

Cluster C – Datenschutzmaßnahmen

Was kann ich konkret tun? | 5.–8. Klasse | ca. 90 Min

Fach	Medien und Informatik / Gemeinschaftskunde
Dauer	2 Lektionen à 45 Min oder 1 Doppelstunde
Folien	Abrufbar unter: https://www.datapro.education/datapro-webgames/ unter "Class Material" → "Presentations: Data Protection Measures" → DE Neben Deutsch auch in Englisch, Spanisch und weiteren Sprachen verfügbar (7 Folien)
Weitere Materialien	- Arbeitsblatt Phishing, DataPro Chatbot (für Quiz-Aufgabe), Kahoot: https://www.datapro.education/tools/ - vor Unterrichtsbeginn: Game Guide für Lehrkräfte beides verfügbar unter https://www.datapro.education/datapro-webgames/
Vorwissen	Nach Cluster A + B – kann aber auch eigenständig eingesetzt werden
Spiel	https://dataprogames.ph-freiburg.de/nothing-to-hide/

Lernziele

- Starke Passwörter nach Merkwort-Methode erstellen (C.2)
- 2FA-Faktoren erklären und Einsatzbeispiele nennen (C.2)
- Phishing-Merkmale und Social-Engineering-Taktiken erkennen (C.4)
- Richtig auf Phishing-Versuche reagieren: nicht klicken, melden, Absender prüfen (C.4)
- Mit dem DataPro Chatbot eigenständig recherchieren und Lernmaterial erstellen (C.5)

Unterrichtsablauf

Zeit	Phase / Ziel	Unterrichtsablauf	Folie / Material
10 Min	Einstieg <i>Bestandsaufnahme</i>	- Impulsfrage: Was tut ihr schon, um euch online zu schützen? - Antworten clustern: was machen viele / was wird oft vergessen - Haltung setzen: Es geht um bewusste Entscheidungen, nicht Perfektion	Keine Folien – offenes Gespräch
25 Min	Input: Passwörter & 2FA <i>Sicherheit technisch</i>	- Folie 2: Passwörter – Aufgabe direkt mit SuS durchführen (Merkwort-Methode) - Folie 3: 2FA – drei Faktoren erklären; Beispiele aus dem Alltag sammeln - Sicherung: Warum reicht ein starkes Passwort allein nicht?	→ Folie 2: Passwörter + Aufgabe (im Folienmaterial integriert) → Folie 3: 2FA
20 Min	Input: Phishing & Social Engineering	- Folie 4: Phishing-Typen und Social-Engineering-Taktiken erklären	→ Folie 4: Phishing + Social Engineering

	<i>Angriffe erkennen</i>	- Folie 5: Beispiele analysieren – Klassendiskussion: Worauf weist das hin? - Arbeitsblatt Phishing: SuS identifizieren Merkmale in Beispielnachrichten	→ Folie 5: Beispiele zur Diskussion → Arbeitsblatt Phishing https://www.datapro.education/tools/
25 Min	Spiel: Nothing to Hide <i>Massnahmen anwenden</i>	- Beobachtungsauftrag: Welche Schutzmassnahmen helfen im Spiel? - Wo hättet ihr anders gehandelt? - Spielpunkte notieren – Vergleich mit früheren Runden möglich	→ dataprogames.ph-freiburg.de → Folie 7: https://dataprogames.ph-freiburg.de/nothing-to-hide/
20 Min	Transfer: Quiz-Aufgabe <i>Wissen anwenden & teilen</i>	- Folie 6: SuS wählen eine Schutzmassnahme und erstellen ein Quiz mit dem DataPro Chatbot - Prompting-Anleitung steht auf Folie 6 – mit SuS durchlesen - Quizze tauschen, Lösungen vergleichen, Ergebnisse im Plenum sichern	→ Folie 6: Quiz-Aufgabe + Prompting-Anleitung → DataPro Chatbot (https://datapro.cyber-geiger.com)

Hinweise

Das PDF hat 7 Folien, Folie 2 enthält eine vollständige Aufgabe mit Beispielen.

Folie 6 enthält eine detaillierte Prompting-Anleitung für den DataPro Chatbot – vorlesen.

Die Quiz-Aufgabe (Folie 6) eignet sich auch als Partnerarbeit.

Phishing-Beispiele auf Folie 5 nicht vorher zeigen – SuS sollen selbst Merkmale finden.

Cluster C funktioniert gut als Abschluss: Spielpunkte mit Cluster A vergleichen zeigt Fortschritt.

Lernkontrolle

- Quiz-Vergleich aus Folie 6: Wer hat mehr richtige Antworten beim Partner-Quiz?
- Kahoot-Quiz zu Schutzmassnahmen auf <https://www.datapro.education/tools/>
- Spielpunkte Nothing to Hide – Vergleich Cluster A vs. Cluster C

Projekt	DataPro – Erasmus+
Institution	Pädagogische Hochschule Freiburg
Autorin	Renata Säuberli
Datum	Juni 2026



Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.