ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles para estudiantes

¿Cuánto sabes sobre ciberseguridad?

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Cuánto sabes sobre ciberseguridad?	
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	
¿Cuánto sabes sobre ciberseguridad?	
Idioma	Español

1) ¿Cuánto sabes sobre ciberseguridad?

Este rompecabezas consta de cinco preguntas relacionadas con los distintos ataques que pueden producirse en una entidad sanitaria. Elige con prudencia para proteger adecuadamente tus datos valiosos frente a los ciberdelincuentes.

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
	☐ Alemán

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	
¿Cuánto sabes sobre ciberseguridad?	
Idioma	Español

	☐ Italiano
	☐ Español (versión en vídeo disponible)
Tipo del material	☑ Preguntas de cuestionario.
	☐ Juegos
	☐ Aplicaciones y vídeos interactivos
	☐ Listas de verificación

3) Preguntas

1) ¿Cuál de las siguientes actividades no es segura al navegar por Internet con tu ordenador de trabajo en el hospital?
    a) Verificar la autenticidad de los enlaces antes de hacer clic en ellos.
    b) Comprar en sitios oficiales.
    c) Descargar aplicaciones desde tiendas oficiales.
    d) Descargar programas o archivos desde enlaces o fuentes desconocidas.

Respuesta correcta: Descargar programas o archivos desde enlaces o fuentes desconocidas.

Feedback: Aunque ninguna de las opciones es recomendable durante la jornada laboral, la opción correcta es la número 4, ya que las descargas procedentes de enlaces o fuentes desconocidas pueden contener *malware*, *ransomware* o software no autorizado que comprometa la red del hospital y la confidencialidad de los datos de los pacientes. Verificar la autenticidad de los enlaces y utilizar fuentes oficiales reduce los riesgos y protege la integridad de la información.

2) ¿Cómo crearías una contraseña segura?
    a) Generando una contraseña larga (más de 14 caracteres).
    b) Utilizando una contraseña diferente para cada plataforma en línea.
    c) No compartiéndola con nadie.
    d) Restaurando las copias de seguridad en nuevos dispositivos y reanudando el trabajo.
    e) Todas las opciones anteriores.

Respuesta correcta: Todas las opciones anteriores.

Feedback: Una contraseña segura debe ser larga (más de 14 caracteres), única para cada plataforma, no compartirse con nadie y combinar letras mayúsculas y minúsculas, números y símbolos. Cada uno de estos elementos reduce la probabilidad de ataques por adivinación o reutilización de credenciales, contribuyendo a la protección de los datos de los pacientes y de los sistemas del hospital.

3) Si recibo un mensaje con un enlace, ¿cuál de las siguientes afirmaciones es correcta?

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.

a) Copio el enlace y lo analizo con un verificador de URL.
b) Compruebo si el texto del enlace coincide con la web oficial.
c) Todas las anteriores son correctas.
d) Hago clic en el enlace para ver a dónde lleva.

Respuesta correcta: Todas las anteriores son correctas.

Feedback: Todas las acciones enumeradas son prudentes: analizar el enlace puede revelar dominios falsos o maliciosos, y comprobar si el texto del enlace coincide con la dirección oficial ayuda a detectar intentos de suplantación (*spoofing*). Hacer clic directamente sin verificar nunca es recomendable. En conjunto, estas prácticas reducen el riesgo de *phishing* y protegen los sistemas y datos de los pacientes.

4) Indica la afirmación que te parece correcta:
   a) Un antivirus solo es útil en dispositivos y sistemas antiguos.
   b) Junto con el antivirus, las actualizaciones son necesarias.
   c) El antivirus solo detecta vulnerabilidades.
   d) El antivirus detecta todos los virus y los elimina automáticamente.

Respuesta correcta: Junto con el antivirus, las actualizaciones son necesarias.

Feedback: El software antivirus requiere actualizaciones periódicas de firmas y heurísticas para reconocer nuevas amenazas. Ningún antivirus detecta “todos” los virus ni los elimina automáticamente sin intervención. Las actualizaciones mejoran la detección y la capacidad de respuesta ante incidentes.

La afirmación 1 es incorrecta (el antivirus no es solo útil en sistemas antiguos); la 3 también (los antivirus no se limitan a detectar vulnerabilidades, sino que identifican y bloquean *malware*); y la 4 es falsa porque no garantiza la eliminación automática de todas las amenazas.

5) Un auxiliar de farmacia está aprendiendo sobre amenazas de ciberseguridad. ¿Cuál de las siguientes opciones describe mejor el *ransomware*?
   a) Un tipo de software malicioso que recopila en secreto los datos personales de los clientes con fines publicitarios.
   b) Un programa malicioso que cifra archivos o sistemas y exige un pago (rescate) para restaurar el acceso.
   c) Un virus informático que actualiza automáticamente el software de la farmacia sin permiso.
   d) Un correo electrónico fraudulento que intenta engañar al personal de farmacia para que comparta contraseñas.

Respuesta correcta: Un programa malicioso que cifra archivos o sistemas y exige un pago (rescate) para restaurar el acceso.

Feedback: Ransomware is a type of malware that locks or encrypts a victim’s files or systems, making them inaccessible. The attacker then demands money (the ransom) to unlock them.

El *ransomware* es un tipo de *malware* que bloquea o cifra los archivos o sistemas de la víctima, impidiendo el acceso. El atacante exige un pago (el rescate) para desbloquearlos.

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.

Por ejemplo, en una farmacia, el *ransomware* podría cifrar la base de datos que contiene las prescripciones o historiales médicos de los pacientes, impidiendo al personal acceder a información esencial. Esta interrupción podría detener la dispensación de medicamentos hasta que se pague el rescate o se restauren los sistemas desde copias de seguridad.

4) More information

Estas preguntas han sido inspiradas y adaptadas al sector sanitario a partir de los escenarios presentados por el INCIBE en la siguiente página web: https://www.incibe.es/menores/juegos/cyberscouts. Este material se encuentra publicado en español, dado que el INCIBE (Instituto Nacional de Ciberseguridad) es una institución española.

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.