CYBER SECURITY QUIZ

LEITFADEN

für den Einsatz der App „Cyber Security Quiz“ in Schulen

Sekundarstufe 2

September 2020

Inhalt

1. Wozu eine Cyber Security Quiz-App?

Online zu sein gehört für Jugendliche dazu wie die Luft zum Atmen. Und auch, wenn sie sich in aller Regel sehr geschickt und kompetent durch die Online-Landschaft bewegen, fehlt ihnen oft der Blick für die größeren Auswirkungen ihres Surf-Verhaltens, Gefahren und Risiken im Internet.

Online-Kompetenzen und digitale Sicherheit werden zweifelsohne auch in Zukunft zunehmend wichtiger – nicht nur für die persönliche Sicherheit, sondern auch als berufliche Alltagskompetenz.

Gleichzeitig ist Digitalisierung nichts Statisches – die Infrastruktur und damit auch geltende Sicherheitsstandards entwickeln sich laufend weiter. Was einmal als sicher galt (z. B. Standards für Passwörter) ist es heute vermutlich bereits nicht mehr.

Es ist daher wichtig, stets interessiert zu bleiben und sich über neue Entwicklungen am Laufenden zu halten. Das ist aber nicht immer einfach und auch eine Frage der Zeit und Motivation.

Umso früher Jugendliche sich mit dem Thema Internetsicherheit auseinandersetzen, desto einfacher ist es für sie, neue Entwicklungen mitzubekommen und richtig einordnen zu können.

Der einfachste Weg Jugendliche zum Lernen zu motivieren, ist sie dort abzuholen, wo sie sich bereits befinden: in der Welt der Smartphones und Apps.

Das *Cyber Security Quiz* ist nicht nur ein raffinierter Weg Wissen zu vermitteln, sondern ist auch unterhaltsam und vergleichsweise einfach in den Alltag zu integrieren. Im Idealfall vergessen Jugendliche bei seiner Nutzung sogar, dass sie gerade Lernen und kippen in ein Spielverhalten, zu dem sie freiwillig immer wieder zurückkehren.

2. Was sind die Vorteile von Game-based Learning und Micro Learning?

Beim Konzept des *Game-based Learning* geht es darum, die Wissensvermittlung mit dem Spielerischen zu verknüpfen. Dieser Zugang soll dabei helfen, zum Lernen zu motivieren und schulische Leistungen zu verbessern.

Der große Vorteil am spielerischen Lernen ist, dass man selbst Lernunwillige gut damit erreichen kann: Denn ist das Spielvergnügen groß genug, rückt das Lernen in den Hintergrund und erfolgt somit eher nebenbei.

Gerade Wettbewerbe, wie sie auch die *Cyber Secuity Quiz*-App anbietet, können manche Menschen ganz besonders dazu anspornen, Wissen aufzuholen und andere zu übertrumpfen.

Unter *Micro-Learning* versteht man das Lernen in kleinen Lerneinheiten. Dieses lässt sich gerade anhand von digitalen Lernspielen gut umsetzen. Gelernt wird dann nicht in großen Blöcken, sondern in kleinen auflockernden Dosen zwischendurch.

Das Lernen lässt sich so leicht in den Tagesablauf integrieren und/oder in bereits strukturierte Lernprozesse aufnehmen. Diese kleinen Lerneinheiten brauchen wenig Zeit und bringen gleichzeitig willkommene Abwechslung. Das *Cyber Security Quiz* lässt sich auch gut zur Pause und als Mini-Lerneinheiten verwenden.

Ein weiterer Vorteil von *Micro-Learning* ist, dass sich die Lernenden die Inhalte selbst auswählen können, je nachdem was für sie gerade relevant ist, und nicht immer ein gesamtes Thema von vorn bis hinten durcharbeiten müssen.

3. Wo finde ich das Cyber Security Quiz?

Das Quiz ist kostenlos verfügbar für:

 Android

 iOS

 Web

Für die Registrierung wird eine E-Mail-Adresse benötigt.

