ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles para estudiantes

Cuestionario de ciberseguridad: Brecha, Ataque ransom, ataque por email, Tierra de las estafas y NFT

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cuestionario de ciberseguridad: Brecha, ataque ransom, ataque por email, tierra de las estafas y NFT	
Idioma	*Español*

Índice

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cuestionario de ciberseguridad: Brecha, ataque ransom, ataque por email, tierra de las estafas y NFT	
Idioma	*Español*

1. Cuestionario de ciberseguridad: Brecha, ataque ransom, ataque por email, tierra de las estafas y NFT

Este conjunto de minijuegos interactivos enseña los conceptos básicos sobre amenazas cibernéticas, incluyendo violaciones de datos, ransomware, phishing y estafas relacionadas con NFTs.

2. Clasificación

Categoría	**Marcar si aplica:**
Sector	☐ Sanitario
	☑ Público general
	☐ Otro
Temas cubiertos	☑ Ciberseguridad
	☐ Protección de datos
Tipo de situación	☑ Prevención
	☐ Impacto (ej. Cuando está ocurriendo o ha ocurrido) en el cuidado del paciente
	☐ Impacto en otras actividades que no implican el cuidado del paciente
Idioma del material original	☐ Neerlandés
	☑ Inglés

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cuestionario de ciberseguridad: Brecha, ataque ransom, ataque por email, tierra de las estafas y NFT	
Idioma	*Español*

	☐ Alemán
	☐ Italiano
	☐ Español
Tipo del material	☑ Preguntas de cuestionario.
	☐ Juegos
	☐ Aplicaciones y vídeos interactivos
	☐ Listas de verificación

3. Descripción

1. ¿Qué es una violación de datos (*data breach*)?

   a) Almacenamiento seguro de archivos

   b) Acceso no autorizado a datos

   c) Copia de seguridad normal

   d) Internet lento

   Respuesta correcta: Acceso no autorizado a datos
   Feedback: Una violación expone información **sensible o confidencial**.

2. ¿Cuál es el objetivo del ransomware?

   a) Borrar datos permanentemente

   b) Bloquear sistemas hasta que se pague un rescate

   c) Acelerar la red

   d) Instalar antivirus

   Respuesta correcta: Bloquear sistemas hasta que se pague un rescate
   Feedback: El ransomware **extorsiona dinero bloqueando el acceso a los archivos o sistemas**.

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

3. ¿Cuál es una señal de phishing?

   a) Solicitar inicio de sesión mediante un enlace

   b) Ortografía correcta

   c) Firma del personal interno

   d) Horario laboral normal

   Respuesta correcta: Solicitar inicio de sesión mediante un enlace
   Feedback: El *phishing* engaña a los usuarios para **revelar información confidencial**.

4. NFT significa:

   a) Non-Fungible Token

   b) New File Transfer

   c) Network Firewall Tool

   d) Node Functional Test

   Respuesta correcta: Non-Fungible Token
   Feedback: Los NFTs son **activos digitales únicos basados en blockchain**.

5. ¿Por qué comprobar los enlaces antes de hacer clic?

   a) Para evitar sitios web maliciosos

   b) Para mejorar la velocidad del PC

   c) Para cargar más rápido

   d) Para obtener mejores resultados de búsqueda

   Respuesta correcta: Para evitar sitios web maliciosos
   Feedback: Los enlaces falsos suelen **propagar malware o estafas**.

4. Más información

- Fuente: Education Arcade Cybersecurity Games

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.