Digital? Sicher! – Lernapp zum Erwerb von digitalen Kompetenzen

Vorschläge zum Unterrichtsverlauf und Informationen für Lehrpersonen

DIGITAL? SICHER!

UNI GRAZ

KNOW Center

LOGO! JUGENDMANAGEMENT

Business Analytics and Data Science-Center BANDAS-Center

ortweinschule BAUTECHNIK_KUNST×DESIGN

Das Land Steiermark
Wissenschaft und Forschung

Inhaltsverzeichnis

1. Worum es bei der *Digital?Sicher!* Lernapp geht

Soziale Netzwerke, Nachrichtendienste oder Blogs sind aus dem Online-Alltag nicht mehr wegzudenken. Die Gründe sind viele spannende Möglichkeiten: Persönliche Kontakte pflegen, sich im Netz präsentieren, neue Leute kennenlernen, Informationen erhalten, weiterleiten oder recherchieren oder der einfache Austausch von Fotos und Videos.

Es geht also bei der Digital? Sicher! - Lernapp um den Erwerb digitaler Kompetenzen, speziell um **Fragen über den Schutz unserer Privatsphäre** und **wie man sich sicher im Netz verhält**.

Wir sind ständig von technischen Geräten umgeben, die unsere Daten erheben, verarbeiten, speichern und weiterleiten. Täglich überwachen Hersteller mit GPS unseren Standort, mit elektronischer Bezahlung wird nachvollziehbar, was wir wann und wo gekauft haben und das Fitness Armband weiß, wie viel wir heute gelaufen sind und kennt unseren allgemeinen Gesundheitszustand. Unsere Handys sind Minicomputer mit zahlreichen Apps, denen wir viele Berechtigungen erlauben.

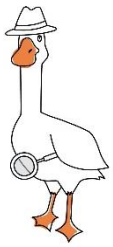
Im Internet hinterlassen wir weitere Datenspuren: Zum einen offensichtliche Spuren, indem wir etwas in sozialen Netzwerken posten. Zum anderen unbewusste Spuren, wenn Firmen unser Surfverhalten aufzeichnen und die dabei gewonnenen Informationen langfristig speichern. Es ist kein Geheimnis, dass Unternehmen wie Facebook, Google oder Amazon — um nur die größten Datensammler zu nennen — mit unseren Daten Milliardengewinne erzielen: Die Nutzer*innen geben teils freiwillig teils unfreiwillig Daten preis, um bestimmte Dienste kostenlos nutzen zu können. Diese Daten werden dann algorithmisch ausgewertet, um Usern möglichst passende Online-Werbung anzeigen zu können, die für sie auch relevant ist. So entstehen mit der Zeit detailreiche Personenprofile. Diese werden international und meist intransparent gehandelt und sind nicht nur für Firmen und Behörden, sondern auch für Kriminelle interessant – etwa zum Identitätsdiebstahl oder um Menschen zu erpressen.

Haben Sie Sich jemals gefragt, wie viele Daten an einem normalen Tag ohne unser Wissen gesammelt werden? Nach EU-Recht hat grundsätzlich jede*r Bürger*in das Recht zu erfahren, welche personenbezogenen Daten über ihn oder sie gespeichert wurden. Doch unsere Datenschutzgesetze gelten nicht weltweit und werden oft von international agierenden Konzernen ignoriert oder geschickt umgangen. Als Konsument*in sollte man daher selbst tätig werden und neben dem kritischen Hinterfragen eigener Kaufentscheidungen Vorkehrungen treffen, die die eigenen Daten schützen. Das bedeutet, dass man früh genug damit beginnen muss, digitale Kompetenzen im Bereich der Datensicherheit im Netz zu erwerben.

2. Was bietet *Digital?Sicher!* Schülerinnen und Schülern?

Digital?Sicher! ist (und bleibt!) ein kostenloses, Moodle-basiertes Lernspiel, das Schüler*innen ein tieferes Verständnis für Themen wie Cybersecurity, Privatsphäre, Tracking und Datafication vermitteln soll.

Die Zielgruppe sind Jugendliche im Alter von 14-16 Jahren, obwohl hier besonders auf die bestehenden Vorkenntnisse zu achten ist und das Lernspiel durchaus von jüngeren bzw. älteren Schüler*innen verwendet werden kann. Die zu diesem Material erstellten Übungen sollen junge Menschen dabei unterstützen, sich bewusster, sicherer und damit mündiger im digitalen Raum zu bewegen. Die Materialien wurden gemeinsam mit verschiedenen Expert*innen, inklusive Schüler*innen und Lehrpersonen entwickelt und getestet. Schüler*innen der HTBLVA Ortweinschule Graz haben dafür attraktive Designs und Grafiken für diverse Charaktere erstellt, die den Spielverlauf begleiten.



Lernapp Konzept:

Im Laufe des Spiels sollen Schüler*innen selbst aktiv werden und eine von vier verschiedenen digitalen Karrieren auswählen. Sie erstellen dazu ihr eigenes Profil und lernen, was einen sicheren Nicknamen und ein gutes Passwort auszeichnen. Doch all diese Aufgaben bewältigen sie nicht alleine, denn es steht ihnen der Avatar und Sicherheitsexpertin, Goosy die Gans, mit Rat und Tat zur Seite. Auch andere Charaktere, wie ihre Freund*innen Kim und Chris, begleiten den Spielverlauf über einen integrierten Chat. Neben zahlreichen Inhalten in Form von Blogposts, kurzen Videos, Infografiken oder Instagram-Posts gibt es auch in jedem der 4 Spielmodule Aufgaben, bei denen die Spieler*innen zeigen können, was sie gelernt haben und sich dadurch Punkte verdienen können. Lehrer*innen müssen während des Spiels keine aktive Rolle übernehmen.

Egal ob verpatzte Bewerbungsgespräche, öffentliche Liebesgeständnisse oder Familiendramen - die Spieler*innen dürfen durch interaktive Elemente laufend eigene Entscheidungen treffen und können so ihre Beliebtheit verstärken und neue Followers dazugewinnen oder aber auch Followers verlieren. Nebenbei erfahren sie anhand von lebensnahen Beispielen, welche potentiellen Gefahren das Internet birgt und wie man diese minimieren kann.

Nach Abschluss der einzelnen Module wird das jeweils folgende Modul freigeschaltet. Einen spannenden Abschluss bietet Modul 4 mit der Gruppenchallenge, die wahlweise alleine oder in Kleingruppen bewältigt werden kann.

Nach Abschluss dieses letzten Spielmoduls wird **nach ca. 1-2 Wochen** das **Reflexionsmodul** 5 zur Post-Reflection freigeschaltet, wo die Schülerinnen und Schüler nochmals über die Anwendung des Gelernten im eigenen Online-Alltag reflektieren können.