Wichtige Infos zur App und vor allem das Benutzerhandbuch gibt es auf www.cybersecurityquiz.at.

4. Was sind die Lernziele und Themen der App?

Ziele der *Cyber Security Quiz*-App sind:

- Gefahrenpotenziale im Internet erkennen können
- kompetent mit Gefahren im Internet (z. B. Internetbetrug, Fake-News oder Cyber-Mobbing) umgehen können
- das eigene Verhalten im Internet zu reflektieren
- zeitgemäße und attraktive Methoden für den Unterricht zu bieten: Game based-Learning und Micro-Learning
- beim Erwerb der Kompetenzen nach dem digitalen Kompetenzmodell DigComp 2.2 AT zu unterstützen
- Motivation der SchülerInnen steigern

Das *Cyber Security Quiz* gliedert sich in vier Themen und ihre Unterthemen:

1. Technische Bedrohungen
   Infos zu Schadsoftware und Ransomware bis hin zu Updates und Backups.
2. Sich vor Betrug schützen
   Wie kann man sich vor Phishing, Abo-Fallen, Fake-Shops, etc. schützen?
3. Datenschutz
   Bei diesem Thema geht es um den digitalen Fußabdruck und den Ruf im Netz, aber auch um Privatsphäre und Passwörter.
4. Cyber-Mobbing
   Auch genannt Cyber-Bullying: Hass im Netz und was man dagegen tun kann.
5. Fake-News
   Wahr oder falsch? Informationen im Internet richtig bewerten.

Auf dem „HOME“-Dashboard der App werden außerdem unter „MEINE KOMPETENZEN“ fünf Kompetenzbereiche und Kompetenzen angezeigt, die sich am Digitalen Kompetenzmodell für Österreich - DigComp 2.2 AT orientieren und die mit dem Quiz gefördert werden:

- Kompetenzbereiche 0. Grundlagen
- Kompetenzbereich 4. Sicherheit:
    - 4.1. Geräte schützen
    - 4.2. Personenbezogene Daten und Privatsphäre schützen
    - 4.3. Gesundheit und Wohlbefinden schützen
    - 4.4. Sich vor Betrug und Konsumentenschutzmissbrauch schützen

Der Balken unter jeder Kompetenz zeigt an, welche Fortschritte seit der Verwendung der App gemacht wurden. So wird für die Nutzerinnen und Nutzer die stetige Entwicklung der eigenen Kompetenzen sichtbar.

5. Wie lässt sich die App in den Schulunterricht integrieren?

Die Einsatzszenarien der App für den Schulunterricht sind vielfältig:

- In einer abgeschlossenen Unterrichtseinheit
- Blended Learning/Flipped Classroom
- Tag der offenen Tür oder Messestand
- Schulweiter Wettbewerb
- Peer-Learning und Peer-Mediation
- Aktionstag

5.1. Die abgeschlossene Unterrichtseinheit

Das Quiz lässt sich gut für abgeschlossene Unterrichtseinheiten oder Supplierstunden verwenden.

Vorbereitung:

Vor der Stunde (oder zu Beginn der Stunde) muss jede Spielerin bzw. jeder Spieler einen eigenen Account anlegen. Dazu brauchen die SchülerInnen Zugang zu einer E-Mail-Adresse.

Die Lehrperson erstellt eine Liste mit allen MitspielerInnen und macht diese auch für die SchülerInnen zugänglich (z. B. auf der Tafel oder in einer digitalen Lernplattform). Wichtig ist, dass man erkennt, wer hinter welchem Nickname steckt.

Schritt 1:

Die SchülerInnen spielen („Lesen“ und „Üben“) so lange, bis sie für den Duell-Modus (= TRAINING) freigeschaltet werden.

> **Hinweis:**
>
> Um im Duell gegen andere SpielerInnen antreten zu können, müssen zuerst bestimmte Lerninhalte („Lesen“ und „Üben“ der Einführung) erarbeitet werden.

