Margit Scholl (Hrsg.)

Lernszenarien
Anleitungen

Sensibilisierung von Schülerinnen und Schülern zum bewussten Umgang mit Informationssicherheit durch erlebnisorientierte Lernszenarien

Regina Schuktomow, Stefanie Gube, Margit Scholl (Prof. Dr.),
Peter Koppatz und Denis Edich

Margit Scholl (Hrsg.)

Lernszenarien
Anleitungen

Sensibilisierung von Schülerinnen und Schülern zum bewussten Umgang mit Informationssicherheit durch erlebnisorientierte Lernszenarien

Regina Schuktomow
Stefanie Gube
Margit Scholl (Prof. Dr.)
Peter Koppatz
Denis Edich

ISBN 978-3-9819225-4-7

Lernszenarien - Anleitungen
Sensibilisierung von Schülerinnen und Schülern
zum bewussten Umgang mit Informationssicherheit durch
erlebnisorientierte Lernszenarien

Printed in Germany

Vorwort

Das Projekt SecAware4school „Informationssicherheitsbewusstsein für den Schulalltag“, gefördert von der Horst Görtz Stiftung (HGS) von September 2018 bis Dezember 2020, hatte das Ziel, bei Schülerinnen und Schülern das Interesse an Informationssicherheit zu wecken. Sie sollen zudem nachhaltig mit spielbasierten analogen und digitalen Lernszenarien, sogenannten Serious Games, für einen achtsamen Umgang mit Informationen und persönlichen Daten sensibilisiert werden. Dafür werden die entwickelten Lernszenarien nach dem Projektende auf der Projektseite öffentlich und kostenlos zur Verfügung gestellt. Das Forschungsteam von Frau Prof. Dr. Scholl der Technischen Hochschule Wildau stellte an fünf Pilotschulen in Berlin und Brandenburg das Projekt in Informationsveranstaltungen vor und führte Awareness Trainings, Kreativworkshops sowie Projekttage durch. Im partizipativen Forschungsdesign wurden die Lernszenarien mit und für die Schulen entwickelt und erprobt. In SecAware4school waren insgesamt ca. 600 Schülerinnen und Schüler sowie ca. 20 Lehrerinnen und Lehrer beteiligt. Die Eltern wurden durch die Informationsveranstaltungen über den Sinn und Zweck informiert und in eine Umfrage einbezogen. Ursprünglich war geplant, dass die Schülerinnen und Schüler als Moderatorinnen und Moderatoren die finalen Lernszenarien auch mit ihren Eltern durchspielen sollten, aber die Corona-Pandemie verhinderte dies vorerst. Es liegt nun an den Schulen, nach dem Projektende die Möglichkeiten dieser Serious Games mit allen Akteuren auszuschöpfen und auch selbst weiterzuentwickeln.

Das Augenmerk des Projektes, die Sensibilisierung für Informationssicherheit, bedeutet, allen Beteiligten eine eigene Risikobewertung zu ermöglichen. Durch aktives Erleben der Lernszenarien sollen die Teilnehmenden die Risiken im Internet erkennen und die Folgen ihres Handelns besser einschätzen können. Da die Lernszenarien in 12 Themenbereiche mit jeweils drei Schwierigkeitsstufen entwickelt wurden, ist tatsächlich für alle Alterstufen etwas dabei. Wir wünschen viel Spaß und interessante Austausche!

Oktober 2020, Margit Scholl und Regina Schuktomow

Methode

Zur Erreichung der Ziele wurden drei unterschiedliche Altersgruppen und Schwierigkeitsgrade definiert: Klassenstufe 6-7 ist Schwierigkeitsgrad 1, Klassenstufe 8-9 ist Schwierigkeitsgrad 2 und Klassenstufe 10-11 ist Schwierigkeitsgrad 3. Diese Unterteilung soll einen höheren Lernerfolg ermöglichen, ist aber keineswegs als Einschränkung gedacht. Methodisch wurde auf Game-Based Learning (GBL) und Accelerated Learning (AccL) gesetzt. GBL wird als unterhaltsame und motivierende Form des Lernens beschrieben (Linek & Albert 2009). Ihre Wirksamkeit gründet sich zum einen auf klaren Zielvorgaben und direktes Feedback (Fang et al. 2013). Zum anderen beruht die Wirksamkeit auf individuell anpassbaren Schwierigkeitsniveaus, sodass spielbasierte Lernszenarien das richtige Maß an Herausforderungen bieten können und zur Erweiterung der Fähigkeiten anregen, ohne die Lernenden zu überfordern (Bressler & Bodzin 2013).

AccL setzt auf eigene Kreation von Wissen, anstatt es zu konsumieren (siehe Bandura 1969, Mataric 1994, Rose & Nicholl 1998, Boyd 2004). AccL verfolgt das Ziel, das volle Lernpotenzial der Teilnehmenden auszuschöpfen, damit sich neues Wissen und vor allem neues Können nachhaltig in ihrem Gedächtnis verankert. AccL verbindet bestehende Methoden mit aktuellen Erkenntnissen aus Hirnforschung und Kognitionswissenschaften. Das Lernen umfasst den menschlichen Geist und Körper als Ganzes mit all seinen Emotionen und Sinnen.

Analoge und digitale erlebnisorientierte Lernszenarien/ Serious Games

Unter Berücksichtigung der Forschungserkenntnisse aus GBL und AccL widmete sich SecAware4school der Entwicklung, dem Einsatz und der Evaluation erlebnisorientierter Lernszenarien im schulischen Umfeld durch sowohl analoge/haptische Spiele als auch Online-Varianten (Apps und browserbasierte Anwendungen). Analoge und digitale Lernszenarien sollen in Kombination zu einer besseren Einschätzung der Möglichkeiten und Gefahren von Informationssicherheit führen.

Danksagung

Das SecAware4school-Team dankt dem gesamten Forschungsteam und den zeitweise im Projekt angestellten Kolleginnen und Kollegen, für intensive inhaltliche Austausche und praktische Unterstützung, insbesondere Peter-Ernst Ehrlich, Josephine Gerlach, Clara Paetow und Frauke Prott.

Wir danken den beteiligten fünf Pilotschulen für ihr Engagement, auch in schwierigen Zeiten.

Wir danken dem Friedrich-Wilhelm-Gymnasium Königs Wusterhausen, insbesondere dem Informatikkurs von Herrn Dr. Hell für das Einbinden der Projektinhalte in den Unterricht und die erfolgreichen Ergebnisse. Wir danken besonders Schülerinnen und Schülern sowie Lehrenden des Friedrich-Schiller-Gymnasiums Königs Wusterhausen für den Willen und die Fähigkeit, Informationssicherheit als Thema im Schulalltag weiterzubringen. Ebenso danken wir der Staatlichen Gesamtschule (ehm. Dr. Hans Bredow Oberschule) Königs Wusterhausen für das gezeigte Interesse an unserem Projekt. Wir danken der Rudolf-Virchow-Oberschule Berlin für die kreativen Ideen der Schülerinnen und Schüler und wir danken dem Humboldt-Gymnasium Berlin für das, von Beginn an, große und anhaltend stetige Interesse am Projekt sowie die Maßnahmen, die in der Schule zur Informationssicherheit getroffen werden.

Darüber hinaus danken wir unserem Projektpartner Dietmar Pokoyski (Firma known_sense) für die ideenreiche Unterstützung und die stets gute Zusammenarbeit als Auftragnehmer.

Das gesamte Vorhaben, das neben den Entwicklungen der Lernszenarien auch die Zertifizierung von fünf Lehrerinnen und Lehrern zu Informationssicherheitsbeauftragten sowie weitere ICDL-Qualifizierungen für die Schülerinnen und Schüler ermöglichte, wäre ohne die Förderung der Horst Görtz Stiftung (HGS) nicht durchführbar gewesen. Wir danken sehr herzlich der HGS, insbesondere Dr. Horst Görtz, für diese Förderung und das in uns gesetzte Vertrauen.

SecAware4school Team

Inhaltsverzeichnis

Kurz und knapp - was sind erlebnisorientierte Lernszenarien?

Liebe Schülerinnen und Schüler sowie Lehrende und Eltern, dieses Buch ist eine Anleitung für insgesamt 13 unterschiedliche analoge und digitale Lernszenarien in drei unterschiedlichen Schwierigkeitsgraden.

Eignung

Die erlebnisorientierten Lernszenarien zu Themen der Informationssicherheit sind für Kinder und Jugendliche zwischen der 6. und 11. Klassenstufe konzipiert und können im Schulunterricht oder als Projektthema behandelt und gespielt werden. Wichtig sind hierbei die diskursiven Elemente - es soll ein lebendiger Austausch gelingen.

Tipp für den Unterricht

Die hier präsentierten Lernszenarien sollen auch zum kreativen Denken anstoßen. Schülerinnen und Schüler können zu einem konkreten Thema der Informationssicherheit versuchen, eigene Ideen zur Moderation zu entwickeln. So könnten sie das gewählte Thema in Eigenverantwortung bestmöglich auch den jüngeren Klassenstufen näherbringen und sensibilisieren.

Tipp für Projekttage „Informationssicherheit an der Schule“

Lassen Sie Schülerinnen und Schüler mit Bastelmaterialien eigene Ideen sammeln und in einen ersten Entwurf für ein analoges Spiel umsetzen. In kleinen Gruppen kann dieser Entwurf eines Lernszenarios, z.B. ein kleines Brettspiel zur Passwortsicherheit, weiter ausgebaut, anderen vorgestellt und anschließend verbessert werden. Mit solchen selbst entwickelten Lernszenarien kann eine lebendige Sensibilisierung für Informationssicherheit gelingen.

Benutzung der Materialien

Alle Anleitungen der im Projekt entwickelten Lernszenarien einschließlich dazugehöriger Wikis sind in diesem Buch zu finden. Sollten mehrere Klassen oder Gruppen parallel spielen wollen, so empfiehlt es sich, die Anleitungen vorher aus dem Buch zu kopieren oder von der Projektwebseite https://secaware4school.wildau.biz herunterzuladen.

Informationssicherheit
Schnelles Begrifferaten

Beim Lernszenario „Informationssicherheit: Schnelles Begrifferaten“ geht es darum, den sicheren Gebrauch von Fachbegriffen im Bereich der Informationssicherheit zu üben. Aufgrund der zunehmenden Menge an online verfügbaren Informationen und Diensten ist es von Bedeutung, sich mit Fachbegriffen der Informationssicherheit vertraut zu machen.

- Spielbar ab 3 Personen. Entweder in 2 Teams (mindestens eine Person pro Team plus eine moderierende Person) oder ein Team plus eine moderierende Person.
- Spieldauer 15-25 Minuten.

Ziel des Lernszenarios

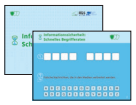
Ziel des Lernszenarios ist es, anhand von Hinweisen Fachbegriffe nach dem „Galgenmännchen“-Prinzip zu erraten. Ihr habt etwa 15 Minuten Zeit, den Stapel an Karten in eurem Schwierigkeitsgrad abzuarbeiten.

Einstiegsfragen

„Kennt ihr einige Fachbegriffe, die mit Informationssicherheit zu tun haben könnten? Welche sind es?“

> Vertraulichkeit (= Schutz vor einem unbefugten Preisgeben der Informationen); Integrität (= Sicherstellung der Korrektheit bzw. Unversehrtheit von Informationen und der korrekten Funktionsweise von Systemen) und Verfügbarkeit (=Informationen und Funktionen von Dienstleistungen, IT-Systemen, IT-Anwendungen oder IT-Netzen sind wie vorgesehen abrufbar).

Bestandteile

	36 laminierte Karten
	2 Whiteboardmarker (abwischbar)

Vorbereitung und Erläuterung des Lernszenarios

- Vereinbart die Spieldauer, wenn ihr nicht nach der empfohlenen Zeit spielen möchtet.
- Bestimmt eine Moderatorin/ einen Moderator. Diese Person ist für die Auflösung verantwortlich, hat die Lösungen zur Hand und spielt nicht im Team mit.
- Bildet Teams.
- Die Karten des ausgewählten Schwierigkeitsgrades liegen verdeckt in der Mitte des Tisches.
- Jedes Team nimmt sich einen Whiteboardmarker.
- Ihr habt 3 Fehlversuche pro Karte! Die moderierende Person kontrolliert dies.
- Beachte: Ä=AE; Ö=OE; Ü=UE

Wählt den passenden Schwierigkeitsgrad!

 Klassenstufen 6-7	Der 1. Schwierigkeitsgrad ist durch die einfache Beschreibung der Fachbegriffe und gegebenen Hinweise für jüngere Klassenstufen geeignet.
 Klassenstufen 8-9	Beim 2. Schwierigkeitsgrad ist die Formulierung der Begriffe konkret sachlich und beinhaltet viele aus dem Bereich der Informationssicherheit spezifischen Begriffe.
 Klassenstufen 10-11	Der 3. Schwierigkeitsgrad ist geprägt durch präzise und spezifische Formulierungen und zeichnet sich durch reduzierte Hinweise aus.

Ablauf

1. Auf ein Startkommando nehmen sich die Teams je eine Karte vom Stapel.
2. Erratet anhand der Hinweise auf den Karten den gesuchten Fachbegriff und schreibt diesen in die vorhandenen Kästchen.
3. Wenn ihr nicht gleich auf die Lösung kommt, könnt ihr nach dem „Galgenmännchen“-Prinzip einzelne Buchstaben erraten. Die moderierende Person sagt euch, ob diese richtig oder falsch sind und an welche Stelle sie gehören.
4. Erst wenn der gesuchte Begriff erraten wurde oder es drei Fehlversuche gab, darf die nächste Karte gezogen werden.

Auflösung und Punktevergabe

1. Die moderierende Person wertet die Karten aus und vergibt die Punkte.
2. Für jede richtig erratene Karte gibt es einen Punkt.
3. Wenn die Karte nach 3 Fehlversuchen nicht erraten wurde, wird sie aussortiert und bei der Punktevergabe nicht berücksichtigt.
4. Das Team mit den meisten Punkten hat gewonnen.

Ende des Spiels

Das Spiel ist zu Ende, wenn einer der beiden Punkte zutrifft:

A. Alle Karten vom Stapel sind aufgebraucht.

B. Die vorher festgelegte Zeit ist abgelaufen.

> Wichtig! Wischt bitte alle Karten wieder ab, damit sich andere Teams nach euch auch an diesem Lernszenario erfreuen können und die Lösungen nicht vorher sehen.

Lösungsmuster - Schwierigkeitsgrad 1

Nr.	Karten
1.	Eine bestimmte Zeichenabfolge, mit der man sich anmeldet. (PASSWORT)
2.	Jemanden regelmäßig ärgern, schikanieren oder quälen, um denjenigen aus der Gruppe oder Klasse auszugrenzen. (MOBBING)
3.	Falsche Nachrichten, die in den Medien verbreitet werden. (FAKE NEWS)
4.	Unerwünscht versandte Werbe-E-Mails. (SPAM)
5.	Ein Verfahren, um z.B. geheime Nachrichten zu senden. (VERSCHLUESSELUNG)
6.	Ein englisches Wort, das den Versuch beschreibt, über gefälschte E-Mails an persönliche Daten zu gelangen. Tipp: Hat etwas mit Fischen zu tun. (PHISHING)
7.	Ein Bereich, in dem man „seine Ruhe“ haben kann, z.B. zu Hause. (PRIVATSPHAERE)
8.	Bösartiger Code oder Programm, das dem Computer schadet. Tipp: Gleicher Name wie ein Krankheitserreger. (VIRUS)
9.	Ein Programm, das heimlich etwas anderes tut als es sollte. Tipp: Figur aus der griechischen Mythologie. (TROJANER)
10.	Was wird vom PC gesendet, wenn man z.B. eine Webseite aufruft? (IP-ADRESSE)
11.	Ein Programm, mit dem man Webseiten im Internet aufruft. (BROWSER)
12.	Ein Programm, das Dateien auf dem Computer verschlüsselt und erst nach Zahlung von Lösegeld wieder entschlüsselt. (ERPRESSUNGS-TROJANER)
13.	Wenn dieses technische Hindernis unberechtigt überwunden wird, geht es dahinter heiß her. (FIREWALL)
14.	Alias- oder Deckname. (PSEUDONYM)
15.	Der gesuchte Begriff bedeutet, dass eine Person oder Gruppe nicht identifiziert werden kann. ODER anderes Wort für inkognito ODER womit kann ich meine Identität schützen? (ANONYMITÄT)

16.	Sicherungskopie von (persönlichen) Daten. (BACKUP)
17.	Damit bezahlt man z.B. verschlüsselte Informationen. (BITCOIN)
18.	EU-weites Gesetz zum Datenschutz. (DSGVO)
19.	Hier agieren die Cyber-Verbrecher. (DARKNET)
20.	Anderes Wort für Fan-Base. (COMMUNITY)
21.	Sie finden Schwachstellen von Systemen, um auf sie aufmerksam zu machen oder sie für bestimmte Zwecke wie unbefugtes Eindringen oder zur Veränderung von Funktionen zu nutzen. (HACKER)
22.	Was ist ein Zusammenschluss von vielen PCs zu einem großen automatisierten Computer-schadprogramm? (BOTNETZ)
23.	Attacke, bei der als Hilfe eine Sammlung beliebter Standardpasswörter genutzt wird. (WOERTERBUCH-ANGRIFF)
24.	Womit sucht man einen Computerschädling? (VIRENSCANNER)
25.	Mächtiges Werkzeug, um Passwörter zu entschlüsseln. (RAINBOW-TABELLE)
26.	Ein illegaler Versuch, Kreditkarten- und Bankinformationen auszuspähen. (SKIMMING)
27.	Was isst das Krümelmonster zum Frühstück? (COOKIES)
28.	Was gewährt ausschließlich autorisierten Personen ordnungsgemäßen Zutritt? (ZUTRITTSKONTROLLE)
29.	Bezeichnung dafür, dass wenig über einen preisgeben wird. (DATENSPARSAMKEIT)
30.	Was ist ein Schriftzeichen, das weder Buchstabe noch Ziffer ist? (SONDERZEICHEN)
31.	Womit kann man vielen Nutzern Daten zur Verfügung stellen? (SERVER)
32.	Wofür wird ein Backup verwendet? (RECOVERY)
33.	Programme, die alle hochgeladenen Inhalte scannen und mit Hilfe von riesigen Datenbanken eine Verletzung von Urheberrechten prüfen. (UPLOAD-FILTER)
34.	Alternative Suchmaschine aus Frankreich. (QWANT)

35.	„In die Wurzeln“ des Betriebssystems (des Smartphones) vordringen/ das Smartphone neu „verwurzeln“ (ROOT)
36.	(Fach-) Hochschule südöstlich von Berlin an der Dahme. (TH WILDAU)

Lösungsmuster - Schwierigkeitsgrad 2

Nr.	Karten
1.	Eine bestimmte Zeichenabfolge, die für den Login gebraucht wird. (PASSWORT)
2.	Das regelmäßige und wiederholte Schikanieren von Personen, um sie zu quälen, seelisch zu verletzen und sie aus der Klasse oder Gruppe auszugrenzen. (MOBBING)
3.	Vorgetäuschte und manipulative Nachrichten, die sich überwiegend im Internet, insbesondere in sozialen Netzwerken und anderen sozialen Medien verbreiten. (FAKE NEWS)
4.	Unerwünschte bzw. rechtswidrig versandte Werbe-E-Mails. (SPAM)
5.	Mit diesem Verfahren werden Daten mittels elektronischer bzw. digitaler Codes oder Schlüssel inhaltlich in unlesbare Formen übersetzt. Damit ist es möglich, z.B. eine geheime Nachricht zu verfassen. (VERSCHLUESSELUNG)
6.	Ein Versuch, über gefälschte Webseiten, Kurznachrichten oder E-Mails an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen und der Person zu schaden. (PHISHING)
7.	Ein nicht öffentlicher Bereich, in dem ein Mensch uneingeschränkt von äußeren Einflüssen sein Recht auf freie Entfaltung der Persönlichkeit wahrnimmt. (PRIVATSPHAERE)
8.	Bösartiger Code oder Programm, das Veränderungen an Software oder Betriebssystem vornehmen kann. (VIRUS)
9.	Bezeichnung für ein Programm, das ohne das Wissen des Anwenders eine unbekannte Hintergrundfunktion ausführt. (TROJANER)
10.	Wird vom PC gesendet, wenn man im Internet surft. (IP-ADRESSE)
11.	Eine Software, die zum Zugriff auf das World Wide Web verwendet wird. (BROWSER)

12.	Ein Programm, das die Inhalte einer Festplatte unaufgefordert verschlüsselt und für Entschlüsselung Lösegeld verlangt. (ERPRESSUNGS-TROJANER)
13.	Es kontrolliert alle Daten, die ins eigene Netzwerk hineinkommen oder es verlassen. (FIREWALL)
14.	Ich bin's, aber der Name stimmt nicht. (PSEUDONYM)
15.	Was wurde mir gegeben, gehört mir, ich verleihe es nicht an andere? Es wird aber von allen Menschen benutzt, die mich kennen. Nur im Internet sollte ich es nicht verwenden, um die ... zu wahren! (ANONYMITÄT)
16.	Wie nennt man den Vorgang, Daten zu sichern? (BACKUP)
17.	Wonach schürft man im digitalen/virtuellen Bergwerk? (BITCOIN)
18.	Wer oder was garantiert die Herausgabe deiner persönlichen Daten bei Service-Anbietern im Internet? (DSGVO)
19.	Wo kann man Drogen, Waffen und geknackte Passwörter kaufen? (DARKNET)
20.	Zusammenschluss Gleichgesinnter im Internet. (COMMUNITY)
21.	Für diese Gruppe gibt es den „...“-Paragraphen. (HACKER)
22.	Fernsteuerbares Netzwerk ODER Was ist aus technischer Sicht ein Zusammenschluss von unabhängigen Computern, die sich als ein einziges System darstellen? Tipp: Es nutzt einen Computer ohne Zustimmung des Inhabers. (BOTNETZ)
23.	Attacke auf Passwörter mit Hilfe einer Wörterliste. (WOERTERBUCH-ANGRIFF)
24.	Programm, das einen Computer nach Malware durchsucht. (VIRENSCANNER)
25.	Was ist eine kompakte Repräsentation von zusammenhängenden Passwortsequenzen? (RAINBOW-TABELLE)
26.	Der gesuchte Begriff ist ein Man-in-the-Middle-Angriff, der das Auslesen von Bank- und Kreditdaten zum Ziel hat. (SKIMMING)
27.	Woran erkennt eine Webseite, dass du sie ein zweites Mal aufrufst? (COOKIES)
28.	Was steuert den Zutritt nach einem festgelegten Regelwerk „Wer, wann, wo?“, damit nur berechtigte Personen Einlass zu dem für sie freigegebenen Gebäudebereich haben. (ZUTRITTSKONTROLLE)

