ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles para estudiantes

¿Cómo de seguro estás? Un cuestionario para profesionales de la salud

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Cómo de seguro estás? Un cuestionario para profesionales de la salud	
Idioma	*Español*

Índice

1. ¿Cómo de seguro estás? Un cuestionario para profesionales de la salud 3
2. Clasificación 3
3. Preguntas del cuestionario 4
4. Más información 6

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	
¿Cómo de seguro estás? Un cuestionario para profesionales de la salud	
Idioma	*Español*

1. ¿Cómo de seguro estás? Un cuestionario para profesionales de la salud

Esta ficha presenta seis preguntas tipo test que introducen prácticas clave para mantenerse seguro en entornos sanitarios. Las preguntas se han adaptado del curso en línea 'Sicherheit am Arbeitsplatz' de la plataforma secaware.nrw, un proyecto de sensibilización del Ministerio del Interior de Renania del Norte-Westfalia.

2. Clasificación

Categoría	Marcar lo que corresponda
Sector	☐ Sanitario
	☑ **General**
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 de los materiales originales	☐ Neerlandés
	☐ Inglés
	☑ **Alemán**
	☐ Italiano
	☐ Español
Tipo de material	☑ **Preguntas tipo test**
	☐ 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: Preparing healthcare professionals for cyberattacks	
¿Cómo de seguro estás? Un cuestionario para profesionales de la salud	
Idioma	*Español*

	☐ Aplicaciones y vídeos interactivos
	☐ Listas de verificación

3. Preguntas del cuestionario

1) Trabajas en la recepción de un centro sanitario. Una persona que dice ser técnico informático quiere acceder a tu ordenador sin mostrar ninguna identificación. ¿Qué deberías hacer?

   a. Permitirle usar el ordenador si parece de confianza.

   b. Darle acceso si dice que es urgente y menciona problemas técnicos.

   c. Negarte educadamente y comunicar la situación a tu supervisor o al departamento de informática.

   d. Dejarle usar el ordenador si lleva ropa de trabajo que parece oficial.

Respuesta correcta: c. Negarte educadamente y comunicar la situación a tu supervisor o al departamento de informática.

Comentario: Nunca permitas que alguien acceda a los sistemas sin la identificación adecuada. La ingeniería social suele basarse en la urgencia y en la autoridad aparente para eludir los protocolos de seguridad.

2) Encuentras una memoria USB en la sala del personal. ¿Cuál es la mejor forma de actuar?
   a. Conectarla a para encontrar al propietario.
   b. Entregarla al departamento de informática o al responsable de seguridad.
   c. Dejarla en un cajón del puesto de enfermería.
   d. Llevártela a casa para guardarla.

Right answer: b. Entregarla al departamento de informática o al responsable de seguridad.

Comentario: Los dispositivos desconocidos pueden estar infectados con malware. Siempre deben entregarse al personal de seguridad.

3) Alguien del “servicio técnico” llama y te pide con urgencia tus credenciales de acceso al sistema. ¿Qué deberías hacer?
   a. Proporcionarlas, ya que afirma ser del departamento de informática.
   b. Pedirle que envíe primero un correo electrónico.
   c. Negarte y comunicar el incidente a tu supervisor o al departamento de informática.
   d. Compartir solo una parte de tu contraseña por seguridad.

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: c. Negarte y comunicar el incidente a tu supervisor o al departamento de informática.

Comentario: El personal informático legítimo nunca solicita contraseñas. Verifica siempre las peticiones y comunica los contactos sospechosos.

4) Recibes un correo sospechoso con un archivo adjunto. ¿Cuál es la actuación más segura?
   a. Eliminar el correo o reportarlo mediante el canal de seguridad.
   b. Abrirlo para comprobar si es relevante para tu trabajo.
   c. Reenviarlo a un compañero para pedir consejo.
   d. Responder al remitente para confirmar su identidad

Right answer: a. Eliminar el correo o reportarlo mediante el canal de seguridad.

Comentario: Los correos sospechosos nunca se deben abrir ni reenviar. Usa las herramientas internas de comunicación para avisar a tu equipo de informática.

5) ¿Cuál de los siguientes hábitos fomenta un comportamiento seguro en el entorno sanitario?
   a. Apuntar los PIN y contraseñas en una nota adhesiva escondida en tu taquilla.
   b. Cerrar la sesión en el ordenador cuando te ausentas del puesto de trabajo.
   c. Compartir tu tarjeta de acceso con compañeros de tu equipo.
   d. Usar la misma identificación para equipos personales y profesionales.

Right answer: b. Cerrar la sesión en el ordenador cuando te ausentas del puesto de trabajo.

Comentario: Cerrar sesión garantiza que nadie pueda acceder a los sistemas sensibles durante tu ausencia. Las credenciales personales deben mantenerse seguras.

6) No estás seguro de si tu área de trabajo cumple las normas actuales de seguridad laboral. ¿Qué deberías hacer?
   a. Esperar hasta la próxima reunión de equipo.
   b. Consultarlo informalmente con tus compañeros.
   c. Revisar las directrices internas de la organización o contactar con el personal de seguridad.
   d. Suponer que todo está en orden si nadie ha presentado quejas.

Respuesta correcta: c. Revisar las directrices internas de la organización o contactar con el personal de seguridad.

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	
¿Cómo de seguro estás? Un cuestionario para profesionales de la salud	
Idioma	*Español*

Comentario: La seguridad laboral es una responsabilidad compartida. Si tienes dudas, busca aclaraciones a través de los canales oficiales.

4. Más información

Las preguntas y escenarios se basan en el módulo de autoaprendizaje en línea 'Sicherheit am Arbeitsplatz', disponible en https://secaware.nrw/selbstlernakademie. Este módulo se ha desarrollado como parte de la iniciativa 'SecAware', financiada por el Ministerio del Interior de Renania del Norte-Westfalia. El contenido original está orientado a la seguridad general en los lugares de trabajo de las instituciones públicas.

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.