Schritt 2:

Die SchülerInnen treten im Duell-Modus gegeneinander an. Am besten wird dafür von der Lehrperson vorab ein konkreter Zeitrahmen festgelegt. In ausgewählten Settings können auch andere Personengruppen, wie Eltern, Lehrpersonen oder ExpertInnen miteinbezogen werden (z. B. am Tag der offenen Tür).

Schritt 3:

Am Ende der Unterrichtseinheit erfolgt eine Reflexion.

Wer hat die meisten Punkte erspielt (diese sind unter „MEINE KOMPETENZEN“ abrufbar)? Welche Fragen waren überraschend? Welche Fragen waren besonders schwierig? Wo hat die Klasse noch weiteren Informationsbedarf?

> **Hinweis zur Punkteermittlung:**
>
> Bei Spielewiederholungen an mehreren Tagen müssen sich die SchülerInnen die Punktedifferenz selbst ausrechnen (Vergleich der Punkteanzahl zu Beginn und am Ende der Unterrichtseinheit). Ansonsten sind manche Jugendliche in ihrem Punktestand nicht mehr einzuholen, wodurch die Motivation der restlichen SpielerInnen schwindet.

Ergänzungsaufgaben:

- Die SchülerInnen recherchieren online nach einer ausgewählten Online-Bedrohung.
- Die SchülerInnen halten allein oder in Gruppen kurze Referate über ausgewählte Themengebiete der App.

5.2. Blended Learning/Flipped Classroom

Das Quiz lässt sich gut selbstständig zuhause durchspielen und anschließend im Unterricht aufgreifen.

Vorbereitung:

Jede Spielerin bzw. jeder Spieler braucht einen eigenen Account. Dazu brauchen die SchülerInnen Zugang zu einer E-Mail-Adresse und einem digitalen Gerät.

Die Lehrperson erstellt eine Liste mit allen MitspielerInnen und macht diese auch für die SchülerInnen zugänglich (z. B. in einer digitalen Lernplattform). Wichtig ist, dass man erkennt, wer hinter welchem Nickname steckt.

Schritt 1:

Die SchülerInnen spielen im Rahmen einer Hausübung zuhause das Quiz und treten in mindestens vier Duellen zu je drei Runden gegen andere MitschülerInnen an.

Bevor man in ein Duell gehen kann, müssen erst bestimmte Lerninhalte („Lesen“ und „Üben“ der Einführung) absolviert werden. Um den Umfang einzuschränken, kann die Lehrperson die zu bearbeitenden Themen festlegen. Der entsprechende Lernfortschritt wird damit auch besser vergleichbar.

> **Tipp:**
>
> Die SchülerInnen können z. B. Screenshots ihrer Duelle anfertigen, um ihre Hausaufgabe nachweisen zu können. Dazu ist allerdings wichtig, sicherzustellen, dass alle SchülerInnen wissen, wie man einen solchen erstellt.

Schritt 2

Die Lehrperson bespricht in der nächsten Unterrichtseinheit mit den SchülerInnen anhand der Lese-Beiträge in den Kapiteln der App, welche Themen besonders herausfordernd waren. Die Lehrperson sammelt so die Themen, zu denen es die meisten Rückfragen gibt und bespricht diese dann im Unterricht.

5.3. Tag der offenen Tür/Messestand

> **Hinweis:**
>
> Kontaktieren Sie Saferinternet.at unter office@saferinternet.at, um ein *Cyber Security Quiz*-Rollup für Ihren Stand auszuleihen!

Variante 1: am Stand sind Tablets vorhanden

Jede Person, die an den Stand kommt, kann mit einem vorab angelegten Profil gegen eine weitere Person (idealerweise ebenfalls am Stand anwesend) im Duell-Modus antreten.

Variante 2: das eigene Gerät wird verwendet

Der Link zur App oder der Website wird am Stand – eventuell anhand eines QR-Codes – ausgehängt. StandbesucherInnen können sich so selbstständig anmelden und so lange spielen, wie sie Zeit und Lust haben. Dann zeigen sie den Standbetreuenden ihren Highscore. Diese notieren die Highscores mit Namen (wenn die Spielenden damit einverstanden sind auch öffentlich sichtbar).