29.	Es werden bei der Datenverarbeitung nur so viele Daten gesammelt, wie für die jeweilige Anwendung notwendig sind. (DATENSPARSAMKEIT)
30.	Womit wird ein Passwort sicherer? (SONDERZEICHEN)
31.	Computer oder Computerprogramm, dass Funktionalitäten (z.B. Daten oder Programme) bereitstellt, damit andere Computer darauf zugreifen können, oft über ein Netzwerk. (SERVER)
32.	Wiederherstellung von Daten nach einem Datenverlust. (RECOVERY)
33.	Was ist eine serverseitige Software, die Medien und Dateien beim Hochladen prüft und gegebenenfalls abweist? (UPLOAD-FILTER)
34.	Alternative Suchmaschine aus Frankreich. (QWANT)
35.	Wie wird der Vorgang genannt, bei dem man sich volle Administratorrechte bei einem (Android-) Betriebssystem verschafft? (ROOT)
36.	(Fach-) Hochschule südöstlich von Berlin an der Dahme. (TH WILDAU)

Lösungsmuster - Schwierigkeitsgrad 3

Nr.	Karten
1.	Eine bestimmte Zeichenabfolge, durch die sich jemand ausweist und dadurch die eigene Identität bestätigt. (PASSWORT)
2.	Das regelmäßige und wiederholte Schikanieren von Personen, um sie zu quälen, seelisch zu verletzen und sie aus der Klasse oder Gruppe auszugrenzen. (MOBBING)
3.	Vorgetäuschte und manipulative Nachrichten, die sich überwiegend in den Medien verbreiten. (FAKE NEWS)
4.	Unerwünschte bzw. rechtswidrig versandte Werbe-E-Mails. (SPAM)
5.	Mit diesem Verfahren werden Daten mittels elektronischer bzw. digitaler Codes oder Schlüssel inhaltlich in unlesbare Formen übersetzt. (VERSCHLUESSELUNG)
6.	Ein Versuch, über gefälschte Webseiten, Kurznachrichten oder E-Mails an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen und der Person zu schaden. (PHISHING)

7.	Ein nichtöffentlicher Bereich, in dem ein Mensch uneingeschränkt von äußeren Einflüssen sein Recht auf freie Entfaltung der Persönlichkeit wahrnimmt. (PRIVATSPHAERE)
8.	Bösartiger Code oder Programm, das Veränderungen an Software oder Betriebssystem vornehmen kann. (VIRUS)
9.	Bezeichnung für ein Programm, welches das Betriebssystem manipuliert. (TROJANER)
10	Wird vom PC gesendet, wenn man im Internet surft. (IP-ADRESSE)
11	Eine Software, die zum Zugriff auf das World Wide Web verwendet wird. Das Programm interpretiert die ankommenden Daten und stellt sie als Text und Bild auf dem Bildschirm dar. (BROWSER)
12	Ein Begriff, der Ransomware bezeichnet. (ERPRESSUNGS-TROJANER)
13	Womit schützt man Netzwerke vor Angreifern? (FIREWALL)
14	Vorgetäuschter Name, um eine wahre Identität zu verbergen. (PSEUDONYM)
15	Was wurde mir gegeben, gehört mir, ich verleihe es nicht an andere? Es wird aber von allen Menschen benutzt, die mich kennen. Nur im Internet sollte ich es nicht verwenden. (ANONYMITÄT)
16	Wofür wird die 3-2-1-Regel empfohlen? (BACKUP)
17	Für welche Währung benötigt man sehr viel Strom? (BITCOIN)
18	Was trat am 24. Mai 2016 in Kraft und ist seit dem 25. Mai 2018 verpflichtend anzuwenden? (DSGVO)
19	Hier kann man nur mit Kryptowährung bezahlen. (DARKNET)
20	Was ist ein organisiertes und soziales Netzwerk von miteinander in Interaktion stehenden Individuen? (COMMUNITY)
21	Für diese Gruppe existiert der Paragraph 202c im Strafgesetzbuch. (HACKER)
22	Per Fernsteuerung zusammengeschlossene PCs, die für bestimmte Aktionen, wie das Versenden von Spam-Mails, missbraucht werden. (BOTNETZ)

23	Methode der Kryptoanalyse, um ein unbekanntes Passwort mit Hilfe einer Wörterliste zu ermitteln. (WOERTERBUCH-ANGRIFF)
24	Software, die elektronische Datenverarbeitungsanlagen vor Trojanern schützen/nach ihnen durchsuchen soll. (VIRENSCANNER)
25	Womit lassen sich Passwörter mit relativ geringem Rechenaufwand knacken, die mittels eines Hash-Wertes (= Zeichenfolge, die mittels Algorithmus aus einem Passwort ermittelt wurde) ohne Salt (zufällig gewählte Zeichenfolge) gespeichert und verglichen werden? (RAINBOW-TABELLE)
26	Der gesuchte Begriff ist ein Man-in-the-Middle-Angriff. (SKIMMING)
27	Womit speichern Webseiten Nutzerdaten? (COOKIES)
28	Was gewährleistet, dass sich in einem Raum lediglich Menschen aufhalten, die für den Aufenthalt berechtigt sind? (ZUTRITTSKONTROLLE)
29	Grundsatz der DSGVO zur Minimierung personenbezogener Daten. (DATENSPARSAMKEIT)
30	Alt Gr+Q, Alt Gr+M, # !? ^^ @µ|€ (SONDERZEICHEN)
31	Computer oder Computerprogramm, das Funktionalitäten bereitstellt, damit andere Computer darauf zugreifen können. (SERVER)
32	Wiederherstellung der Originaldaten aus einer Sicherungskopie. (RECOVERY)
33	Was wird in Artikel 13 der Reform des EU-Urheberrechts nicht explizit gefordert, ist für die technische Umsetzung aber erforderlich? (UPLOAD-FILTER)
34	Alternative Suchmaschine aus Frankreich. (QWANT)
35	Was bezeichnet das nichtautorisierte Entfernen von Nutzungsbeschränkungen auf einem Smartphone mit Android-Betriebssystem (Jailbreak unter Apple)? (ROOT)
36	(Fach-) Hochschule südöstlich von Berlin an der Dahme. (TH WILDAU)

Digital sozial
Internetregeln erkennen

- Spielbar mit 2 Teams.
  (Mindestens eine Person pro Team plus eine moderierende Person)
- Spieldauer 25-45 Minuten.

Ziel des Lernszenarios

Bei diesem Lernszenario geht es um das Verhalten auf sozialen Plattformen im Internet sowie den Umgang mit dem Smartphone in deiner Umwelt. Das Lernszenario soll zur Diskussion bezüglich des Verhaltens gegenüber anderen Personen anregen und für den kritischen Umgang mit den „neuen“ Medien sensibilisieren.

Einstiegsfragen

„Welche Verhaltensregeln rund um Smartphone und Internet kennt ihr und welche davon findet ihr (nicht) sinnvoll?“

Vorbereitung und Erläuterung des Lernszenarios

- Vereinbart die Spieldauer, wenn ihr nicht nach der empfohlenen Zeit spielen möchtet.
- Bestimmt eine Moderatorin/ einen Moderator. Diese Person ist für den fairen Ablauf, die Zeit und die Auflösung verantwortlich und spielt nicht in einem der Teams mit.
- Bildet zwei Teams.
- Wählt den passenden Schwierigkeitsgrad!
- Das Spielfeld im gewählten Schwierigkeitsgrad, die verdeckten Karten, Pins und ggf. der Würfel liegen in der Mitte des Tisches.

Wählt den passenden Schwierigkeitsgrad!

 Klassenstufen 6-7	Der 1. Schwierigkeitsgrad verwendet klare und präzise Aussagen, die eine Entscheidung erleichtern. Die Spielmechanik sowie die Darstellung ermöglichen einen Wettbewerb mit interessanten und erleuchtenden Diskussionen.
 Klassenstufen 8-9	Den 2. Schwierigkeitsgrad zeichnet die Komplexität der zu beantwortenden Fragen aus. Diese sollen aus der Erfahrung heraus beantwortet und diskutiert werden. Die Spielmechanik basiert auf Zuordnung und führt zu Diskussionen im Team.
 Klassenstufen 10-11	Beim 3. Schwierigkeitsgrad sind die Fragen offen gestaltet, sodass Aussagen aus mehreren Blickwinkeln betrachtet werden können. Der gegebene Inhalt und die Komplexität fördern den Austausch sowie eine Diskussion während des Spielens.

Schwierigkeitsgrad 1

Bestandteile

	Spielfeld
	16 Fragekarten
	2 Spielfiguren
	1 Würfel

Ablauf

1. Jedes Team nimmt sich eine Figur und platziert diese vor dem ersten Zahlenfeld.
2. Beide Teams würfeln. Das Team mit der höheren Würfelaugenzahl beginnt und heißt Team A.
3. Team A würfelt erneut und rückt entsprechend der gewürfelten Augenzahl auf ein Zahlenfeld.
4. Deckt eine Fragekarte vom Stapel auf und beantwortet diese aus eurer Sicht und Erfahrung. Zu welcher Aussage passt die Frage? Diskutiert über die Antwort und eine mögliche Zuordnung.
   Hinweis: Manche Karten lassen sich auf den ersten Blick mehreren Aussagen zuordnen, doch am Ende gehört zu jeder Fragenkarte eine Aussage.
5. Nach der Zuordnung verdeckt ihr das zugeordnete Feld mit der beantworteten Fragekarte.
6. Die moderierende Person gibt die Auflösung. Für die richtige Zuordnung erhält das jeweilige Team einen Punkt.
7. Team B ist nun an der Reihe und würfelt.
8. Ziel ist es, alle Aussagen auf dem Spielfeld mit den passenden Fragekarten zu matchen und über die Zuordnung zu diskutieren.
9. Das Team mit der höchsten Zahl an richtig gelegten Fragekarten gewinnt.

Ende des Spiels

Das Spiel ist zu Ende, wenn einer der beiden Punkte zutrifft:

A. Alle Felder sind mit Fragekarten zugedeckt.

B. Die vorher festgelegte Zeit ist abgelaufen.

Lösungsmuster - Schwierigkeitsgrad 1

Nr.	Frage	Lösung
A.	Wie ist die Benutzung von Smartphones an deiner Schule geregelt?	6
B.	Sollte es in deinem Freundeskreis oder deiner Familie ein Nutzungsverbot von Smartphones während des Essens oder eines Gesprächs geben? Warum?	8
C.	Was tust du, damit andere in der Öffentlichkeit deine Nachrichten nicht mitlesen?	13
D.	Warum wird die Benutzung des Smartphones im Straßenverkehr mit einem Bußgeld geahndet?	14
E.	Warum ist es wichtig, Freunde real zu treffen und nicht nur virtuell?	15
F.	Warum solltest du die Seriosität eines Links prüfen, bevor du darauf klickst?	10
G.	In welchen Situationen stört dich ein Benachrichtigungston?	11
H.	Was bedeutet dieses Emoji? (**Hinweis:** Bedienung)	7
I.	Warum ist das echte Leben spannender?	16
J.	Wie ist deine Privatsphäre-Einstellung in den sozialen Netzwerken?	3
K.	Warum solltest du deine Passwörter für dich behalten (privat)?	1
L.	Was kannst du gegen Cybermobbing tun?	4
M.	Warum solltest du nicht in der Öffentlichkeit telefonieren?	12
N.	An wen wendest du dich bei Kummer? (**Hinweis:** Andere Beispiele/ Hilfsangebote)	5
O	Wann und warum solltest du dein Smartphone auch mal ausschalten?	2
P	Was würde ein Fremder über dich erfahren, wenn er dich googelt?	9

Schwierigkeitsgrad 2

Bestandteile

	Spielfeld
	20 Fragekarten
	1 Pin blau, 1 Pin orange

Ablauf

1. Jedes Team nimmt sich 10 Pins in einer Farbe.
2. Ihr deckt nacheinander eine Fragekarte auf und beantwortet diese aus eurer Sicht und Erfahrung. (Jedes Team nimmt immer eine Karte.)
3. Zu welcher Aussage passt die Frage? Diskutiert über die Antwort und eine mögliche Zuordnung. Hinweis: Manche Karten lassen sich auf den ersten Blick mehreren Aussagen zuordnen, doch am Ende gehört zu jeder Fragekarte eine Aussage.
4. Setzt eure Pins auf die Aussagen, die eurer Meinung nach zu der Frage passen würden.
5. Die moderierende Person gibt die Auflösung bekannt und vergibt die Punkte. Ist eine Zuordnung nicht in der Musterlösung enthalten, die Argumentation des jeweiligen Teams jedoch für die moderierende Person überzeugend, so kann diese die Zuordnung in der Bewertung berücksichtigen. Für das Team mit den meisten Treffern gibt es einen Punkt. Bei Gleichstand erhalten beide Teams einen Punkt.
6. Das Team mit den meisten Punkten gewinnt.

Ende des Spiels

Das Spiel ist zu Ende, wenn einer der beiden Punkte zutrifft:

A. Alle Felder mit Fragekarten sind beantwortet.

B. Die vorher festgelegte Zeit ist abgelaufen.

Lösungsmuster - Schwierigkeitsgrad 2

Nr.	Frage	Lösung
A.	Wirst du gerne ohne Erlaubnis fotografiert? Warum / Warum nicht?	1
B.	Sollte es in deinem Freundeskreis oder deiner Familie ein Nutzungsverbot von Smartphones während des Essens oder eines Gesprächs geben? Warum?	10
C.	Würdest du Cybermobbing melden? An wen?	19
D.	Warum wird die Benutzung des Smartphones im Straßenverkehr mit einem Bußgeld geahndet?	14
E.	Warum ist es wichtig, Freunde real zu treffen und nicht nur virtuell?	18
F.	Warum solltest du die Seriosität eines Links prüfen, bevor du darauf klickst?	17
G.	In welchen Situationen stört dich ein Benachrichtigungston?	6
H.	Was bedeutet dieses Emoji?  (**Hinweis:** Bedienung)	15
I.	Muss jeder wissen, wann du online warst? Warum?	7
J.	Wie ist deine Privatsphäre-Einstellung in den sozialen Netzwerken?	3
K.	Warum solltest du deine Passwörter für dich behalten (privat)?	4
L.	Was kannst du gegen Cybermobbing tun?	5
M.	Warum solltest du nicht in der Öffentlichkeit telefonieren?	12

N.	An wen wendest du dich bei Kummer?	11
O.	Welche Zugriffsrechte gewährst du deinen Apps? (**Hinweis:** z.B. Zugriff auf Mikrofone, auf Adressbuch, Kamera, Galerie etc.)	9
P.	Was würde ein Fremder über dich erfahren, wenn er dich googelt?	13
Q.	Wann und warum solltest du dein Smartphone auch mal ausschalten?	2
R.	Warum ist das echte Leben spannender? (**Hinweis:** Den ersten Kuss kannst du schlecht online fühlen. Deinen besten Freund kannst du nicht online in den Arm nehmen.)	8
S.	Was tust du, damit andere in der Öffentlichkeit deine Nachrichten nicht mitlesen? (**Hinweis:** z.B. Schutzfolie, die Hand davorhalten, dunkler schalten, Handy in der Tasche lassen etc.)	20
T.	Wie ist die Benutzung von Smartphones an deiner Schule geregelt?	16

Schwierigkeitsgrad 3

Bestandteile

	Spielfeld
	10 Fragekarten
	10 Pins blau, 10 Pins orange

Ablauf

1. Jedes Team nimmt sich 10 Pins in einer Farbe.
2. Ihr deckt nacheinander eine Fragekarte auf und beantwortet diese aus eurer Sicht und Erfahrung.
3. Zu welcher Aussage passt die Frage? **Hinweis:** Es können mehrere Aussagen zu einer Frage passen. Diskutiert über die Antwort und eine mögliche Zuordnung.
4. Setzt eure Pins auf die Aussagen, die eurer Meinung nach zu der Frage passen würden.
5. Die moderierende Person gibt die Auflösung bekannt und vergibt die Punkte. Ist eine Zuordnung nicht in der Musterlösung enthalten, die Argumentation des jeweiligen Teams jedoch für die moderierende Person überzeugend, so kann diese die Zuordnung in der Bewertung berücksichtigen. Für das Team mit den meisten Treffern gibt es einen Punkt. Bei Gleichstand erhalten beide Teams einen Punkt.
6. Das Team mit den meisten Punkten gewinnt.

Ende des Spiels

Das Spiel ist zu Ende, wenn einer der beiden Punkte zutrifft:

A. Alle Felder mit Fragekarten sind beantwortet.

B. Die vorher festgelegte Zeit ist abgelaufen.

Lösungsmuster - Schwierigkeitsgrad 3

Nr.	Frage	Lösung
A.	Wann und warum schaltest du dein Smartphone aus? Hast du schon mal Digital Detox ausprobiert? (**Hinweis:** Ausschalten in Kino, Theater, Beerdigung, Krankenhaus, Flugzeug etc.) Stumm/lautlos: Während des Essens (Restaurant, zu Hause), während des Unterrichts. Stichwort „Phubbing“=im Gespräch am Handy sein	2,6,7,8, 10,12, 14,16
B.	Was machst du öfter und warum: chatten, telefonieren oder dich Face-to-Face unterhalten?	6,8,10, 12,15

C.	Wurdest du schon einmal im Chat missverstanden, weil z.B. deine eigentliche Betonung des Satzes nicht mit rüber kam? Wenn ja, was ist danach passiert?	3,8,10, 15,18
D.	Hattest du schon einmal eine brenzlige Situation im Straßenverkehr oder solche beobachtet, weil auf das Smartphone geschaut wurde? Berichte darüber.	14
E.	Wie nutzt du selbst dein Smartphone im Straßenverkehr? Wie nimmst du die Umwelt dabei wahr?	6,8,12, 14,18
F.	Hast du dich oder deine Freunde schon mal gegoogelt? Was würde ein Fremder über dich oder deine Freunde/Familie erfahren?	1,3,4, 13
G.	Wie wichtig ist für dich Privatsphäre? Was verstehst du da-runter?	1,3,4, 7,9,12, 13,20
H.	Hast du schon einmal Nachrichten auf anderen Smartphones mitgelesen, z.B. in öffentlichen Verkehrsmitteln? Hast du etwas dagegen, wenn deine Nachrichten von anderen mitgelesen werden? Warum?	4,6,8, 20
I.	Warum sollte man sich das Kleingedruckte (z.B. AGBs, Datenschutzerklärung, Lizenz etc.) anschauen, bevor man etwas herunterlädt oder akzeptiert? Wie verhältst du dich in solchen Situationen?	9,17
J.	Mobbing passiert leider viel zu oft und überall. Tust du etwas dagegen? Was könnte man dagegen tun?	3,5,11, 13,19

Security Surfer

Gefahren und Schutzmaßnahmen erkennen

In diesem Lernszenario „Security Surfer – Gefahren und Schutzmaßnahmen erkennen“ wird das globale Thema Internet aufgegriffen und die Untiefen des Internets näher beleuchtet. Surft durch das weite Meer im Internet, erkennt dabei die Gefahren und findet die passenden Schutzmaßnahmen.

- Spielbar mit 4 Teams, eine bis maximal drei Personen pro Team.
- Spieldauer 25-45 Minuten.

Ziel des Lernszenarios

Das Ziel des Lernszenarios ist es, durch das World Wide Web entlang der Inseln zu surfen, die möglichen Gefahren zu erkennen und Schutzmaßnahmen anzuwenden. Es gibt insgesamt 6 Inseln, die ihr vor Gefahren schützen müsst. Jede Insel symbolisiert einen Bereich des Internets und setzt sich aus einer unterschiedlichen Anzahl von Teilinseln zusammen. Eure Aufgabe ist es, die Inseln zu schützen, indem ihr auf die Fragen zum Thema sicheres Surfen im Internet antwortet und Schutzmaßnahmen findet. Wichtig ist dabei, eine Strategie zu verfolgen, um so viele Inseln wie möglich zu schützen.

Einstiegsfragen

„Wozu nutzt ihr hauptsächlich das Internet? Für welche Zwecke?“

Bestandteile

	Spielfeld
	3 x18 Fragekarten
	6 Phishing-Karten
	4 Spielfiguren 4 x 10 Pins

Vorbereitung und Erläuterung des Lernszenarios

- Vereinbart die Spieldauer, wenn ihr nicht nach der empfohlenen Zeit spielen möchtet.
- Bildet Teams.
- Wählt den passenden Schwierigkeitsgrad!
- Das Spielfeld und die Karten im gewählten Schwierigkeitsgrad liegen nach Kategorien geordnet verdeckt am Tisch.
- Legt die 6 Fragekarten mit dem Symbol nacheinander in nicht festgelegter Reihenfolge verdeckt auf die Wellen mit Symbol des Spielfeldes.
- Legt die restlichen Fragekarten ebenfalls verdeckt in nicht festgelegter Reihenfolge auf die noch freien Wellensymbole des Spielfeldes.
- Jede Spielerin/ jeder Spieler bzw. jedes Team sucht sich eine Spielfigur aus und nimmt sich die dazugehörigen 10 Spielsteine in der gleichen Farbe.
- Stellt die Spielfiguren auf das Startfeld.
- Die Startreihenfolge kann beliebig festgelegt werden (z.B. Münzwurf, jüngstes/ältestes Team beginnt usw.).

