ESCAPE:

Gesundheitsfachkräfte auf Cyberangriffe vorbereiten

Material für Lernende

Eine integrierte kybernetische Bewusstseinsstrategie zur Bewertung von Einstellungen und Verhaltensweisen zur

Cybersicherheit im schulischen Kontext

ESCAPE: Gesundheitsfachkräfte auf Cyberangriffe vorbereiten	
Eine integrierte kybernetische Bewusstseinsstrategie zur Bewertung von Einstellungen und Verhaltensweisen zur Cybersicherheit im schulischen Kontext	
Sprache	*Englisch*

Inhaltsverzeichnis

1. Name des Materials und Beschreibung 3
2. Klassifizierung 3
3. Beschreibung 4
3.1. Herkunft 4
3.2. Warum ist es relevant/wichtig für ESCAPE? 5
3.3. Erkenntnisse 5
4. Direkter Link zum Material 6
5. Weiterführende Materialien (optional) 6

Co-funded by the European Union

Das Projekt „ESCAPE: Vorbereitung von Angehörigen der Gesundheitsberufe auf Cyberangriffe“ wird von der Europäischen Union kofinanziert. Die in diesem Protokoll geäußerten Meinungen und Standpunkte sind ausschließlich für den/die Autor(en) (ESCAPE-Konsortium) verbindlich und spiegeln nicht unbedingt die Meinung der Europäischen Union oder des Servicio Español para la Internacionalización de la Educación (SEPIE) wider. Weder die Europäische Union noch die Nationale Agentur SEPIE können dafür verantwortlich gemacht werden.

ESCAPE: Gesundheitsfachkräfte auf Cyberangriffe vorbereiten	
Eine integrierte kybernetische Bewusstseinsstrategie zur Bewertung von Einstellungen und Verhaltensweisen zur Cybersicherheit im schulischen Kontext	
Sprache	*Englisch*

1. Name des Materials und Beschreibung

Dies ist ein Forschungsartikel, der eine umfassende Strategie zur Förderung des Cyberbewusstseins bei Schüler*innen der Sekundarstufe I vorstellt. Die Strategie kombiniert Bewertungstools (Fragebögen), Selbsteinschätzungen und strukturierte Unterrichtspläne, die auf die Lehrpläne der Fächer Informations- und Kommunikationstechnologie (IKT) sowie Staatsbürgerkunde abgestimmt sind. Die Studie misst riskante Einstellungen und Verhaltensweisen in Bezug auf Cybersicherheit bei Schüler*innen der 6. und 9. Klasse und bietet sowohl zusammengefasste als auch individuelle Auswertungen.

2. Klassifizierung

Kategorie	Zutreffendes markieren
Sektor	☐ Gesundheitswesen
	☐ Allgemeinheit
	☑ Andere
Behandelte Themen	☑ Cybersicherheit
	☐ Datenschutz
Situationstyp	☑ Prävention
	☐ Auswirkungen (d. h. wann sie auftreten oder aufgetreten sind) auf die Patientenversorgung.
	☐ Auswirkungen auf alle anderen Aktivitäten, die nicht die direkte Patientenversorgung betreffen.
Sprache der Originalmaterialien	☐ Niederländisch

Co-funded by the European Union

Das Projekt „ESCAPE: Vorbereitung von Angehörigen der Gesundheitsberufe auf Cyberangriffe“ wird von der Europäischen Union kofinanziert. Die in diesem Protokoll geäußerten Meinungen und Standpunkte sind ausschließlich für den/die Autor(en) (ESCAPE-Konsortium) verbindlich und spiegeln nicht unbedingt die Meinung der Europäischen Union oder des Servicio Español para la Internacionalización de la Educación (SEPIE) wider. Weder die Europäische Union noch die Nationale Agentur SEPIE können dafür verantwortlich gemacht werden.

ESCAPE: Gesundheitsfachkräfte auf Cyberangriffe vorbereiten	
Eine integrierte kybernetische Bewusstseinsstrategie zur Bewertung von Einstellungen und Verhaltensweisen zur Cybersicherheit im schulischen Kontext	
Sprache	*Englisch*

	☑ Englisch
	☐ Deutsch
	☐ Italienisch
	☐ Spanisch
Art des Materials	☐ Richtlinien oder Handbücher
	☐ Fallbeispiele
	☐ Schulungen
	☑ Sonstige

3. Beschreibung

Dies ist eine integrierte Bildungsstrategie, die entwickelt wurde, um Einstellungen und Verhaltensweisen in Bezug auf Cybersicherheit im schulischen Kontext zu bewerten und zu verbessern. Sie basiert auf einem dreistufigen Prozess, der Erhebung, Selbstdiagnose und gezielte Unterrichtseinheiten umfasst.

3.1. Herkunft

Autor*innen: Mário Antunes, Carina Silva und Frederico Marques.

Veröffentlicht in: Applied Sciences, Band 11 (23), 2021; Artikelnummer 11269. Open Access über MDPI.

