SBG
Serious Business Gaming

SERIOUS BUSINESS GAMING QUARTERLY

MANAGEMENT SCIENCE TECHNOLOGY

Digital aufwachsen – aber auch digital resilient?



Warum wir in der Grundschule mit der **Cyber-Resilienz** beginnen müssen und nie aufhören dürfen - und wie es gelingen kann

SPECIAL zu Cyber-Resilienz in Schulen und Hochschulen Issue 04 · Nov 2026

Editorial



Liebe Leserinnen, liebe Leser,

Bildung soll Menschen befähigen, selbstständig zu urteilen und verantwortlich zu handeln. Hybride Bedrohungen, digitale Täuschung und gezielte Desinformation fordern unsere Gesellschaft heraus. Cyber-Resilienz und Medienkompetenz gehören deshalb zum Bildungsauftrag. Wir brauchen sicheres, reflektiertes Handeln und begründetes Vertrauen. Schulen und Hochschulen können dafür entscheidende Grundlagen schaffen – bei Lernenden und Verantwortlichen.

Wir brauchen sicheres, reflektiertes Handeln, und begründetes Vertrauen

Statt Bildungseinrichtungen mit zusätzlichen Aufträgen und umfangreichen Programmen zu überlasten, schlagen wir einen spielerischen Zugang vor: ein 30-minütiges Lernspiel, integriert in bestehende Unterrichts- oder Projektangebote. Anhand konkreter Situationen treffen die Beteiligten Entscheidungen, diskutieren unterschiedliche Sichtweisen und hinterfragen ihre ersten Impulse.

Spielen schafft damit einen Übungsraum für Urteilsvermögen und sicheres Handeln. Eine überzeugende Täuschung, eine ungewöhnliche Anfrage oder eine vorschnell geteilte Nachricht motivieren zu Reflexionen, die das Gelernte mit dem eigenen Alltag verbinden.

Dieses Bildungs-Special zeigt, wie Schulen und Hochschulen solche Übungsräume schaffen können. Unser kostenfreies Angebot lädt dazu ein, den ersten Schritt in Richtung Cybersicherheit zu machen. Sicherheit gibt Menschen den Rückhalt, Neues zu wagen.

Ihr Marcus Schaper

Executive Navigator

In dieser Sonderausgabe zu Cyber-Resilienz in der Bildung zeigt ab Seite **03** der wissenschaftliche Leitartikel, **dass bereits Achtjährige regelmäßig das Internet nutzen** – und weshalb Resilienz auch schon ab der dritten Klasse wichtig ist. Wir haben auch ein kleines Spiel eingebaut: im **Wimmelbild** auf Seite **06** kann jeder die versteckten Cybergefahren selbst suchen.

Ab Seite **07** zeigen zwei **Praxisartikel** auf, wie Cyber-Resilienz auch ohne neue Stellen oder Extrabudgets spielerisch in die bestehenden Unterrichtsformate eingebaut werden kann. **Meinungen von Lehrenden** auf Seite **10** aus verschiedenen Schulformen helfen bei der Einordnung.

What the Hack! bietet inzwischen eine Breite von Inhalten für Schulen und Hochschulen, die auf Seite **11** in einer **Kampagnenübersicht** dargestellt sind.

Den Abschluss bilden wie immer auf Seite **12** kostenlose **Mitmach-Angebote für Akteure im Bildungssektor**, um mehr über Serious Gaming und What the Hack! zu erfahren. Wir freuen uns, wenn Sie mit uns spielen und die Inhalte weiterentwickeln.

Schon online, aber auch schon vorbereitet?

Warum Medienkompetenz und Cyber-Resilienz bereits in die Grundschule gehören

„Bei uns in der Grundschule ist das noch kein Thema." Diese Einschätzung klingt zunächst plausibel, da häufig angenommen wird, dass die eigentlichen digitalen Herausforderungen erst mit dem Wechsel auf die weiterführende Schule beginnen. Doch die Lebenswelt vieler Kinder sieht anders aus.