3. Step-by-Step Anleitungen

3.1. Erste Schritte – Schnellstart

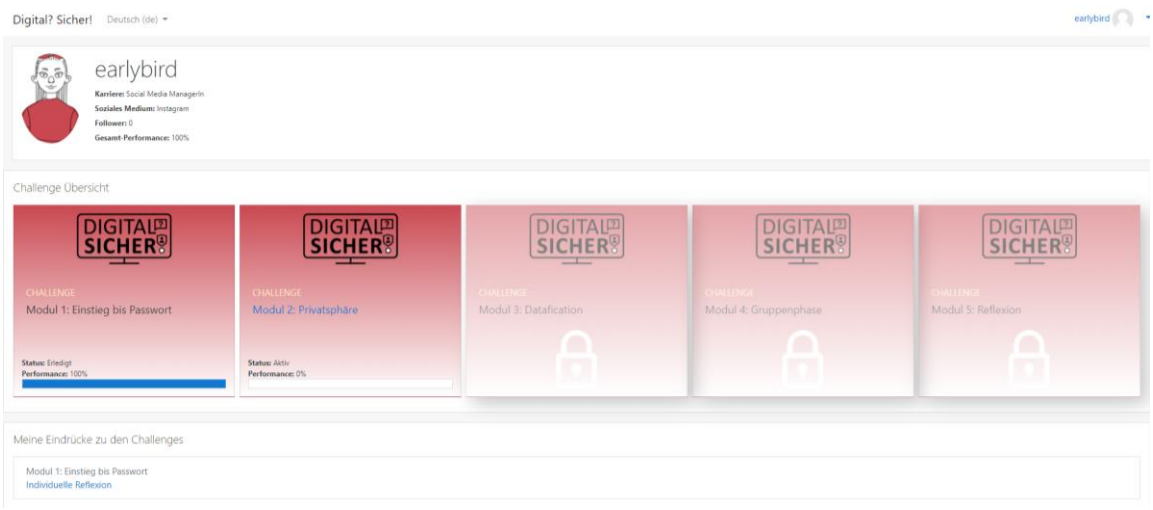
Digital? Sicher! ist ein **kostenloses Selbstläufer-Lernspiel**, bei dem **keine externen Personen** an die Schule kommen. Für Lehrer*innen ist kein spezielles Vorwissen notwendig. Die Schüler*innen spielen das Spiel selbstständig an einem eigenen (Schul)-**Computer** und erstellen dafür zu Beginn einen **Account**. Für die Teilnahme kann je nach Schule auch eine Einverständniserklärung seitens der Erziehungsberechtigten nötig sein (v.a. bei jüngeren Schüler*innen).

Die Lehrer*innen übernehmen während des Spiels keine aktive Rolle (z.B. müssen nicht selbst mitspielen), sondern stehen zur **Erklärung** des Spiels zur Seite, weshalb es wichtig ist, sich vorher mit dieser Anleitung vertraut zu machen. Die geschätzte **Vorbereitungszeit**, die seitens der Lehrperson benötigt wird, sind etwa 1-2 Stunden sowie ca. 15min um einen Probe-Account aufsetzen und 1 Modul durchzuklicken.

- Zu Beginn www.digital-sicher.at in die Adresszeile des Browsers tippen. Danach oben rechts auf „Anmelden“ klicken, um ein kostenloses Konto zu erstellen. Hinweis: Es gibt dabei keine speziellen Lehrer*innen-Accounts, allerdings können Lehrpersonen auch einen eigenen Account erstellen, um das Spiel selbst auszuprobieren bzw. sich damit vertraut zu machen.

HERZLICH WILLKOMMEN BEI "DIGITAL? SICHER!"

- Danach stehen 5 aufbauende Module/Spielteile bereit, die hintereinander gespielt werden. Im Verlauf des Spiels können Punkte gesammelt werden. Erst wenn die vorgegebene Punkteanzahl erreicht wurde, kann das nächste Modul gestartet werden. Bis dahin sind die Module gesperrt. Ein blauer Balken zeigt den jeweiligen Fortschritt im Modul. Lehrer*innen sind Berater*innen bei der Nutzung und müssen selbst nicht mitspielen.

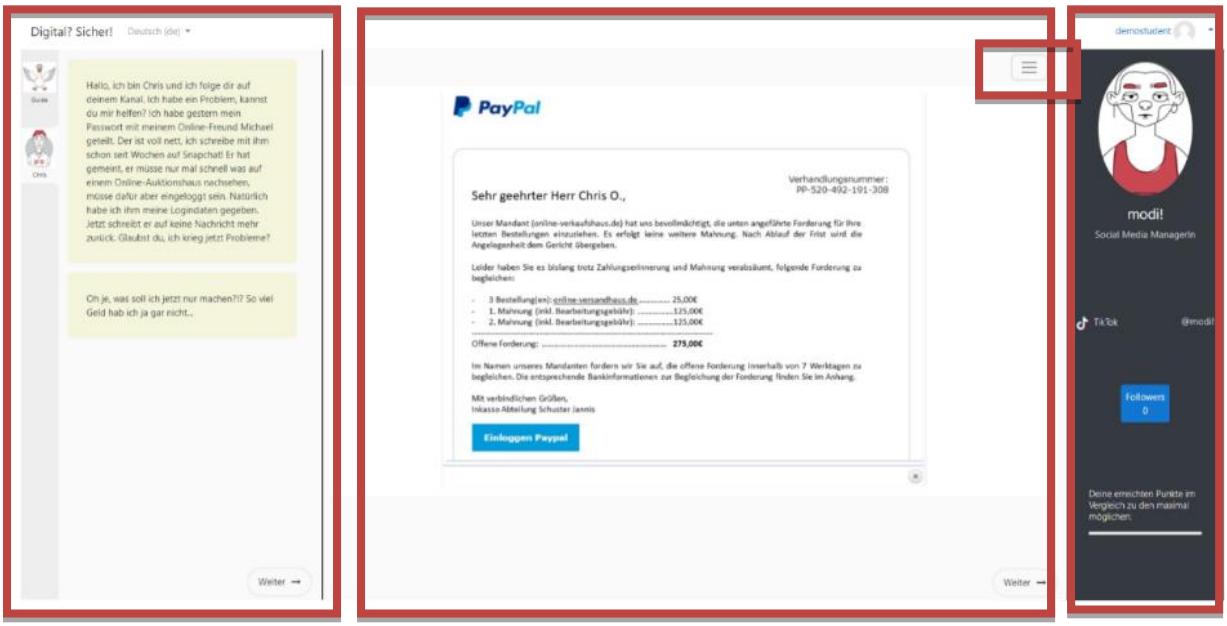


- Das Fenster im Spielbereich teilt sich in drei Bereiche:

    1. Links, das Nachrichtenfeld: Hier kommunizieren Charaktere in Chatform mit den Spielenden, die mit einer Handlung durch das Spiel führen.

    2. Mittig, das Inhaltsfeld: Hier werden Inhalte, Aufgaben, Rätsel, Video, Bilder, usw angezeigt. Auf dem Feld rechts oben mit drei horizontalen Strichen kann man das Profilfeld ein- oder ausklappen.

    3. Rechts, das Profilfeld: Hier sieht man das selbst gewählte Profilbild, den Spieler*innennamen, den Kanal, die Punkte und die Follower*innenzahl.



Nachrichtenfeld Inhaltsfeld Profilfeld

- Die ersten drei Module können allein gespielt werden. Im vierten Modul können die Aufgaben auch gemeinsam in der Gruppe gelöst werden.

- Die Module sind so konzipiert, dass Sie im Schulunterricht oder zu Hause absolviert werden können. Alle notwendigen Schritte oder Aufgaben werden im Spielverlauf erklärt.

- Das Spiel kann auch auf einem Smartphone oder Tablet gespielt werden. Zur übersichtlicheren Darstellung wird aber ein Computer/Laptop empfohlen.

- Browser-Empfehlung: Wir empfehlen, einen anderen Browser als den Internet Explorer zu verwenden (z.B. Chrome).

- Nach der kurzen Reflexion am Ende jedes Moduls kommt man zum Endbildschirm, wo es die Optionen „Zurück zum Dashboard“ sowie „Challenge erneut starten“ gibt. Möchte man den Spielstand speichern und weiter zur nächsten Challenge, klickt man auf „Zurück zum Dashboard“. Möchte man die Challenge lieber noch einmal wiederholen, klickt man auf „Challenge erneut starten“ – der Spielstand des 1. Versuchs wird somit nicht gespeichert.

