ESCAPE:

Gesundheitsfachkräfte auf Cyberangriffe vorbereiten

Material für Lernende

Eine kritische Analyse von Frameworks und Trainingsmodellen zur

Cybersicherheitsbewusstseinsförderung

ESCAPE: Gesundheitsfachkräfte auf Cyberangriffe vorbereiten	
Eine kritische Analyse von Frameworks und Trainingsmodellen zur Cybersicherheitsbewusstseinsförderung	
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 für ESCAPE relevant/wichtig..... 4
3.3. Erkenntnisse..... 4
4. Direktlink zum Material..... 5
5. Weitere Ressourcen (optional)..... 5

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 kritische Analyse von Frameworks und Trainingsmodellen zur Cybersicherheitsbewusstseinsförderung	
Sprache	*Englisch*

1. Name des Materials und Beschreibung

Diese Open-Access-Studie bietet eine quantitative Übersicht über verschiedene Ansätze zur Förderung des Cybersicherheitsbewusstseins und zur Durchführung von Schulungsmaßnahmen. Sie versteht diese Programme als strategische Initiativen, die Sicherheitsvorfälle und organisatorische Kosten reduzieren, während sie gleichzeitig die Resilienz und die gesamte Sicherheitslage von Organisationen verbessern. Die Analyse legt den Schwerpunkt auf reale Belege für die Wirksamkeit strukturierter Sensibilisierungs- und Trainingsprogramme.

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 kritische Analyse von Frameworks und Trainingsmodellen zur Cybersicherheitsbewusstseinsförderung	
Sprache	*Englisch*

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

3. Beschreibung

Diese evidenzbasierte Literaturübersicht wendet quantitative Methoden an, um Frameworks und Schulungsmodelle zum Cybersicherheitsbewusstsein hinsichtlich Kostenreduktion, Vorfallprävention und Förderung organisatorischer Resilienz zu bewerten.

3.1. Herkunft

Autor: Hamed Taherdoost

Veröffentlichung: Procedia Computer Science, Band 235, April 2024, Seiten 1649–1663. Open-Access-Publikation unter einer Creative-Commons-Lizenz.

3.2. Warum ist es wichtig/relevant für ESCAPE?

Quantitative Bewertung: Die Studie bietet Entscheidungsträgern ein fundiertes, datenbasiertes Verständnis darüber, welche Schulungs- und Sensibilisierungsmethoden tatsächlich die organisatorische Resilienz verbessern.

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 kritische Analyse von Frameworks und Trainingsmodellen zur Cybersicherheitsbewusstseinsförderung	
Sprache	*Englisch*

Strategische Erkenntnisse: Sie zeigt, dass strukturierte Sensibilisierungsinitiativen nicht nur Sicherheitsvorfälle und Kosten verringern, sondern auch als Katalysatoren für die Entwicklung von Cyber-Resilienz dienen – ein klarer Mehrwert für Organisationen, die Schulungsmaßnahmen im Bereich Cybersicherheit gestalten oder evaluieren.

3.3. Erkenntnisse

Ergebnisse der Analyse:
Die Studie betont, dass klar strukturierte Frameworks und Trainingsprogramme zur Förderung des Cybersicherheitsbewusstseins messbare Verbesserungen der Sicherheitslage und Kosteneffizienz erzielen können.
Zielgruppe: Führungskräfte, Verantwortliche für Schulungsentwicklung sowie politische Entscheidungsträger, die in evidenzbasierte und wirksame Cybersicherheitsausbildung investieren möchten.
Behandelte Risiken: Ineffiziente Schulungsmaßnahmen, steigende Zahl von Sicherheitsvorfällen und fehlende Nachweise über den tatsächlichen Nutzen von Sensibilisierungsprogrammen.
Vorgeschlagene Lösungen: Bewertung und Auswahl von Trainingsmethoden auf Grundlage quantitativer Ergebnisse, um Investitionen gezielt auf Ansätze zu lenken, die nachweislich Risiken und Kosten reduzieren.

Hinweise zur Umsetzung:

- Nutzung quantitativer Kennzahlen zur Bewertung der Wirksamkeit von Trainingsmaßnahmen (z. B. Veränderung der Vorfallraten, Kosteneinsparungen).
- Einbindung messbarer Ziele in Awareness-Initiativen, um Ressourceneinsatz und Nutzen nachvollziehbar zu belegen.

4. Direkter Link zum Material

Abrufbar über *Procedia Informatik*, Band 235 (2024), Seiten 1649–1663. DOI: 10.1016/j.procs.2024.04.156https://www.sciencedirect.com/science/article/pii/S1877050924008329?via%3Dihub

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.

5. Weiterführende Materialien (optional)

Verwandte Frameworks und Evaluierungen

Taherdoosts weiterführende Analyse von Cybersicherheits-Frameworks und Standards (2022)

Vergleichsstudien zu Schulungsmodellen und -fähigkeiten in verschiedenen Sektoren

Theoretische und interdisziplinäre Ansätze zu menschenzentrierter Cybersicherheit, die Verhaltens-, Sozial- und Organisationsdimensionen einbeziehen

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.