ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles para estudiantes

Amenazas digitales en el ámbito sanitario

ESCAPE: Preparing healthcare professionals for cyberattacks	
Amenazas digitales en el ámbito sanitario	
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	
Amenazas digitales en el ámbito sanitario	
Idioma	*Español*

1. Amenazas digitales en el ámbito sanitario

Esta ficha contiene cinco preguntas tipo test destinadas a mejorar la concienciación sobre ciberseguridad entre los profesionales sanitarios. Se centra en amenazas comunes como el phishing, el ransomware, el malware y las prácticas poco seguras en el lugar de trabajo. Las preguntas se basan en contenido interactivo del sitio web educativo cybersecurityquiz.app.ovosplay.com, que presenta temas clave de ciberseguridad mediante cuestionarios prácticos y escenarios realistas.

2. Clasificación

Categoría	Marcar lo que corresponda
Sector	☑ Sanitario
	☑ **General**
Temas cubiertos	☐ Ciberseguridad
	☐ Protección de datos
Tipo de situación	☑ **Prevención**
	☐ Impacto directo sobre la atención al paciente.
	☐ Impacto sobre otras actividades que no implican atención directa al paciente
Idioma de los materiales originales	☐ Neerlandés
	☑ Inglés
	☑ **Alemán**
	☑ Italiano
	☐ Español
Tipo de material	☑ **Preguntas tipo test**

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	
Amenazas digitales en el ámbito sanitario	
Idioma	*Español*

	☐ Juegos
	☐ Aplicaciones y vídeos interactivos
	☑ **Listas de verificación**

3. Preguntas del cuestionario

1) ¿Qué puede hacer el malware una vez que ha infectado el sistema informático de un hospital?

a. Instalar automáticamente actualizaciones útiles de software médico.

b. Mejorar la velocidad de Internet para acceder más rápido a los historiales de pacientes.

c. Cifrar o eliminar datos importantes, interrumpir servicios o espiar a los usuarios.

d. Optimizar el consumo energético de los dispositivos médicos.

Respuesta correcta: c. Cifrar o eliminar datos importantes, interrumpir servicios o espiar a los usuarios.

Comentario: El malware puede causar grandes trastornos en los centros sanitarios. Puede cifrar archivos (ransomware), destruir datos, interrumpir el acceso a los historiales de los pacientes o permitir que los ciberdelincuentes espíen las actividades del personal. Esto supone graves riesgos para la atención al paciente y la protección de datos.

2) ¿Cuál de las siguientes NO es una forma fiable de detectar una notificación de correo falsa?

a. Revisar la dirección del remitente y el contenido del mensaje en busca de incoherencias.

b. Comprobar si los archivos adjuntos son inusuales (por ejemplo, .exe, .zip).

c. Prestar atención a saludos impersonales como 'Estimado usuario'.

d. Ignorar las advertencias del sistema si el correo parece profesional.

Respuesta correcta: d. Ignorar las advertencias del sistema si el correo parece profesional.

Comentario: Las notificaciones falsas suelen parecer muy profesionales, pero las advertencias del sistema son fundamentales. Si tu programa de correo marca un mensaje como sospechoso, tómatelo en serio. El diseño y el formato pueden ser engañosos.

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) ¿Qué es el ransomware y cómo afecta a las instituciones sanitarias?

a. Un antivirus gratuito utilizado para prevenir el robo de datos en clínicas.

b. Una extensión del navegador que bloquea sitios web inseguros.

c. Un tipo de malware que cifra los datos y exige un pago para restaurar el acceso.

d. Un protocolo legal para las copias de seguridad y la recuperación de datos hospitalarios.

Respuesta correcta: c. Un tipo de malware que cifra los datos y exige un pago para restaurar el acceso.

Comentario: El ransomware bloquea archivos o sistemas completos mediante cifrado y exige un rescate para desbloquearlos. En el ámbito sanitario, puede impedir el acceso a los historiales de pacientes o a sistemas críticos, poniendo en riesgo las vidas de los pacientes y la continuidad asistencial.

4) ¿Por qué son tan importantes las actualizaciones periódicas de los sistemas informáticos hospitalarios para la ciberseguridad?

a. Porque corrigen vulnerabilidades de seguridad conocidas y mejoran la estabilidad del sistema.
b. Porque añaden nuevos colores y diseños a la interfaz.
c. Porque restablecen las contraseñas con frecuencia para confundir a los ciberdelincuentes.
d. Porque son necesarias para mantener el funcionamiento del Wi-Fi del hospital.

Respuesta correcta: a. Porque corrigen vulnerabilidades de seguridad conocidas y mejoran la estabilidad del sistema.

Comentario: Las actualizaciones del software cierran brechas de seguridad que los hackers podrían aprovechar. En el ámbito sanitario, los sistemas obsoletos suponen riesgos graves, desde el robo de datos hasta fallos durante tratamientos críticos.

5) ¿Qué es el phishing y por qué es peligroso en el entorno sanitario?

a. Un método para limpiar los historiales de pacientes obsoletos.

b. Un ciberataque en el que se utilizan mensajes falsos para robar información sensible.

c. Un sistema de inicio de sesión seguro para el acceso médico remoto.

d. Una actualización rutinaria del antivirus del hospital.

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.

Respuesta correcta: b. Un ciberataque en el que se utilizan mensajes falsos para robar información sensible.

Comentario: Los ataques de phishing utilizan correos o mensajes falsos para engañar al personal y conseguir las credenciales de acceso o instalar malware. En el entorno sanitario, pueden permitir accesos no autorizados a datos de pacientes o interrumpir los sistemas clínicos.

4. Más información

Las preguntas del cuestionario se han adaptado de la plataforma oficial de aprendizaje en ciberseguridad disponible en cybersecurityquiz.app.ovosplay.com. El contenido interactivo ha sido desarrollado por varias instituciones austriacas, incluido el Ministerio Federal de Educación, Ciencia e Investigación de Austria, junto con otros socios educativos y de ciberseguridad. La plataforma presenta escenarios reales de ciberseguridad en formato de cuestionario y tiene como objetivo aumentar la concienciación sobre las amenazas digitales entre los usuarios finales. Aunque no fue diseñado originalmente para el ámbito sanitario, el material de esta ficha se ha adaptado para contribuir a la formación de los profesionales de la salud. El acceso a la plataforma es gratuito, aunque requiere la creación de una cuenta personal. Todo el contenido es de acceso público y está diseñado para promover comportamientos digitales seguros en todos los sectores.

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.