Wählt den passenden Schwierigkeitsgrad!

 Klassenstufen 6-7	Der 1. Schwierigkeitsgrad ist durch eine explizite Auswahl an Fragen thematisch und inhaltlich an die Klassenstufen 6-7 abgestimmt. Dies ermöglicht einen regen Austausch.
 Klassenstufen 8-9	Den 2. Schwierigkeitsgrad zeichnet die Komplexität der zu beantwortenden Fragen aus. Durch die verschiedenen Themenbereiche kommt es zu übergreifenden Diskussionen und Allgemeinwissensbildung.
 Klassenstufen 10-11	Beim 3. Schwierigkeitsgrad sind die Fragen auf das aktuelle Internetverhalten der Jugendlichen abgestimmt. Der gegebene Inhalt und die Komplexität fördern den Austausch sowie eine Diskussion während des Spielens.

Ablauf und Regeln

- Die Spielfiguren werden entlang der Fragekarten im Uhrzeigersinn gesetzt.
- Die Felsen können dabei nicht übersprungen werden.
- Das Team, welches die meisten Spielsteine auf den Inseln aufstellen und somit diese Inseln schützen konnte, gewinnt.

1. **Das Team, welches an der Reihe ist** (z.B. Team A), setzt eine Spielfigur auf das nächste mit einer Fragekarte belegte Feld.
2. **Ein anderes Team** (z.B. Team B) liest die Frage auf der Fragekarte laut vor.
3. **Das aktive Team** (z.B. Team A) bespricht und diskutiert die Antwort.
4. Anschließend wird anhand der Musterlösung bewertet, ob die vom aktiven Team gegebene Antwort richtig oder falsch ist.
5. Entfernt nun die gespielte Fragekarte vom Spielfeld.
6. **Das nächste Team** (z.B. Team B) ist nun am Zug und setzt seine Spielfigur auf das nächste mit einer Fragekarte belegte Feld.

Auflösung

1. Die Auflösung erfolgt unmittelbar nach der Beantwortung der Frage. Sollte eine Antwort nicht vollständig genannt sein, aber den richtigen Sinn erfassen, kann man die Antwort als richtig gelten lassen.
2. Zusätzlich zu der Musterlösung gibt es einen Paragrafen-Wiki und zu etlichen Antworten weitere Hinweise, Tipps oder rechtliche Grundlagen. Diese können entweder nach Beendigung des Lernszenarios besprochen werden oder gleich nach der Auflösung, falls kein Zeitlimit vorher vereinbart wurde.
3. Bei einer richtigen Antwort setzt das Team einen Spielstein auf die entsprechende Themeninsel.
4. Bei einer falschen Antwort geht das Team leer aus und wartet auf den nächsten Zug.

Ende des Spiels

Das Spiel ist zu Ende, wenn einer der beiden Punkte zutrifft:

A. Alle Felder mit Fragekarten sind beantwortet.

B. Die vorher festgelegte Zeit ist abgelaufen.

Lösungsmuster - Schwierigkeitsgrad 1

Nr.	Frage	Lösung
	Suchmaschinen und Co.	
1	Was ist ein Cookie?	Cookies sind browserspezifische Textdateien, die Informationen über dein Surf-Verhalten auf deinem Rechner speichern. Diese werden beim erneuten Besuch einer Webseite ausgelesen.
2	Nenne mindestens drei alternative Suchmaschinen mit besserem Datenschutz als Google.	Alternative Suchmaschinen wie DuckDuckGo und StartPage verhindern, dass Privates gespeichert und weitergegeben wird. Qwant (französische Suchmaschine), Metager (deutsche Meta-Suchmaschine), Ecosia (Berliner Öko-Suchmaschine).
3	Wo kann ich die Standardsuchmaschine austauschen?	Im Browser unter Einstellungen > Suchmaschine > Suchmaschinen verwalten > Hinzufügen

	E-Mail & Co.	
4	Was ist Phishing? .	„Phishing“ ist abgeleitet von „fi-shing“ und bezeichnet das Angeln nach Passwörtern und Kontodaten. Durch gefälschte Webseiten und E-Mails wird versucht, diese Daten von Internetnutzern zu erbeuten.
5	Welche Phishing-Merkmale erkennst du in der folgenden Nachricht? Ziehe Phishing-Karte 1.	Die E-Mail enthält einen verdächtigen Anhang sowie eine unpersönliche Anrede. Hinter der Dateinamenerweiterung „.exe“ steckt eine ausführbare Datei. Diese kann Schadsoftware enthalten. EXE-Dateien als E-Mail-Anhang solltest du daher niemals öffnen. Auch andere mitgesendete Anhänge wie PDFs können Schadsoftware enthalten.
6	Handelt es sich um eine Phishing-Mail? Was sind deine Entscheidungsgründe? Ziehe Karte 2	Es handelt sich um eine Phishing-Mail. Zum einen nutzt du kein Video-on-Demand-Service. Zum anderen weisen die nicht vorhandene Anrede, die Dringlichkeit sowie die Aufforderung einen Link zu folgen auf eine Phishing-Mail hin.
	Soziale Netzwerke	
7	Wann endet das Urheberrecht für Bilder, Filme, etc.? **Tipp:** Siehe auch § 64 UrhG: Allgemeines und § 72 Abs. 3 UrhG: Lichtbilder unter „Nützliche Info“.	In Deutschland endet das Urheberrecht grundsätzlich 70 Jahre nach dem Tod der Urheberin/des Urhebers. Das Urheberrecht für Fotografien endet 50 Jahre nach dem Erscheinen.
8	Du liest folgende Nachricht im Gruppenchat. Wie reagierst du? *„Ha, ha, Lisa aus der 9b schreibt „Matte“ statt „Mathe“. Wie blöd kann man sein?“*	So fängt (Cyber-)Mobbing an. Du hast die Möglichkeit etwas dagegen zu schreiben oder zu sagen (z.B. „Vielleicht hat sie sich vertippt. Du schreibst auch nicht immer perfekt.“). Ggf. kannst du das Geschriebene einer Vertrauensperson melden, besonders, wenn es nicht der erste Vorfall ist.

9	Du bekommst folgende Nachricht inklusive Video von einem Klassenkameraden. Was ist das Problem? *„Habt ihr das Video von Leonie aus der 10a gesehen? Voll peinlich!!! Teilt es weiter, will den Spaß niemanden vorenthalten“* **Tipp:** Siehe auch § 22 KUG/KunstUrhG: Recht am eigenen Bild unter „Nützliche Info“. Zu den Konsequenzen, siehe auch § 201 StGB: Verletzung der Vertraulichkeit des Wortes unter „Nützliche Infos“.	Zum einen ist das eine Form des (Cyber-) Mobbings. Zum anderen wird Leonies Recht am eigenen Bild verletzt, dadurch, dass das Video ungefragt weitergeleitet wird. Was im Klassenchat beginnt, landet häufig für alle sichtbar im Internet. Dies kann schlimme Folgen für die Betroffenen nach sich ziehen.
10	Du willst das neueste Selfie von dir bei Instagram posten. Was solltest du dabei beachten?	Du solltest dich hinterfragen, wieviel du an Informationen von dir Preis gibst und ob du dir mit diesem Bild in der Zukunft Steine in den Weg legen könntest.
	Onlinespiele	
11	Was sind In-App bzw. In-Game-Käufe?	In-App-Käufe sind Käufe innerhalb eines Spiels, wodurch du dir mit relativ kleinen Beträgen Verbesserungen für das Spiel kaufen oder bestimmte Funktionen freischalten kannst.
12	Was musst du bei der Kommunikation mit Mitspielern in einem Onlinespiel beachten?	Vertraue keine privaten Informationen Mitspielenden an, die du nicht aus dem echten Leben kennst. Hinter den Avataren können Kriminelle oder Pädophile stecken, die sich dein Vertrauen erschleichen wollen.
13	Worauf musst du vor dem Herunterladen eines Onlinespiels aus dem App-Store achten?	Prüfe die Seriosität der App z.B. anhand der Bewertungen. Achte auf das Geschäftsmodell der App, wie z.B. In-App-Käufe oder Abonnements. Prüfe, welche Zugriffe die App auf dein Smartphone verlangt und wäge für dich ab.

	Onlineshopping	
15	Welche Pflichtangaben gehören in ein Impressum?	▪ Name, Anschrift (kein Postfach) und ggf. Rechtsform ▪ Geschäftsführer*in oder Vorstand ▪ E-Mail-Adresse ▪ Handelsregister oder Handwerkskammer ▪ Steuernummer, ggf. Umsatzsteuer-Identifikationsnummer
16	Du möchtest online shoppen. Worauf solltest du vorher achten?	Prüfe die Seriosität eines Onlineshops (vollständige Pflichtangaben im Impressum, Hinweis auf Rücktrittsrecht in AGB, Rechtschreibung und Grammatik).
	YouTube, Streaming & Co.	
17	Was ist Clickbait?	Clickbait bedeutet so viel wie Klick-Köder. Durch irreführende, reißerische Titel und Vorschaubilder (engl. „Thumbnails“) werden Klicks generiert, was sich wiederum positiv auf die Schaltung von Werbeanzeigen auswirkt. Dabei sind die Beiträge häufig ohne Mehrwert.
18	Woran erkennst du Videos, die als Clickbait dienen?	Starke Adjektive wie „schockierend“, oder Superlative wie „das Niedlichste“, aktive Verben wie „weinen“ sowie Zahlen, aber auch Handlungsaufforderungen wie „Nicht verpassen!“, Cliffhänger und Abkürzungen wie „WOW“ sorgen für die nötigen Klicks.
19	Wie kannst du herausfinden, ob Informationen aus einem Video vertrauenswürdig sind?	Zuerst kannst du in der Infobox Quellen und Nachweise (über)prüfen. Auf seriösen Webseiten kannst du recherchieren, ob die Informationen dort ebenfalls zu finden sind. Zur Sicherheit kannst du auch deine Eltern oder Lehrkräfte um Rat fragen.

Lösungsmuster - Schwierigkeitsgrad 2

Nr.	Frage	Lösung
	Suchmaschinen und Co.	
1	Was ist der Cache?	Ein Puffer-Speicher, der dafür sorgt, dass z.B. Webseiten schneller erneut geladen werden können.
2	Was musst du bei den Ergebnissen einer Suchmaschinen-Anfrage beachten?	Die ersten Ergebnisse sind häufig Werbeanzeigen, die als solche gekennzeichnet sind. Die Ergebnisse unterscheiden sich je nach Suchmaschine.
3	Im Netz werden viele Daten gespeichert. Aber was passiert mit deinen Daten?	Suchmachinen wie Google verdienen an dir, indem bei jeder Suchanfrage deine IP-Adresse, der verwendete Webbrowser, das Betriebssystem, Datum und Uhrzeit gespeichert und für Werbekunden ausgewertet werden.
	E-Mail & Co.	
4	Welche Merkmale können auf einen Phishing-Versuch hinweisen?	Rechtschreibung und Grammatik, verdächtiger Absender, Dringlichkeit oder Drohung, verdächtiger Anhang, unpersönliche Anrede, Aufforderung einem Link zu folgen, Button zum Anklicken.
5	Welche Phishing-Merkmale erkennst du in der folgenden Nachricht? Ziehe Karte 3.	Das wichtigste Merkmal ist der verdächtige Absender. In der Mailadresse gibt es einen Buchstabendreher, was eindeutig auf eine Fälschung hinweist. Des Weiteren enthält die E-Mail keine Anrede sowie die Aufforderung einen Link zu folgen.
6	Handelt es sich um eine Phishing-Mail? Was sind deine Entscheidungsgründe? Ziehe Karte 4.	Hier handelt es sich nicht um einen Phishing-Versuch. Du kannst dich erinnern, genau dieses E-Book gekauft zu haben.

	Soziale Netzwerke	
7	Welche Gesetze musst du beachten, wenn du selbsterstellten Inhalt wie Bilder und Videos postest? **Tipp:** Siehe auch § 22 KUG/KunstUrhG: Recht am eigenen Bild unter „Nützliche Info“.	Insbesondere musst du das Persönlichkeitsrecht anderer Personen beachten. Jeder hat das Recht am eigenen Bild.
8	Du liest folgende Nachricht im Gruppenchat. Wie reagierst du? *„Der Alex aus meiner Klasse ist voll in Lea verknallt. Wie peinlich, dass er sich mit ihr abgeben will!“*	So fängt (Cyber-)Mobbing an. Du hast die Möglichkeit etwas dagegen zu schreiben, zu Sagen oder das Geschriebene einer Vertrauensperson zu melden, besonders, wenn es nicht der erste Vorfall ist.
9	Du bekommst folgende Nachricht mit Foto von einem Klassenkameraden. Was ist das Problem? *„Erik wird ab jetzt Popel genannt! LOL, dieses Einschulungsbild!!! Erik der 2. von links mit ‘nem Finger in der Nase.“*	Dieser Post stellt einen regelrechten Aufruf zum (Cyber-)Mobbing dar. Hinzu kommt, dass ein Klassenfoto ungefragt verbreitet wird. Wende dich unbedingt an eine Vertrauensperson und melde diesen Vorfall.
10	Du willst einen Kartenausschnitt zu einer Vereinsparty posten. Was musst du dabei beachten? **Tipp:** Open Content/Freier Inhalt/Creative Commons sind nicht frei von Urheberrechten. Die Nutzungserlaubnis ist an bestimmte Bedingungen geknüpft. Informiere dich zu den Creative Commons Lizenzen unter https://creativecommons.org/licenses/	Achtung, bei der Verwendung von Google-Street-Maps drohen Abmahnungen. Nutze z.B. OpenStreetMap. Die in der Standard-Ansicht gewählte Karte steht unter der Creative-Commons-Lizenz „Namensnennung-Weitergabe unter gleichen Bedingungen“ (CC BY-SA).

	Onlinespiele	
11	Was ist das “Freemium”-Prinzip?	Ein Spiel kann gratis heruntergeladen werden, Zusatzfunktionen kosten aber Geld.
12	Wie kannst du dich vor In-App bzw. In-Game-Käufen schützen?	Informiere dich vorher, welche Funktionen kostenfrei nutzbar sind und ob du die Zusatzfunktionen benötigst. Du kannst In-App-Käufe auf IOS-Geräten deaktivieren und auf Android-Geräten mit einem Passwort sperren.
13	Was steckt hinter kostenlosen Spiele-Apps?	Kostenlose Apps sind reine Datensammler, die dazu dienen, ein User-Profil von dir zu erstellen und auf dich zugeschnittene Werbung zu schalten. Je nach Zugriff der App auf dein Smartphone, kann sogar dein Standort ermittelt werden.
	Onlineshopping	
14	Was bedeutet HTTPS?	HTTPS steht für die englischen Begriffe „Hypertext Transfer Protocol Secure“ (auf Deutsch: sicheres Hypertext-Übertragungsprotokoll) und weist auf eine verschlüsselte Verbindung hin.
15	Was solltest du vor der Kaufbestätigung beim Onlineshopping beachten?	Informiere dich über die Gesamtkosten und die Verpflichtungen, die du laut AGB mit dem Kauf eingehst. Achte bei der Zahlung auf eine sichere HTTPS-Verbindung.
	YouTube, Streaming & Co.	
16	Auf bestimmten Seiten kannst du dir kostenlos die neusten Kinofilme herunterladen. Ist das erlaubt?	Nein, das Downloaden von urheberrechtlich geschützten Filmen ist eindeutig strafbar, wenn das Werk aus einer offensichtlich illegalen Quelle stammt.

17	Was ist der Unterschied zwischen Download, Filesharing und Streaming? **Tipp:** Mit dem EuGH-Urteil ist das Streaming von urheberrechtlichen Werken aus illegaler Quelle endgültig rechtswidrig, wenn der User über die Rechtswidrigkeit Kenntnis hätte haben müssen. Siehe auch unter „Nützliche Info“.	Beim Download lädst du dir Dateien auf dein Endgerät herunter. Beim Filesharing bietest du eine heruntergeladene Datei wieder im Internet an. Beim Streaming konsumierst du direkt auf einer Webseite, jedoch werden im Cache temporär Dateien gespeichert.
18	Unter welchen Bedingungen darfst du (YouTube)-Videos herunterladen?	Ein Video darf von dir nur heruntergeladen werden, wenn das Video rechtmäßig erstellt und veröffentlicht wurde und das heruntergeladene Video ausschließlich deines Privatgebrauchs dient.

Lösungsmuster - Schwierigkeitsgrad 3

Nr.	Frage	Lösung
	Suchmaschinen und Co.	
1	Was ist ein Hoax?	Ein Hoax ist eine Falschmeldung im Netz und bedeutet so viel wie „Zeitungsente“ oder „schlechter Scherz“. Unter anderem gehören Kettenbriefe zu dieser Kategorie der Fake News.
2	Woran erkennst du Falschmeldungen (Hoax) im Netz?	Recherchiere einige der Begriffe der Meldung im Internet. Meist kursieren solche Meldungen schon länger im Netz und sind bekannt.
3	“Ich habe nichts zu verbergen.” – Stimmt das? Begründe deine Meinung.	Hinterfrage dich, ob du sensible Daten wie Krankheitsdaten im Internet für alle zugänglich wiederfinden möchtest und ob bestimmte Informationen deinem späteren Berufsleben schaden könnten.

	E-Mail & Co.	
4	Worin unterscheiden sich Phishing, Spear-Phishing und Pharming?	Beim Phishing wird eine große Anzahl an E-Mails versendet. Das Spear-Phishing zielt auf bestimmte Personen oder Unternehmen ab. Beim Pharming wird nicht nur die Website, sondern auch die Internetadresse gefälscht.
5	Welche Phishing-Merkmale erkennst du in der folgenden Nachricht? Ziehe Karte 5.	Das wichtigste Merkmal ist der verdächtige Absender. In der Mailadresse wird Instagram mit „mm“ geschrieben, was eindeutig auf eine Fälschung hinweist. Des Weiteren enthält die E-Mail eine unpersönliche Anrede sowie die Aufforderung, einem Link zu folgen.
6	Handelt es sich um eine Phishing-Mail? Was sind deine Entscheidungsgründe? Ziehe Karte 6.	Es handelt sich um eine Phishing-Mail. Zum einen weisen die unpersönliche Anrede sowie die Aufforderung einem Link zu folgen auf eine Phishing-Mail hin. Das wichtigste Merkmal ist jedoch die Aufforderung, dein Passwort zu ändern.
	Soziale Netzwerke	
7	Welche Gesetze musst du beachten, wenn du Inhalte wie Bilder, die von anderen erstellt wurden, postest? **Tipp:** Siehe auch § 106 UrhG: Unerlaubte Verwertung urheberrechtlich geschützter Werke unter „Nützliche Info“. Zu den Konsequenzen, siehe auch § 97 UrhG: Anspruch auf Unterlassung und Schadenersatz, unter „Nützliche Info“.	Du musst insbesondere das Urheberrecht beachten.
8	Du liest folgende Nachricht im Gruppenchat. Wie reagierst du? *„Habt ihr Toms Shirt gesehen? So was von total out... Der Junge hat 0 Stil.“*	So fängt (Cyber-)Mobbing an. Du hast die Möglichkeit etwas dagegen zu schreiben, zu sagen oder das Geschriebene einer Vertrauensperson zu melden, besonders, wenn es nicht der erste Vorfall ist.

9	Du bekommst folgende Nachricht inklusive Foto von einem Klassenkameraden. Was ist das Problem? „Hier sind die Fotos von Hannas Geburtstag bei ihr zu Hause. Sind echt ein paar lustige Schnappschüsse dabei.“ **Tipp:** Siehe auch § 22 KUG/KunstUrhG: Recht am eigenen Bild unter „Nützliche Info“. Zu den Konsequenzen, siehe auch § 201a StGB: Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen unter „Nützliche Info“.	Je nachdem, was abgebildet ist, kann es sich bereits um (Cyber-) Mobbing handeln. In jedem Fall wird das Recht am eigenen Bild der Geburtstagsgäste verletzt, da die Bilder höchstwahrscheinlich ungefragt weitergeleitet wurden. Was im Klassenchat beginnt, landet häufig für alle sichtbar im Internet. Dies kann schlimme Folgen für die Betroffenen nach sich ziehen.
10	Du willst ein Partybild von deinen Freunden bei Instagram posten. Was solltest und musst du dabei beachten? **Tipp:** Siehe auch § 22 KUG/KunstUrhG: Recht am eigenen Bild unter „Nützliche Info“.	Du solltest deine Freunde um Erlaubnis fragen und dich hinterfragen, ob du dieses Bild z.B. deinem zukünftigen Chef zeigen würdest.
	Onlinespiele	
11	Was ist ein Bot in einem Onlinespiel?	Ein Bot ist ein selbstlaufendes Programm, das auf die Spielemechanik und Technik zugreift, um dem Spieler einen Vorteil zu verschaffen (z.B. Erwerb besserer Items und Skills).
12	Wie kannst du deinen Spieleaccount vor fremden Zugriffen schützen?	Schütze deinen Account mit einem sicheren Passwort. Schütze auch dein(e) Endgerät(e) vor fremden Zugriffen. Klicke nicht auf dubiose Links.
13	Wie kannst du dich vor Apps, die mit Malware modifiziert sind, schützen?	Lade Apps nur aus vertrauenswürden Quellen herunter, nachdem du vorher Bewertungen gelesen hast. Überprüfe regelmäßig dein Smartphone mit einem mobilen Viren-/Malware-Scanner..