Bereits jedes dritte acht- bis neunjährige Kind besitzt ein eigenes Smartphone. Unter den Kindern dieses Alters, die das Internet nutzen, sind 40% täglich online. Zwei Jahre zuvor waren es lediglich 23%. Digitale Bildung in der Grundschule bereitet damit nicht nur auf spätere Erfahrungen vor, sie greift einen bereits bestehenden Alltag auf.

Die entscheidende Frage lautet nicht: „Ist das Internet bei uns schon ein Thema?" Sondern: „Welche digitalen Erfahrungen machen unsere Kinder bereits, und wie begleiten wir sie dabei?"

Bildschirmzeit ist nicht alles

Mit der frühen Nutzung entstehen Situationen, in denen Kinder Informationen bewerten, anderen Menschen vertrauen und Entscheidungen treffen müssen. Eine britische Untersuchung dokumentiert beispielsweise Betrugsversuche in Online-Spielen und berichtet ausdrücklich von Achtjährigen, die durch Onlinebetrug bereits Geld verloren haben. Das ist kein Prävalenzwert für deutsche Grundschulen, zeigt aber, dass solche Erfahrungen bereits in diesem Alter vorkommen.

Auch problematische Kontaktaufnahmen gehören zu den Themen früher Prävention. Laut einer deutschen Befragung der Landesanstalt für Medien NRW ist für 45 Prozent der Acht- bis Neunjährigen Cybergrooming (= sexuell motivierte Kontaktanbahnungen durch Erwachsene) noch nie thematisiert worden, obwohl sie bereits in diesem Alter im Internet davon betroffen sein können.

Damit entsteht eine pädagogische Herausforderung: Kinder können Situationen erleben, für die ihnen noch Begriffe, Handlungsmöglichkeiten oder bekannte Hilfswege fehlen. Prävention sollte deshalb nicht erst beginnen, wenn ein konkreter Vorfall bekannt wird.

Was Erwachsene wissen – und was sie nicht voraussetzen sollten

Viele Erwachsene wissen zwar, dass Kinder im Internet unterwegs sind, aber nicht genau, welche Erfahrungen sie dort machen. In einer repräsentativen Befragung von Eltern Zwölf- bis 18-Jähriger fühlten sich 35 Prozent eher schlecht oder sehr schlecht darüber informiert, was ihr Kind in seiner Freizeit im Internet macht. Beim Prüfen, ob eine Person online tatsächlich diejenige ist, für die sie sich ausgibt, schätzten 24 Prozent ihre Unterstützungsmöglichkeiten als eher oder sehr schlecht ein. Diese Ergebnisse zeigen, dass ausreichende Information und Unterstützung nicht selbstverständlich sind.

Für Schulen folgt daraus eine praktische Aufgabe: den tatsächlichen Medienalltag der Kinder erfragen, geeignete Gesprächsanlässe schaffen und Eltern bei der Begleitung unterstützen.

Von der Sicherheitsregel zur Handlungsfähigkeit

Medienkompetenz ist mehr als die Fähigkeit, ein Gerät zu bedienen. Der Kompetenzrahmen der Kultusministerkonferenz (KMK) verbindet Informationsbewertung, verantwortliches Kommunizieren sowie das Schützen und sichere Agieren. Sicherheit wird damit als Teil eines umfassenderen Bildungsauftrags verstanden.

Teil der laut KMK zu vermittelnden Medienkompetenz ist also auch die hier als **Cyber-Resilienz** bezeichnete Fähigkeit, problematische digitale Situationen zu erkennen, angemessen zu handeln, Unterstützung zu nutzen und nach negativen Erfahrungen wieder handlungsfähig zu werden.

Folgendes Beispiel verdeutlicht den Unterschied zwischen Regelwissen und dieser Handlungsfähigkeit:
Ein Kind bekommt in einem Online-Spiel kostenlose Ausrüstung angeboten. Dafür soll es sofort seine Zugangsdaten eingeben.