> Tipp:
>
> Um den Spaß beim Spielen zu erhöhen, können kleine Preise im Rahmen einer Preisverleihung vergeben werden. Dafür zeigen sie den Standbetreuenden ihren Highscore. Diese notieren die Highscores mit Namen (wenn die Spielenden damit einverstanden sind auch öffentlich sichtbar). Ebenfalls empfehlenswert ist es, den BesucherInnen einen Flyer mit dem Link zum Spiel mitzugeben – so

5.4. Der schulweite Wettbewerb

Das *Cyber Security Quiz* wird im Duell-Modus in der gesamten Schule (idealerweise inklusive der Lehrenden) durchgeführt. Dies kann über die Infoscreens in der Schule oder einer Lernplattform begleitet werden. Eine Einführung in das Quiz durch Lehrende während einer Unterrichtseinheit (oder im Rahmen von Saferinternet.at-Workshops) ist empfehlenswert.

Die Teilnahme:

- Nicknames mit Schulkürzel im Namen:
  Die SchülerInnen vergeben sich selbst einen Nutzernamen, aus dem der Schulbezug sichtbar wird (z. B. mit einem vorab festgelegten Kürzel). So ist für alle ersichtlich, wer zur Schule gehört und wer nicht.

- Listen mit Namen liegen auf:
  Alternativ können Nicknames zugeteilt oder im Intranet für alle einsehbar sein. Auf diese Weise spielen die SpielerInnen nicht anonym gegeneinander.

Ablauf:

- Der Wettbewerb geht über einen bestimmten Zeitraum (z. B. einen Tag oder eine Woche)

- Zu einem Stichdatum muss ein Screenshot vom „HOME"-Screen (dort sieht man die erspielten Punkte und erlernten Kompetenzen) an eine bestimmte E-Mail-Adresse geschickt werden.

- Die GewinnerInnen werden veröffentlicht und erhalten einen kleinen Preis.

5.5. Peer-Learning und Peer-Mediation

- An manchen Schulen ist es üblich, dass Peers (=zu ExpertInnen ausgebildete MitschülerInnen) Schulungen zur sicheren und verantwortungsvollen Internetnutzung durchführen. Das *Cyber Security Quiz* lässt sich auch im Rahmen von solchen Schulungen einsetzen. Hier ist es wichtig, dass die Inhalte des Quiz nach dem Spielen gemeinsam reflektiert und nachbearbeitet werden.

- Der Ablauf ist vergleichbar mit „4.1. Die abgeschlossene Unterrichtseinheit".

5.6. Aktionstag

> Hinweis:
>
> Kontaktieren Sie Saferinternet.at unter office@saferinternet.at, um ein *Cyber Security Quiz*-Rollup für Ihren Stand auszuleihen!

Ein Aktionstag wird oft mit einem themenbezogenen Anlass verknüpft. Für das Cyber Scurity Quiz eigenen sich zum Beispiel folgende Anlässe:

- Safer Internet Day (jährlich am 2. Dienstag im Februar)
  www.saferinternetday.at
- Cyber Security Month (Oktober)
  https://cybersecuritymonth.eu/
- Europäischer Datenschutztag am 28. Jänner
  www.coe.int/de/web/portal/28-january-data-protection-day

Ein Aktionstag bietet sich dazu an, das Quiz als schulweiten Wettbewerb (siehe „ 4.4. Der schulweite Wettbewerb“) oder Klassen-Projekt durchzuführen. Um die App zu verbessern oder zu erweitern können SchülerInnen sich im Rahmen von Projekten ausgewählten Fragestellungen annehmen, wie z. B. folgenden:

- Wie kann man das Thema der Internet-Sicherheit bei Kindern und Jugendlichen sichtbarer machen?
- Welche Bedrohungen fehlen in der App?
- Wie könnte weiterführende Information zu einzelnen Themen aussehen?
- …