	Onlineshopping	
14	Was bedeutet eine dynamische Preisgestaltung beim Onlineshopping?	Bei der dynamischen Preisgestaltung („Dynamic Pricing“) werden unter anderem Daten zum benutzten Gerät, zum Standort und zur Tageszeit ausgewertet, um die Preise individuell anzupassen.
15	Warum ist es möglich, dass Bestellungen über Apple-Endgeräte teurer sind als über Windows-Endgeräte?	Durch das Hinterlassen von Spuren im Internet ist es den Anbietern nicht nur möglich, individualisierte Werbung zu schalten, sondern auch Preise individuell zu gestalten. Apple-Nutzer gelten in der Regel als zahlungskräftiger.
	YouTube, Streaming & Co.	
16	Darf man gestreamte Filme oder Musik mitschneiden? **Tipp:** Siehe auch § 53 UrhG: Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch unter „Nützliche Info“.	Ja, sofern man dafür bezahlt (hat). Hier existiert das Recht auf eine Privatkopie. Ein Veröffentlichen oder Weitergeben dieses Mitschnitts ist jedoch nicht erlaubt.
17	Was muss vor dem Hochladen eines Videos, z.B. bei YouTube, beachtet werden?	Die Genehmigung aller abgebildeten Personen wurde eingeholt. Das Urheberrecht wird beachtet. Für die zu hörende Musik (auch die im Hintergrund), liegt von der GEMA eine Genehmigung vor.
18	Welche Verdienstmöglichkeit hat ein YouTube-Influencer? **Tipp:** Siehe auch § 5a UWG: Irreführung durch Unterlassen unter „Nützliche Info“.	Die Influencer verdienen durch Werbeclips vor, zwischen und nach den Videos, Affiliate-Links, Produktplatzierung, Fan-Artikel sowie Unternehmens-Kooperationen. Klicks, Abos und Likes erhöhen die Reichweite und somit den Marktwert der Influencer.

Tipps und Hinweise

- Um deine Privatsphäre zu schützen, solltest du Cookies unter den Browsereinstellungen regelmäßig löschen bzw. gleich die Verwendung von Cookies ablehnen.
- Wenn du ein Programm aus dem Internet auf deinen PC herunterlädst, erhältst du eine EXE-Datei, um es zu installieren. Prüfe daher vorher, ob die Quelle vertrauenswürdig ist.
- Falls bei dir keine Endungen der Dateien sichtbar sind, kannst du die „Dateinamenerweiterung“ in der Ordneroption einstellen.
- Gehe mit deiner Smartphone-Kamera oder einer Digitalkamera auf Entdeckungsjagd und poste statt Selfies doch einfach mal eine wunderschöne Landschaft.
- Achtung: Die auf den ersten Blick niedrigen Beträge in Onlinespielen sollen dich immer wieder zum Kauf von Extras animieren, sodass du schnell den Überblick über die Gesamtkosten verlieren kannst. Prepaid-Nutzung anstreben!
- Benutze keinen Namen für deinen Avatar, der persönliche Dinge wie dein Alter oder deinen richtigen Namen verrät.
- Achtung vor Fake-Bewertungen, die die Qualität hochstufen oder das Ranking verändern. Lies dir vor allem die schlechteren Bewertungen durch.
- Alternative Suchmaschinen wie DuckDuckGo und StartPage verhindern, dass Privates gespeichert und weitergegeben wird.
- Vermeide auch möglichst die automatische Anmeldung auf anderen Websites über Google oder Facebook.
- Wäge für dich ab, ob dir ein kostenloses Spiel wichtiger ist als die Preisgabe deiner Daten.
- Bevor du irgendwelche Meldungungen an andere Personen weiterleitest, prüfe ihre Richtigkeit.
- Dein Passwort sollte nach aktuellem Stand mind. 12 Zeichen lang ein.
- Nutze alle verfügbaren Zeichen (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen).

- Dein Passwort sollte nicht in Wörterbüchern vorkommen und nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern wie „asdfgh“ oder „1234abcd“ bestehen.
- Zum Merken entweder Passwort aus Merksatz bilden oder Passwortmanager benutzen.
- Apps können sich als vertrauenswürdig tarnen und legitim wirken (Achtung auch vor gefälschten Viren-/Malware-Scannern). Eine Nachforschung zu den Entwicklern einer App kann dir ebenfalls helfen.
- Achte bei Online-Shops darauf, dass diese häufig auf dynamische Preisgestaltung zurückgreifen und die Preise auf der Auswertung deiner Daten beruhen.
- Bei den Videos vieler Influencer verschwimmen häufig Realität und Inszenierung ineinander. Videos mit Produktplatzierungen müssen entsprechend gekennzeichnet werden, da sie sonst als Schleichwerbung gelten. Auch Affiliate-Links, welche die User zu einem Onlineshop weiterleiten, wofür die Influencer Provisionen erhalten, müssen als solche erkennbar sein.

§

Gesetz gegen den unlauteren Wettbewerb (UWG)

§ 5a UWG: Irreführung durch Unterlassen

(6) Unlauter handelt auch, wer den kommerziellen Zweck einer geschäftlichen Handlung nicht kenntlich macht, sofern sich dieser nicht unmittelbar aus den Umständen ergibt, und das Nichtkenntlichmachen geeignet ist, den Verbraucher zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte.

Gesetz über das Urheberrecht an Werken der bildenden Künste und der Fotographie (KUG/KunstUrhG)

§ 22 KUG/KunstUrhG: Recht am eigenen Bild

Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden [...]

Gesetz über Urheberrecht und verwandte Schutzrechte

(Urheberrechtsgesetz - UrhG)

§ 53 UrhG: Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch

(1) Zulässig sind einzelne Vervielfältigungen eines Werkes durch eine natürliche Person zum privaten Gebrauch auf beliebigen Trägern, sofern sie weder unmittelbar noch mittelbar Erwerbszwecken dienen, soweit nicht zur Vervielfältigung eine offensichtlich rechtswidrig hergestellte oder öffentlich zugänglich gemachte Vorlage verwendet wird. Der zur Vervielfältigung Befugte darf die Vervielfältigungsstücke auch durch einen anderen herstellen lassen, sofern dies unentgeltlich geschieht, oder es sich um Vervielfältigungen auf Papier oder einem ähnlichen Träger mittels beliebiger fotomechanischer Verfahren, oder anderer Verfahren mit ähnlicher Wirkung, handelt.

(6) Die Vervielfältigungsstücke dürfen weder verbreitet noch zu öffentlichen Wiedergaben benutzt werden [...]

(7) Die Aufnahme öffentlicher Vorträge, Aufführungen oder Vorführungen eines Werkes auf Bild- oder Tonträger, die Ausführung von Plänen und Entwürfen zu Werken der bildenden Künste und der Nachbau eines Werkes der Baukunst sind stets nur mit Einwilligung des Berechtigten zulässig.

§ 64 UrhG: Allgemeines

Das Urheberrecht erlischt siebzig Jahre nach dem Tode des Urhebers.

§ 72 UrhG: Lichtbilder

(3) Das Recht nach Absatz 1 erlischt fünfzig Jahre nach dem Erscheinen des Lichtbildes, oder wenn seine erste erlaubte öffentliche Wiedergabe früher erfolgt ist nach dieser, jedoch bereits fünfzig Jahre nach der Herstellung [...]

§ 97 UrhG: Anspruch auf Unterlassung und Schadensersatz

(1) Wer das Urheberrecht oder ein anderes nach diesem Gesetz geschützten Recht verletzt, kann von dem Verletzten auf Beseitigung der Beeinträchtigung, bei Wiederholungsgefahr auf Unterlassung verklagt werden. Der Anspruch auf Unterlassung besteht auch dann, wenn eine Zuwiderhandlung erstmalig droht.

(2) Wer die Handlung vorsätzlich oder fahrlässig vornimmt, ist dem Verletzten zum Ersatz des daraus entstehenden Schadens verpflichtet. Bei der Bemessung des Schadensersatzes kann auch der Gewinn, den der Verletzende durch die Verletzung des Rechts erzielt hat, berücksichtigt werden.

§ 106 UrhG: Unerlaubte Verwertung urheberrechtlich geschützter Werke

(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung bzw. Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, muss mit einer Freiheitsstrafe von bis zu drei Jahren oder mit einer Geldstrafe rechnen.

(2) Der Versuch ist strafbar.

Strafgesetzbuch (StGB)

§ 201 Strafgesetzbuch: Verletzung der Vertraulichkeit des Wortes

(1) Mit einer Freiheitsstrafe von bis zu drei Jahren oder mit einer Geldstrafe wird bestraft, wer unbefugt

1. das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder
2. eine so hergestellte Aufnahme gebraucht oder diese einem Dritten zugänglich macht.

§ 201a StGB: Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

1. von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt eine Bildaufnahme herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt,
2. eine Bildaufnahme, die die Hilflosigkeit einer anderen Person zur Schau stellt, unbefugt herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt,
3. eine durch eine Tat nach den Nummern 1 oder 2 hergestellte Bildaufnahme gebraucht oder einer dritten Person zugänglich macht, oder
4. eine befugt hergestellte Bildaufnahme, der in den Nummern 1 oder 2 bezeichneten Art wissentlich unbefugt einer dritten Person zugänglich macht und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt.

Verhalten in sozialen Netzwerken

Internetregeln erkennen

An dieser Lernstation geht es darum, Lösungen und Ansprechpartner in verschiedenen Situationen zu finden und sich den adäquaten und freundlichen Umgang in sozialen Netzwerken bewusst zu machen. „Behandle andere so, wie du selbst behandelt werden möchtest!“ Diese „Goldene Regel“ gilt sowohl im wirklichen Leben als auch in sozialen Netzwerken.

- Geeignet für 2 Teams bis je 6 Personen.
- Spieldauer 25-45 Minuten.

Ziel des Lernszenarios

Ziel des Lernszenarios ist es, dass sich die Teilnehmenden über potenzielle

Sicherheitsgefahren in sozialen Netzwerken und im Schulalltag bewusst werden und entsprechende Schutzmaßnahmen erkennen und ergreifen können. Hierbei werden sowohl Themen der Informationssicherheit als auch der physischen Sicherheit angesprochen.

Einstiegsfragen

„Sind euch Situationen (aus den sozialen Netzwerken) bekannt, in denen leicht sensible Informationen preisgegeben werden? Ist euch schon mal aufgefallen, dass jemand in sozialen Netzwerken gemobbt wurde?“

„Wie viele Apps nutzt ihr für die Kommunikation in den sozialen Netzwerken?“

„Achtet ihr auf die richtige Schreibweise und den richtigen Umgangston beim Chatten in den sozialen Netzwerken?“

Bestandteile

	Spielfeld
	**Frage-/Fallkarten:** jeweils 12 für Schwierigkeitsgrad 1 jeweils 13 für Schwierigkeitsgrad 2 und 3 **Begriffskarten:** 10 für alle Schwierigkeitsgrade
	2 Spielfiguren, 4 Chips
	Sanduhr, Würfel

Vorbereitung und Erläuterung des Lernszenarios

- Vereinbart die Spieldauer, wenn ihr nicht nach der empfohlenen Zeit spielen möchtet.
- Bestimmt eine Moderatorin/ einen Moderator. Die moderierende Person kontrolliert den Zeitablauf, legt Wert auf vollständige Antworten und gibt die Auflösung. Sie spielt nicht in einem der Teams mit. Bildet zwei Teams.
- Das Spielfeld, die Sanduhr und der Würfel liegen in der Mitte des Tisches.
- Die Karten liegen nach drei Kategorien geordnet und verdeckt stapelweise am Rand des Spielfeldes.
- Wählt die Spielfigur für euer Team aus und stellt diese an den Start.
- Einigt euch darauf, welches Team „A“ heißen wird und beginnen darf.

Wählt den passenden Schwierigkeitsgrad!

 Klassenstufen 6-7	Die 3 Schwierigkeitsgrade beinhalten Begriffe und / oder Aussagen, die auf das entsprechende Alter angepasst sind. Nehmt das gewählte Kartenset heraus und legt es verdeckt auf den Tisch.
 Klassenstufen 8-9	
 Klassenstufen 10-11	

Ablauf eines Spielzuges

1. **Team A** beginnt und würfelt. Das gewürfelte Symbol zeigt an, um welche Kategorie ihr spielen müsst.
2. **Bevor ihr die Karte vom Stapel zieht – lest zunächst die Erklärung der Kategoriekarten in der Anleitung durch!**
3. Zieht nun die Karte und lest diese laut vor. Diskutiert und entscheidet euch als Team gemeinsam für eine Antwort, innerhalb einer Minute.
4. Die Chips sind dazu da, um eure Zuordnung während des Zuges auf dem Spielfeld zu markieren.

Auflösung

5. Die moderierende Person gibt die Auflösung anhand der Musterlösung. Entspricht eine Antwort nicht der Musterlösung, wurde jedoch nachvollziehbar begründet, kann die moderierende Person diese Antwort gelten lassen.
6. Hat das Team die richtige Antwort gegeben, darf es um ein Feld weiterziehen. Bei falscher Antwort muss das Team auf dem Feld stehen bleiben.
7. Team B ist an der Reihe.

Kategoriekarten

	**Fall - Richtig agieren!** Um diese Aufgabe zu gewinnen, bestimmt eine Spielerin/ einen Spieler aus eurem Team, die/der eine Aussage laut vorliest. Danach wird die Sanduhr umgedreht und ihr müsst euch im Team beraten und die Karte einer Kategorie und dem richtigen Ansprechpartner/Instanz (Eltern, Lehrer, Schulleitung, Notruf, Nummer gegen Kummer, Hausmeister) innerhalb einer Minute zuordnen.
	**Frage - Eine Frage zu sozialen Netzwerken beantworten.** Um diese Aufgabe zu gewinnen, bestimmt eine Spielerin/ einen Spieler aus eurem Team, die / der eine Frage zu sozialen Netzwerken laut vorliest. Dabei nimmt sie/er eine Karte vom Stapel und die Sanduhr wird umgedreht. Das Team muss innerhalb einer Minute eine Antwort abgeben.
	**Begriff - Begriff erklären, ohne dabei die verwandten Wörter zu benennen.** Um diese Aufgabe zu gewinnen, bestimmt eine Spielerin/ einen Spieler aus eurem Team, die/der einen Begriff innerhalb einer Minute dem eigenen Team erklärt. Dabei dürfen keine Wörter benutzt werden, die auf der Karte stehen. Das eigene Team muss versuchen den Begriff zu erraten. Das gegnerische Team kontrolliert dabei die Richtigkeit der verwendeten Begriffe. Die ausgewählte Person nimmt eine Karte, bereitet sich kurz vor und die Sanduhr wird umgedreht.

Auflösung

Die Musterlösung dient der Aufklärung, schließt aber andere mögliche Vorgehensweisen nicht aus, wenn diese nachvollziehbar begründet werden.

Lösungsmuster - Schwierigkeitsgrad 1

Nr.	Fragekarten	Lösung
1	Was solltest du beachten, wenn du dich bei einem sozialen Netzwerk anmelden möchtest? Nenne mind. 1 Punkt.	Ich frage vorher meine Eltern und wir schauen uns gemeinsam die AGB und die Datenschutzerklärung an. Außerdem informieren wir uns bei einer sicheren Quelle wie z.B. klicksafe.de
2	Was machst du, wenn du eine Freundschaftsanfrage im Internet bekommst?	Ich schaue mir die Person genau an. Wenn ich die Person nicht kenne oder unsicher bin, lehne ich die Anfrage lieber ab.
3	Du möchtest deine neusten Urlaubsbilder posten. Was musst du beachten?	Ich überlege genau, welche Bilder ich noch nach 10 Jahren nicht peinlich finden werde und wäge ab, wie notwendig es ist Bilder von mir zu posten. Das Internet vergisst nichts. Ich möchte nicht, dass die ganze Welt über mich alles weiß, weil es sich negativ auf mich, meine Familie und Freunde auswirken kann.
4	Eine unbekannte Person ruft dich an und stellt sich als Telekom-Mitarbeiter vor. Er fordert dich auf, ein Update auf deinem PC durchzuführen. Er meint, dass es dringend ist und man nicht warten könne, bis deine Eltern zuhause sind. Wie verhältst du dich?	Ich gebe mein Passwort nicht bekannt und kontaktiere meine Eltern und den Kundenservice meines Telefonie-Anbieters.
5	Worauf musst du besonders achten, wenn du Bilder in einem Sozialen Netzwerk hochlädst?	Private Fotos sollten nur auf privaten Profilen gepostet werden. Man sollte nur Fotos posten zu denen man wirklich steht. Ich achte darauf, was Bilder über mich verraten. Frage abgebildete Personen auf dem Foto vorher um die Erlaubnis es zu posten. Peinliche Fotos sollte man sofort versuchen aus dem Internet zu löschen. Fotos, die jemand anderes gemacht hat, darf ich nicht einfach hochladen.

6	Worauf musst du beim Weiterleiten und Posten von Bildern und Videos achten, die du nicht selbst erstellt?	Wahrung der Rechte Dritter. Urheberrecht-gesetz beachten. Das Foto/Video gehört demjenigen, der es gemacht hat. Ich muss erst heraus-bekommen, wer der Fotograf ist und diesen um Erlaubnis bitten. Das Hochladen ohne Erlaubnis fremder Werke ist strafbar.
7	Wo kann man Beschwerden über umstrittene und / oder verbotene Internetangebote anbringen? Würdest du es nutzen?	Eltern informieren. Polizei informieren. Inter-net-Beschwerdestelle.de
8	Was kann eine große Gefahr bei öf-fentlichen WLAN-Hotspots sein?	Fehlende Verschlüsselung. Hacker können auf meine Daten zugreifen. Die Sicherheit ist nicht unbedingt gewährleistet, wenn ich die Geschäftsbedingungen zu kostenlosem WLAN akzeptiere. Kriminelle können gefälschte Netze erstellen, um an mein Passwort zu kommen.
9	Was ist das Recht auf informationelle Selbstbestimmung?	Dies ist das Recht, welches, das meine persön-lichen Daten (Name, Adresse...) vor unerlaub-ter Verwendung schützt.
10	Warum sollte ich sparsam bei Profil-informationen sein?	Private Dinge verrät man nicht jedem. Persönli-che Daten sollte man nur an Freunde freige-ben. Kriminelle können diese Informationen nutzen, um z.B. Zugangsdaten zu stehlen.
11	Gehe ein Feld vor und würfle erneut, um deinen Zug zu beenden.	
12	Dein Team setzt eine Runde aus.	

Nr.	Fall/Aussage-Karten	Maßnahmenfeld
1	Der Mathelehrer erhält eine Whats-App von einem Schüler, der ihm schreibt: „mein Vater schenkt Ihnen einen 100 Euro-Gutschein, wenn Sie mir eine glatte 2 geben würden “ Was ist bei so einem Vorfall zu tun, wenn ich es mitbekommen sollte?	Schulleitung (Bestechung, Korruption); auch möglich: Eltern, Polizei
2	Ein Schüler aus der 10a beschwert sich bei Instagram schon wieder über eine Lehrerin, aber wie - der Ton ist ja nicht mehr feierlich, das geht ganz klar unter die Gürtellinie. Wirst du eingreifen, bevor es eska-liert?	Vertrauenslehrer, Schulleitung (Fehlverhalten in Sozialen Medien); kann zum Mobbing werden; Zivilcourage zeigen und eingreifen.
3	**Klassenchat** Lisa: Hey Leute, echt cool, dass morgen erste Stunde ausfällt. Ich mache morgen gleich blau und geh ne Runde chillen am Sportplatz. Der, der nicht mitmacht ist blöd und wird gleich am Mittwoch in der Schule bloßgestellt!!!	Eltern/Lehrende
4	**Klassenchat** Moritz: Riecht irgendwie verbrannt hier. Ist doch nicht bei uns, oder? Falls doch, wüsste ich jetzt gar nicht, was ich tun sollte – an wen wende ich mich da bloß? Hat jemand ne Idee???	Hausmeister (Bei Reparaturen im Gebäude an Hausmeister/ Lehrende)
5	**Klassenchat** Mona: Aus der Heizung im Ge-schichtsraum fließt auf einmal heißes Wasser raus. So heiß, dass man sich verbrennen kann. Soll ich es melden?	Hausmeister (Reparaturen im Gebäude)

6	**Mein Tagebuch** Ich bin echt die schlechteste in der ganzen Klasse, keiner mag mich. Außerdem haben sich meine Eltern getrennt, das zieht mich total runter. Wer könnte mir bloß helfen?	Nummer gegen Kummer/ Vertrauenslehrende/ Eltern
7	**Klassenchat** Max: Habt ihr den Kindergartenrucksack von Tom gesehen ? Voll peinlich mit solchen Sachen rumzurennen. Den machen wir morgen auf dem Schulhof zur Sau, das wird ein Spaß!	Eltern, Schulleitung, ggf. Polizei (Mobbing)
8	**Klassenchat** Nina: hey Leute habt ihr gesehen, dass Lena die ganze Zeit in der Nase popelt. Sie wird ab jetzt die Popellena genannt. Wer nicht mitmacht wird auch Popel genannt!	Eltern, Schulleitung, ggf. Polizei, Nummer gegen Kummer (Mobbing)
9	**Klassenchat** Luna: Der Lars schafft es nicht in die nächste Klassenstufe, wie peinlich, dass er sitzen bleiben muss Maya: Na und, ist doch nicht dein Problem. Außerdem wird ihm das gut tun und er wird sich bessern. Luna: Biste verknallt in ihn oder was? Maya gibt sich mit dummen ab!	Eltern/ Vertrauenslehrende/ Schulleitung (Mobbing) Zivilcourage zeigen und eingreifen.
10	Zwei Schüler haben ein Fenster in der Umkleide kaputt gemacht und sich davon gemacht. Sven hat das ganze heimlich auf seinem Smartphone gefilmt, weiß aber nicht was er jetzt tun soll. Er hat auch Angst als Petze dazustehen.	Hausmeister/ Lehrer/ Schulleitung
11	Jungs posten ein Video in einem der Sozialen Netzwerke worauf zu sehen ist, wie ein Schüler brutal verhauen wird. Maria weiß nicht was sie tun soll und ob und wem sie es melden soll.	Polizei 110/ Eltern
12	Gehe ein Feld vor und würfle erneut, um deinen Zug zu beenden.	