Auch wenn das Kind grundsätzlich weiß, dass „Passwörter nicht weitergeben“ eine wichtige Regel ist, bleiben wichtige Fragen offen: Erkennt es in der konkreten Situation, dass diese Regel hier relevant ist? Kennt es eine sichere Alternative? Und weiß es, was nach einer bereits erfolgten Eingabe zu tun ist? Hat es gelernt, sich auch bei eigenen Fehlern Hilfe zu holen?

Kein zusätzliches Fach – aber ein gemeinsamer Auftrag

Um diese Fragestellungen in den Unterricht einzubringen, ist kein eigenständiges Schulfach nötig. Vielmehr lässt sich an alltägliche Unterrichtsinhalte anschließen. Im Deutschunterricht können Kinder die Absichten hinter Nachrichten untersuchen. Im Sachunterricht können sie persönliche Daten und einfache Kriterien für verlässliche Informationen besprechen. In Ethik / Religion bieten sich Fragen nach Einwilligung, Ausgrenzung und Verantwortung beim Weiterleiten von Bildern an. Weitere Beispiele zeigt die folgende Grafik auf:



Über die Einbindung in einzelne Schulfächer hinaus, wäre eine Auseinandersetzung mit Cyberresilienz auch im Rahmen einer Projektwoche denkbar.

Bei einem spielorientierten Ansatz ließe sich auch ein schulweiter Wettbewerb organisieren, in dem die Schüler in jeweils auf die Jahrgangsstufe angepassten Spiel-Kampagnen um den Titel “resilienteste Klasse” wetteifern.

Diese Beispiele sind Unterrichtsvorschläge, keine Vorgaben für einzelne Fächer. Entscheidend ist die gemeinsame Planung: Welche Fähigkeiten werden wo eingeführt, aufgegriffen und vertieft? Der Whole-School-Ansatz des UKCIS verbindet beispielsweise Unterricht, schulische Unterstützung und die Verantwortung der gesamten Schule.

Geeignete Formate verbinden Erfahrung und Reflexion

Zur Vermittlung von Cyberresilienz sind verschiedenste Formate denkbar, darunter Geschichten, Comics, Rollenspiele und spielbasierte Entscheidungssituationen. Bei der Auswahl ist vor allem das Lernziel entscheidend, nicht allein der Unterhaltungswert.

Eine Meta-Analyse von Clark, Tanner-Smith und Killingsworth liefert Hinweise auf einen durchschnittlichen Lernvorteil digitaler Spiele gegenüber Unterricht ohne Spiele.

> *Digitale Lernspiele erzielten im Durchschnitt bessere Lernergebnisse als die untersuchten Lernangebote ohne Spiele – mit einer mittleren Effektstärke von Hedges' g = 0,33.*
>
> *[Clark, Tanner-Smith & Killingsworth, 2016]*

Für spielbasiertes Lernen zeigt eine weitere Metaanalyse, dass zusätzliche didaktische Unterstützung den Lernerfolg verbessern kann. Die Ergebnisse stammen aus unterschiedlichen Lernkontexten und belegen nicht unmittelbar die Wirksamkeit eines bestimmten Cybersicherheits-Spiels für Grundschulkinder. Sie sprechen aber dafür, Spiel und pädagogische Begleitung zusammenzudenken.

Frühe Cyber-Resilienz-Bildung bedeutet dabei nicht, Kindern die Verantwortung für jede Gefahr zu übertragen. Ihr Ziel ist Orientierung und Handlungsfähigkeit – verbunden mit verlässlicher Unterstützung.

Welche digitalen Erfahrungen Kinder in der Grundschule konkret machen, ist nicht wissenschaftlich untersucht, aber vielleicht hilft hier ein kleines Spiel: auf der nächsten Seite finden Sie ein Wimmelbild mit einigen Szenen - welche davon könnten Sie sich an Ihrer Schule vorstellen?

