ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles para estudiantes

Concienciación en Seguridad Digital

ESCAPE: Preparing healthcare professionals for cyberattacks	
Concienciación en seguridad digital	
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	
Concienciación en seguridad digital	
Idioma	*Español*

1. Concienciación en seguridad digital – Clases de la plataforma DiFü Learning

Esta hoja informativa contiene cinco preguntas de prueba para aumentar la conciencia básica sobre las amenazas a la ciberseguridad en entornos de atención médica. Todas las preguntas están adaptadas del curso de aprendizaje electrónico público y gratuito "Gefahrenschutz" (https://difue.de/lernzentrale/privat/level1/gefahrenschutz/) proporcionada por la plataforma Digitalführerschein (DiFü).

2. Clasificación

Categoría	Marca si aplica
Sector	☑ **Sanitario**
	☐ General
Temas cubiertos	☐ Ciberseguridad
	☐ Protección de datos
Tipo de situación	☑ **Prevención**
	☐ Impacto (por ejemplo cuando está ocurriendo o ha ocurrido) sobre el cuidado del paciente.
	☐ Impacto sobre todas las demás actividades que no impliquen atención directa al paciente.
Idioma de los materiales originales	☐ Neerlandés
	☐ Inglés
	☑ **Alemán**
	☐ Italiano

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	
Concienciación en seguridad digital	
Idioma	*Español*

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

3. Preguntas del cuestionario

1. Estás utilizando un smartphone o una tableta de trabajo. Durante una reunión de equipo, una compañera te habla de una aplicación que usa en privado para gestionar sus planes de medicación. ¿Qué deberías tener en cuenta antes de instalar dicha aplicación en tu dispositivo del trabajo?

   a. Prueba la aplicación ahora mismo. Las recomendaciones de tus colegas suelen ser confiables.

   b. Otorga todos los permisos para garantizar que la aplicación funcione sin problemas.

   c. Verifica qué datos solicita la aplicación y si provienen de una fuente confiable.

   d. Instala la aplicación a través de un enlace que encontres en un foro de discusión.

Respuesta correcta: c. Verifica qué datos solicita la aplicación y si provienen de una fuente confiable.

Comentarios: Las aplicaciones suelen solicitar acceso a información confidencial, como contactos, ubicación o archivos almacenados. En entornos sanitarios, instalar únicamente aplicaciones confiables y verificadas, es fundamental para proteger los datos de los pacientes y garantizar el cumplimiento de la normativa de protección de datos.

2. Recibes las credenciales de acceso para un nuevo sistema de documentación utilizado en la atención al paciente. Se te solicita que establezcas una contraseña. ¿Qué tipo de contraseña debería evitar por razones de seguridad?

   a. Una contraseña larga con letras mayúsculas y minúsculas, números y símbolos.

   b. Una contraseña que incluya tu fecha de nacimiento o el nombre de su hijo.

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.

c. Una contraseña generada aleatoriamente almacenada en un administrador de contraseñas.

d. Una contraseña que se cambia periódicamente.

Respuesta correcta: b. Una contraseña que incluya tu fecha de nacimiento o el nombre de tu hijo.

Comentarios: La información personal suele ser fácil de adivinar o encontrar en línea. El uso de contraseñas seguras y únicas es fundamental para evitar el acceso no autorizado a los sistemas clínicos.

3. Mientras trabajas desde casa, accedes a los historiales de tus pacientes a través de un portal web. Algo en la dirección del sitio web parece extraño. ¿Cuál es una señal clara de que un sitio web puede ser inseguro?

   a. El sitio está disponible en alemán.

   b. Presenta imágenes médicas y parece profesional.

   c. La URL comienza con “http://” instead of “https://”.

   d. Se carga inusualmente rápido

Respuesta correcta: c. La URL empieza con «http://» en lugar de «https://».

Comentarios: Los sitios web seguros utilizan cifrado y siempre comienzan con "https://". Los sitios web sin cifrado transmiten datos en texto plano, lo que supone un grave riesgo, especialmente al manejar información médica confidencial.

4. Una de los ordenadores de su unidad muestra una ventana emergente que le recuerda instalar una actualización de seguridad para una aplicación médica. ¿Por qué es arriesgado posponer las actualizaciones de software en un entorno sanitario?

   a. La interfaz puede parecer obsoleta.

   b. La actualización podría ralentizar el dispositivo.

   c. Los hackers podrían aprovechar vulnerabilidades de seguridad conocidas.

   d. Es posible que el dispositivo ya no sea compatible con su teclado o ratón.

Respuesta correcta: c. Los hackers podrían explotar vulnerabilidades de seguridad conocidas.

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.

Comentarios: Las actualizaciones de software solucionan vulnerabilidades de seguridad que los atacantes podrían explotar. Retrasar las actualizaciones puede dejar los sistemas clínicos vulnerables al malware y al acceso no autorizado.

5. Recibes un correo electrónico con el asunto "URGENTE: Restablecer su contraseña", que supuestamente proviene del departamento de informática de su hospital. El mensaje incluye un enlace. ¿Qué indica que podría tratarse de un intento de phishing?

   a. El mensaje fue enviado después de que terminó su turno.

   b. Menciona una fiesta del personal.

   c. Le pide que ingrese sus credenciales de inicio de sesión a través de un enlace.

   d. La dirección del remitente incluye el nombre del hospital.

Respuesta correcta: c. Le pide que ingrese sus credenciales de inicio de sesión a través de un enlace.

Comentarios: Los correos electrónicos de phishing suelen parecer legítimos y usar nombres o logotipos conocidos. Solicitar credenciales de inicio de sesión mediante un correo electrónico inesperado es una táctica común para robar datos confidenciales.

4. Más información

Estas preguntas del cuestionario están adaptadas del módulo gratuito de aprendizaje electrónico "Gefahrenschutz" de la plataforma Digitalführerschein (DiFü). El material está disponible gratuitamente en: https://difue.de/lernzentrale/privat/level1/gefahrenschutz/. El curso ofrece orientación práctica sobre ciberseguridad para la vida digital cotidiana y ha sido desarrollado por instituciones públicas y educativas en Alemania. Todos los escenarios de esta hoja informativa se han contextualizado para reflejar los desafíos de seguridad digital en entornos de atención médica.

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.