3.2. Warum ist es relevant/wichtig für ESCAPE?

Die Sudie betont die Bedeutung frühzeitiger Bildung im Bereich Cybersicherheit und legt den Fokus auf grundlegendes Bewusstsein und digitale Bürgerkompetenz bei Jugendlichen – eine oft übersehene, aber entscheidende Zielgruppe für langfristige Cyberresilienz.

Co-funded by the European Union

Das Projekt „ESCAPE: Vorbereitung von Angehörigen der Gesundheitsberufe auf Cyberangriffe“ wird von der Europäischen Union kofinanziert. Die in diesem Protokoll geäußerten Meinungen und Standpunkte sind ausschließlich für den/die Autor(en) (ESCAPE-Konsortium) verbindlich und spiegeln nicht unbedingt die Meinung der Europäischen Union oder des Servicio Español para la Internacionalización de la Educación (SEPIE) wider. Weder die Europäische Union noch die Nationale Agentur SEPIE können dafür verantwortlich gemacht werden.

ESCAPE: Gesundheitsfachkräfte auf Cyberangriffe vorbereiten	
Eine integrierte kybernetische Bewusstseinsstrategie zur Bewertung von Einstellungen und Verhaltensweisen zur Cybersicherheit im schulischen Kontext	
Sprache	*Englisch*

Sie bietet praxisnahe Werkzeuge – validierte Fragebögen, ein Selbsteinschätzungsinstrument und sofort einsetzbare Unterrichtspläne – für Lehrkräfte, die direkt im Unterricht verwendet werden können.

Darüber hinaus fördert die Strategie die Integration von Cybersicherheitsbildung in bestehende Lehrpläne der Fächer IKT und Staatsbürgerkunde und unterstützt damit eine nachhaltige und skalierbare Umsetzung.

3.3. Erkenntnisse

Bildungsstrategie im Detail:
Die Studie hebt hervor, dass Schulen der zunehmenden digitalen Exposition junger Menschen durch die Förderung von Cybersicherheitsbewusstsein als Teil ihrer digitalen Bildung begegnen müssen.
Zielgruppe: Schüler*innen der Sekundarstufe I (6. und 9. Klasse).
Behandelte Risiken: Riskantes Online-Verhalten und problematische Einstellungen infolge mangelnden Bewusstseins bei sogenannten „digital natives“.
Vorgeschlagene Lösungen:

- Fragebögen zur Bewertung von Einstellungen und Verhaltensweisen.
- Ein Selbstdiagnose-Tool, das Schüler*innen hilft, ihre eigene Cybersicherheitskompetenz zu reflektieren.
- Ein Unterrichtsplan, der in den Fächern IKT und Staatsbürgerkunde umgesetzt werden kann.

Hinweise zur Umsetzung:

- Verwendung von globalen und individuellen Auswertungen (z. B. Histogrammen), um Lernfortschritte zu verfolgen und gezielte Unterstützung zu ermöglichen.
- Integration von Selbstreflexion und Gruppendiskussionen, um den Lerneffekt zu vertiefen.

4. Direkter Link zum Material

Abrufbar über *Angewandte Wissenschaften*(MDPI): Artikelnummer 11269, Band 11 (23), 2021https://www.mdpi.com/2076-3417/11/23/11269

Co-funded by the European Union

Das Projekt „ESCAPE: Vorbereitung von Angehörigen der Gesundheitsberufe auf Cyberangriffe“ wird von der Europäischen Union kofinanziert. Die in diesem Protokoll geäußerten Meinungen und Standpunkte sind ausschließlich für den/die Autor(en) (ESCAPE-Konsortium) verbindlich und spiegeln nicht unbedingt die Meinung der Europäischen Union oder des Servicio Español para la Internacionalización de la Educación (SEPIE) wider. Weder die Europäische Union noch die Nationale Agentur SEPIE können dafür verantwortlich gemacht werden.

ESCAPE: Gesundheitsfachkräfte auf Cyberangriffe vorbereiten	
Eine integrierte kybernetische Bewusstseinsstrategie zur Bewertung von Einstellungen und Verhaltensweisen zur Cybersicherheit im schulischen Kontext	
Sprache	*Englisch*

5. Weiterführende Materialien (optional)

Verwandte MDPI-Publikationen:

- Adaptive Schulungsmechanismen für Cybersicherheit mithilfe pädagogischer Modellierung.
- Studien zur Bewertung des Cybersicherheitsbewusstseins bei Universitätsstudierenden.
- Forschung zu menschlichem Verhalten und Frameworks für Cybersicherheitsbewusstsein.

Co-funded by the European Union

Das Projekt „ESCAPE: Vorbereitung von Angehörigen der Gesundheitsberufe auf Cyberangriffe“ wird von der Europäischen Union kofinanziert. Die in diesem Protokoll geäußerten Meinungen und Standpunkte sind ausschließlich für den/die Autor(en) (ESCAPE-Konsortium) verbindlich und spiegeln nicht unbedingt die Meinung der Europäischen Union oder des Servicio Español para la Internacionalización de la Educación (SEPIE) wider. Weder die Europäische Union noch die Nationale Agentur SEPIE können dafür verantwortlich gemacht werden.