6. Anknüpfungspunkte an den Unterricht (Lehrplanbezug)

Anknüpfungspunkte an den Unterricht lassen sich in der *Cyber Security App* viele finden:

- Informatik, EDV, IKT
- Persönlichkeitsentwicklung
- Politische Bildung
- Kaufmännische Fächer
- Betriebswirtschaftliche Grundlagen
- Sicherheit am Arbeitsplatz
- Cyber-Crime, Datenschutz
- Internetbetrug, technische Sicherheit
- Informationsbewertung
- Datenschutz, Schutz der Privatsphäre
- Selbstdarstellung
- Cyber-Mobbing
- Ethik

7. Anknüpfungspunkte an die nachhaltigen Entwicklungsziele (SDGs)

Die insgesamt 17 Ziele für nachhaltige Entwicklung (= Sustainable Development Goals) wurden bereits 2015 von den Vereinten Nationen für die Sicherung einer nachhaltigen Entwicklung auf ökonomischer, sozialer und ökologischer Ebene beschlossen. Ziel ist die Umsetzung bis 2030.

Da es sich hierbei um Entwicklungsziele handelt, die die gesamte Gesellschaft betreffen, sind auch Schulen dazu angehalten, diese Ziele in ihrem Unterricht aufzugreifen.

Hier eine Zusammenstellung jener SDGs, für welche das Cyber Security Quiz relevant sein kann:

- 3.4 Bis 2030 die Frühsterblichkeit aufgrund von nichtübertragbaren Krankheiten durch Prävention und Behandlung um ein Drittel senken und die psychische Gesundheit und das Wohlergehen fördern
- 5.b Die Nutzung von Grundlagentechnologien, insbesondere der Informations- und Kommunikationstechnologien, verbessern, um die Selbstbestimmung der Frauen zu fördern
- 8.2 Eine höhere wirtschaftliche Produktivität durch Diversifizierung, technologische Modernisierung und Innovation erreichen, einschließlich durch Konzentration auf mit hoher Wertschöpfung verbundene und arbeitsintensive Sektoren
- 8.b Bis 2020 eine globale Strategie für Jugendbeschäftigung erarbeiten und auf den Weg bringen und den Globalen Beschäftigungspakt der Internationalen Arbeitsorganisation umsetzen
- 9.1 Eine hochwertige, verlässliche, nachhaltige und widerstandsfähige Infrastruktur aufbauen, einschließlich regionaler und grenzüberschreitender Infrastruktur, um die wirtschaftliche Entwicklung und das menschliche Wohlergehen zu unterstützen, und dabei den Schwerpunkt auf einen erschwinglichen und gleichberechtigten Zugang für alle legen

- 16.4 Bis 2030 illegale Finanz- und Waffenströme deutlich verringern, die Wiedererlangung und Rückgabe gestohlener Vermögenswerte verstärken und alle Formen der organisierten Kriminalität bekämpfen

Link:

www.bundeskanzleramt.gv.at/themen/nachhaltige-entwicklung-agenda-2030/entwicklungsziele-agenda-2030.html