3.2. Anleitung für die Gruppenchallenge

- **Voraussetzung** für die Teilnahme: alle Module (1-3) vor der Gruppenchallenge sind abgeschlossen
- Die Gruppenchallenge ist Teil von Modul 4. Modul 4 **startet** wie gewohnt so, dass die Schüler*innen **einzeln** an ihren Geräten spielen (bis zur Frage „Willst du die Challenge alleine oder in einer Gruppe spielen?“)
- Wir empfehlen, diesen Teil des 4. Moduls in einer Gruppe mit mind. 2 Teilnehmer*innen zu spielen, hierfür antworten die SuS auf die Frage „Willst du die Challenge alleine oder in einer Gruppe spielen?“ mit „**Als Gruppe spielen**“. Es gibt aber auch die Möglichkeit, diesen Teil alleine durchzuspielen. Hierfür klicken die SuS auf „**Alleine spielen**“ (siehe Abbildung Modul 4 - Moderator*in oder Teilnehmer)

- Die SuS organisieren sich selbst und bilden eine Gruppe. Hat sich eine Gruppe gefunden, wird ein Gruppenmitglied zum/zur **Moderator*in** gewählt. Die Gruppenmitglieder setzen sich um das Gerät des/der Moderators*in. Der/Die Moderator*in meldet die Teilnehmer*innen mit dem Nicknamen ihres Moodle Benutzerkontos zur Gruppenchallenge an (siehe Abbildungen Modul 4 - Ansicht Moderator*in um Teilnehmer*in hinzuzufügen und Modul 4 - Ansicht Moderator*in nachdem drei Teilnehmer hinzugefügt wurden). Der Nickname wird in der App oben rechts angezeigt (siehe Abbildung Nickname eines Benutzerkontos)

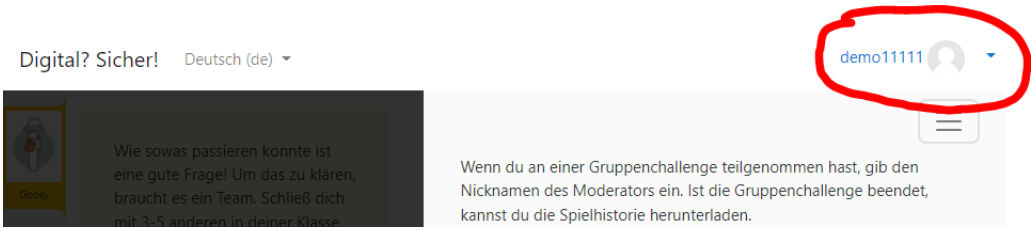


Abbildung 1: Nickname eines Benutzerkontos

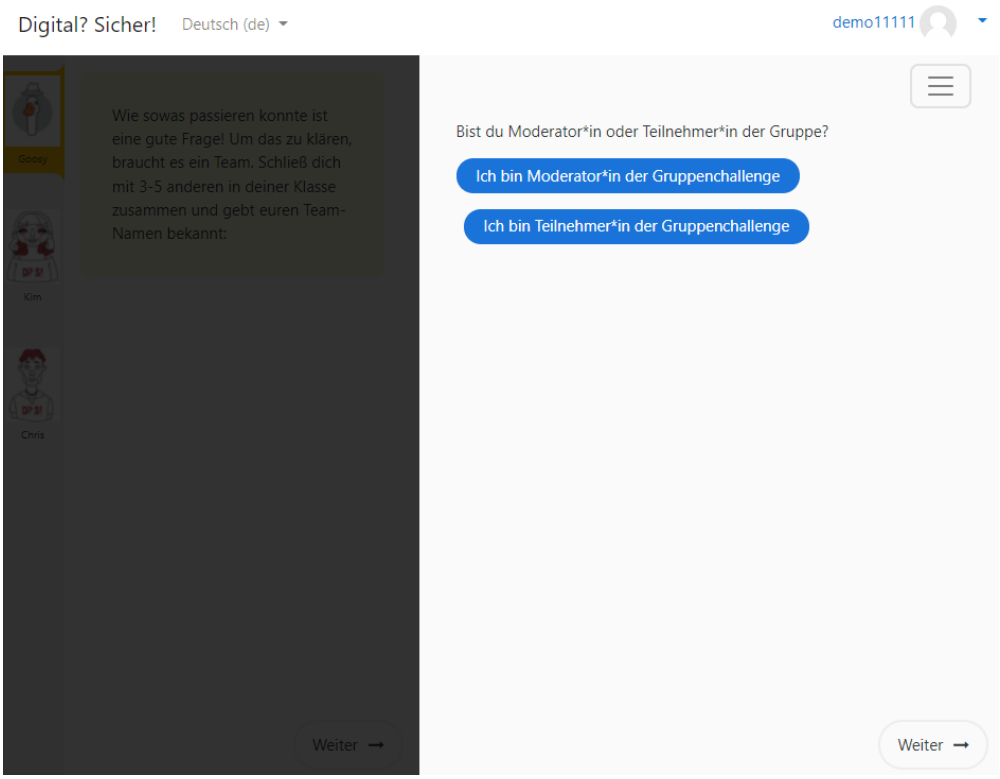


*Abbildung 2: Modul 4 - Moderator*in oder Teilnehmer*

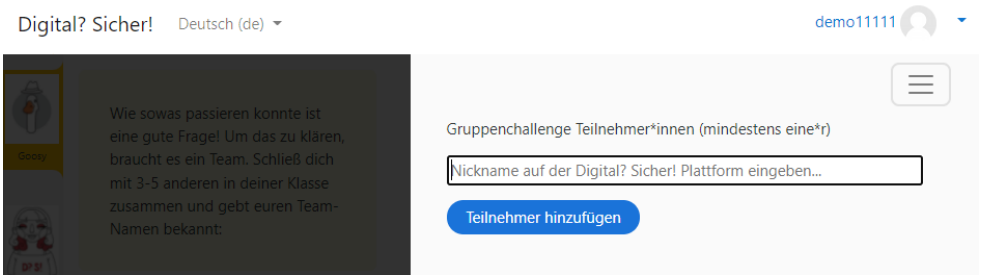


*Abbildung 3: Modul 4 - Ansicht Moderator*in um Teilnehmer*in hinzuzufügen*

(anschließend: Klick auf „Weiter“ rechts unten)