Nr.	Begriffskarten	Begriffe, die man nicht verwenden darf
1	Cybermobbing	Ärgern
2	Hate speech	Hass
3	Smartphone	Telefonieren
4	Community	Soziales Netzwerk
5	Virenscanner	Virus
6	Suchmaschine	Google
7	Big Data	Datenhandel
8	Handyspiel	Spielen
9	Follower	Jemandem folgen
10	Account	Anmelden

Lösungsmuster - Schwierigkeitsgrad 2

Nr.	Fragekarten	Empfohlene Antwort
1	Was solltest du beachten, wenn du dich bei einem sozialen Netzwerk anmelden möchte? Nenne mind. 2 Punkte.	Ich frage vorher meine Eltern und wir schauen uns gemeinsam die AGBs und die Datenschutzerklärung an. Außerdem informieren wir uns bei einer sicheren Quelle wie z.B. klicksafe.de
2	Was machst du, wenn du eine Freundschaftsanfrage im Internet bekommst? Erläutere dein Vorgehen.	Ich schaue mir die Person genau an. Wenn ich die Person nicht kenne oder unsicher bin, lehne ich die Anfrage lieber ab.
3	Du möchtest deine neusten Urlaubsbilder posten. Was musst du beachten? Benenne mind. 2 Punkte.	Ich überlege genau, welche Bilder ich noch nach 10 Jahren nicht peinlich finden werde und wäge ab, wie notwendig es ist Bilder von mir zu posten. Das Internet vergisst nichts. Ich möchte nicht, dass die ganze Welt über mich alles weiß, weil es sich negativ auf mich, meine Familie und Freunde auswirken kann.
4	Eine unbekannte Person ruft dich an und stellt sich als O2-Mitarbeiter vor. Er fordert dich auf, dein Passwort für ein neues Update zu nennen. Wie verhältst du dich? Begründe.	Ich gebe mein Passwort nicht bekannt und kontaktiere meine Eltern und den Kundenservice meines Telefonie-Anbieters.
5	Worauf musst du besonders achten, wenn du Bilder oder Videos in einem Sozialen Netzwerk hochlädst? Benenne mind. 2 Punkte und begründe diese.	Private Fotos sollten nur auf privaten Profilen und geschlossenen in Gruppen erscheinen. Man sollte nur Fotos posten zu denen man wirklich steht. Ich achte darauf, was Bilder über mich verraten. Ich Frage abgebildete Personen auf dem Foto um die Erlaubnis es zu posten. Ich versuche peinliche Fotos sofort aus dem Internet zu löschen. Fotos, die jemand anderes gemacht hat, darf ich nicht einfach hochladen.

6	Worauf musst du beim Weiterleiten und Posten von Bildern und Videos achten, die du nicht erstellt hast? Benenne mind. 2 Punkte.	Wahrung der Rechte Dritter. Urheberrecht-gesetz beachten. Das Foto/Video gehört demjenigen, der es gemacht hat. Ich muss erst herausbekommen, wer der Fotograf ist und diesen um Erlaubnis bitten. Das Hochladen von fremden Werken ist strafbar.
7	Worauf musst du besonders achten, wenn du Daten in eine Cloud lädst? Benenne mind. 2 Schritte und begründe diese.	Wenn ich Daten in eine Cloud lade, muss ich: - die Einstellung des Smartphones überprüfen, - sensible Daten verschlüsseln z.B. mit 7-Zip Software, - ein sicheres Passwort (ggf. auch eine Zwei-Faktor-Authentifikation) verwenden, und - auf eine verschlüsselte Übertragung achten.
8	Wo kann man Beschwerden über umstrittene und / oder verbotene Internetangebote anbringen? Benenne mind. 2 Möglichkeiten. Würdest du es nutzen? Begründe.	Eltern informieren. Polizei informieren. Internet-Beschwerdestelle.de
9	Warum solltest du öffentliche WLAN-Hotspots vermeiden? Benenne mind. 2 Punkte. Begründe.	Fehlende Verschlüsselung. Hacker können auf meine Daten zugreifen. Die Sicherheit ist nicht unbedingt gewährleistet, wenn ich die Geschäftsbedingungen zu kostenlosem WLAN akzeptiere. Kriminelle können gefälschte Netze erstellen, um an mein Passwort zu kommen.
10	Was ist das Recht auf informationelle Selbstbestimmung?	Das ist das Recht, welches, das meine persönlichen Daten (Name, Adresse...) vor unerlaubter Verwendung schützt.
11	Warum solltest du sparsam bei Profilinformationen sein? Benenne mind. 2 Punkte.	Private Dinge verrät man nicht jedem. Private Fotos und Informationen gehören nicht in ein solches Profil. Persönliche Daten sollte man nur an Freude freigeben.
12	Gehe ein Feld vor und würfle erneut, um deinen Zug zu beenden.	
13	Dein Team setzt eine Runde aus.	

Nr.	Fall/Aussage-Karten	Maßnahmenfeld
1	Der Mathelehrer erhält eine Whats-App von einem Schüler, der ihm schreibt: „mein Vater schenkt Ihnen einen100 Euro-Gutschein, wenn Sie mir eine glatte 2 geben “ Was ist bei so einem Vorfall zu tun, wenn ich es mitbekommen sollte? Begründe und nenne mind. 2 Vorgehensweisen.	Schulleitung (Bestechung, Korruption); auch möglich: Eltern, Polizei
2	Ein Schüler aus der 10a beschwert sich bei Instagram schon wieder über eine Lehrerin, aber wie - der Ton ist ja nicht mehr feierlich, das geht ganz klar unter die Gürtellinie. Würdest du eingreifen bevor es eskaliert? Begründe mit mind. 2 Punkten.	Vertrauenslehrer, Schulleitung (Fehlverhalten in Sozialen Medien); kann zum Mobbing werden; Zivilcourage zeigen und eingreifen.
3	**Gruppenchat** Anton: Sturmfreie Bude am Wochenende Katy: dann wissen wir ja jetzt alle, wo wir Peets B-Day nachfeiern können Karl: Alle zu Anton am Samstag um 8! Das wird der Hammer Sammy: Bin dabei und bringe noch ein paar Freunde mit	Eltern, Polizei. Private Informationen sollte man nicht preisgeben, es kann sich negativ auswirken und strafrechtlich verfolgt werden.
4	**Klassenchat** Lisa: Hey Leute, echt cool, dass morgen erste Stunde ausfällt. Ich mache morgen gleich blau und geh ne Runde chillen am Sportplatz. Der, der nicht mitmacht ist blöd und wird gleich am Mittwoch in der Schule bloßgestellt!!! Warum ist es Fehlverhalten? Begründe.	Eltern/Lehrende Aufruf zum Regelverstoß/ Gruppenzwang

5	**Instagram-Video-Story** Moritz: Ey Leute, muss ich mir Sorgen machen, wenn es nach Verbranntem in der Wohnung riecht? Hab echt ein komischen Gefühl. Was würdet ihr in meinem Fall tun?	Notruf 112, Polizei, Brandschutzhelfer (Feueralarm mit Gebäudeevakuierung)
6	**Klassenchat** Viky: Aus der Heizung im Geschichtsraum fließt auf einmal heißes Wasser raus. So heiß, dass man sich verbrennen kann. An wen melde ich es? HELP Benenne deine Vorgehensweise.	Hausmeister (Reparaturen im Gebäude)
7	**Mein Tagebuch** Ich bin echt die schlechteste im ganzen Jahrgang und keiner mag mich. Außerdem haben sich meine Eltern getrennt, das zieht mich total runter. Wer könnte mir bloß helfen? Was würdest du tun?	Vertrauenslehrende/ Eltern/ Nummer gegen Kummer
8	**Klassenchat** Mailo: Habt ihr die Mütze von Tom gesehen? Voll peinlich mit solchen Sachen rumzurennen. Gebt euch nicht mit ihm ab, sonst werdet ihr von dem Kindergarten angesteckt!“ Beschreibe deine Vorgehensweise.	Eltern, Schulleitung, ggf. Polizei (Mobbing)
9	**Klassenchat** Fenja: hey Leute habt ihr gesehen, dass Lena und Alex ein Paar sind? Voll krass, dass sie sich mit ihm abgibt. Der stinkt doch immer nach dem Sportunterricht wie ne Sau. Das Stinke-Paar werden sie ab jetzt genannt!“ Wie reagierst du?	Eltern, Schulleitung, ggf. Polizei (Mobbing)

10	**Klassenchat** Lucy: wie peinlich, dass Timo sitzen bleiben muss Maya: Na und, ist doch nicht dein Problem. Lucy: Biste verknallt in ihn oder was? Das wird morgen der Renner in der Schule sein! Was läuft hier falsch? Begründe.	Eltern/ Vertrauenslehrende/ Schulleitung (Mobbing) Zivilcourage zeigen und eingreifen.
11	Zwei Schüler haben ein Fenster in der Umkleide kaputt gemacht und sich davon gemacht. Sven hat das ganze heimlich auf seinem Smartphone gefilmt, weiß aber nicht was er jetzt tun soll. Er hat auch Angst als Petze dazustehen. Was soll Sven tun? Begründe.	Hausmeister/ Lehrer/ Schulleitung Diesen Vorfall anonym melden.
12	Jungs posten ein Video in einem der Soz. Netzwerke worauf zu sehen ist, wie ein Schüler brutal verhauen wird. Maria weiß nicht was sie tun soll und ob und wem sie es melden soll. Was soll Maria tun? Begründe.	Polizei 110/ Eltern Diesen Vorfall diskret melden. Das Opfer kontaktieren und erzählen, dass man es gemeldet hat.
13	Gehe ein Feld vor und würfle erneut, um deinen Zug zu beenden.	

Nr.	Begriffskarten	Begriffe, die man nicht verwenden darf
1	Cybermobbing	Ärgern, Schikanieren, Bloßstellen
2	Hate speech	Hass(rede), Kommentar, Neid,
3	Smartphone	Telefonieren, Chatten, Spielen
4	Community	Soziales Netzwerk, Posten, Chatten
5	Virenscanner	Virus, Krankheit, Checken
6	Suchmaschine	Google, Safari, Internet
7	Big Data	Datenhandel, Sammeln, Massendaten
8	Handyspiel	Spielen, Game, Zocken
9	Follower	Jemandem folgen, Liken Abonnement
10	Account	Anmelden, Erstellen, Profil

Lösungsmuster - Schwierigkeitsgrad 3

Nr.	Fragekarten	Empfohlene Antwort
1	Was solltest du beachten, wenn du dich bei einem sozialen Netzwerk anmelden möchte? Benenne mind. 3 Punkte	Ich frage vorher meine Eltern und wir schauen uns gemeinsam die AGBs und die Datenschutzerklärung an. Die erlaubte Altersnutzung. Außerdem informieren wir uns bei einer sicheren Quelle wie z.B. klicksafe.de
2	Was machst du, wenn du eine Freundschaftsanfrage im Internet bekommst? Benenne dein Vorgehen und Begründe es.	Ich schaue mir die Person genau an. Wenn ich die Person nicht kenne oder unsicher bin, lehne ich die Anfrage lieber ab.
3	Du möchtest deine neusten Urlaubsbilder posten. Was musst du beachten? Benenne mind. 3 Punkte und begründe.	Ich überlege genau, welche Bilder ich noch nach 10 Jahren nicht peinlich finden werde und wäge ab, wie notwendig es ist, Bilder von mir zu posten. Das Internet vergisst nichts. Ich möchte nicht, dass die ganze Welt über mich alles weiß, weil es sich negativ auf mich, meine Familie und Freunde auswirken kann.
4	Eine unbekannte Person ruft dich an und stellt sich als O2-Mitarbeiter vor. Diese fordert dich auf, dein Passwort für ein neues Update zu nennen. Wie verhältst du dich? Benenne mind. 3 Schritte und begründe diese.	Ich gebe mein Passwort nicht bekannt und kontaktiere meine Eltern und den Kundenservice meines Telefonie-Anbieters.
5	Worauf musst du besonders achten, wenn du Bilder oder Videos in einem Soz. Netzwerk hochlädst? Benenne mind. 3 Punkte und begründe diese.	Private Fotos sollten nur auf privaten Profilen erscheinen. Man sollte nur Fotos posten zu denen man wirklich steht. Ich achte darauf, was Bilder über mich verraten. Ich Frage abgebildete Personen auf dem Foto um die Erlaubnis es zu posten. Ich versuche, peinliche Fotos sofort aus dem Internet zu löschen. Fotos, die jemand anderes gemacht hat, darf ich nicht einfach hochladen.

6	Worauf musst du beim Weiterleiten und Posten von Bildern und Videos achten, die du nicht erstellt hast? Benenne mind. 3 Punkte und begründe diese.	Wahrung der Rechte Dritter. Urheberrechtgesetz beachten. Das Foto/Video gehört demjenigen, der es gemacht hat. Ich muss erst herausbekommen, wer der Fotograf ist und diesen um Erlaubnis fragen. Hochloden ohne Erlaubnis von Fremden Werken, ist strafbar.
7	Worauf musst du achten, wenn du Daten in eine Cloud lädst? Benenne mind. 3 Schritte und begründe diese.	Wenn ich Daten in eine Cloud lade, muss ich: - die Einstellung des Smartphones überprüfen, - sensible Daten verschlüsseln z.B. mit 7-Zip Software, - ein sicheres Passwort (ggf. auch eine Zwei-Faktor-Authentifikation) verwenden, und - auf eine verschlüsselte Übertragung achten.
8	Wo kann man Beschwerden über umstrittene und / oder verbotene Internetangebote anbringen? Benenne mind. 3 Möglichkeiten. Würdest du es nutzen? Begründe.	Eltern informieren. Polizei informieren. Internet-Beschwerdestelle.de
9	Welche Gefahr gibt es bei öffentlichen WLAN-Hotspots? Benenne mind. 3 Punkte. Begründe.	Fehlende Verschlüsselung. Hacker können auf meine Daten zugreifen. Die Sicherheit ist nicht unbedingt gewährleistet, wenn ich die Geschäftsbedingungen zu kostenlosem WLAN akzeptiere. Kriminelle können gefälschte Netze erstellen, um an mein Passwort zu kommen.
10	Was ist das Recht auf informationelle Selbstbestimmung?	Dies ist das Recht, welches das meine persönlichen Daten (Name, Adresse...) vor unerlaubter Verwendung schützt.
11	Warum solltest du sparsam bei Profilinformationen sein? Benenne mind. 3 Punkte. Begründe	Private Dinge verrät man nicht jedem. Private Fotos und Informationen gehören nicht in ein solches Profil. Persönliche Daten sollte man nur an Freude freigeben.
12	Gehe ein Feld vor und würfle erneut, um deinen Zug zu beenden.	
13	Dein Team setzt eine Runde aus.	

Nr.	Fall/Aussage-Karten	Maßnahmenfeld
1	Der Mathelehrer erhält eine Whats-App von einem Schüler, der ihm schreibt: „mein Vater schenkt Ihnen einen 100 Euro-Gutschein, wenn Sie mir eine glatte 2 geben würden “ Was ist bei so einem Vorfall zu tun, wenn ich es mitbekommen sollte? Begründe und nenne mind. 3 Vorgehensweisen.	Schulleitung (Bestechung, Korruption); auch möglich: Eltern, Polizei
2	Ein Schüler aus der 10a beschwert sich bei Instagram schon wieder über eine Lehrerin, aber wie - der Ton ist nicht mehr feierlich, das geht ganz klar unter die Gürtellinie. Würdest du eingreifen bevor es eskaliert? Begründe mit mind. 3 Punkten.	Vertrauenslehrer, Schulleitung (Fehlverhalten in Sozialen Medien); kann zum Mobbing werden; Zivilcourage zeigen und eingreifen.
3	**Gruppenchat** Anton: Sturmfreie Bude am Wochenende Katy: dann wissen wir ja jetzt alle, wo wir Peets B-Day nachfeiern können Karl: Alle zu Anton am Samstag um 8! Das wird der Hammer Sammy: Bin dabei und bringe noch ein paar Freunde mit Levin: hab den Post in den Klassenchat weitergeleitet Begründe was hier falsch gelaufen ist. Was ist in dieser Situation zu machen?	Eltern Private Informationen sollte man nicht preisgeben, es kann sich negativ auswirken und strafrechtlich verfolgt werden.
4	**Klassenchat** Timmy: Hey Leute, echt cool dass morgen erste Stunde ausfällt. Ich mache morgen gleich blau und geh ne Runde chillen am Sportplatz. Der der nicht mitmacht ist Scheiße und wird gleich am Mittwoch in der Schule bloßgestellt!!! Was ist hier zu tun?	Eltern/Lehrende Aufruf zum Regelverstoß/ Gruppenzwang

5	**Instagram-Video-Story** Moritz: Ey Leute muss ich mir Sorgen machen, wenn es nach Verbranntem in der Wohnung riecht? Hab echt ein komischen Gefühl Was würdet ihr in meinem Fall tun? Erläutere deine Vorgehensweise. Begründe.	Notruf 112, Polizei, Brandschutzhelfer (Feueralarm mit Gebäudeevakuierung)
6	**Klassenchat** Mona: Aus der Heizung im Geschichtsraum fließt auf einmal heißes Wasser raus. So heiß, dass man sich verbrennen kann. Muss ich es melden? HELP Benenne deine Vorgehensweise. Begründe.	Hausmeister (Reparaturen im Gebäude)
7	**Tagebuch** Ich bin echt die schlechteste im ganzen Jahrgang und keiner mag mich. Außerdem haben sich meine Eltern getrennt, das zieht mich total runter. Wer könnte mir bloß helfen? Was würdest du tun? Begründe.	Vertrauenslehrende/ Eltern/ Nummer gegen Kummer
8	**Klassenchat** Michi: Habt ihr die Mütze von Tom gesehen? Voll peinlich mit solchen Sachen rumzurennen. Gebt euch nicht mit ihm ab, sonst werdet ihr von dem Kindergarten angesteckt!“ Beschreibe deine Vorgehensweise. Begründe.	Eltern, Schulleitung, ggf. Polizei (Mobbing)
9	**Klassenchat** Nia: hey Leute habt ihr gesehen, dass Lena und Alex ein Paar sind ? Voll krass, dass sie sich mit ihm abgibt. Der stinkt doch immer nach dem Sportunterricht wie ne Sau. Das Stinke-Paar werden sie ab jetzt genannt! Wie reagierst du? Was ist hier zu tun?	Eltern, Schulleitung, ggf. Polizei (Mobbing)

10	**Klassenchat** Lucy: wie peinlich, dass Timo sitzen bleiben muss Maya: Na und, ist doch nicht dein Problem. Lucy: Biste verknallt in ihn oder was? Das wird morgen der Renner in der Schule sein! Was ist hier zu tun? Begründe.	Eltern/ Vertrauenslehrende/ Schulleitung (Mobbing) Zivilcourage zeigen und eingreifen.
11	Zwei Schüler haben ein Fenster in der Umkleide kaputt und sich davon gemacht. Sven hat das ganze heimlich auf seinem Smartphone gefilmt, weiß aber nicht was er jetzt tun soll. Er hat auch Angst als Petze dazustehen. Benenne deine Vorgehensweise. Begründe.	Hausmeister/ Lehrer/ Schulleitung
12	Jungs posten ein Video in einem der Soz. Netzwerke worauf zu sehen ist, wie ein Schüler brutal verhauen wird. Maria weiß nicht was sie tun soll und ob und wem sie es melden soll. Was ist hier zu tun? Begründe.	Polizei 110/ Eltern. Diesen Vorfall diskret melden. Das Opfer kontaktieren und erzählen, dass man es gemeldet hat.
13	Gehe ein Feld vor und würfle erneut, um deinen Zug zu beenden.	

Nr.	Begriffskarten	Begriffe, die man nicht verwenden darf
1	Cybermobbing	Ärgern, Schikanieren, Belästigung; Stalking/ Bullying
2	Hate speech	Hass(rede), Kommentar, Neid, Herabsetzung
3	Smartphone	Telefonieren, Chatten, Spielen, Ladekabel
4	Community	Soziales Netzwerk, Posten, Chatten; Unterhalten
5	Virenscanner	Virus, Krankheit, Checken, Trojaner
6	Suchmaschine	Google, Safari, Internet, Informationen
7	Big Data	Datenhandel, Sammeln, Massendaten, Datenverarbeitung
8	Handyspiel	Spielen, Game, Zocken, Computer
9	Follower	Jemandem folgen, Liken, Abonnement, Influencer
10	Account	Anmelden, Erstellen, Profil, Einstellungen

Storytelling
in der Informationssicherheit

- Spielbar mit 2 Teams, 1-6 Personen pro Team.
- Spieldauer 25-45 Minuten.

Ziel des Lernszenarios

Ziel des Lernszenarios ist es, sich mit grundlegenden Begriffen der Informationssicherheit auseinanderzusetzen und sich in das Thema einzuarbeiten. Beim Lernszenario „Storytelling in der Informationssicherheit“ geht es darum, eine kurze Geschichte zu einem bestimmten Thema der Informationssicherheit zu erfinden und die gewürfelten Symbole in die Geschichte einzubauen. Die Geschichte kann lustig, ernst oder ausgefallen sein. Der Fantasie sind keine Grenzen gesetzt. Wichtig ist, dass alle gewürfelten Symbole eingebunden werden und ihr das Thema trefft.

Warm-up: Formuliert einen Satz, der dieses  Icon enthält.

Bestandteile

	Whiteboards
	Whiteboard-Marker (abwischbar)
	6 verschiedene Würfel mit Icons
	6 Themenkarten je Schwierigkeitsgrad

Vorbereitung und Erläuterung des Lernszenarios

- Vereinbart die Spieldauer, wenn ihr nicht nach der empfohlenen Zeit spielen möchtet.
- Bildet zwei Teams.
- Optional könnt ihr eine moderierende Person wählen, die euch die Hinweise zu den Themen vorliest.
- Die Würfel und die Karten des ausgewählten Schwierigkeitsgrades liegen verdeckt in der Mitte des Tisches.
- Nehmt pro Team 1x Whiteboard-Marker und 1x Mini-Whiteboard.