8. Das Wichtigste im Überblick

<table>
<tr>
<td>Alter:
ab 15 Jahre</td>
<td>Nachweis der Beteiligung:
Screenshot vom „HOME“-Screen</td>
</tr>
<tr>
<td>Ziele der App:
- Gefahrenpotenziale im Internet erkennen können
- kompetent mit Gefahren im Internet umgehen können
- das eigene Verhalten im Internet reflektieren
- Game-based Learning und Micro Learning
- Motivation der SchülerInnen steigern</td>
<td>Themen der App:
- Technische Bedrohungen
- Sich vor Betrug schützen
- Datenschutz
- Cyber-Mobbing
- Fake News</td>
</tr>
<tr>
<td>Zu beachten ist:
- Jede Spielerin bzw. jeder Spieler braucht einen eigenen Zugang.
- Für die Registrierung ist eine E-Mail-Adresse notwendig.
- Es muss eine Liste mit den Nicknames angelegt werden, um die SchülerInnen zuordnen zu können.
- Zugangsdaten notieren
- Lehrende können den Spielstand der SchülerInnen nicht selbstständig sehen.</td>
<td>Einsatzgebiete im Schulkontext:
- In einer abgeschlossenen Unterrichtseinheit
- Blended Learning/Flipped Classroom
- Tag der offenen Tür oder Messestand
- Schulweiter Wettbewerb
- Peer-Learning und Peer-Mediation
- Aktionstag</td>
</tr>
<tr>
<td>Anknüpfungspunkte:
- Informatik, EDV, IKT
- Persönlichkeitsentwicklung
- Politische Bildung
- Betriebswirtschaftliche Grundlagen
- Sicherheit am Arbeitsplatz
- Cyber-Crime, Datenschutz
- Internetbetrug, technische Sicherheit
- Cyber-Mobbing</td>
<td>Kostenlos verfügbar für:
  Android
  iOS
  Web

Fragen, Fehler und Feedback an:
office@cybersecurityquiz.at</td>
</tr>
</table>

9. Cyber Security – weiterführende Links

- www.onlinesicherheit.gv.at
  Ein zentrales Internetportal zu Themen rund um die Sicherheit zu Informations- und Kommunikationstechnologie. Es ist eine interministerielle Initiative in Kooperation mit der österreichischen Wirtschaft.

- www.watchlist-internet.at
  Die Watchlist Internet ist eine unabhängige Informationsplattform zu Internet-Betrug und betrugsähnlichen Online-Fallen aus Österreich. Sie informiert über aktuelle Betrugsfälle im Internet und gibt Tipps, wie man sich vor gängigen Betrugsmaschen schützen kann. Opfer von Internet-Betrug erhalten konkrete Anleitungen für weitere Schritte.

- www.saferinternet.at
  Saferinternet.at unterstützt vor allem Kinder, Jugendliche, Eltern und Lehrende beim sicheren, kompetenten und verantwortungsvollen Umgang mit digitalen Medien.

- www.ombudsstelle.at
  Die Internet Ombudsstelle ist eine unabhängige Streitschlichtungs- und Beratungsstelle rund um die Themen Online-Shopping, Datenschutz, Internetbetrug, Persönlichkeitsrechtsverletzungen etc.

- www.fit4internet.at
  Der Verein fit4internet ist eine überparteiliche und unabhängige Initiative zur Qualifizierung und Quantifizierung digitaler Kompetenzen der österreichischen Bevölkerung. Oberstes Ziel ist es, die kompetente Nutzung digitaler Technologien zu ermöglichen und die gesamte Gesellschaft an der Digitalisierung teilhaben zu lassen.

- www.cybersecurityaustria.at
  Cyber Security Austria ist ein gemeinnütziger, unabhängiger und überparteilicher Verein mit dem Ziel, Sicherheits-Querschnittthemen im Bereich der IT-/Cyber-Sicherheit zu adressieren.

10. Impressum

Österreichisches Institut für angewandte Telekommunikation (ÖIAT)
September 2020
Medieninhaber, Herausgeber und Sitz der Redaktion:
Saferinternet.at/Österreichisches Institut für angewandte Telekommunikation
Ungargasse 64–66/3/404, 1030 Wien

Redaktion:
DI[in] Barbara Buchegger, M.Ed., Mag.[a] Frederica Summereder, BA

Pädagogische und didaktische Beratung:
Dipl.-Päd. Werner Prüher, BEd MA
Mag.[a] Sandra Maria Kuchling MSc

Rückfragen:
Saferinternet.at/Österreichisches Institut für angewandte Telekommunikation
Ungargasse 64–66/3/404, 1030 Wien
Website: www.saferinternet.at
E-Mail: office@saferinternet.at
Telefon: +43 1 595 21 12-0