Literatur (Auswahl):

- Clark, D. B., Tanner-Smith, E. E., & Killingsworth, S. S. (2016). Digital Games, Design, and Learning: A Systematic Review and Meta-Analysis. Review of Educational Research, 86(1), 79–122.
- forsa. (2026). Medienkompetenzen von Eltern und Kindern: Ergebnisse einer repräsentativen Befragung von Eltern mit Kindern im Alter von 12 bis 18 Jahren. Körber-Stiftung.
- Hanghøj, T., Silseth, K., & Arnseth, H. C. (2021). Games, Dialogue and Learning: Exploring Research Perspectives. In Proceedings of the 15th European Conference on Game Based Learning, S. 315–321.
- Kultusministerkonferenz. (2017). Bildung in der digitalen Welt: Strategie der Kultusministerkonferenz (Beschluss vom 8. Dezember 2016 in der Fassung vom 7. Dezember 2017).
- Landesanstalt für Medien NRW. (2024, 15. Mai). Cybergrooming: Kinder wünschen sich mehr Unterstützung [Pressemitteilung].
- Medienpädagogischer Forschungsverbund Südwest. (2025). KIM-Studie 2024: Kindheit, Internet, Medien. Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger.
- UK Safer Internet Centre. (2025, 11. Februar). Almost half of 8 to 17-year-olds have been scammed online.
- Wouters, P., & van Oostendorp, H. (2013). A meta-analytic review of the role of instructional support in game-based learning. Computers & Education, 60(1), 412–425.

Wimmelbild: Cyber-Gefahren auf dem Schulhof

In diesem Bild sind 20 Cyber-Gefahren versteckt. Schon gefunden?



Welche Erfahrungen haben Ihre Kinder gemacht?
Bloßstellung • Clickbait • Cyber-mobbing / Troll • Desinformation • Fake-Identitäten • Foto ohne Erlaubnis • Gefährliche Online-Challenge • Gerüchte / Badmouthing • Gruppendruck • Heimliches Filmen • Love Scam • Manipuliertes USB-Kabel / Keylogger • Quishing • Shoulder Surfing • Standortfreigabe • Tailgating • Trojanisches Pferd • USB-Stick-Falle • Vertrauensmissbrauch • Wolf im Schafspelz

5 T-Shirts für mehr Cyber-Resilienz

Wie flexibel Cyber-Resilienz in bestehende Formate eingebettet werden kann - am Beispiel des Spiels What the Hack!

What the Hack! ist ein interaktives Cyberresilienz-Spiel: Teams treten gegen einen virtuellen Hacker an, beurteilen knifflige Alltagssituationen und entscheiden gemeinsam über die beste Antwort. Dabei zählen Wissen, gute Argumente und Zusammenarbeit. Eine Spielrunde dauert rund 30 min. Der anschließende Spielbericht erlaubt Reflexion. Punkte, Badges und Zertifikate machen die Spielergebnisse greifbar.

What the Hack! lässt sich solo spielen; für Schulen empfehlen wir das **Teamspiel**. Eine Lehrkraft kann die Runde moderieren. Alternativ spielen die Kinder selbstständig in Kleingruppen: Sie diskutieren die Fragen, während ein „Gamer" die gemeinsam gewählten Antworten einloggt. So können alle mitdenken und mitentscheiden. Auch eine reine Online-Version ist verfügbar und kann per Meeting-Tools und Link gespielt werden.

Spielerisch lernen. Im passenden Format.

What the Hack! in bestehende Lernangebote einbetten · vom kurzen Impuls bis zur Projektwoche

Mehr Zeit schafft Raum für Reflexion und Eigenarbeit. Auch das kleine Format hat einen eigenen Wert.