Wählt den passenden Schwierigkeitsgrad!

 Klassenstufen 6-7	Die 3 Schwierigkeitsgrade beinhalten Begriffe der Informationssicherheit, die auf das entsprechende Alter angepasst sind. Nehmt das gewählte Kartenset heraus und legt es verdeckt auf den Tisch.
 Klassenstufen 8-9	
 Klassenstufen 10-11	

Ablauf

1. Zieht eine Karte pro Team aus dem Stapel. Diese Karte ist euer Thema, zu dem ihr eure Geschichte erfindet.
2. Klärt zuallererst, was ihr unter dem gezogenen Begriff versteht.
3. Im Anschluss lest ihr oder die moderierende Person die dazugehörige Erläuterung aus der Anleitung vor.
4. Würfelt zusammen die 6 Würfel. Die gewürfelten Icons gelten für beide Teams.
5. Die Aufgabe jedes Teams ist es nun, eine Geschichte zum gezogenen Thema zu erfinden und die gewürfelten Symbole in die Geschichte einzubauen.
6. Benutzt das Mini-Whiteboard, um die Geschichte schriftlich festzuhalten.

Ende des Spiels

- Das Spiel endet nach Ablauf der vereinbarten Spieldauer.
- Lest euch die Geschichten gegenseitig vor.
- Diskutiert, ob alle Symbole eingebaut wurden und die Geschichte dem Thema entspricht.
- Für das getroffene Thema und jedes richtig eingebaute Icon gibt es jeweils einen Punkt. Im Zweifel entscheidet die moderierende Person.
- Ihr könnt eure Geschichte abfotografieren und später eurer Klasse präsentieren.

Lösungsmuster - Schwierigkeitsgrad 1

Nr.	Thema	Hinweis
1	Sicheres Passwort	Je länger und komplexer das Passwort ist, desto sicherer ist es. z.B. Sicher: Wx98,b´f§-al‘276(gK Unsicher: 123456
2	Personenbezogene Daten	Personenbezogene Daten sind Informationen, mit denen man eine Person direkt oder indirekt identifizieren kann. Dazu gehören zum Beispiel: ▪ allgemeine Personendaten (Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer), ▪ physische Merkmale (Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergröße usw.), ▪ Kennnummern wie Personalausweisnummern, ▪ Bankdaten wie Kontonummern, ▪ Online-Daten wie IP-Adresse und Standortdaten ▪ Besitzmerkmale wie Kfz-Kennzeichen.

3	Schadsoftware	Schadsoftware (auch Malware genannt) sind Computer-programme, die entwickelt wurden, um schädliche Funktionen auf deinem Endgerät auszuführen. Dazu gehören zum Beispiel Viren, Würmer oder Trojaner.
4	Shoulder Surfing	Shoulder Surfing lässt sich aus dem Englischen mit “Über die Schulter schauen” übersetzen. Diese Technik dient dem Ausspähen von Passwörtern, PINs (persönlichen Identifikationsnummern) oder anderen Informationen.
5	Schutzmaßnahmen	Schutzmaßnahmen sind alle Maßnahmen, die dem Schutz von etwas Bestimmten dienen. Eine Schutzmaß-nahme gegen Schadsoftware kann zum Beispiel der Einsatz eines Virenscanners sein.
6	Videoüberwachung	Die Videoüberwachung dient der Beobachtung eines Ortes, eines Objektes, oder einer Person. Ob eine Videoüberwachung in Deutschland zulässig bzw. notwendig ist, ist von verschiedensten Faktoren abhängig.

Lösungsmuster - Schwierigkeitsgrad 2

Nr.	Thema	Hinweis
1	Zutrittskontrolle	Eine Zutrittskontrolle regelt, wer wann wo hinein darf. Dabei wird die Berechtigung einer Person geprüft und der Zutritt von unbefugten Personen verhindert.
2	Datensparsamkeit	Datensparsamkeit ist ein Grundsatz des Datenschutzes. Dabei sollen personenbezogene Daten nur sparsam erhoben werden. Dies bedeutet, dass zum Beispiel ein Onlineshop nur Daten von dir erheben darf, die für die Bestellung unbedingt erforderlich sind. Du selbst kannst jedoch von dir aus sparsam mit deinen Daten umgehen, z.B. indem du immer nur die Pflichtfelder in Onlineformularen füllst.
3	Recovery	Recovery steht für die Wiederherstellung von Originaldaten aus einer Sicherungskopie (Backup).
4	Backup	Ein Backup ist eine Sicherungskopie, mit deren Hilfe man Daten, z.B. im Falle eines Systemausfalls, wieder herstellen kann. Von für dich wichtigen Daten solltest du regelmäßig ein Backup machen.
5	Phishing	Phishing nennt man den Versuch, über gefälschte E-Mails, Webseiten oder Kurznachrichten an z.B. Pass-wörter zu gelangen.
6	Social Engineering	Social Engineering ist die Beeinflussung bzw. Manipulation von Personen, mit dem Ziel, zum Beispiel an geheime Informationen zu gelangen.

Lösungsmuster - Schwierigkeitsgrad 3

Nr.	Thema	Hinweis
1	Datenschutzerklärung	Eine Datenschutzerklärung beschreibt, wie deine Daten von einer Organisation verarbeitet werden. Das heißt sie gibt an, wo, wie und zu welchem Zweck deine Daten gesammelt werden und ob sie an Dritte weitergegeben werden.
2	Sensible Daten	Sensible Daten sind personenbezogene Daten, welche die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, Gesundheitsdaten, oder Daten über das Sexualleben oder die sexuelle Orientierung eines Menschen offenbaren.
3	Cloud Computing	Cloud Computing ist ein Sammelbegriff für die Speicherung und Verarbeitung von Daten auf angemieteten Servern. Es erlaubt dir jederzeit und überall, bequem über das Internet auf die dort gespeicherten Daten zu gelangen. Die Datenschutzerklärungen des jeweiligen Anbieters sollten dabei aufmerksam gelesen werden. Wusstest du, dass Google als Cloudanbieter alle E-Mails vollautomatisch durchsucht und analysiert?
4	Data Leak	Ein Data Leak ist eine Datenpanne. Es stellt einen Verstoß gegen die Datensicherheit und den Datenschutz dar, bei dem z.B. Betriebsgeheimnisse an Unberechtigte weitergegeben wurden. Es spielt keine Rolle, ob die Daten in analoger oder elektronischer Form vorliegen.

5	Verschlüsselung	Verschlüsselung ist eine Methode, um Informationen, Daten, Passwörter u. ä. zu codieren, damit Unberech-tigte keinen Zugang dazu finden. Auch Nachrichten können verschlüsselt versendet werden.
6	Spoofing	„Spoofing“ bedeutet so viel wie „fälschen“, „täuschen“, hereinlegen“. Es werden z.B. E-Mail-Adressen, Anruferanzeigen oder URL verfälscht, um eine vertrauenswürdige Identität vorzutäuschen, mit der Absicht z.B. an Passwörter zu gelangen.

Storytelling
in der Informationssicherheit (Digital)

- Spielbar einzeln oder im Team bis zu 3 Personen.
- Spieldauer 20-45 Minuten.

Eignung

Die digitale Variante von „Storytelling“ ist mit dem analogen Lernszenario übereinstimmend. Dieses Lernszenario eignet sich gut zur Vertiefung und Wiederholung von grundlegenden Begriffen der Informationssicherheit. Das digitale Lernszenario fördert das selbstständige Lernen einzeln und im Team. Gespielt kann entweder gemeinsam in der Schule (z.B. im Computerraum), unterwegs mit Smartphone / Tablet oder von zu Hause. Die digitale Variante von „Storytelling in der Informationssicherheit“ ist klassenstufenübergreifend und kann altersunabhängig gespielt werden. Dieses Lernszenario ist nicht auf das Thema Informationssicherheit beschränkt und kann für beliebige Themen adaptiert werden. Im Projekt SecAware4school stehen die Themen rund um den Schwerpunkt Informationssicherheit im Mittelpunkt. Daran ist diese Anleitung ausgerichtet.

Ziel des Lernszenarios

Beim Lernszenario „Storytelling in der Informationssicherheit“ geht es darum, eine kurze Geschichte zu einem bestimmten Thema der Informationssicherheit zu erfinden und die gewürfelten Symbole in die Geschichte einzubauen. Die Geschichte kann lustig, ernst oder ausgefallen sein. Der Fantasie sind keine Grenzen gesetzt, doch sollten die Begriffe zu dem gewählten Thema korrekt in die Geschichte eingebaut werden. Durch das Erzählen von kleinen Geschichten verbessert sich die Merkfähigkeit zu den verschiedenen Begriffen. Den Effekt nennt man „Mnemonik“ (=Gedächtnisstütze). Um das Lernziel nicht zu verfehlen, ist es wichtig, auch alle vorgegebenen Symbole in die Geschichte einzubinden. Die Interpretation der Symbole ist den Spielenden überlassen und soll wiederum die Fantasie anregen.

Benötigte Materialien

	Computer, Tablet oder Smartphone
	Beiliegender USB-Stick mit digitalen Lernszenarien
	Internetverbindung für die Online Version: https://szenarien.wildau.biz/storytelling/storytelling.html

Vorbereitung und Erläuterung des Lernszenarios

- Vereinbart die Spieldauer, wenn ihr nicht nach der empfohlenen Zeit spielen möchtet.
- Lest die Anleitung durch und klickt danach auf „OK, verstanden“.
- Wählt ein Thema aus der Liste oder denkt euch selbst eines aus.
- Das Lernszenario ist schwierigkeitsgradunabhängig und kann klassenstufenübergreifend gespielt werden.

Ablauf

1. Klickt auf den „Würfel“, um Symbole zu würfeln.
2. Tippt eure Sätze, die Geschichte zu einzelnen Würfelsymbolen, in das dafür vorgesehene Feld ein.

Beispiel 

Nika ist Hobby-Fotografin (Kamera). Einmal kam sie auf die Idee (Glühbirne), auf das Dach zu klettern (Pfeil), um ihren Hof von oben für eine Streetmap zu fotografieren. Plötzlich kam Gewitter auf, es donnerte (Blitz). Vor Schreck ließ Nika ihre Kamera vom Dach herunterfallen. Die Kamera war nicht mehr zu reparieren und all ihre Daten auf der Kamera gingen verloren. Glücklicherweise (Würfel) hatte Nika all ihre Daten bereits vorher auf einer externen Festplatte gespeichert. Nika hat eine Sphynx-Katze (Alien-Symbol). Diese kippte ein auf dem Tisch stehendes Glas mit Wasser um, sodass ihre Festplatte auch kaputt ging. Was soll Nika nun tun (fragendes Emoji)? Auf der Festplatte waren Fotos der letzten drei Jahre gespeichert.

Ende des Spiels

- Das Spiel endet nach Ablauf der vereinbarten Spieldauer.
- Lest euch die Geschichten gegenseitig vor.
- Diskutiert, ob alle Symbole eingebaut wurden und die Geschichte dem Thema entspricht.
- Ihr könnt eure Geschichte abfotografieren und später eurer Klasse präsentieren.

Da digitale Lernszenarien modifizierbar sind, ist die Auswahl an möglichen Themen variierbar. Dies hängt von der Aktualität der Themen ab, zumal die vorgegebenen Themen als Denkanstoß dienen und zum Erfinden eigener passender Ideen anregen sollen.

Fake or real

Fake News erkennen

- Spielbar ab 2 Personen. Mindestens 1 bis 10 Personen im Team, plus eine moderierende Person.
- Spieldauer 20-30 Minuten.

Ziel des Lernszenarios

Beim Lernszenario „Fake or real“ geht es um eigene Reflektion bei der Informationsaufnahme. Mit diesem Lernszenario wird demonstriert, dass innerhalb der Medien Fehlinformation existieren und diese in mehrfacher Hinsicht ein Risiko für Schülerinnen und Schüler darstellen. Ziel des Lernszenarios ist es, Falsch-meldungen auf den Karten zu erkennen und sich bewusst über deren Eigenschaften zu werden.

Bestandteile

	16 Karten mit Meldungen (pro Schwierigkeitsgrad)
	1 rote Filzdecke, 1 grüne Filzdecke
	Die „Goldene Regel“-Karte
	Definitionskarte

Vorbereitung und Erläuterung des Lernszenarios

- Vereinbart die Spieldauer, wenn ihr nicht nach der empfohlenen Zeit spielen möchtet.
- Bestimmt eine Moderatorin/ einen Moderator. Diese Person ist für die Durchführung dieses Lernszenarios und die Auflösung verantwortlich, hat die Lösungen und Anleitung zur Hand, kontrolliert die Spielzeit und spielt nicht im Team mit.
- Die Karten in dem ausgewählten Schwierigkeitsgrad liegen verdeckt in der Mitte des Tisches.
- Die rote und grüne Filzdecke liegen nebeneinander auf dem Tisch.
- Die Teilnehmenden verteilen sich um den Tisch herum.
- Die moderierende Person macht nun die Einführung und gibt wichtige Informationen. Der Moderationstext ist dabei zu beachten.
- Die Spielmechanik basiert auf dem Zuordnungsprinzip und soll zu regen Diskussionen bei den Teilnehmenden führen.

Wählt den passenden Schwierigkeitsgrad!

 Klassenstufen 6-7	Der 1. Schwierigkeitsgrad ist durch präzise Auswahl der inhaltlichen Themen an die jüngeren Klassenstu-fen abgestimmt. Die Ausdruckweise und Sprache wurden entsprechend angepasst.
 Klassenstufen 8-9	Den 2. Schwierigkeitsgrad zeichnet die Komplexität der gewählten Meldungen im Internet aus sowie die Aktualität dieser Meldungen in den Medien.
 Klassenstufen 10-11	Der gegebene Inhalt und die Komplexität beim 3. Schwierigkeitsgrad spiegeln die aktuellen Medienthemen wider und lassen sich effektiv in die Austausch- und Diskussionsrunden einbinden.

Moderationstext

Einführung (5-7 Minuten)

„In diesem Lernszenario geht es um das Erkennen von Fake News. Daher würde ich gerne von euch wissen:“

„Wisst ihr, worum es sich bei Desinformationen handelt? Welche anderen Bezeichnungen kennt ihr?“

Die Teilnehmenden sollen zunächst sammeln und diskutieren. Danach gibt die moderierende Person die „Definitionskarte“ an die Teilnehmenden und fasst zusammen.

Definitionskarte

	Desinformation ist die gezielte Verbreitung falscher oder irreführender Informationen.
	Fake News entstehen infolge von „schlechtem“ Journalismus, Parodie (Aprilscherz, Hoax, s. Fragen), Provokation, Leidenschaft, Parteilichkeit, Profitgier oder wirtschaftlichen bzw. politischen Einflusses bzw. Propaganda.
	Die meisten Schöpfer und Verbreiter von Fake News verfolgen politische oder wirtschaftliche Ziele. Sie haben erkannt, dass sich Themen, die sehr emotional diskutiert werden, besonders gut dafür eignen, (öffentliche) Stimmung zu erzeugen, die sie zu ihren Zwecken manipulieren wollen.
	Fake News sind auch ein Risiko für Schulen, öffentliche Einrichtungen, Regierungen oder sogar Unternehmen, da u. a. durch gefälschte Pressemitteilungen oder inszenierte Shit Stormsz. B. innerhalb der Medien das Ansehen beschädigt werden kann.
	Aufgrund dieses hohen Einfluss-Potenzials von Desinformation ist es für uns alle wichtig, *News* zu überprüfen und zu verifizieren und Fake News zu erkennen, indem wir z. B. Hinweisen kritisch nachgehen.

Die „Goldenen Regeln Karte“ sollte erst nach der ersten Runde diskutiert werden.

Erklärung der Aufgabe und Spielablauf (5 Minuten)

1. *„Eure Aufgabe ist es zu entscheiden, welche Meldungen wahre Nachrichten sind und welche die falschen. Ich lese die Überschrift sowie auffällige Auszüge der jeweiligen Meldung laut vor (max. 15-20 Sekunden pro Karte) und lege diese in die Mitte zwischen den beiden Filzdecken hin.*
2. *Dann zähle ich 3,2,1 und ihr müsst euch an die Seite der roten Filzdecke (für Fake News) oder der grünen Filzdecke (für reale Meldung) stellen.*
3. *Je nach Mehrheitsmeinung unter euch lege ich die jeweilige Karte auf der roten oder grünen Decke ab und lese die nächsten Meldungen vor, bis alle Karten zugeordnet sind.*
4. *Das Team kann (z.B. bei unterschiedlichen Meinungen) die Karte schieben.*
5. *Für die Zuordnung aller Karten gibt es ca. 4 Minuten Zeit, erst danach wird die Auswertung vorgenommen.“*

Auflösung und Punktevergabe (10 - 15 Minuten)

1. Die Teilnehmenden bekommen nun „Die goldenen Regeln“ auf einem A4-Blatt an die Hand.
2. Anhand der „Die goldenen Regeln“ sollen die Teilnehmenden ihre Zuordnung begründen und ggf. korrigieren.
3. Die moderierende Person wertet die zugeordneten Karten aus. Für jede richtig erratene Karte gibt es einen Punkt. Wenn alle 16 Karten noch vor Ablauf der Zeit und Herausgabe der „Goldenen Regel-Karte“ richtig erraten wurden, erhält das Team zusätzlich 5 Bonuspunkte.

Ende des Spiels

Das Spiel ist zu Ende, wenn einer der beiden Punkte zutrifft:

A. Alle Karten wurden zugeordnet, ausgewertet und die Zusatzinformationen besprochen.

B. Die vorher festgelegte Zeit ist abgelaufen.

Die goldenen Regeln

Hinweis	Bemerkung	Prüfungsstrategie
Überschriften	Insbesondere reißerische Headlines (formal auch mit Großbuchstaben, Ausrufezeichen etc.) sind unseriös.	Kopiere die Überschrift, setze diese in Anführungszeichen bei einer Suchmaschine ein. Wenn die Überschrift keine „seriösen“ Treffer erzielt, ist sie vermutlich manipuliert.
URLs	Unrechte (z. B. mit minimalen Abweichungen) oder nachahmende URL (z. B. von bekannten Nachrichtenquellen) überprüfen.	Gebe den Anbieter der Nachricht direkt über eine Suchmaschine ein und vergleiche das Ergebnis mit der URL.
Quellen	Überprüfe den Ruf bzw. das Image der Quelle. Ist diese bekannt für glaubwürdige Organisationen oder Personen?	Wirkt das Impressum seriös? Gibt es andere Quellen, die Zitate oder Informationen bestätigen? Um die Webseite zu prüfen, kann man bei einer Suchmaschine die URL eingeben und “site:“ davorsetzen, damit die Suchmaschine sämtliche Beiträge anzeigt, die auf der Webseite veröffentlicht wurden. Sind diese sehr einseitig, handelt es sich vermutlich nicht um eine objektive Quelle. Gibt man die URL in Anführungszeichen ein, erhält man Treffer, bei denen ÜBER diese Webseite von anderen Seiten berichtet wird.
Qualität von Sprache bzw. visuelles Erscheinungsbild		Überprüfe seltsame Formatierungen bzw. Layouts, Rechtschreib-, Tipp- oder Übersetzungsfehler.
Datumsangaben		Ist die Logik der Chronologie nachvollziehbar?
Fußnoten bzw. Verweise		Mangelnde oder falsche Verweise sind ein Hinweis auf Falschmeldungen.

Alternative Berichte	Bei Veröffentlichung von mehreren vertrauenswürdigen Quellen steigt die Wahrscheinlichkeit die Wahrheit.	
Ironie		Überprüfe die Tonalität auf Parodien bzw. Scherze.
Potenzielle Vorteile		Du solltest dich stets fragen, welche Vorteile Falschmeldung dem Absender bringen könnten.
Vorsicht auch bei Bildern	Falschmeldungen enthalten häufig manipulierte bzw. zweckentfremdete Abbildungen (z. B. generische Stockfotos, die jeder herunterunterladen kann, oder Portraits gestohlener Identitäten) und Videos.	Visuelle Inhalte kannst du mithilfe von Bildsuchmaschinen (z. B. TinEye) verifizieren, um die Quelle zu überprüfen. Im Zweifel kannst du eine Bildquelle per Rückwärtssuche mithilfe von Suchmaschinen zurückverfolgen. Hierzu lädst du das verdächtige Bild hoch oder ziehst es direkt in die Suchleiste. Dadurch wird Bild und Name der Datei analysiert und es werden Webseiten angezeigt, auf denen dieses oder ähnliche Bilder zu finden sind. Vorsicht ist auch bei Videos geboten. Achte bei YouTube vor allem auf das Upload-Datum, Informati-onen zum Absender und Kommentare.

Lösungsmuster

Schwierigkeitsgrad	Fake	Real
	1, 3, 5, 6, 7, 8, 9, 10, 11, 16	2, 4, 12, 13, 14, 15
	1, 3, 6, 8, 10, 11, 12, 13, 14, 16	2, 4, 5, 7, 9, 15
	2, 4, 6, 7, 8, 9, 10, 11, 15, 16	1, 3, 5, 12, 13, 14

Nachbereitung

Um das Wissen über die Fake News zu festigen, können folgende Fragen von der moderierenden Person an die Teilnehmenden gestellt und diskutiert werden. Nach dem Lernszenario ist es von Vorteil, die Tipps am Ende dieser Anleitung an die Beteiligten weiterzugeben.

