisch] für zuhause mit den Eltern.
Weitere spezifische Unterrichtsmaterialien	Informationen zu „Dark Patterns“ [auf Englisch]: https://better-internet-for-kids.europa.eu/en/dark-patterns https://www.storyboard18.com/how-it-works/dark-patterns-explained-the-digital-design-tactics-misleading-millions-68150.htm
Tipps für die Durchführung	**1. Einführung: Die Online-Welt zwischen Wahrheit und Täuschung (10 Minuten)**

einer Unterrichtseinheit	• **Einstieg**: Zeigen Sie ein Beispiel für „Fake News“ oder sensationalistische Nachrichten (vorab von der Lehrperson ausgewählt) und fragen Sie die SuS: „Wie können wir feststellen, ob diese Nachrichten wahr oder falsch sind?“ • **Diskussion**: Leiten Sie eine Diskussion über die Bedeutung der Überprüfung von Online-Quellen und die Gefahren davon, alles zu glauben, was man im Internet liest oder sieht, an. **2. Bewertung von Online-Informationen und -quellen (20 Minuten)** • **Hauptaktivität**: Die SuS spielen „Entlarve die Nachrichten!“, wodurch sie ihre Urteilsfähigkeit üben können. • **Diskussion nach dem Spiel**: Besprechen Sie nach dem Spiel die Strategien, mit denen die SuS die Quellen bewertet haben, und die Warnsignale, die sie identifiziert haben. • **Tool (optional)**: Der DataPro Assistent kann für eine kurze Übung zur Überprüfung der Glaubwürdigkeit eines bestimmten Links oder einer bestimmten Quelle durch Simulation von Szenarien verwendet werden. **3. „Dark Patterns“: Versteckte Web-Tricks (20 Minuten)** • **Erklärung**: Führen Sie das Konzept der „Dark Patterns“ ein, indem Sie die oben verlinkten Artikel gemeinsam lesen. Dabei handelt es sich um Techniken zur Gestaltung von Benutzeroberflächen, die Nutzer:innen dazu verleiten, Dinge zu tun, die sie normalerweise nicht tun würden. Zeigen Sie gängige Beispiele (z. B. „Alle akzeptieren“-Buttons, die auffälliger sind als „Anpassen“-Buttons, Abonnements, die schwer zu kündigen sind, irreführende Pop-ups, gefälschte Countdowns für Angebote, versteckte Kosten). • **Diskussion**: Fragen Sie die SuS, ob sie diesen „Tricks“ online schon begegnet sind und wie sie sich dabei gefühlt haben. Diskutieren Sie, wie „Dark Patterns“ unsere Entscheidungen, unsere Privatsphäre und unsere Online-Zeit beeinflussen. • **Praktische Übung**: Die SuS können mit ihren Geräten Websites oder Apps durchsuchen, mit denen sie vertraut sind, um nach Beispielen für „Dark Patterns“ zu suchen.

	Alternativ kann die Lehrperson vorab ausgewählte Beispiele projizieren und gemeinsam mit der Klasse analysieren. **4. Zusammenfassung und Abwehrstrategien (5 Minuten)** • **Zusammenfassung**: Fassen Sie die wichtigsten Konzepte der Unterrichtseinheit zusammen: die Bedeutung von kritischem Denken, die Überprüfung von Quellen, das Erkennen von „Dark Patterns“ und das Bewusstsein für Online-Manipulation. • **Brainstorming**: Fragen Sie die SuS, welche Strategien sie anwenden können, um sich gegen Desinformation und Manipulation im Internet zu wehren. **5. Fragen und Abschluss (5 Minuten)** • **Fragen und Antworten**: Raum für Fragen und abschließende Klarstellungen. • **Fazit**: Ermutigen Sie die SuS, achtsame, kritische und aufmerksame Internetnutzer:innen zu sein, die zwischen Wahrheit und Lüge unterscheiden und sich vor Fallen im Netz schützen können. **Hausaufgabe für zuhause mit den Eltern:** • Mini-Arbeitsheft „News Detective – Mini Anti Fake News Guide.“ Die SuS können diese Aufgabe erledigen, indem sie das Mini-Arbeitsheft gemeinsam mit ihren Eltern ausfüllen, das in der Schule Gelernte anwenden und ihnen beibringen, wie man Fake News erkennt und sich sicherer im Internet bewegt.

DataPro Syllabi
<Germany> Workpackage 2

Kontaktperson Dr. Bernd Remmele
Institution Pädagogische Hochschule Freiburg
E-Mail bernd.remmele@ph-freiburg.de

Projekt DataPro
Disseminations-Level öffentlich
Jahr der Veröffentlichung 2026

Kofinanziert von der Europäischen Union

Disclaimer
Von der Europäischen Union finanziert bzw. kofinanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union [oder der Bewilligungsbehörde] wider. Weder die Europäische Union noch die Bewilligungsbehörde können dafür verantwortlich gemacht werden.