Syllabus Nr. 5 – Schutz Ihrer Daten

Sicheres Surfen – Schutz Ihrer Online-Daten

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, sichere Passwörter
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 Designmuster) • Interaktives Whiteboard oder Beamer mit Audio • Zugang zu Tools zur Überprüfung von Datenlecks (z. B. Tools zur Überprüfung, ob eine E-Mail kompromittiert wurde)

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	• Die Bedeutung des Schutzes persönlicher Daten im Internet verstehen. • Die eigenen persönlichen Daten und den eigenen digitalen Fußabdruck im Internet erkennen. • Datenschutzeinstellungen in Apps und Browsern verwalten und anpassen. • Erstellen starker und sicherer Passwörter. • Prüfen, ob die eigenen Zugangsdaten von einem Datenleck betroffen sind.
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. Eine kurze Präsentation mit dem Titel „Protect yourself online: privacy, security and Digital Best Practices“ [auf Englisch], die sich für eine Unterrichtsstunde zu bewährten Vorgehensweisen und Online-Sicherheit eignet Online-Quiz „Richtig oder falsch“: „Cyberfallen: Wer fällt darauf rein?“, das Sie anhand realistischer Szenarien aus dem digitalen Alltag testet und Ihnen hilft, die Risiken für den Online-Datenschutz besser zu verstehen.
Weitere spezifische Unterrichtsmaterialien	Offizielle Website zum Prüfen auf Datenlecks persönlicher Daten: https://haveibeenpwned.com/?utm_source=chatgpt.com

	Infografik zu bewährten Verfahren im Datenschutz [auf Englisch]:
Tipps für die Durchführung einer Unterrichtseinheit	**1. Einführung und Brainstorming: Dein digitaler Fußabdruck (10 Minuten)** • **Aktivität**: Beginnen Sie mit einer offenen Frage: „Was postet ihr online (Fotos, Kommentare, Videos usw.) und wer kann das eurer Meinung nach sehen?“ Führen Sie eine kurze Diskussion. • **Konzept**: Führen Sie das Konzept des „digitalen Fußabdrucks“ im Internet (alles, was wir beim Surfen im Internet hinterlassen) und dessen Fortbestand ein. • **Diskussion**: Fragen Sie die SuS, was sie unter „personenbezogenen Daten“ verstehen und warum es wichtig ist, diese zu schützen. **2. Datenschutzverwaltung: Einstellungen und Apps (15 Minuten)** • **Präsentation**: Verwenden Sie die ersten Abschnitte der Präsentation „Protect yourself online: privacy, security and Digital Best Practices“, um die Bedeutung von Datenschutzeinstellungen in Apps und sozialen Medien zu erläutern. • **Praktisch angeleitete Aktivität**: Bitten Sie die SuS, eine beliebte App, die sie regelmäßig nutzen (z. B. Instagram, TikTok, WhatsApp) oder den Webbrowser auf ihrem Gerät zu öffnen. Leiten Sie sie an, die Datenschutzeinstellungen zu finden und zu überprüfen (z. B. wer Beiträge, Profilinformationen und den Standort sehen kann). • **Tool**: Verwenden Sie den DataPro Assistenten für eine praktische Übung zur Analyse der Datenschutzeinstellungen in bestimmten Apps oder zur Überprüfung allgemeiner digitaler Schnittstellen. **3. Starke Passwörter und Erkennen von Datenschutzverletzungen (20 Minuten)** • **Erklärung**: Erläutern Sie, was ein Passwort „stark” macht (Länge, Komplexität, Einzigartigkeit) und warum es gefährlich ist, dasselbe Passwort auf mehreren Websites zu verwenden. Führen Sie das Konzept der

	„Datenverletzung" (Datenmissbrauch oder Datenleck) ein. • **Praktische Übung 1 – Passwortüberprüfung**: Die SuS können ein Online-Tool (z. B. einen Passwortgenerator/-bewerter oder einen in ihren Browser integrierten Passwortprüfer) verwenden, um die Stärke eines von ihnen verwendeten Passworts (oder eines fiktiven Passworts, das sie sich spontan ausdenken) zu bewerten. Betonen Sie, dass sie niemals echte Passwörter auf unsicheren Websites eingeben sollten. • **Praktische Übung 2 – Kontrolle von Datenschutzverletzungen**: Stellen Sie eine offizielle Website zur Überprüfung von Datenschutzverletzungen vor (Have I Been Pwned). Erklären Sie, wie sie funktioniert. Wenn die SuS sich damit wohlfühlen, können sie (unter Anleitung der Lehrperson und in dem Bewusstsein, dass es sich um eine persönliche Entscheidung handelt) überprüfen, ob ihre E-Mail-Adresse von bekannten Datenschutzverletzungen betroffen ist. **4. Interaktives Quiz und Zusammenfassung (10 Minuten)** • **Aktivität**: Die SuS absolvieren das Online-Quiz, um die Risiken für die Online-Privatsphäre besser zu verstehen. • **Diskussion**: Besprechen Sie am Ende des Quiz gemeinsam die Antworten, klären Sie offene Fragen und vertiefen Sie die gelernten Konzepte. • **Zusammenfassung**: Fassen Sie die wichtigsten Punkte der Unterrichtseinheit zusammen: die Bedeutung des Schutzes personenbezogener Daten, die Verwaltung der Datenschutzeinstellungen, das Erstellen sicherer Passwörter und die Überwachung von Datenschutzverletzungen (hier können Sie die Infografik zu guten Datenschutzpraktiken verwenden). **5. Fragen und Abschluss (5 Minuten)** • **Fragen und Antworten**: Raum für Fragen und abschließende Erläuterungen. • **Fazit**: Ermutigen Sie die SuS, sich weiter mit den Datenschutzeinstellungen ihrer Konten zu beschäftigen und sich über gute Online-Sicherheitspraktiken auf dem Laufenden zu halten.

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.