GRÖSSE / ZEIT	FORMAT	SO LÄUFT ES AB	CHARAKTERISTIK	AUFWAND / GRENZE
XS 10–15 Minuten	**Ein Fall, ein Gespräch** Einzelne Situation in eine bestehende Unterrichtseinheit einbauen.	Bild und Frage zeigen; einzeln entscheiden; Gründe vergleichen; einen Gedanken für den Alltag festhalten.	Niedrige Einstiegshürde. Ein konkreter Denkimpuls und ein gemeinsamer Merksatz.	Wenig Vorbereitung. Deckt nur einen ausgewählten Aspekt ab.
S 45 Minuten[1]	**Eine Spielstunde** Kurzer Einstieg, eine Spielrunde und eine kompakte gemeinsame Auswertung.	5 Min. Einstieg + 30 Min. Spiel + 10 Min. Reflexion zu einer ausgewählten Entscheidung.	Einfach planbar. Gemeinsames Spielerlebnis mit erster Reflexion.	Vorbereiteter Spielstart nötig. Wenig Zeit für vertiefende Diskussion.
M 90 Minuten[1]	**Spielen und vertiefen** Doppelstunde mit Themenauftakt und gezielter Nachbesprechung.	15 Min. Einstieg + 30 Min. Spiel + 35 Min. Reflexion ausgewählter Fälle aus dem Spielbericht + 10 Min. Transfer.	Begründungen vergleichen, erste Impulse hinterfragen und Alltagsbezüge entwickeln.	Mehr Moderation. Wenige Fälle bewusst auswählen statt alles nachbesprechen.
L Ein Workshop-Tag	**Spielen und gestalten** Vom Spielerlebnis zum eigenen Add-on-Entwurf für Schule oder Region.	Spielen und auswerten; Themen in Gruppen bearbeiten; eigene Fragen und Antworten entwickeln; gegenseitig prüfen und testen.	Aktive Mitgestaltung. Eigene Erfahrungen werden zum Lernmaterial.	Hoher Begleitbedarf. Neue Inhalte vor Einsatz fachlich und didaktisch prüfen.
XL Eine Projektwoche	**5 Themen, 5 Tage** Jeden Tag ein Add-on als Schwerpunkt mit Spiel, Reflexion und eigenem Ergebnis.	Psychische Gesundheit & Algorithmen Betrug, Hacks & Ransom Bilder, Beziehungen & Grooming Radikalisierung & Desinformation KI, Teamarbeit & Organisation.	Zeit für Recherche, eigene Kampagnenfragen, Plakate oder eine Abschlusspräsentation.	Größter Planungsbedarf. Inhalte und Aufgaben altersgerecht auswählen.

L-SONDERFORMAT | Schulweite Spiel-Challenge

Mehrere Klassen spielen über einen vereinbarten Zeitraum. Ein Aktionstag oder Schuljahresabschluss bildet den gemeinsamen Höhepunkt.

Vorab vergleichbare Spielbedingungen festlegen. Highscores zeigen Spielleistung – keine nachgewiesene Resilienz. Reflexion und Teamleistung mit würdigen.

[1] Planungsannahme: 45 Minuten je Unterrichtsstunde; Spielrunde 30 Minuten. Zeiten bei Bedarf anpassen.

Mehr als die richtige Antwort

Wie eine kurze Spielsituation zum Gespräch über digitale Sicherheit wird. Beispiel für das 10min-Format XS

Eine Entscheidungssituation bietet einen konkreten Anlass, über digitale Sicherheit zu sprechen. Für den Unterricht kann per Handreichung daraus ein kompaktes Format werden. Der folgende Entwurf verbindet eine kurze Aufgabe mit Fragen zum Erkennen, Entscheiden und Hilfeholen.

Die Situation: Ein Geschenk vom vermeintlichen Freund

Mila spielt ein Online-Spiel. Plötzlich erhält sie eine Nachricht. Der Name und das Profilbild sehen aus wie die ihres Online-Freundes Ben. Er bietet ihr einen seltenen Tier-Skin an. Dafür soll sie ihm ihre Handynummer geben. Sie möchte den Skin gern haben.

Was sollte Mila zuerst tun?

1. Sie gibt ihm die Nummer und bittet ihn, sie nicht weiterzugeben
2. Sie fragt andere im Spiel, ob sie ihm ihre Nummer gegeben haben
3. Sie gibt die Nummer nicht weiter und bespricht die Bitte mit einer vertrauten erwachsenen Person
4. Sie lässt sich den Skin schicken und gibt ihm danach die Nummer

Als beste Antwort ist Möglichkeit 3 vorgesehen: Mila gibt die Nummer nicht preis und bespricht den Fall mit einer vertrauten erwachsenen Person. Sie könnte auch auf einem anderen, sicheren Weg prüfen, ob das Angebot echt ist und die Nummer sicher verarbeitet wird.

