ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles para estudiantes

El eslabón más débil. Parte 2

ESCAPE: Preparar a los profesionales sanitarios para los ciberataques.	
El eslabón más débil - Parte 2	
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: Preparar a los profesionales sanitarios para los ciberataques.	
El eslabón más débil - Parte 2	
Idioma	*Español*

1. El eslabón más débil - Parte 2

Este puzzle consta de 5 nuevas preguntas cuyo objetivo es educar a los usuarios sobre los riesgos de seguridad en el entorno laboral del sector sanitario. El propósito es ayudar a los usuarios a evitar convertirse en 'el eslabón más débil' de la cadena de seguridad.

2. Clasificación

Categoría	**Marcar lo que corresponda**
Sector	☑ Sanitario
	☑ General
Temas tratados	☑ Ciberseguridad
	☑ Protección de datos
Tipo de situación	☑ Prevención
	☑ Impacto en la atención al paciente
	☑ Impacto en todas las demás actividades que no impliquen atención directa al paciente
Idioma de los materiales originales	☐ Holandés
	☑ Inglés
	☐ Alemán
	☐ Italiano
	☐ Español
Tipo de material	☑ Preguntas de cuestionario
	☐ Juegos

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: Preparar a los profesionales sanitarios para los ciberataques.	
El eslabón más débil - Parte 2	
Idioma	*Español*

	☐ Aplicaciones y vídeos interactivos
	☐ Listas de verificación

3. Preguntas del cuestionario

Es tu primera semana como asistente de farmacia en un hospital. También debes aprender las prácticas de ciberseguridad de la farmacia.

1. Recibes tu teléfono de trabajo. No está protegido con contraseña ni con seguridad biométrica.

¿Qué haces?

A. Bloqueas manualmente la pantalla cuando no lo estás usando. Es más rápido sin contraseña.

B. Configuras un código simple como 1234 para trabajar más rápido.

C. Configuras un código fuerte o bloqueo biométrico de acuerdo con la política del hospital.

D. Usas tu teléfono personal y dejas el teléfono de trabajo en tu casillero.

Respuesta correcta: C

Comentario: Los dispositivos de trabajo siempre deben estar protegidos con contraseñas fuertes o acceso biométrico. Esto previene el acceso no autorizado en caso de pérdida o robo.

2. Recibes un correo electrónico de 'Soporte Técnico' pidiéndote que hagas clic en un enlace y confirmes tu contraseña debido a una 'actividad sospechosa'.

A. Haces clic en el enlace e introduces tus datos de inmediato para evitar problemas.

B. Respondes pidiendo aclaraciones.

C. Ignoras el correo porque parece sospechoso.

D. Verificas el remitente y luego llamas al departamento de TI para confirmar el correo.

Respuesta correcta: D

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.

Comentario: Siempre verifica los correos electrónicos sospechosos. No hagas clic en enlaces ni proporciones tus credenciales. Contacta directamente con el departamento de TI para comprobar su legitimidad.

3. Durante tu descanso, usas un ordenador compartido del personal para navegar por una tienda online. Te pide que guardes tu contraseña en el navegador.

A. Guardas la contraseña; es conveniente ya que rara vez usas este ordenador.

B. Rechazas y borras tus datos de navegación después.

C. Dejas el ordenador desbloqueado para la siguiente persona.

D. Guardas la contraseña pero te aseguras de cerrar sesión.

Respuesta correcta: B

Comentario: Nunca guardes contraseñas en dispositivos compartidos. Siempre cierra sesión y borra el historial de navegación para proteger tus datos.

4. Un proveedor visita la farmacia para realizar mantenimiento en un ordenador. Te pide usar tu cuenta para instalar software.

A. Introduces tus datos de acceso para que pueda proceder rápidamente.

B. Inicias sesión por él y lo supervisas mientras trabaja.

C. Te niegas y reportas la solicitud al departamento de TI.

D. Le dices que consulte con tu supervisor.

Respuesta correcta: C

Comentario: Nunca compartas tus credenciales de acceso ni permitas que terceros utilicen tu cuenta. Todo acceso externo debe realizarse por los canales adecuados y bajo la supervisión del departamento de TI.

5. Recibes una memoria USB de un compañero que la encontró en el pasillo. Él dice que podría pertenecer a alguien de tu departamento.

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. La conectas a tu ordenador de trabajo para ver qué contiene e identificar al propietario.

B. La apartas y preguntas más tarde entre tus compañeros.

C. La entregas al departamento de TI sin conectarla a ningún dispositivo.

D. Asumes que es basura y la tiras.

Respuesta correcta: C

Comentarios: Los dispositivos USB desconocidos pueden contener malware. Nunca los conectes a un ordenador de trabajo. Siempre informa y entrégaselo al departamento de TI.

4. Mas información

Estas preguntas se inspiraron en escenarios del juego *User Security Awareness* de IS Decisions: https://www.isdecisions.com/user-security-awareness-game/

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.