1. **Um die Ecke gedacht: Fake News als Farbe (oder Tier, Film, Musikstück bzw. Kinofilm)** - was wäre das? Sammelt und diskutiert eure Antworten im Team.
2. **Wie verhält sich jeder Einzelne von uns, wenn man eine „starke", zum Teil unglaublich klingende Nachricht liest?** Wann verbreiten wir etwas weiter, wann nicht? An wen und warum? Sammelt und diskutiert eure Antworten im Team.
3. **Wo kann man unseriöse Inhalte melden?** Gewaltvideos: Informiere deine Eltern bzw. Lehrer. Diese sollten die Beiträge direkt an den Betreiber der Website melden oder sich bei Verdacht auf Straftaten mit Screenshots an externe Beschwerdestellen wie https://www.internet-beschwerdestelle.de/ oder die Polizei wenden. Hass im Netz: Du findest hierzu unter hass-im-netz.info oder unter https://no-hate-speech.de/ Informationen.
4. **Welche Online-Werkzeuge helfen beim Entlarven von Fake News?** https://www.mimikama.at/ klärt über Falschmeldungen auf. https://www.schau-hin.info/ ist ein Portal für Kinder und Jugendliche über Falschmeldungen.

Zusatzfragen

1. Was sind Social Bots? Habe ich ggf. schon einmal Erfahrung mit Social Bots gemacht und wenn ja, welche?

In Social Media werden Social Bots eingesetzt, um automatische Antworten zu generieren. Bei Twitter lassen sich Social Bots installieren, die auf spezifische Hashtags reagieren und dann vorher programmierte Informationen absetzen. Dazu werden realistisch wirkende Accounts mit Profilbild, Posts und Followern geschaffen, die selbst auch anderen Nutzern folgen. Sie werden in der Regel eingesetzt, um Werbung zu verbreiten oder Mehrheiten vorzutäuschen, z. B. um politische Propaganda im Sinne ihrer Auftraggeber zu verbreiten.

2. Kann jemand die Abgrenzungen zwischen Fake News, False News, alternativen Fakten bzw. Hoax, Ente, Aprilscherz oder Urban Legend erklären?

Als Hoax (engl. für Jux, Scherz, Schabernack; auch Schwindel) wird meist eine Falschmeldung bezeichnet, die in Printmedien (Büchern, Zeitschriften oder Zeitungen) oder digital (per E-Mail, Messenger, SMS, MMS bzw. über soziale Netzwerke) verbreitet, von vielen Empfängern für wahr gehalten und daher an das eigene Umfeld weitergegeben wird. Es wurde erstmals 1796 verwendet und leitet sich vermutlich von der Bezeichnung Hocus (Pocus) ab.

Die Ente bzw. Zeitungsente stammt vermutlich aus dem Französischen (‚donner des canards' = ‚Enten geben'/ "lügen" oder ‚vendre des canards à moitié'= ‚Enten zur Hälfte verkaufen'/ ‚nicht die ganze Wahrheit sagen').

Während ein Hoax eben auch über die (virale) Weiterverbreitung via Medien definiert ist, handelt es sich bei **Urban Legends** um Großstadtlegenden in Nachfolge sogenannter Ammen- und Schauermärchen, mithin skurrile Anekdoten, die überwiegend mündlich übermittelt wurden (heute aber durch eine zusätzliche digitale Verbreitung in Abgrenzung zum Hoax verschwimmen).

Fake News sind manipulativ verbreitete, vorgetäuschte Nachrichten oder Falschmeldungen, auch als politisches Schlagwort und Kampfbegriff genutzt, die sich überwiegend online, z. T. viral verbreiten und dabei manchmal auch von Journalisten aufgegriffen werden. Die Bezeichnung ist nicht neu und geht mindestens auf das Jahr 1890 zurück.

False News ist u. a. eine Prägung der Bostoner Hochschule MIT, die in einer Desinformationsstudie praktisch als Synonym für Fake News genutzt wird, um angeblich den menschlichen Anteil daran stärker herauszustellen.

Bei alternativen Fakten handelt es sich um eine Formulierung von Kellyanne Conways, der Beraterin des US-Präsidenten Donald Trump im Januar 2017. Sie nutzte die Bezeichnung in der amerikanischen Polit-Talksendung Meet the Press, um falsche Aussagen des Pressesprechers des Weißen Hauses Sean Spicer bezüglich der Größe des Publikums während der Amtseinführung von Trump in Washington zu rechtfertigen.

3. **Welche seriösen Webseiten kann man vor allem Kindern anbieten, die sich (geschützt vor Fake News auf Basis von geprüften Inhalten) informieren wollen?**

   Vor allem Medien mit moderierten und verständlichen Inhalten. Weiterführende Links sind unter „Weiterführende Informationen und Materialien“ zu finden.

Fake News

Mit Fake News richtig umgehen

- Spielbar in Gruppen oder zu zweit.
- Spieldauer 25-45 Minuten.

Fake ist der moderne Ausdruck für eine Information, die von allgemein bekannten Tatsachen ablenken und diese im Extremfall verfälschen soll. Diese Art der Informationsverbreitung ist so alt wie die Menschheit. Oft wurden Bilder und Nachrichten nachträglich verfälscht. Heute versucht man, unter Einsatz moderner Medien Wahlen zu beeinflussen bzw. Unsicherheit und/oder Stimmungen zu erzeugen.

Ziel des Lernszenarios

Das Ziel des Lernszenarios ist das Finden und Herstellen der Zusammenhänge zwischen den Fällen, die ein konkretes Ereignis beschreiben. In Gruppendiskussion muss eine Übereinstimmung gefunden werden, die die logische Zusammengehörigkeit von Werkzeug-, Begriffs- und Strategiekarten zum betrachteten Fall sinnvoll erscheinen lässt.

Begriffe, die neu oder unbekannt sind, können im beiliegenden Wiki nachgeschlagen werden. Dort findet ihr auch weiterführende Informationen.

Einstiegsfragen

„Kennt ihr den Begriff Zeitungsente?“

„Von welchen Fake News habt ihr schon gehört? Wie wurde der Fall öffentlich und entlarvt?“

Bestandteile

	Spielfeld mit Fällen
	8 Werkzeugkarten (orange) 10 Begriffskarten (blau) 8 Strategiekarten (grün)
	Wiki

Wählt den passenden Schwierigkeitsgrad!

 Klassenstufen 6-7	Der Schwierigkeitsgrad ist für die Klassenstufen 6-8 geeignet. **Achtung:** Fälle mit Nummern **102**, **108** und **111** werden in diesem Schwierigkeitsgrad **nicht berücksichtigt**, genau wie die Karte mit der Nummer **406**.
 Klassenstufen 8-11	Die Schwierigkeitsgrad 2 und 3 sind hier vereint. Diese setzen Grundwissen über Fake News voraus und beinhalten komplexere Themen.

Vorbereitung und Erläuterung des Lernszenarios

- Vereinbart die Spieldauer, wenn ihr nicht nach der empfohlenen Zeit spielen möchtet.
- Bildet zwei Gruppen (A und B), die gegeneinander spielen.
- Sortiert alle Karten nach Farben und legt die vier Stapel (Fallkarten, Werkzeugkarten, Begriffskarten, Strategiekarten) neben das Spielfeld, welches auf dem Tisch für alle gut sichtbar platziert wird.
- Sortiert ggf. die Karten aus, die nicht für Schwierigkeitsgrad 1 geeignet sind.

Erklärung der Kategorien

Plakat mit Fällen	Alle Fälle sind gefälschte Meldungen, also Fake News. Um diese erkennen zu können, müssen die Begriffe bekannt sein, Werkzeuge zum Aufdecken eingesetzt werden und die Weiterverbreitung durch geeignete Strategien unterbunden werden.
Begriffskarte	Begriffskarten enthalten andere Bezeichnungen für Fälschungen aller Art, z.B. ist Hoax ein anderer Begriff für einen Fake.
Werkzeugkarte	Werkzeuge werden benötigt, um Fake News aufzudecken, z.B. die Überprüfung von Wetter- und Zeitangaben.
Strategiekarte	Mit den Strategiekarten werden Möglichkeiten gezeigt, die verhindern, selbst Fake News und andere Unwahrheiten zu verbreiten.

Ablauf

1. Team A zieht eine Fallkarte und liest diese vor. Legt diese Fallkarte auf das Spielfeld. Dieser Fall ist zu lösen!
2. Um diesen Fall zu lösen, braucht ihr Begriff/Werkzeug und/oder Strategie. Sucht dazu aus anderen Stapeln die passende(n) Karten heraus.

   Hinweis: Nicht jedem Fall sind exakt drei Karten zuzuordnen! Mehrfach- und Alternativzuordnungen sind möglich. Ist ein Begriff oder Sachverhalt nicht bekannt, kann dieser im beiliegenden Wiki nachgeschlagen werden.
3. Die ausgewählten Karten zum Fall werden auf dem Spielfeld in den dazugehörigen Fällen abgelegt.
4. Team B ist an der Reihe.
5. Am Ende wird die Ablage mit der Musterlösung verglichen. Für jede Übereinstimmung gibt es einen Punkt. Gewonnen hat das Team mit den meisten Punkten.

Ende des Spiels

Das Spiel ist zu Ende, wenn einer der Punkte zutrifft:

A. Allen Fällen wurde eine oder mehrere Begriffs-/Werkzeug-/Strategiekarte(n) zugeordnet.

B. Alle Karten wurden zugeordnet, ausgewertet und die Zusatzinformationen besprochen.

C. Die vorher festgelegte Zeit ist abgelaufen.

LösungsmusterLösungsmuster

Fall Nr.	Passendes Werkzeug	Passender Begriff	Passende Strategie
101	207	305	
102	201, 202	304, 310	402
103	204, 205, 207, 208	303	405
104	203	302	403
105	204, 208	301, 309	403, 408
106	203	308	408
107	206	307, 309	404
108	201, 202	306, 309	404, 405, 406
109		301, 307	403
110		307	401, 404, 407
111	204, 207, 208		
112		301, 308	401, 403, 406, 407, 408

Achtung: die Musterlösung dient der Aufklärung, schließt aber andere mögliche Zuordnung nicht aus, wenn diese nachvollziehbar begründet werden.

Security Duell

Informationssicherheit im Unternehmen

- Spielbar mit 2 Teams. Mindestens eine Person pro Team plus eine moderierende Person.
- Spieldauer 25-45 Minuten.

Ziel des Lernszenarios

Das Lernszenario „Security Duell – Informationssicherheit im Unternehmen“ bietet die Möglichkeit, potenzielle Angriffspunkte in einem Unternehmen zu erkennen und passende Schutzmaßnahmen zu finden.

Das Ziel des Lernszenarios ist es, sich mit den möglichen Sicherheitsobjekten vertraut zu machen, die Schwachstellen zu finden und zu erkennen, mit welchen Mitteln man angreifen und gleichzeitig Schutzmaßnahmen präventiv treffen kann. Pro Spielzug wechseln sich Angreifer- und Verteidiger-Team ab. Bei der Angriffs-Aktion muss das Team versuchen, Schwachstellen des Unternehmens zu finden, um diese auszunutzen. Bei der Verteidigungs-Aktion muss das Team das Unternehmen, so gut es geht, schützen. Bei diesem Duell der Unternehmen müsst ihr so viele erfolgreiche Aktionen wie möglich durchführen.

Einstiegsfragen

„Was denkt ihr, was unter Informationssicherheit zu verstehen ist?“

„Was denkt ihr, welche Sicherheitsobjekte es in einem Unternehmen gibt?“

> Objekte in Unternehmen, wie Kundendatenbank, Serverraum, Buchhaltung, Homepage, Netzwerk etc., müssen permanent sicherheitstechnisch als auch organisatorisch geschützt werden. Sicherheitskonzepte mit verschiedenen Maßnahmen müssen eingeführt werden, um mögliche Risiken und Angriffe umgehen zu können.

Bestandteile

	Spielfeld
	29 Karten „Verteidigung“
	29 Karten „Angriff“
	20 Pins blau, 20 Pins gelb
	12 Wiki-Chips, Würfel
	Wiki

Vorbereitung und Erläuterung des Lernszenarios

- Vereinbart die Spieldauer, wenn ihr nicht nach der empfohlenen Zeit spielen möchtet.
- Bestimmt eine Moderatorin/ einen Moderator. Diese Person ist für die Auflösung verantwortlich und spielt nicht im Team mit.
- Bildet zwei Teams.
- Das Spielfeld und der Würfel liegen in der Mitte des Tisches.
- Die Karten liegen nach Kategorien geordnet und verdeckt auf dem Tisch.
- Würfelt nacheinander. Das Team mit der höchsten gewürfelten Zahl beginnt - spielt als Team A und wählt die Pin-Farbe aus.

Wählt den passenden Schwierigkeitsgrad!

 Klassenstufen 6-7	Der 1. Schwierigkeitsgrad ermöglicht die unbegrenzte Nutzung des Wikis. Wiki ist ein Wörterbuch dieses Lernszenarios, welches als Extraheft aufgeführt ist. Wenn ihr einen Begriff nicht wissen solltet, dann könnt ihr euch jederzeit schlau machen und im Wiki nachschlagen.
 Klassenstufen 8-9	Beim 2. Schwierigkeitsgrad nehmt 6 Wiki-Chips pro Team. Diese Chips dienen dazu, um Informationen zu kaufen. Das bedeutet, wenn ihr einen Begriff nicht kennt, könnt ihr gegen Abgabe der Chips im Wiki nachschlagen. Wiki ist ein Wörterbuch dieses Lernszenarios und gibt euch die benötigten Infos. Achtung: Pro Wiki-Chip dürft ihr nur 1 x im Wiki nachschlagen! Wiki findet ihr als Extraheft.
 Klassenstufen 10-11	Beim 3. Schwierigkeitsgrad nehmt nur 3 Wiki-Chips pro Team. Diese Chips dienen dazu, Informationen zu kaufen. Das bedeutet, wenn ihr einen Begriff nicht kennt, könnt ihr gegen Abgabe der Chips im Wiki nachschlagen. Wiki ist ein Wörterbuch dieses Lernszenarios und gibt euch die benötigten Infos. Achtung: Pro Wiki-Chip dürft ihr nur 1 x im Wiki nachschlagen! Wiki findet ihr als Extraheft.

Ablauf eines Spielzuges

Ein Spielzug besteht immer aus einer Angriffs-Verteidigungs-Aktion. Je nach Schwierigkeitsgrad habt ihr die Möglichkeit, unbekannte Begriffe im Wiki nachzuschlagen. Hinweis: Die angegebenen Nummern auf den Karten verweisen auf die Erklärungen im Wiki. Die Nummern auf dem Spielfeld bedeuten Punkte, die man für die jeweiligen Bereich erreichen kann.

Angriff 

1. Team A, nehmt aus dem Angriffs-Stapel 2 Karten.
2. Überlegt, welchen Bereich im Unternehmen ihr angreifen möchtet.
3. Welche Karte könnte passen?
4. Legt nun die Karte aufgedeckt auf das gewählte Feld.
5. Begründet euren Angriff.

Verteidigung 

6. Team B, nehmt aus dem Verteidigungs-Stapel 3 Karten.
7. Überlegt, mit welcher der 3 Karten ihr euch gegen den Angriff schützen könnt.
8. Legt nun die Karte aufgedeckt auf das angegriffene Feld.
9. Begründet eure Verteidigung.

Auflösung

1. Die moderierende Person gibt die Auflösung und vergibt die Punkte.
2. Das Team, welches gewonnen hat, setzt einen Pin in deren Farbe auf das gespielte Feld.
3. Dieses Feld ist nicht mehr spielbar.
4. Vor jedem Zug, egal ob Angriff oder Verteidigung, zieht jedes Team eine Karte, sodass insg. immer 2 Angriffs-Karten und 3 Verteidigungs-Karten auf der Hand des Teams sind.
5. Nach der Angriffs-Verteidigungs-Aktion ist ein Spielzug vorbei. Team B ist mit Angreifen dran und Team A verteidigt sich nun.

Ende des Spiels

Das Spiel ist zu Ende, wenn einer der Punkte zutrifft:

A. Alle Felder sind mit Pins besetzt.

B. Es gibt keine Karten mehr.

C. Die vorher festgelegte Zeit ist abgelaufen.

D. Wenn eins der Teams mindestens 15 Punkte erreicht hat.

Punktevergabe

Ist der **Angriff richtig** gelegt worden und die Verteidigung aber falsch, so wird ein Pin in der Farbe des Teams, welches den Angriff vollzogen hat, auf das Feld gesetzt.

Ist der **Angriff falsch** gelegt worden bzw. passt nicht auf den Bereich, aber die Verteidigung hat richtig auf den Angriff reagiert, so setzt das Team, welches sich gerade verteidigt hat, ein Pin in seiner Farbe auf das Feld.

Sollte der **Angriff und die Verteidigung** falsch gelegt werden, bekommt keiner der Teams Punkte/die Pins werden nicht gesetzt.

> Karten, die falsch gelegt werden, müssen in den Kartenstapel zurückgelegt werden. Karten die ausgespielt werden, werden aussortiert. Am Ende werden die verteilten Pins gezählt. Das Team mit der höchsten Zahl hat gewonnen.

Lösungsmuster

Hinweis: die Sonderkarte „IT-Informationsbeauftragter“ gilt gegen alle Angriffe, auch gegen die Hacker Joker-Karte.

Nr	Angriffskarte	Passende Angriffsbereiche	Passende Schutzkarten
1	Social Engineering face2face	Mitarbeiter, Buchhaltung, Personalabteilung, Vertrieb, Geschäftsführung, Forschungslabor	Schulungsmaßnahme gegen Social Engineering, beschränkte Zugangsberechtigung, beschränkte Informationseinteilung
2	Social Engineering Telefon	Mitarbeiter, Buchhaltung, Personalabteilung, Vertrieb, Geschäftsführung, Forschungslabor	Schulungsmaßnahme gegen Social Engineering, Zwei-Faktor-Authentifizierung, beschränkte Zugangsberechtigung, beschränkte Informationseinteilung
3	DDOS-Angriff	Online-Shop, Homepage	Mirror-Server, Firewall, System Administrator
4	Einbruch	Büro, Serverraum, Cloud	Alarmanlage, Videoüberwachung, Vorort-Security

5	Dumpster Diving	Mitarbeiter, Geschäftsführung	Sicherheitsgrundlagen Schulung, biometrische Authentifizierung, Schredde
6	Phishing	Mitarbeiter, Buchhaltung, Personalabteilung	Schulungsmaßnahme gegen Phishing, beschränkte Zugangsberechtigung, beschränkte Informations-einteilung, Zwei-Faktor-Authentifizierung
7	Spear Phishing	Geschäftsführung, Buchhaltung	Schulungsmaßnahme gegen Spear-Phishing, Zwei-Faktor-Authentifizierung
8	Alarm deaktivieren	Büro, Serverraum, Vertrieb	Videoüberwachung, Vorort-Security, biometrische Authentifizierung
9	Trojanisches Pferd	E-Mail Server, Kundendatenbank, Netzwerk, Arbeitsrechner	Firewall, Antivirus, beschränkte Ports Freigabe, Sicherheitsgrundlagen Schulung, beschränkte Zugangsberechtigung, aktuelles Software-Patch, System Administrator
10	Virus	E-Mail Server, Kundendatenbank, Backup, Server, Arbeitsrechner, Cloud	Antivirus, Sicherheitsgrundlagen, beschränkte Zugangsberechtigung, aktuelles Software-Patch, System Administrator
11	Videoüberwachung deaktivieren	Büro, Serverraum, Vertrieb	Vorort-Security, Biometrische Authentifizierung, Alarmanlage
12	Passwort knacken	Arbeitsrechner	Stärke Passwörter, Sicherheitsgrundlagen Schulung, Zwei-Faktor-Authentifizierung, biometrische Authentifizierung
13	Hardware Sabotage	Arbeitsrechner, Serverraum, Videoüberwachung, Alarmanlage, Vertrieb	Vor-Ort-Security, Mirror Server, Backup Server, System Administrator, Videoüberwachung, Alarmanlage
14	SQL-Injection	Kundendatenbank, E-Mail Server, Online-Shop	Aktuelles Software-Patch, System Administrator

Nr	Angriffskarte	Passende Angriffsbereiche	Passende Schutzkarten
15	Spionage	Mitarbeiter, Buchhaltung, Personalabteilung, Vertrieb, Geschäftsführung, Forschungslabor	beschränkte Zugangsberechtigung, beschränkte Eintrittsberechtigung, Mitarbeiterausweis, Vorort-Security
16	Sniffing	Arbeitsrechner	Antivirus, Sicherheitsgrundlagen Schulung, System Administrator
17	Man in the Middle	Überall, wo digitale Austausch stattfindet	Ende-zu-Ende-Verschlüsselung, Zwei-Faktor-Authentifizierung
18	IP Spoofing	Netzwerk, Online-Shop, Homepage	Schulung gegen Spoofing, Firewall, SSL, System Administrator
19	DNS Spoofing	Netzwerk, Online-Shop, Homepage	Schulung gegen Spoofing, Firewall, SSL, System Administrator
20	Mail Spoofing	Netzwerk, E-Mail Server, Mitarbeiter, Geschäftsführung	Schulung gegen Spoofing, Firewall, System Administrator
21	ID Call Spoofing	Mitarbeiter, Geschäftsführung, Buchhaltung, Personalabteilung	Schulung gegen Spoofing, Schulungsmaßnahme gegen Social Engineering, restriktive Zugangsberechtigung
22	Spyware	Arbeitsrechner	Aktueller Software-Patch, Antivirus, Sicherheitsgrundlagen Schulung, System Administrator
23	Ransomware	Arbeitsrechner	Aktuelles Software-Patch, Antivirus, Sicherheitsgrundlagen Schulung, Backup, System Administrator
24	Korruption	Mitarbeiter, Geschäftsführung	Anti-Korruption-Maßnahmen, Videobeobachtung
25	Shoulder Surfing	Mitarbeiter, Geschäftsführung	Blickschutzfolie, Sicherheitsgrundlagen Schulung, starkes Kennwort

26	Data-Leak	Mitarbeiter, Geschäftsführung, Personalabteilung, Forschungslabor	Sicherheitsgrundlagen Schulung, beschränkte Informationseinteilung
27	Hacker (Joker-Karte)	Kann alle Bereiche angreifen	Eine dem angegriffenen Bereich passende Schutzkarte oder IT-Sicherheitsbeauftragter
28	Exploit	Alle Server	Software-Patch, System Administrator
29	WLAN Hack	WLAN	WPA3, System Administrator, starkes Kennwort

Datenspionage
Sicherer Raum (Digital)

- Spielbar einzeln oder im Team bis zu 3 Personen.
- Spieldauer 5-10 Minuten.