Erst beobachten, dann auflösen

Die Lehrkraft zeigt zunächst nur Bild und Nachricht. Die Kinder beschreiben, was sie sehen. Die Antwortmöglichkeiten kommen erst anschließend hinzu.

Mögliche Fragen:

- Was macht die Nachricht interessant?
- Woran glaubt Mila zu erkennen, wer ihr schreibt?
- Welche Information fehlt ihr?
- Was soll sie besonders schnell tun?

Danach entscheiden sich die Kinder für eine Antwort und begründen ihre Wahl. Abweichende Antworten werden als Gesprächsanlass genutzt, nicht als Anlass zur Korrektur.



WHAT THE HACK! / UNTERRICHTSIMPULS / MUSTERFALL

Mila und das Geschenk

Klasse 3-6 · 10-15 Minuten · Online-Kontakte und persönliche Grenzen

FÜR EURE RUNDE

Die Situation

Mila spielt online mit jemandem, den sie nur aus dem Spiel kennt. Er bietet ihr einen seltenen Tier-Skin an. Dafür soll sie ihm ihre Handynummer geben. Sie möchte den Skin gern haben.

Ein Skin verändert das Aussehen einer Figur im Spiel.

Was sollte Mila tun?

A Sie gibt ihm die Nummer und bittet ihn, sie nicht weiterzugeben

B Sie fragt andere im Spiel, ob sie ihm ihre Nummer gegeben haben

C Sie gibt die Nummer nicht weiter und bespricht die Bitte mit einer vertrauten erwachsenen Person

D Sie lässt sich erst den Skin schicken und gibt ihm danach die Nummer

Erst überlegen, dann austauschen

Welche Antwort wählst du? Warum wirkt eine andere Antwort vielleicht auch verlockend?

Mein Gedanke für den Alltag: _____

Hier abtrennen oder nur den oberen Bereich kopieren · Die Auflösung bleibt bei der Lehrkraft.

FÜR LEHRKRÄFTE | Kurzanleitung & Auflösung

Lernziel

Die Kinder erkennen: Ein Geschenk verpflichtet nicht dazu, persönliche Daten weiterzugeben. Sie üben, eine Grenze zu setzen und Unterstützung zu holen.

Ablauf · mit oder ohne Spiel

2 Min.: Bild ansehen – „Was zeigt die Maske? Was kann Mila online tatsächlich erkennen?"
3 Min.: Vorlesen, einzeln wählen, zu zweit begründen.
4–7 Min.: Antworten vergleichen und reflektieren.
1–3 Min.: Gedanken für den Alltag festhalten.

Beste Antwort: C

Die Nummer bleibt privat; eine vertraute erwachsene Person hilft beim Einordnen. Die Bitte beweist keine böse Absicht. Ein Versprechen (A), Erfahrungen anderer (B) oder das Geschenk zuerst (D) klären nicht, wer die Person ist oder was sie mit der Nummer macht.

Bild & Schutzraum

Das Bild ist sinnbildlich; Mila trifft die Person nicht auf dem Schulhof. Die Maske zeigt eine unbekannte Identität, keinen bewiesenen Täter. Keine privaten Erlebnisse abfragen. Persönliche Fälle anschließend vertraulich und ohne Vorwurf besprechen.

Redaktioneller Musterfall · keine übernommene Kampagnenkarte · Illustration vom Auftraggeber bereitgestellt

Gesprächsimpulse für die Antwortoptionen:

1. Direkt anmelden – „Reichen Name und Profilbild aus, um sicher zu wissen, wer schreibt? Wie weißt Du es sicher?“
2. Andere fragen – „Was verändert sich durch das Fragen – und was bleibt ungeprüft?“
3. Unabhängig prüfen – „Wie kann Mila das Angebot ihres Online-Freundes sicher prüfen?“
4. Skin schicken lassen – „Was könnte passieren, wenn man unbekannte Dateien öffnet?“

Die Auflösung soll nicht nur erklären, welche Antwort die beste ist. Sie soll die Entscheidung nachvollziehbar machen: Ein attraktives Angebot, ein bekannt wirkendes Profil und ein seltener Skin ersetzen keine genaue Überprüfung.

