ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles para estudiantes

Cuestionario sobre la seguridad de las contraseñas para profesionales sanitarios

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cuestionario sobre la seguridad de las contraseñas para profesionales sanitarios	
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	
Cuestionario sobre la seguridad de las contraseñas para profesionales sanitarios	
Idioma	*Español*

1. Cuestionario sobre la seguridad de las contraseñas para profesionales sanitarios

Esta ficha contiene seis preguntas tipo test destinadas a mejorar la seguridad de las contraseñas entre los profesionales sanitarios. Se centra en riesgos comunes y estrategias prácticas derivadas de passwortcheck.ch para reforzar el acceso seguro a sistemas y datos sensibles. Este sitio web también ofrece una herramienta profesional para la verificación de la seguridad de las contraseñas.

2. Clasificación

Categoría	Marcar lo que correpsonda
Sector	☑ **Sanitario**
	☐ General
Temas cubiertos	☐ Ciberseguridad
	☐ Protección de datos
Tipo de situación	☑ **Prevention**
	☐ 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

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	
Cuestionario sobre la seguridad de las contraseñas para profesionales sanitarios	
Idioma	*Español*

Tipo de material	☑ **Preguntas tipo test**
	☐ Juegos
	☐ Aplicaciones y vídeos interactivos
	☑ **Listas de verificación**

3. Preguntas del cuestionario

1) Trabajas en un hospital y accedes a varios sistemas informáticos a diario. ¿Qué método se recomienda para crear una contraseña segura pero fácil de recordar?
    a. Utilizar una sola palabra larga con caracteres especiales.
    b. Utilizar una contraseña simple como 'Pflege123', que sea fácil de recordar y rápida de escribir.
    c. Usar una frase personal y tomar las iniciales, números y mayúsculas para generar una contraseña compleja pero fácil de recordar.
    d. Usar la misma contraseña que para tus cuentas personales para evitar confusiones.

Respuesta correcta: c. Usar una frase personal y tomar las iniciales, números y mayúsculas para generar una contraseña compleja pero fácil de recordar.

Comentario: Una frase fácil de recordar (por ejemplo: “Trabajo 4 veces con María cinco lunes a partir de las 9:00 H”) convertida en iniciales (t4vcM5lapdl9H) genera una contraseña compleja pero fácil de recordar.

2) Ves a un compañero apuntando los datos de acceso en una nota adhesiva junto a la pantalla. ¿Cuál sería la alternativa más segura?
    a. No hay problema siempre que nadie más esté cerca. Mantenerla a la vista está bien en esos casos.
    b. Guardar las contraseñas en un gestor de contraseñas seguro.
    c. Crear en el ordenador un archivo de texto con las contraseñas y ponerle un nombre que no sea evidente.
    d. Esconder las notas bajo el teclado para que sea menos probable que alguien las encuentre.

Respuesta correcta: b. Guardar las contraseñas en un gestor de contraseñas seguro.

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: Guardar las contraseñas en notas adhesivas o en archivos sin protección supone un riesgo de seguridad significativo. Utiliza un gestor de contraseñas seguro para almacenar credenciales sensibles.

3) Usas la misma contraseña para acceder al hospital, al correo personal y a las redes sociales. ¿Cuál es el problema?
    a. Si olvidas la contraseña, tendrás un problema en varios sistemas.
    b. Reutilizar contraseñas aumenta el riesgo de múltiples brechas de seguridad.
    c. Si utilizas un gestor de contraseñas, no hay problema.
    d. Activar la autenticación en dos pasos (2FA) es menos eficaz en este caso.

Respuesta correcta: b. Reutilizar contraseñas aumenta el riesgo de múltiples brechas de seguridad.

Comentario: Reutilizar contraseñas implica que una sola contraseña filtrada puede comprometer varios sistemas, incluidos aquellos que contienen datos sanitarios sensibles.

4) Te das cuenta de que la aplicación web de tu hospital usa “http://” en lugar de “https://”. ¿Existe un riesgo de seguridad?
    a. No hay riesgo mientras se use el sitio oficial.
    b. Sí, hay un riesgo. Las contraseñas pueden transmitirse sin cifrar.
    c. No hay riesgo. Usar contraseñas largas es suficiente para mantener los datos seguros, incluso en sitios HTTP.
    d. Sí, hay un riesgo. HTTPS se usa principalmente por motivos de velocidad, no de seguridad.

Respuesta correcta: b. Sí, hay un riesgo. Las contraseñas pueden transmitirse sin cifrar.

Comentario: Los sitios HTTP no ofrecen cifrado. Los datos sensibles (inicios de sesión, información de pacientes) solo deben introducirse en sitios protegidos con la versión segura, HTTPS. El protocolo HTTPS se utiliza por razones de seguridad.

5) A menudo se utilizan contraseñas como '123456' o 'qwertz', incluso en el sector sanitario. Evalúa el uso de este tipo de contraseñas.
    a. Son contraseñas establecidas y adecuadas, por lo que su uso frecuente está justificado.
    b. Combinadas, formarían una contraseña fuerte, ya que incluyen números y letras.
    c. Son secuencias de teclado muy conocidas. Siguen patrones predecibles y están incluidas en la mayoría de los diccionarios de descifrado de contraseñas. Esto supone un grave problema.
    d. El principal problema es que no contienen caracteres especiales.

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 Son secuencias de teclado muy conocidas. Siguen patrones predecibles y están incluidas en la mayoría de los diccionarios de descifrado de contraseñas. Esto supone un grave problema.

Comentario: Este tipo de contraseñas son extremadamente inseguras. Su previsibilidad las convierte en un objetivo común para herramientas automáticas de descifrado y deben evitarse por completo, especialmente en entornos clínicos.

6) Tu clínica activa la autenticación en dos pasos (2FA). ¿Qué deberías hacer?
    a. Usar solo tu contraseña habitual, ya que la 2FA ya está activada y ofrece suficiente protección.
    b. Activar la 2FA siempre que sea posible para añadir una capa extra de seguridad, además de usar una contraseña fuerte.
    c. Guardar la contraseña en un archivo de texto sin cifrar en el escritorio para no olvidarla.
    d. Introducir la contraseña varias veces para aumentar la seguridad mediante la repetición.

Respuesta correcta: b Activar la 2FA siempre que sea posible para añadir una capa extra de seguridad, además de usar una contraseña fuerte.

Comentario: La autenticación en dos pasos (2FA) es una de las formas más eficaces de prevenir accesos no autorizados, especialmente en entornos sanitarios.

4. Más información

Las preguntas del cuestionario se han adaptado desde las directrices oficiales sobre contraseñas publicadas en www.passwortcheck.ch por la Universidad de Ciencias Aplicadas y Artes de Lucerna. Estas directrices tienen como objetivo sensibilizar sobre el uso seguro de contraseñas entre los usuarios finales, con especial atención a los profesionales sanitarios. Los materiales están disponibles públicamente y se publican en alemán, francés, italiano e inglés. El sitio web ofrece una herramienta profesional para verificar la seguridad de las contraseñas.

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.