Eignung

Dieses Lernszenario eignet sich gut zur Bewusstmachung möglicher sicherheitsrelevanter Objekte am Arbeitsplatz, die einer besonderen Aufbewahrung bedürfen. Das digitale Lernszenario fördert das selbstständige Lernen einzeln und im Team. Es wird lediglich ein internetfähiges mobiles Endgerät (mit Internetzugang) benötigt. Gespielt werden kann entweder gemeinsam in der Schule (z.B. im Computerraum), unterwegs mit Smartphone / Tablet oder von zu Hause. „Datenspionage – sicherer Raum“ ist klassenstufenübergreifend und kann altersunabhängig gespielt werden.

Ziel des Lernszenarios

Beim Lernszenario „Datenspionage – sicherer Raum“ geht es darum, gegen Datenklau auf verschiedenen Sicherheitsobjekten vorzugehen und diese sachgerecht zu verstauen. Ziel ist es, die Objekte mit sensiblen Informationen zu erkennen und die richtige Art der Aufbewahrung für diese am Arbeitsplatz zu erlernen.

Bestandteile

	Computer, Tablet oder Smartphone
	Beiliegender USB-Stick mit digitalen Lernszenarien
	Internetverbindung für die Online-Version: https://szenarien.wildau.biz/secroom/story.html

Vorbereitung und Erläuterung des Lernszenarios

- Vereinbart die Spieldauer, wenn ihr nicht nach der empfohlenen Zeit spielen möchtet.
- Lest die Anleitung durch.
- Das Lernszenario ist schwierigkeitsgradunabhängig und kann klassenstufenübergreifend gespielt werden.

Ablauf

1. Klickt auf „Start“, um das Spiel zu beginnen. Das „Fragezeichen-Symbol“ gibt weitere Hinweise.
2. In einem Büro sind unterschiedliche Objekte verteilt.
3. Sucht verschiedene Sicherheitsobjekte heraus. Klickt auf die Objekte und wählt aus den möglichen Vorgehensweisen, wie mit dem Objekt umgegangen werden soll.
4. Wenn ihr der Meinung seid, dass alle Sicherheitsobjekte gefunden wurden, verlasst den Raum durch einen Klick auf die „Tür“.

Jedes Objekt hat individuelle Aktionen, jede Aktion hat verschiedene Gewichtspunkte, z.B.

Objekt: Zettel mit Passwort

Anfangszustand: Angehängt an der Pinnwand

Aktionen:

In Papierkorb werfen: -2 Punkte

Schreddern: 2 Punkte

In Schublade verstecken: 1 Punkt

Nichts tun: -1 Punkt

Ende des Spiels

A. Das Spiel endet nach Ablauf der vereinbarten Spieldauer.

B. Das Spiel wird beendet, wenn man sich dazu entscheidet, den Raum zu verlassen.

Lösung:

Alle gefundenen Sicherheitsobjekte werden aufgelistet, nachdem man den Raum verlässt. Dabei werden die Punkte für die gewählten Objekte vergeben. Nach der Auflösung ist es möglich, erneut zu spielen, um ggf. noch nicht gefundene Objekte zu finden und/oder optimale Aktionen auszuwählen.

Nr.	Objekt	Hinweis
1	Zettel mit Passwort	Sensible Zugangsdaten, wie Passwörter, dürfen nicht an Dritte gelangen.
2	Papierkorb	Im Papierkorb können sich personenbezogene Daten befinden, die zum Identitätsklau genutzt werden können.
3	Kalender	Im Kalender können wichtige Informationen zu möglichen Terminen stehen, die Aussage darüber geben können, wann und wo sich die Person befindet.
4	(Video-)/Fotokamera	Kann Bilder enthalten, die zweckentfremdet werden können.
5	Dokumente	Können sensible Informationen über die Firma, Kontodaten, Personenangaben etc. beinhalten – dürfen nicht von Dritten eingesehen werden.
6	Schublade	In einer nicht abgeschlossenen Schublade können private und wichtige Informationen in Dokumenten liegen.
7	Ordner	Manche Ordner können Dokumentenordner sein, die z.B. nur firmenintern eingesehen werden dürfen.
8	Computer	Das Nichtausschalten von Computern beim Verlassen des Arbeitsplatzes kann anderen den Zugang zu Daten ermöglichen.
9	Drucker und Scanner	Oft werden ausgedruckte oder kopierte Blätter im Drucker vergessen. Diese können wichtige interne Informationen beinhalten.
10	Schredder	Manchmal lassen sich unvollständig geschredderte Dokumente wieder zusammensetzen und können so Informationen verraten.

11	Tür	Beim Verlassen des Büros muss die Tür abgeschlossen werden, um Daten- und Sachdiebstahl zu vermeiden.
12	Fenster	Beim Verlassen des Büros müssen alle Fenster wieder geschlossen werden, um Diebstahl vorzubeugen.
13	Smartphone	Wertgegenstände müssen sorgsam aufbewahrt werden.
14	Tasche/Rucksack	Wertgegenstände müssen sorgsam aufbewahrt werden.
15	Portemonnaie	Wertgegenstände müssen sorgsam aufbewahrt werden.
16	Schlüssel	Die Schlüssel dürfen nicht beim Verlassen des Raumes vergessen werden.

Bildrechte
(Digital)

- Spielbar einzeln oder im Team bis zu 3 Personen.
- Spieldauer 10-20 Minuten.

Eignung

Dieses Lernszenario hilft bei der Auseinandersetzung mit dem Thema Bildrechte. Der allgemein sorglose Umgang mit Multimediainhalten wirft zahlreiche Fragen auf. Die Sensibilisierung der Teilnehmenden soll zu einem zukünftig rechtskonformen Verhalten beitragen. Die Fragen werden als Quiz mit vielen praxisnahen Beispielen und in drei Levels präsentiert. Eine Bewertung durch die Gegenüberstellung der korrekt und falsch beantworteten Fragen gibt Aufschluss darüber, wie das Thema bei den Teilnehmenden bereits verankert ist.

Ziel des Lernszenarios

Urheberrecht, Quellennachweis, der rechtskonforme Umgang mit multimedialen Inhalten im Allgemeinen und Bildmaterial im Besonderen stehen im Zentrum des digitalen Lernszenarios.

Schnell eine Präsentation zusammenstellen, aus einer Fülle von Bildern im Internet auswählen oder Fotos in den sozialen Netzwerken teilen - alles kein Problem und kinderleicht umzusetzen!

Aber es kann teuer werden, ungefragt einen Kartenausschnitt für ein Treffen oder eine Dokumentation zu verwenden. Was ist mit den abgebildeten Personen, was ist mit dem „Recht am eigenen Bild“? Willst du ein Bild von dir durch unbekannte Personen verteilt sehen (vielleicht sogar in einer dir peinlichen Situation)?

Mit diesem Lernszenario wirst du deine Kompetenzen verbessern. Aufmerksames Betrachten der Situationen auf den Bildern und Lesen der im Text genannten Ausgangssituation hilft, die Anzahl falscher Entscheidungen zu minimieren.

Benötigte Materialien

	Computer, Tablet oder Smartphone
	Beiliegender USB-Stick mit digitalen Lernszenarien
	Internetverbindung für die Online-Version: https://szenarien.wildau.biz/bildrechte

Vorbereitung und Erläuterung des Lernszenarios

- Vereinbart die Spieldauer, wenn ihr nicht nach der empfohlenen Zeit spielen möchtet.
- Wählt ein Level aus: leicht, mittel oder schwer. Das Lernszenario beinhaltet drei unterschiedliche Levels, die nach Schwierigkeit geordnet sind. Das Lernszenario kann klassenstufenübergreifend gespielt werden. Jedoch empfiehlt sich leicht für die Klassenstufen 6-7, mittel für die Klassenstufen 8-9 und schwer ab der 10. Klassenstufe. Besonders effektiv ist es dabei, alle drei Levels nacheinander abzuarbeiten.

Ablauf

1. Klickt auf das von euch gewählte Level.
2. Beantwortet die einzelnen Fragen nacheinander.

Ende des Spiels

Das Spiel ist zu Ende, wenn einer der Punkte zutrifft:

A. Das Spiel endet nach Ablauf der vereinbarten Spieldauer.

B. Das Spiel wird beendet nach Ablegen eines oder mehreren Levels.

Lösung

Die Auflösung gibt es nach Beenden eines Levels und/oder nach dem Beenden aller drei Level.

Hacker Terminal
(Digital)

- Spielbar einzeln oder im Team bis zu 3 Personen.
- Spieldauer 10 Minuten.

Eignung

Dieses Lernszenario eignet sich gut zur Vertiefung und Wiederholung von grundlegenden Begriffen der Informationssicherheit. „Hacker Terminal“ fördert das selbstständige Lernen einzeln und im Team. Gespielt werden kann entweder gemeinsam in der Schule (z.B. im Computerraum), unterwegs mit Smartphone / Tablet oder von zu Hause aus. „Hacker Terminal“ ist klassenstufenübergreifend und kann altersunabhängig gespielt werden.

Ziel des Lernszenarios

In der Rolle der Retro-Hacker ist das Ziel, anhand von Hinweisen „verschlüsselte“ Kennwörter zu erraten, um an mögliche Zugänge und ins System zu gelangen. Dabei werden Fachbegriffe erlernt und die assoziative Kette verstärkt.

Benötigte Materialien

	Computer, Tablet oder Smartphone
	Beiliegender USB-Stick mit digitalen Lernszenarien
	Internetverbindung für die Online-Version: https://szenarien.wildau.biz/terminal-hacker/

Vorbereitung und Erläuterung des Lernszenarios

- Vereinbart die Spieldauer, wenn ihr nicht nach der empfohlenen Zeit spielen möchtet.
- Das Lernszenario kann beliebig oft gespielt werden.
- Es ist empfohlen, alle drei Kategorien mehrmals abzuarbeiten, um den Lerneffekt zu verstärken.

Ablauf

1. Wählt eine der vorgegebenen Kategorien aus, die ihr „hacken“ bzw. entschlüsseln möchtet.
2. Folgt den Anweisungen im Menü.

Ende des Spiels

Das Spiel endet nach Ablauf der vereinbarten Spieldauer.

Als vertiefende Ergänzung ist empfohlen, das analoge Lernszenario „Informationssicherheit: Schnelles Begrifferaten“ im Anschluss zu spielen.

Security Sketch

Umgang mit Passwörtern (Digital)

- Spielbar einzeln.
- Spieldauer 10 Minuten.

Eignung

Dieses Lernszenario eignet sich gut zur Vertiefung und Wiederholung von grundlegenden Kenntnissen zur Passwortsicherheit. Security Sketch fördert das selbstständige Lernen und zeigt Fehler sowie auch richtige Vorgehensweisen beim Umgang mit Passwörtern auf. Gespielt werden kann entweder in der Schule (z.B. im Computerraum), unterwegs mit dem Smartphone/Tablet oder von zu Hause aus. Das Lernszenario ist klassenstufenübergreifend und kann altersunabhängig gespielt werden.

Ziel des Lernszenarios

In der Rolle von Frau Hackermann sollen die richtigen Entscheidungen in Bezug auf die Passwortsicherheit getroffen werden. Beispielsweise soll entschieden werden, wie mit einem neu erhaltenen Passwort umgegangen werden soll und ob/ wo dieses notiert wird. Ziel ist es, für den richtigen Umgang mit Passwörtern zu sensibilisieren.

Benötigte Materialien

	Computer, Tablet oder Smartphone
	Beiliegender USB-Stick mit digitalen Lernszenarien
	Internetverbindung für die Online-Version: Deutsch: https://szenarien.wildau.biz/security_sketch_passwords/story_html5.html Englisch: https://szenarien.wildau.biz/security_sketch_passwords_eng/story_html5.html

Vorbereitung und Erläuterung des Lernszenarios

Das Lernszenario kann beliebig oft gespielt werden.

Ablauf

1. Schaut euch den Film an.
2. Wählt die Vorgehensweisen aus.

Ende des Spiels

Das Spiel endet nach Auswahl der richtigen Antwortmöglichkeiten und Ablauf des Films.

Glossar

Begriff	Erklärung
AccL	Accelerated Learning
Administratorin/ Administrator/ Admin	Eine Person, die etwas verwaltet, z.B. ein Forum im Internet oder eine Gruppe in sozialen Netzwerken.
AGB	Allgemeine Geschäftsbedingungen
Backup	Vorgang, um Daten zu sichern
Botnetz	Fernsteuerbares Netz aus zusammengeschlossenen PCs
Catfishing	Falsche Identität annehmen
Chronologie	Zeitmessung, zeitliche Abfolge; Wissenschaft der Zeitmessung
Coockies	Speicherung der Nutzerdaten auf Webseiten
Cybermobbing	Beleidigung, Bedrohung, Bloßstellung oder Belästigung von Personen mithilfe von Kommunikationsmedien
Digital Detox	Digitale Entgiftung, Entzug digitaler Geräte und des Internets
DSGVO	Datenschutz-Grundverordnung
Evakuierung	Räumung eines Gebietes oder Gebäudes von Menschen
EXE-Datei	Engl. executable = ausführbar; eine Dateinamenserweiterung für ausführbare Dateien
Fake News	Falsche oder vorgetäuschte Nachrichten, die überwiegend in den Medien verbreitet werden.
Firewall	Kontrolliert alle Daten, die ins eigene Netzwerk hineinkommen oder es verlassen.

GBL	Game-Based Learning (spielbasiertes Lernen)
Hash-Wert	Zeichenfolge, die mittels Algorithmus aus einem Passwort ermittelt wurde.
Hate speech	Hassrede
HGS	Host Görtz Stiftung
In-App-Käufe	Käufe innerhalb eines Online-Spiels
Integrität	Sicherstellung der Korrektheit bzw. Unversehrtheit von Informationen und der korrekten Funktionsweise von Systemen.
Informations-sicherheit	Dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von (wirtschaftlichen) Schäden und der Minimierung von Risiken.
IP-Adresse	IP - Internetprotokoll. Wird Geräten zugewiesen, die an das Netz angewiesen sind. Macht die Geräte adressierbar und erreichbar.
Korruption	Bestechung, bestechliches Handeln oder bestechliche/korrupte Geschäfte
Parodie	Nachahmung, Nachbildung, Nachdichtung
Phishing	Ein Versuch, über gefälschte Webseiten, Kurznachrichten oder E-Mails an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen und der Person zu schaden.
Phubbing	Im Gespräch am Handy sein
Profitgier	Habgier, Gewinnsucht
Propaganda	Systematische Verbreitung politischer, weltanschaulicher o. ä. Ideen und Meinungen mit dem Ziel, das allgemeine Bewusstsein in bestimmter Weise zu beeinflussen.
Rainbow-Tabelle	Datenstruktur, die eine schnelle, speichereffiziente Suche nach der ursprünglichen Zeichenfolge für einen gegebenen Hashwert ermöglicht.

Recovery	Wiederherstellung der Originaldaten aus einer Sicherungskopie.
Salt	Zufällig gewählte Zeichenfolge
SecAware4school	Information Security Awareness for Daily life at School
Security Exploit	Zeigt Sicherheitslücken von Software auf und ermöglicht deren Ausnutzung.
Seriosität	Ernsthaftigkeit
Serious Game	Engl.: ernsthaftes Spiel. Das Ziel dabei ist, Informationen und Bildung mit ausgeglichenen Unterhaltungsaspekten zu vermitteln.
Server	Ein Computerprogramm oder Gerät, welches für andere Programme oder Geräte Funktionalitäten bereitstellt.
Serviceprovider	Internetdienstleister
Shit storm	Weitverbreitete und lautstarke negative Kritik/Empörung im Internet. Bezieht sich vor allem auf Blogeinträge, Kommentare, Nachrichten, Meldungen in sozialen Netzwerken.
Skimming	Kreditkarten- oder Bankkartenbetrug
Spam	Spam oder Junk-Nachrichten sind unerwünschte Werbe-E-Mails.
Spionage	Auskundschaftung, geheimdienstliche Tätigkeit
Terminal	hier gemeint: Benutzerendgerät im Sinne von Computer
THW	Technische Hochschule Wildau
Tonalität	hier gemeint: Art und Weise der Ansprache
Upload-Filter	Programme, die alle hochgeladenen Inhalte scannen und mithilfe von riesigen Datenbanken eine Verletzung von Urherberrechten prüfen.
UrhG	Urheberrechtsgesetz

Verfügbarkeit	Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen, IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.
Vertraulichkeit	Schutz vor dem unbefugten Preisgeben der Informationen.
WHO	Weltgesundheitsorganisation
Wörterbuch-angriff	Methode der Kryptoanalyse, um ein unbekanntes Passwort mithilfe einer Wörterliste zu ermitteln
Zivilcourage	Mut, den jemand beweist, indem er menschliche oder demokratische Werte ohne Rücksicht auf mögliche Folgen vertritt.
Zutrittskontrolle	Steuert den Zutritt nach einem festgelegten Regelwerk
3-2-1-Regel	Regel zur Datensicherung: mindestens 3 Sicherheitskopien auf 2 unterschiedlichen Speichermedien, von denen mindestens 1 Kopie an einem externen Speicherort verwahrt wird.

Tipps und Tricks*

Weiterführende Informationen und Materialien

Zum Verhalten in sozialen Netzwerken

https://medien-knigge.de/

http://www.knigge.de/themen/verschiedenes/handy-knigge-5385.htm

https://karrierebibel.de/social-media-knigge/

http://www.stil.de/knigge-thema-der-woche/details/artikel/social-media-knigge-wie-sie-sich-stilvoll-im-virtuellen-raum-bewegen.html

Werkzeuge zum Entlarven von Fake News

https://www.schau-hin.info/ ist ein Portal für Kinder und Jugendliche über Falschmeldungen

https://hoaxmap.org/ dokumentiert Falschmeldungen über Flüchtlinge

https://www.br.de/sogehtmedien/index.html von ARD und ZDF bietet für Jugendliche Tipps mit Videos, wie man Fake News erkennen kann, und darüber hinaus gibt es auch Unterrichtsmaterialien zum Thema

Der Faktenfinder https://www.tagesschau.de/faktenfinder/ ist ein so genannter „Faktenchecker“ des gemeinnützigen Recherchenetzwerks-Correktivs

https://correctiv.org/faktencheck/

Seriöse Webseiten für Kinder, die sich (geschützt vor Fake News auf Basis von geprüften Inhalten) informieren wollen

https://www.hanisauland.de/kindernetz.de

https://kinder.wdr.de/tv/neuneinhalb/index.htmlnews4kids.de

Oder die Kindersuchmaschinen:

https://www.blinde-kuh.de/index.html

https://www.fragfinn.de/

https://www.helles-koepfchen.de/

**Alle nachfolgenden URLs wurden zuletzt am 15. Juli 2020 geprüft.*

Informationen zu Internetnutzung und Smartphone

https://www.klicksafe.de/

https://www.handysektor.de/

https://www.bsi-fuer-buerger.de/

https://www.gesetze-im-internet.de/

Download

Der Download von urheberrechtlich geschützten Werken, die ohne Zustimmung der Urheber im Netz angeboten werden, ist eindeutig strafbar, wenn das Werk aus einer offensichtlich illegalen Quelle stammt.

Filesharing

Sowohl der Download als auch die Verbreitung von urheberrechtlich geschützten Werken, die ohne Zustimmung der Urheber im Netz angeboten werden, ist strafbar.

Streaming

Das Streaming von urheberrechtlich geschützten Werken, die ohne Zustimmung der Urheber im Netz angeboten werden, war bis zum Urteil des Europäischen Gerichtshofs (EuGH) vom 26.04.2017 eine rechtliche Grauzone. Bis dahin waren sich Juristen uneinig, ob die Zwischenspeicherung im Cache bereits als Download zu werten und damit strafbar ist. Bisher wurde als Gegenargument der § 44a UrhG herangezogen. Dieser besagt, dass vorübergehende Vervielfältigungshandlungen, die flüchtig oder begleitend sind und einen wesentlichen Teil eines technischen Verfahrens darstellen, zulässig sind.

Quellen

Linek, S. B. & Albert, D., 2009.
Game-based Learning: Gender-specific Aspects of Parasocial Interaction and Identification.

Fang, X., Zhang, J. & Chan, S. S., 2013.
Development of an Instrument for Studying Flow in Computer Game Play. Interna-tional Journal of Human-Computer Interaction, 29(7), pp. 456-47.

Bressler, D. & Bodzin, A., 2013.
A Mixed Methods Assessment of Students' Flow Experiences During a Mobile Augmented Reality Science Game. Journal of Computer Assisted Learning, 29(6), pp. 505-517.

Gesetze

Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung vom 3. März 2010 (BGBl. I S.254), zuletzt geändert durch Artikel 5 des Gesetzes vom 18. April 2019 (BGBl. I S. 466).

Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266).

Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 5 des Gesetzes vom 10. Juli 2020 (BGBl. I S. 1648).

Die Forschungsgruppe von Frau Prof. Dr. Scholl (ohne Fr. Prott), das Projektteam SecAware4school und der Projektpartner Pokoyski (Firma “known_sense”) im Jahr 2019.

Informationssicherheitsbewusstsein für den Schulalltag (SecAware4school)
Ein Projekt der Technischen Hochschule Wildau.
Die aus dem Vorhaben resultierenden Lernszenarien und das zugrundeliegende Anleitungsbuch wurden mit Mitteln der Horst Görtz Stiftung (HGS) gefördert.

Projektlaufzeit: 01.09.2018 bis 31.12.2020

Weitere Informationen zum Projekt und weitere Materialien finden Sie unter www.secaware4school.wildau.biz.

ISBN 978-3-9819225-4-7