ESCAPE:

Vorbereitung von Gesundheitsfachkräften auf Cyberangriffe

Material für Lernende

Webseminare zu zentralen Aspekten der Cybersicherheit

ESCAPE: Vorbereitung von Gesundheitsfachkräften auf Cyberangriffe	
Webseminare zu zentralen Aspekten der Cybersicherheit	
Sprache	Spanisch

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

„Seminarios web sobre aspectos clave de la ciberseguridad“ (Webseminare zu zentralen Aspekten der Cybersicherheit). Diese Videoveröffentlichungen wurden entwickelt, um Wissen und technische Grundlagen der Cybersicherheit anschaulich und zugänglich zu vermitteln.

1. Klassifizierung

Kategorie	Zutreffendes markieren
Sektor	☐ Gesundheitswesen
	☑ Allgemeinheit
	☐ Andere
Behandelte Themen	☑ Cybersicherheit
	☐ Datenschutz
Situationstyp	☑ Prävention
	☐ Auswirkungen

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: Vorbereitung von Gesundheitsfachkräften auf Cyberangriffe	
Webseminare zu zentralen Aspekten der Cybersicherheit	
Sprache	Spanisch

	☐ Auswirkungen auf alle anderen Aktivitäten, die nicht die direkte Patientenversorgung betreffen.
Sprache der Originalmaterialien	☐ Niederländisch
	☐ Englisch
	☐ Deutsch
	☐ Italienisch
	☑ Spanisch
Art des Materials	☑ Richtlinien oder Handbücher
	☐ Fallbeispiele
	☐ Schulungen
	☐ Sonstige

2. Beschreibung

Dieses Material bietet eine Reihe von Tutorial-Videos, in denen verschiedene Aspekte der Cybersicherheit vorgestellt werden, die für die Anwendung sicherer Praktiken von Bedeutung sind. Ziel ist es, auf leicht verständliche Weise Wissen zu vermitteln, das zur Verbesserung der digitalen Sicherheit in Organisationen beiträgt.

2.1. Herkunft

Das Material wurde von INCIBE, der spanischen Nationalen Agentur für Cybersicherheit, entwickelt. Sie ist eine öffentliche Einrichtung, die dem Ministerium für digitale Transformation und wirtschaftliche Angelegenheitenunterstellt ist. INCIBE gilt als zentrale Referenzinstitution in Spanien für die Entwicklung der Cybersicherheit, die Stärkung des digitalen Vertrauens der Bürgerinnen und Bürger sowie für Forschung und Ausbildung in diesem Bereich.

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: Vorbereitung von Gesundheitsfachkräften auf Cyberangriffe	
Webseminare zu zentralen Aspekten der Cybersicherheit	
Sprache	Spanisch

2.2. Warum ist es für ESCAPE relevant/wichtig?

Dieses Material ist für das ESCAPE-Projekt von hoher Relevanz, da es die Bedeutung der Cybersicherheit für den Schutz sensibler Patientendaten und unternehmensinterner Informationen hervorhebt. Es zeigt, dass übliche Sicherheitsmaßnahmen wie Antivirensoftware oder Backups allein nicht ausreichen, um die Integrität vertraulicher Daten zu gewährleisten. Stattdessen betont es die Wichtigkeit eines strukturierten Sicherheitsplans und vermittelt praktische Hinweise, um die Cybersicherheitsstandards deutlich zu erhöhen.

2.3. Erkenntnisse

Das Material führt in verschiedene Werkzeuge und Methoden zur Verbesserung der Cybersicherheit ein. Es richtet sich an System- und Netzwerkadministratorinnen und -administratoren, Supporttechnikerinnen und -techniker sowie andere IT-Fachkräfte. Thematisiert werden Risiken wie Probleme im Netzwerkverkehr, unsichere WLAN-Verbindungen, Softwareschwachstellen, Phishing, das Teilen von Passwörtern, ungeschützte Arbeitsstationen, offenliegende sensible Dokumente, Datenlecks, veraltete oder unzureichend geschützte Software, Ransomware, das Abfangen von Datenpaketen („Packet Sniffing“), „Man-in-the-Middle“-Angriffe und MAC-Spoofing.

Zur Risikominimierung empfiehlt das Material den Einsatz von Analyse- und Sicherheitswerkzeugen wie Wireshark, Snort IDS oder Owas-Zap, die Stärkung der WLAN-Sicherheit, die sichere App-Entwicklung, die Erkennung von Phishing-Versuchen, die Nutzung von Verschlüsselungstechnologien, den Aufbau sicherer Netzwerke sowie die Sensibilisierung der Nutzerinnen und Nutzer.

Weitere Maßnahmen betreffen das regelmäßige Aktualisieren von Firmware, das Verbergen der SSID, die Aktivierung von Gastnetzwerken, die Begrenzung des IP-Adressbereichs, die Reduzierung der Signalstärke von Zugangspunkten, den Wechsel von Standardpasswörtern, die Verschlüsselung von Daten und die Implementierung von Richtlinien für Software-Updates. Ergänzend wird die kontinuierliche Schulung von Mitarbeitenden empfohlen.

Besondere Aufmerksamkeit gilt der Passwortsicherheit. Das Material rät, Passwörter niemals zu teilen, starke und unterschiedliche Passwörter zu erstellen, diese regelmäßig zu ändern und digitale Passwortmanager wie KeePass oder Bitwarden zu verwenden. Zudem wird empfohlen, auf „Passwort merken“- oder „Angemeldet bleiben“-Funktionen zu verzichten und Zwei-Faktor-Authentifizierung zu aktivieren.

Das Material weist außerdem darauf hin, Ressourcenfreigaben oder automatische Synchronisierungen vor dem Verbinden mit unsicheren Netzwerken zu deaktivieren, das

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.

Verhalten innerhalb des Netzwerks zu überwachen, verdächtige Zugriffe mit einem Intrusion Detection System zu erkennen sowie Standardkonfigurationen zu überprüfen und eine Politik der minimalen Exposition umzusetzen.

3. Direkter Link zum Material

https://www.incibe.es/incibe-cert/publicaciones/seminarios-web

4. Weiterführende Materialien (Optional)

Das Material enthält zahlreiche weiterführende Links zu spezifischen Themen und zusätzlichen Inhalten zur Vertiefung.

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.