Die wichtige Anschlussfrage: „Und wenn Mila ihre Nummer schon geteilt hat?“

Hier wechselt die Aufgabe von Prävention zu Bewältigung: „Mila hat ihre Handynummer bereits weitergegeben. Jetzt ist ihr die Sache unheimlich. Was sollte sie tun?“

Die Lehrkraft sammelt zunächst Vorschläge. Als gemeinsamer Handlungsweg wird festgehalten: nicht weiter ausprobieren, sondern eine vertrauenswürdige erwachsene Person hinzuholen und gemeinsam klären, welche nächsten Schritte für das betroffene Konto erforderlich sind.

Die pädagogische Botschaft lautet: „Du musst das Problem nicht allein lösen. Hilfeholen ist auch dann richtig, wenn du vorher einen Fehler gemacht hast. Hilfeholen ist eine Stärke.“

Eine zweite Situation prüft das Gelernte

Zum Abschluss wird ein Merkmal verändert: „Die Nachricht kommt tatsächlich von Bens Konto. Ben sagt später aber, dass er sie gar nicht selbst geschrieben hat.“

Die Kinder überlegen erneut: Welche Teile ihrer bisherigen Entscheidung bleiben sinnvoll? So lässt sich besprechen, warum ein bekanntes Konto nicht jede Nachricht automatisch vertrauenswürdig macht.

Als kurze Lernbeobachtung kann die Lehrkraft prüfen, ob die Kinder:

- mindestens ein auffälliges Merkmal benennen können;
- eine sichere Alternative erklären;
- eine Ansprechperson nennen;
- nach einem Fehler einen nächsten Schritt formulieren können.

Der Aufbau greift die pädagogische Idee auf, spielbasierte Entscheidungen durch Anleitung und Reflexion zu ergänzen – ein Ansatz, für den die Forschung zu didaktischer Unterstützung in spielbasierten Lernumgebungen Anhaltspunkte liefert:

> *Lernen durch Spiele findet nicht nur während des Spielens statt, sondern auch in der Kommunikation und Reflexion, die Lehrkräfte vor, während und nach den Spielerfahrungen der Schülerinnen und Schüler begleiten.*
>
> *[Hanghøj, Silseth & Arnseth, 2021]*

Dies ist ein Beispiel, wie sich spielerisches Lernen in bestehende Schul- und Hochschulformate integrieren lässt. Auf S. 11 finden Sie konkrete Angebote, dies und andere Formate einmal auszuprobieren. Mila und ihre Klassenkamerad:innen werden einen Versuch zu schätzen wissen.



Erfahrungen & Meinungen

Welche Erfahrungen machen Lehrer:innen und Dozent:innen mit What the Hack! in den Schulen und Hochschulen?

Phyllis Wiechert, Grundschule Bünningstedt:

„Die Kinder meiner Grundschulklasse fanden WTH sehr motivierend, da der spielerische Aspekt und auch der Wettkampfcharakter alle motiviert hat, den Hacker zu besiegen. Da die Klasse gemeinsam als Team arbeitet und sich bei Unstimmigkeiten einigen muss, führt das dazu, dass die Kinder alle miteinander im Gespräch über die aktuelle Frage sind und somit auch Kindern anderen Kindern etwas erklären, was oft gewinnbringender ist, als wenn Erwachsene es tun.

Schwächere Kinder werden durch ihre Team-Mitglieder unterstützt, so dass alle mit einem guten Gefühl an dem Spiel teilhaben können und mitgenommen werden.

Bei Fragen, die die gesamte Klasse falsch beantwortet hat, ist es großartig, dass What the Hack! den Schülern eine kindgerechte Erklärung liefert, so dass alle auch von falschen Antworten profitieren und Neues dazu lernen können."