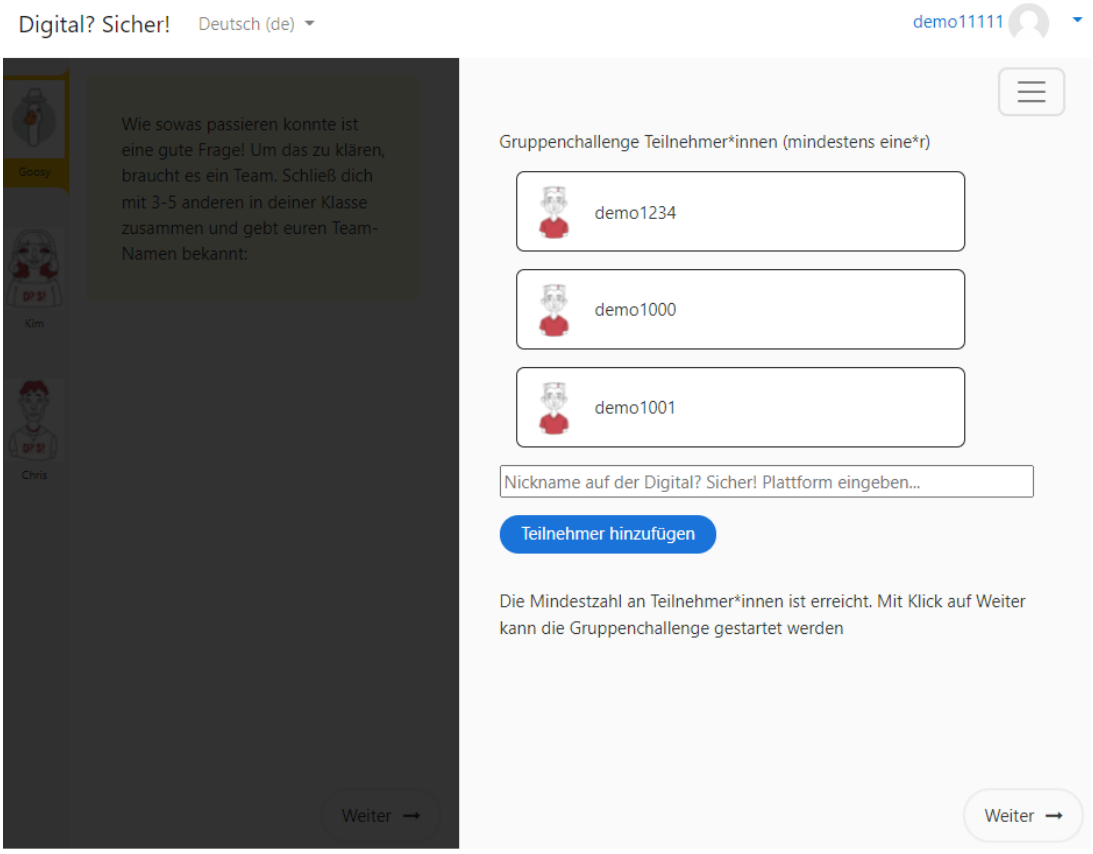


*Abbildung 4: Modul 4 - Ansicht Moderator*in nachdem drei Teilnehmer hinzugefügt wurden*

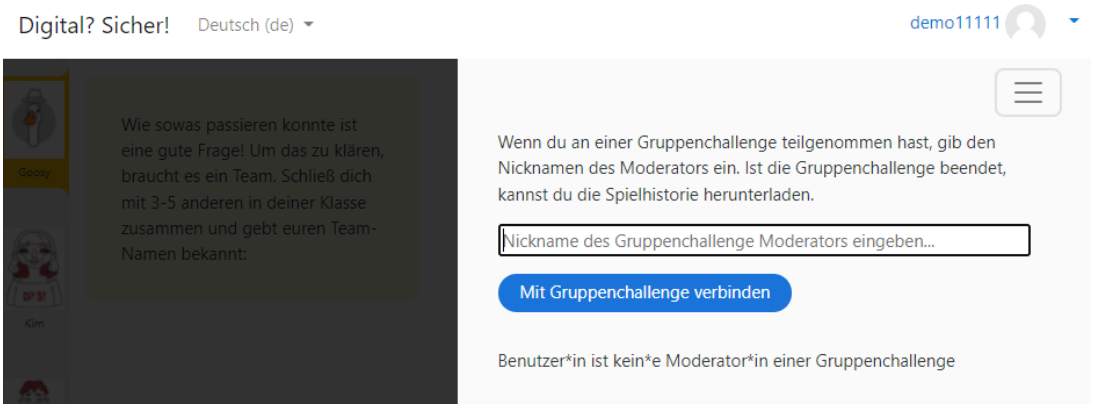


*Abbildung 5: Modul 4 - Ansicht Teilnehmer*in einer Gruppe, um sich mit gespielter Gruppenchallenge zu verbinden*

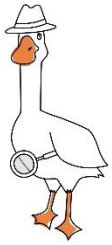
- Das **Spielende** der Gruppenchallenge ist ähnlich wie in den vorigen Modulen, allerdings kann dieses Modul **nicht nochmals gespielt** werden.
- Damit alle Gruppenmitglieder die **Ergebnisse** bekommen, starten anschließend auch die Teilnehmer*innen, die nicht Moderator*in waren, die Gruppenchallenge und geben den Nicknamen des/der Moderators*in an (siehe Abbildung Modul 4 - Ansicht Teilnehmer*in einer Gruppe, um sich mit gespielter Gruppenchallenge zu verbinden). Der Spielstand wird somit übertragen und das nächste Modul wird freigeschaltet.

4. Lernziele und Curriculum: Lehrplankonformer Kompetenzerwerb

Die Zielgruppe des Projekts *Digital? Sicher!* sind Schülerinnen und Schüler im Alter von ca. 14-16 Jahren (8. bis 10. Schulstufe). Die Jugendlichen setzen sich im Laufe des Spiels mit diversen Szenarien, Fallbeispielen, Erklärtexten und Quizfragen auseinander und können dadurch ihre digitalen Kompetenzen anwenden und erweitern.

Die durch *Digital? Sicher!* entwickelten Kompetenzen sind auf die Lernziele aus dem Lehrplan der verbindlichen Übung Digitale Grundbildung, dem Lehrplan für Informatik (AHS) sowie für Angewandtes Informationsmanagement (HLW), Angewandte Informatik und Medieninformatik (HAK) abgestimmt. Es ist nicht notwendig, die einzelnen Bereiche dieser Lehrpläne im Vorfeld auszuarbeiten. Dieses Lernspiel kann prinzipiell in allen Unterrichtsfächern verwendet werden, da kein spezielles Vorwissen nötig ist.

Digital? Sicher! fokussiert sich insbesondere auf die Vertiefung der folgenden vier **Bereiche des Lehrplans für digitale Grundbildung**:



1. Gesellschaftliche Aspekte von Medienwandel und Digitalisierung
2. Digitale Kommunikation und Social Media
3. Sicherheit
4. Computational Thinking

(Verordnung des Bundesministers für Bildung, Wissenschaft und Forschung, mit der die Verordnung über die Lehrpläne der Neuen Mittelschulen sowie die Verordnung über die Lehrpläne der allgemeinbildenden höheren Schulen geändert werden, BGBl. II Nr. 71/2018)

4.1. Gesellschaftliche Aspekte von Medienwandel und Digitalisierung

Digital?Sicher! hilft Schülerinnen und Schülern die Digitalisierung im Alltag bewusst wahrzunehmen und zu nutzen. Dabei sollen die folgenden Lernziele gemäß dem Lehrplan für Digitale Grundbildung erreicht werden:

- *Die Lernenden sind in der Lage, "die Nutzung digitaler Geräte in ihrem persönlichen Alltag [zu] gestalten", sie "reflektieren die eigene Medienbiografie sowie Medienerfahrungen im persönlichen Umfeld" und können "mögliche Folgen der zunehmenden Digitalisierung im persönlichen Alltag" erklären.*

- *Mit Hilfe der Digital? Sicher! Szenarien und Charaktere werden sich Schülerinnen und Schüler so der Rolle digitaler Medien im eigenen Umfeld bewusst und können diese in Folge gezielter einsetzen.*

4.2. Digitale Kommunikation und Social Media

Digital? Sicher! legt großen Wert auf die Vertiefung der Lernziele in Bezug auf digitale Kommunikation und Social Media. Anhand der Storyline gilt es, verschiedene Social Media Kanäle zu unterscheiden und ihren Nutzen sowie ihre Gefahren kennenzulernen. Somit werden folgende Ziele des Lehrplans für digitale Grundbildung erreicht:

- *Die Lernenden "kennen verschiedene digitale Kommunikationswerkzeuge", "beschreiben Kommunikationsbedürfnisse und entsprechende Anforderungen an digitale Kommunikationswerkzeuge", und "schätzen die Auswirkungen des eigenen Verhaltens in virtuellen Welten ab und verhalten sich entsprechend".*

- *Die Schülerinnen und Schüler erkennen außerdem "das Internet als öffentlichen Raum" sowie die "damit verbundenen Nutzen und Risiken" und "gestalten und schützen eigene digitale Identitäten reflektiert".*

4.3. Sicherheit

Ein weiterer wesentlicher Bestandteil von *Digital? Sicher!* ist die Bewusstseinsbildung Jugendlicher zum Thema Sicherheit im Netz. Dabei sollen Schülerinnen und Schüler lernen, persönliche Daten und ihre Privatsphäre zu schützen sowie digitale Kommunikation über Social Media kritisch zu nutzen.

Dies entspricht folgenden Zielen laut Curriculum für digitale Grundbildung:

- *"Schülerinnen und Schüler verstehen, wie persönlich nachvollziehbare Informationen verwendet und geteilt werden können", sie "treffen Vorkehrungen, um ihre persönlichen Daten zu schützen", und "kennen Risiken, die mit Geschäften verbunden sind, die im Internet abgeschlossen werden".*

- *Außerdem können Lernende "zielgerichtet geeignete digitale Technologien für konkrete Kommunikationsszenarien auswählen und bedenken bei der Auswahl die Interessen der Anbieter von Social Media, den Einfluss von Social Media auf ihre Wahrnehmung der Welt und Art und Umfang der Daten, die durch die Nutzung entstehen."*

4.4. Computational Thinking

In Hinblick auf Computational Thinking lernen Schülerinnen und Schüler durch *Digital? Sicher!* Algorithmen zu verstehen und zu erkennen. Im Lehrplan entspricht dies folgendem Lernziel:

- *"Schülerinnen und Schüler erkennen die Bedeutung von Algorithmen in automatisierten digitalen Prozessen (z. B. automatisiertes Vorschlagen von potenziell interessanten Informationen)."*

- *Bezüglich digitaler Kommunikation und Social Media lernen die Jugendlichen außerdem sich angemessen im Internet zu verhalten: "Schülerinnen und Schüler wenden Verhaltensregeln für die Nutzung digitaler Technologien und zur Interaktion in digitalen Umgebungen an („Netiquette")."*

4.5. Kompetenzerwerb aus (angewandter) Informatik bzw. angewandtem Informationsmanagement und Medieninformatik

Die Lernziele von *Digital? Sicher!* sind darüber hinaus auch auf die Lehrpläne aus (angewandter) Informatik (AHS, HAK) bzw. Angewandten Informationsmanagement (HLW)

und Medieninformatik (HAK) in der Sekundarstufe II abgestimmt. Demnach unterstützt "Digital? Sicher" Schülerinnen und Schüler beim Erwerb folgender Kompetenzen:

- *Fähigkeit zur Erstellung sicherer Passwörter und zum verantwortungsvollen Umgang mit diesen (siehe Lehrplan HLW, 1. Jahrgang sowie HAK, 1. Jahrgang)*
- *Kommunikationskompetenz, die es ermöglicht, "verantwortungsbewusst, effizient und zielgerichtet online [zu] kommunizieren" (Lehrplan HLW, 1. Jahrgang)*
- *Befähigung zur verantwortungsbewussten Nutzung sozialer Netzwerke (Lehrplan HLW, 1. Jahrgang)*
- *Kenntnisse in Bezug auf Datensicherheit, Datenschutz und Urheberrecht (siehe Lehrplan AHS, 5. Klasse)*
- *Kompetenz "Informationsquellen [zu] erschließen, Inhalte [zu] systematisieren, strukturieren, bewerten, verarbeiten und unterschiedliche Informationsdarstellungen verwenden [zu] können" (siehe Lehrplan AHS, 5. Klasse)*
- *Grundwissen über Algorithmen und die Kompetenz, diese und ihre Auswirkungen darstellen zu können (siehe Lehrplan AHS, 5. Klasse)*
- *Bewusstsein über mögliche Gefahren des Internets (HAK 2. Jahrgang angewandte Informatik)*
- *Kompetenz mit diversen Social Media Kanälen umzugehen, Risiken zu erkennen, "Inhalte plattformspezifisch bereit[zu]stellen", "Netiquette an[zu]wenden", sowie "Influencer [zu] identifizieren und einzusetzen" (HAK, 1. Jahrgang Medieninformatik)*

Hinweis: In manchen Schulen kann es notwendig sein, dass eine Genehmigung der Eltern/Erziehungsberechtigten für den Einsatz von Apps/Lernspielen eingeholt wird.

Quellen:

Lehrplan Digitale Grundbildung:
https://www.bmbwf.gv.at/Themen/schule/zrp/dibi/dgb.htm

Lehrplan AHS:
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008568&FassungVom=2017-08-31

Lehrplan HAK:
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008944

Lehrplan HLW:
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009369

saferinternet.at, onlinesicherheit.gv.at, klicksafe.de

5. Pädagogische Grundlage in *Digital?Sicher!*

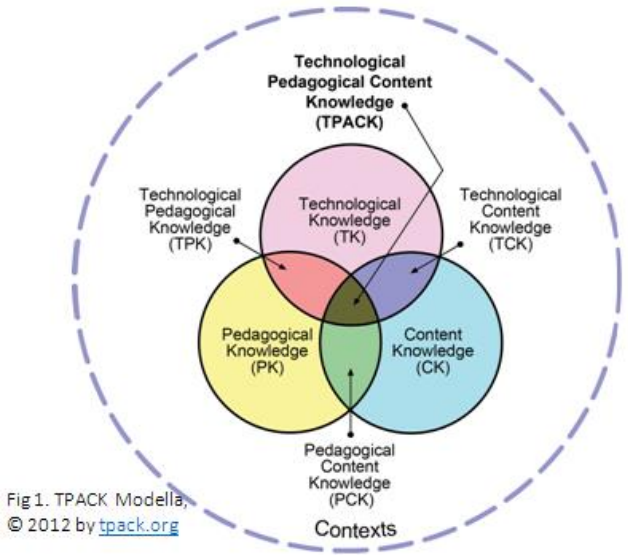


Fig 1. TPACK Modella, © 2012 by tpack.org

Der pädagogische Ansatz von *Digital?Sicher!* basiert auf dem TPACK Framework (Technology, Pedagogy and Content Knowledge). Dieses Konzept wurde 2006 von Punya Mishra und Matthew J. Koehler an der Michigan State University erstellt. Sie unterscheiden drei wesentliche Arten des Wissens, das Lehrpersonen benötigen, um Technologie erfolgreich im Unterricht zu integrieren (siehe Fig. 1): Inhaltliches Wissen bzw. Content Knowledge (CK), Pädagogisches Wissen bzw. Pedagogical Knowledge (PK), und Technologisches Wissen bzw. Technological Knowledge (TK).