Moritz Ringhoff, Berufskolleg Lübbecke:

„What the Hack! schafft es, ein wichtiges und komplexes Thema wie IT-Sicherheit spielerisch und gleichzeitig sehr praxisnah zu vermitteln.

Die Schülerinnen und Schüler sind hoch motiviert, diskutieren miteinander und wollen häufig direkt weiterspielen, weil jede Runde neue Situationen, Strategien und Perspektiven eröffnet. Besonders wertvoll ist für mich, dass das Spiel über den Unterricht hinaus wirkt: Die Lernenden hinterfragen ihr eigenes Verhalten und gehen bewusster mit Risiken und Gefahren in der digitalen Welt um."

Alina Tausch, Universität Witten/Herdecke:

„Mehr Spaß: Die Studierenden waren begeistert, dass ihr Wissen mal nicht nur in einer Klausur abgefragt wird, sondern Teil eines immersiven Erlebnisses ist. Eine Kampagne selbst zu entwickeln ist darüber hinaus genau die praktische Anwendung des Lernstoffs, die sie sich wünschen.

Positive Veränderung: Das Spiel zu spielen hat deutlich gezeigt "Oh, da habe ich noch Lücken, die Antwort konnte ich gar nicht richtig begründen". Das hat zum Lernen für die Klausur nochmal ganz besonders motiviert.

Insgesamt: Alle waren wach, mit Begeisterung und Ehrgeiz in den Sitzungen mit Spiel dabei."

Kampagnen-Übersicht

What the Hack! bietet altersgerechte Inhalte ab der 3. Klasse

Die 10 Kampagnen bilden eine altersgerechte Lernarchitektur, sowohl um die Institutionen zu schützen (HackMySchool und HackMyUniversity), als auch die Lernenden mit Basis-kompetenz (Grundschule, Sekundarstufe, Hochschule) und Vertiefung (die fünf Kästchen rechts) zu versorgen. Die Vertiefungen können individuell als Add-On zu den Basis-Kampagnen beigemischt werden. Außerdem können eigene Fragen erstellt werden.



Ausblick

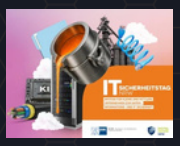
SBG auf Konferenzen und Events



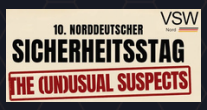
02.12. Cyber Crime Forum München



07.12. Open Game Session (online)



08.12. IT-Sicherheitstag NRW, Duisburg



14.01. Norddeutscher Sicherheitstag, Hamburg

What the Hack! vor Ort erleben

Sie möchten selbst einmal gemeinsam in der Schule oder Hochschule erleben, wie **What the Hack!** funktioniert, wie es sich anfühlt, Teil eines Cyber-Resilienz-Teams zu sein und Hacker zu fangen?

Dann buchen Sie einen Termin für ein Demospiel vor Ort oder Online unter

info@sbg-gaming.com

Call for Participation – wir suchen interessierte Akteure im Bildungssektor, die als Spieler oder Co-Creators mitwirken möchten:

- Schulen und Hochschulen, die What the Hack! ausprobieren möchten, auch in wissenschaftlichen Seminaren und zur Forschung
- Schulträger, Behörden und Verbände, die Impulse für Cyber-Resilienz suchen
- Stiftungen, Bildungsnetzwerke und gemeinnützige Initiativen, die Piloten zur Schulung ihrer Mitglieder suchen

Zum Abonnieren des SBG Quarterly hier scannen:

Die nächste Ausgabe des Quarterly erscheint am 5. Februar 2027.

Impressum

Serious Business Gaming Quarterly ist eine unternehmensbezogene Publikation der

SBG Serious Business Gaming GmbH
Waagenstraße 20 in 40229 Düsseldorf
Vertreten durch: Marcus Schaper, CEO

Kontakt und Website:
info@sbg-gaming.com
www.sbg-gaming.com

Serious Business Gaming Quarterly ist kein journalistisch-redaktionelles Pressemedium

© 2026 SBG Serious Business Gaming