Diese drei Bereiche sind jedoch nicht vollständig separat: die Schnittpunkte sind wesentlich, und zeichnen vertiefte Kompetenzen von Lehrpersonen aus, wenn diese Technologie, Pädagogik und Fachwissen synergistisch für den Unterricht zusammenführen. Das Zentrum des Diagramms, auch bekannt als TPACK, zeigt ein ganzheitliches Verständnis wie man mit Technologie unterrichtet und weist darauf hin, dass es nicht dasselbe ist wie über Wissen aller drei Hauptkonzepte einzeln zu verfügen. Der Kernaspekt von TPACK ist es zu verstehen wie man Technologie einsetzen kann um Konzepte möglichst effektiv und zielgruppengerecht zu unterrichten. Die sorgfältige pädagogische Verwendung von Technologie setzt die Entwicklung einer komplexen Form des Wissens voraus, die mehr als nur die Summe der einzelnen Aspekte ist.

Für das digitale Lernspiel *Digital?Sicher!* bedeutet das, dass eine Lehrperson diese Lernapp nicht isoliert einsetzen sollte, sondern sich mit den technischen und inhaltlichen Vorkenntnissen ihrer Schüler*innen auseinandersetzt um das Spiel in den Unterricht zu integrieren und damit optimale Lernerfolge zu erzielen.

Die technische Umsetzung der Lernapp basiert auf dem Learning Management System Moodle und wird eingesetzt, um Inhalte zu Themen wie Cybersecurity spielerisch zu vermitteln. Das heißt, dass hier mit dem Konzept verschiedener Module gearbeitet wurde, in denen sich Schülerinnen und Schüler mit verschiedenen relevanten Inhalten beschäftigen. Diese Module sind thematisch unterteilt in die Bereiche Sicherheit im Netz, Privatsphäre, Datenschutz sowie Cyberangriffe.

Der Einsatz dieser Lernapp ist aber nur dann komplett, wenn auch pädagogisches Wissen eingesetzt wird. Daher empfehlen wir, die Schülerinnen und Schüler vor, während und nach dem Spiel pädagogisch zu begleiten.

Das heißt, vorab müssen folgende Aspekte durch die Lehrperson evaluiert werden:

- ***Vorwissen der Schüler*innen*** (Vorkenntnisse, Vorerfahrungen) zum Thema Sicherheit im Netz (hierbei ist zu beachten, dass jungen Menschen nicht „automatisch“ gute digitale Kompetenzen haben, nur weil sie zur „digitalen Generation“ gehören.

- ***Soziale Bedingungen und kulturelle Lernvoraussetzungen*** im Klassenverband. Beachten Sie, dass es gerade bei digitalen Kompetenzen viel ausmacht, ob junge Menschen die finanzielle Möglichkeit haben/hatten, Technologie zu Hause zu erleben, beziehungsweise Unterstützung hatten über Sicherheit zu lernen oder aber sich dies selber beigebracht haben.

- ***Technische Grundausstattung*** und deren pädagogische Konsequenzen. Zum Beispiel: Hat jede*r Schüler*in Zugang zu einem Laptop/PC/Tablet mit dem gearbeitet werden kann oder müssen sich Schüler*innen die Geräte teilen? Welche pädagogischen Konsequenzen ergeben sich daraus?

- ***Motivation der Schüler*innen*** um die Lernapp optimal einzusetzen. Hier hilft es, lebensnahe Beispiele zu besprechen in denen junge Menschen in durchaus unangenehme Situationen kommen, wenn sie zum Beispiel in sozialen Medien mit Nachrichten dubioser Natur konfrontiert werden.

- Eventuelle entwicklungspsychologische, kognitive, psychomotorische ***Lernvoraussetzungen*** im Klassenverband.

- ***Beziehungsgefüge und Verkehrsformen*** in der Klasse und Vertrautheit mit unterschiedlichen Sozialformen, um die Lernapp optimal einzusetzen.

6. Konkrete Vorschläge zur Einbettung in den Unterricht

Digital? Sicher! bietet Schüler*innen **insgesamt 5 Module**: die Spielmodule 1-4 sowie das Reflexionsmodul 5.

In **Modul 1** geht es darum, eine Karriere im digitalen Bereich auszuwählen und dafür einen möglichst sicheren Account aufzusetzen. Dafür wählen die Spieler*innen einen passenden Channel für ihre Karriere aus und überlegen sich einen Nicknamen. Ein besonderer Fokus wird in diesem Modul auf die Erstellung eines sicheren Passworts gelegt, das möglichst schwer zu knacken sein soll. Anhand von Videos und Postings wird erklärt, zu welchen Konsequenzen leicht zu knackende Passwörter führen können.
Das **Modul 2** beschäftigt sich mit dem Thema Privatsphäre und zeigt auf, wie wichtig der Schutz intimer Daten ist. Schüler*innen entscheiden in diesem Modul, welche persönlichen Daten man im Internet preisgeben kann und welche man lieber für sich behält. Außerdem beschäftigen sie sich mit den Privatsphäre-Einstellungen beliebter Sozialer Medien wie Instagram oder Tik Tok und erkennen mögliche Konsequenzen von öffentlichen Social Media Postings, die besser nicht für jeden zugänglich sein sollten.
In **Modul 3** dreht sich alles um den täglichen Begleiter der meisten jungen Leute: das Smartphone. Hier entdecken die Schüler*innen, welche Datenspuren sie täglich über ihr Smartphone hinterlassen und wie diese durch Tracking nachverfolgt werden können. Weiters werden die Begriffe Algorithmus, Cookies und digitale Spuren erklärt und unterschieden. Schüler*innen erfahren außerdem, wie Unternehmen diese Daten für maßgeschneiderte Werbung verwenden.
Modul 4 startet mit einer Whatsapp-Nachricht einer vermeintlichen Followerin, die dazu auffordert, auf einen unbekannten Link zu klicken. In diesem Modul entdecken die Spieler*innen verschiedene Formen der Internetkriminalität und unterscheiden Begriffe wie Erpressungstrojaner, Phishing-Angriff, Adware oder Spyware. Das Highlight bietet die Gruppenchallenge, in der die Schüler*innen alleine oder im Team herausfinden sollen, wie und von wem ihr Account gehackt werden konnte.
Das abschließende **Reflexionsmodul 5** dient zur Post-Reflexion, die in etwa 1-2 Wochen nach Spielende erfolgen soll. Dieses Modul soll den Schüler*innen dabei helfen, sich noch einmal an das Erlernte zu erinnern und zu überlegen, inwiefern sie die Erkenntnisse aus den Spielmodulen auch im eigenen Alltag umsetzen können.

Die Module sind so konzipiert, dass **jeweils 1 Modul pro Unterrichtsstunde** (50 min.) erarbeitet werden kann. Für die darauffolgende Stunde bzw. Doppelstunden finden Sie auf den folgenden Seiten Vorschläge für Follow-up Aktivitäten zu den Modulen 1-4. Je nach Vorwissen der Schüler*innen zu den einzelnen Themenbereichen können jedoch auch mehr oder weniger Stunden für die Erarbeitung eingeplant werden.

6.1. Vorschlag zur Bearbeitung von Modul 1 (Erstellung eines sicheren Accounts)

Zeit	Aktivität	Methode	Ziel
15min	Warm-up Aktivität: Finde jemanden, der …	Schüler*innen tauschen sich untereinander zu ihrer eigenen Online-Präsenz aus indem sie mittels Handout nach Personen suchen, die z.B. einen Instagram Account haben	Spielerischer Einstieg in die Thematik
10-15 min	Einleitung: Erklärung des Spiels und Überblick über die Module	Kurze Einführung in Digital? Sicher! durch die Lehrperson und Einstieg am PC (für technische Erklärungen siehe 3. Step-by-Step Anleitungen)	Schüler*innen einen Überblick über die 5 Module verschaffen sowie Einstieg und Erstellung eines Accounts
20-25min	Schüler*innen spielen Modul 1	Schüler*innen spielen individuell	Schüler*innen entdecken das Spiel und lernen, wie man einen sicheren Account aufsetzt
20-30 min	Follow-up: Nachbesprechung (Reflexionsfragen, eigene Social Media Präsenz der Schüler*innen und Fragen der Warm-up Aktivität besprechen)	Austausch im Plenum	Schüler*innen reflektieren ihre eigene Internetpräsenz

Dieses Stundendesign und die Zeitangaben sind als Vorschläge zu verstehen und müssen an die jeweiligen Klassengefüge und Unterrichtssituationen angepasst werden. Für das Spielen von Modul 1 empfiehlt es sich, ca. 20-25 Minuten einzuplanen.

In Modul 1 lernen Schüler*innen das Lernspiel kennen und finden heraus, wie man ein möglichst sicheres Passwort erstellt (z.B. mehrere verschiedene Zeichen, Groß- und Kleinschreibung, keine Namen von Haustieren, Merken durch Eselsbrücken etc.)

Vorbereitung Modul 1 (Erstellung eines sicheren Accounts):

Einstieg ins Thema: Finde jemanden, der…

Beispielfragen (können frei adaptiert werden) – Handout siehe Anhang

- Einen Instagram Account hat
- Einen Tik Tok Account hat

- Einen Facebook Account hat
- Einen kreativen Nicknamen auf Social Media hat
- Weiß wie man ein sicheres Passwort erstellt
- Schon einmal eine komische E-Mail von einem unbekannten Absender erhalten hat
- Jemanden kennt, von dem schon einmal ein Social Media Account von anderen verwendet wurde
- Jemanden kennt, von dem schon einmal ein Passwort geknackt wurde
- Weiß was ein Algorithmus ist

Nachbereitung Modul 1 (Erstellung eines sicheren Accounts):

Beispielfragen für eine Gruppendiskussion

- Welche Vorteile haben Soziale Medien?
- Welche Gefahren gehen von Sozialen Medien aus?
- Welche digitalen Berufe kennst du?
- Worauf achtest du, wenn du etwas postest?
- Hast du schon einmal Probleme wegen eines Postings bekommen?
- Wie stehen deine Verwandten (Geschwister, Eltern, Großeltern) zu Sozialen Medien
- Welche Daten gibst du im Internet preis?

Zusatzmaterial (für die Themen aller Module):

- Sollten einzelne Schüler*innen schneller mit den einzelnen Modulen fertig sein, kann diese Zeit für zusätzliche Online-Übungen, z.B. von der Saferinternet Plattform genutzt werden. Hier finden sich unter anderem Info-Broschüren oder auch interaktive Quizzes (siehe https://www.saferinternet.at/quiz/).

6.2. Vorschlag zur Bearbeitung von Modul 2 (Privatsphäre)

Zeit	**Aktivität**	**Methode**	**Ziel**
15min	Einleitung: Partnerinterview	Schüler*innen interviewen sich gegenseitig zum Thema Privatsphäre im Netz	Einstieg in das Thema „Privatsphäre im Netz“
30-40 min	Schüler*innen spielen Modul 2	Schüler*innen spielen individuell	Schüler*innen entdecken das Spiel und lernen dabei, welche Fragen man sich stellen sollte, bevor man online etwas preisgibt und welche Folgen unangebrachte Postings haben können
15-30 min	Follow-up: Diskussionsrunde	Besprechung der Antworten der Partnerinterviews	Schüler*innen reflektieren ihre eigene Online Präsenz

Dieses Stundendesign und die Zeitangaben sind als Vorschläge zu verstehen und müssen an die jeweiligen Klassengefüge und Unterrichtssituationen angepasst werden. Für das Spielen von Modul 2 empfiehlt es sich, ca. 30-40 Minuten einzuplanen.

Vorschläge für Interview- bzw. Diskussionsfragen zu Modul 2 (Privatsphäre):

- Was sind personenbezogene Daten?
- Was ist ein Persönlichkeitsprofil?
- Welche Fragen sollte man sich stellen, bevor man online etwas über sich preisgibt?
- Welche Daten kann man problemlos veröffentlichen, welche sind problematisch?
- Was sind App-Berechtigungen?
- Worauf hat WhatsApp auf deinem Smartphone Zugriff?
- Welche Folgen können unangebrachte Postings im Internet mit sich bringen?

6.3. Vorschlag zur Bearbeitung von Modul 3 (Datafication)

Zeit	Aktivität	Methode	Ziel
15min	Einleitung: Punkteabfrage zu Datafication	Schüler*innen ordnen ihre eigene Social Media Nutzung auf einer Skala (z.B. auf der Tafel) ein, indem sie darauf einen Punkt kleben	Reflektion der Schüler*innen zur eigenen Social Media Nutzung, Einleitung in Modul 3
30-40 min	Schüler*innen spielen Modul 3	Schüler*innen spielen individuell	Schüler*innen entdecken das Spiel und lernen, welche Daten Online Dienste über sie speichern und was damit geschieht
30 min	Follow-up: Fish-Bowl-Diskussion: „Welche Konsequenzen hat das Smartphone als Datensammler?“	Schüler*innen bekommen Rollenkärtchen (siehe Anhang) und diskutieren die Frage aus der Perspektive ihrer Rolle (siehe Anhang)	Schüler*innen lernen verschiedene Perspektiven zum Thema Datafication kennen und diskutieren Vor- und Nachteile anhand verschiedener Rollen

Dieses Stundendesign und die Zeitangaben sind als Vorschläge zu verstehen und müssen an die jeweiligen Klassengefüge und Unterrichtssituationen angepasst werden. Für das Spielen von Modul 3 empfiehlt es sich, ca. 30-40 Minuten einzuplanen.

Vorbereitung Modul 3 - Beispielfragen für die Punkteabfrage:

- Wie oft bekommst du auf Social Media Werbung für Dinge, die du vorher auf Google gesucht hast? (nie – wöchentlich – täglich – stündlich)
- Wie oft postest du selbst etwas?
- Wie oft glaubst du, dass Social Media Apps Daten über dich speichern?

In Modul 3 beschäftigen sich die Schüler*innen unter anderem mit folgenden Begriffen bzw. Fragestellungen:

- Affiliate Marketing
- Micro-Targeting
- Welche Daten speichern Social Media Apps?
- Was ist ein Bewegungsprofil?
- Warum sind Daten für Unternehmen so wertvoll?

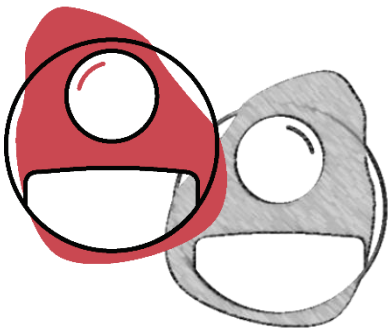
- Was sind Algorithmen? Was sind Cookies?
- Was sind digitale Spuren?

Nachbereitung Modul 3 – Fish-Bowl Diskussion:

Bei einer Fish-Bowl Diskussion bekommen die Schüler*innen je ein Rollenkärtchen (siehe Anhang) und bereiten sich auf die Teilnahme an einer Diskussionsrunde vor der Klasse aus der Perspektive ihrer Rolle vor. Für diese Diskussion eignen sich unter anderem folgende Rollen: besorgter Elternteil, Influencer*in, Smartphone Hersteller*in, Teenager die täglich etwas online posten, Teenager die ihre Daten möglichst gut schützen möchten, Datenschutz-Experte/-Expertin. Selbstverständlich können diese Rollen auch adaptiert werden und andere Perspektiven hinzugefügt werden. Wichtig ist jedoch, darauf zu achten, dass die Rollenverteilung ausgeglichen ist, es also in etwa gleich viele Pro- und Kontra-Argumente geben wird.

Für Modul 3 eignet sich z.B. die Diskussionsfrage: „Welche Konsequenzen hat es, wenn persönliche Daten durch Apps gespeichert werden?“ Sind die Rollenkärtchen verteilt, bekommen die Schüler*innen kurz Zeit, um sich Argumente aus den zugeteilten Sichtweisen zu überlegen. Anschließend werden in der Klasse 6 Stühle aufgestellt, sodass jede Rolle einen Platz bekommt. Ein Platz muss jedoch immer frei bleiben.

Der Moderator bzw. die Moderatorin startet die Diskussion und achtet darauf, dass jedes Mitglied zu Wort kommt. Außerhalb der Diskussionsrunde darf nicht gesprochen werden. Möchte jemand von den beobachtenden Schüler*innen zu Wort kommen, setzt sich dieser auf den freien Stuhl und ein*e andere*r Schüler*in verlässt seinen bzw. ihren Diskussionsstuhl. Sind alle Charaktere zu Wort gekommen und wurden ihre verschiedenen Argumente dargelegt und diskutiert, schließt der Moderator bzw. die Moderatorin die Diskussion.



6.4. Vorschlag zur Bearbeitung von Modul 4 (Cyberangriffe)

Zeit	**Aktivität**	**Methode**	**Ziel**
10min	Einleitung: Welche Arten von Cyberangriffen gibt es?	Brainstorming-Aktivität im Plenum mit dem Wort „Cyberangriffe“ an der Tafel	Vorwissen der Schüler*innen zum Thema Cyberangriffe erheben
30-40 min	Schüler*innen spielen Modul 4	Schüler*innen spielen individuell	Schüler*innen erleben selbst einen Cyberangriff und finden heraus, wie das passieren konnte
20-30 min	Follow-up: Cyberbegriffe-Tabu	In Gruppen oder mit der gesamten Klasse	Schüler*innen ziehen einen Begriff (Druckvorlage siehe Anhang), den sie den anderen erklären. Die Person/Gruppe, die den Begriff richtig errät, bekommt einen Punkt.

Dieses Stundendesign und die Zeitangaben sind als Vorschläge zu verstehen und müssen an die jeweiligen Klassengefüge und Unterrichtssituationen angepasst werden. Für das Spielen von Modul 4 empfiehlt es sich, ca. 30-40 Minuten einzuplanen.

Wichtig: Modul 4 beinhaltet eine **Gruppenphase**. Eine Schritt-für-Schritt Anleitung dafür finden Sie auf Seite 6. Wir empfehlen unbedingt, die Schüler*innen über den Ablauf und ihre Rollen (Moderator*in bzw. Teilnehmer*in) vor dem Spielen dieses Moduls zu informieren.

In Modul 4 lernen die Schüler*innen unter anderem folgende Begriffe kennen:

- Computervirus
- Adware
- Erpressungstrojaner
- Homograph-Attacke
- Identity-Spoofing
- Phishing-Nachricht
- Phishing-Website
- Spam
- Spyware
- Wahrnehmungsbeeinflussung
- Shortlink
- HTTPS
- Popup-Werbung

Vorschlag zur Nachbereitung von Modul 4:

Als Nachbereitung des letzten Spielmoduls empfehlen wir, den Austausch mit dem sozialen Umfeld der Kinder und Jugendlichen zu fördern. Dazu kann z.B. eine Aufgabe gegeben werden, für die Eltern, Geschwister, Freunde und Bekannte zu den verschiedenen Themenbereichen der Module interviewt werden. Diese Personen können z.B. nach der eigenen Social Media Präsenz befragt werden, ihren eigenen positiven und negativen Erfahrungen mit online Postings oder auch darüber, ob sie schon einmal selbst Cyberangriffe erlebt haben. Die Antworten dazu können in der Folgestunde aufgegriffen und diskutiert werden.

6.5. Vorschlag zur Bearbeitung von Modul 5 (Reflexion und Nachbearbeitung, 1-2 Wochen nach Spielende)

Zeit	**Aktivität**	**Methode**	**Ziel**
10min	Einleitung: Rückblick auf die einzelnen Module	Blitzlicht: Schüler*innen nennen einen Begriff, der ihnen von Digital? Sicher! in Erinnerung geblieben ist	Aufwärmübung zur Reflexion, die die behandelten Themengebiete wieder in Erinnerung ruft
20-25min	Schüler*innen reflektieren in Modul 5	individuell	Schüler*innen reflektieren individuell inwiefern sie das Gelernte im eigenen Alltag anwenden
15min	Abschlussdiskussion	Moderiert durch die Lehrperson	Schüler*innen tauschen sich untereinander und mit der Lehrperson darüber aus, welche Aspekte sie aus Digital? Sicher! im Alltag integrieren können

Dieses Stundendesign und die Zeitangaben sind als Vorschläge zu verstehen und müssen an die jeweiligen Klassengefüge und Unterrichtssituationen angepasst werden. Für das Reflexionsmodul 5 empfiehlt es sich, ca. 20-25 Minuten einzuplanen.

Ziel der Reflexion und Nachbearbeitung in Modul 5 ist es, sich über den eigenen Lernprozess bewusst zu werden und Verknüpfungen zwischen den einzelnen Modulen aber auch zwischen den Erfahrungen im Spiel und in der realen Online-Welt herzustellen. Modul 5 fördert durch eine Kombination von Reflexionsfragen und Wiederholungsübungen die selbstständige Wahrnehmung und Anwendung des Gelernten. Somit haben die Schüler*innen noch einmal die Gelegenheit, über die entwickelten Kompetenzen zu reflektieren, sich eigene Ziele für den privaten und beruflichen Umgang mit digitalen Medien festzulegen und sich auch in Zukunft verantwortungsvoll und digital sicher im Netz zu bewegen.

Modul 1: Finde jemanden, der…

Einen **Instagram** Account hat Name:_____	Einen **Tik Tok** Account hat Name:_____	Einen **Facebook** Account hat Name:_____
Einen **kreativen Nicknamen** auf Social Media hat Nickname: _____ Name: _____	Weiß wie man ein **sicheres Passwort** erstellt Name:_____	Schon einmal eine **komische E-Mail** von einem unbekannten Absender erhalten hat Name:_____
Jemanden kennt, von dem schon einmal ein Social Media **Account** von **anderen Personen** verwendet wurde Name:_____	Jemanden kennt, von dem schon einmal ein **Passwort geknackt** wurde Name:_____	Weiß was ein **Algorithmus** ist Name:_____

Modul 3: Rollenkärtchen Fish-Bowl Diskussion

Besorgter Elternteil	Influencer*in	Smartphone Hersteller*in
Teenager, der/die täglich Informationen über sich auf verschiedenen Plattformen postet	Teenager, der/die kein Smartphone verwendet, um seine/ihre Daten zu schützen	Datenschutz-Experte/Expertin

Modul 4: Cyberbegriffe-Tabu

ALGORITHMUS	COOKIES	ADWARE
SPYWARE	SPOOFING	HOMOGRAPH-ATTACKE
AFFILIATE MARKETING	INTIME DATEN	TRACKING