¿Qué tan protegido estás?

Objetivo: Aprender qué es una contraseña y practicar la creación de contraseñas seguras para proteger su información y datos

¿Qué es una contraseña?

Definición: Contraseña
Una cadena protegida/privada de letras, números y/o caracteres especiales que se utiliza para autenticar una identidad o para autorizar el acceso a los datos.

¿Qué hace que una contraseña sea segura y por qué es importante?

Una contraseña segura es aquella que solo conoce el titular de la cuenta y que no es probable que sea adivinada por ningún suplantador. Agregar complejidad, como caracteres especiales, letras mayúsculas o números, puede hacer que esto sea más seguro. Esto es importante ya que aumenta la seguridad de la "puerta de entrada" a la identidad y reputación de alguien y a la información confidencial.

Actividad

1. Piense en la complejidad de las contraseñas de sus diversos sitios y cuentas.
2. Explore el medidor de seguridad de contraseñas visitando: www.passwordmonster.com
3. Inventa algunas contraseñas para probar... Incluso puedes probar el actual.
4. Discuta con otros por qué es importante tener una contraseña segura.
5. Considere actualizar sus contraseñas para aumentar su seguridad.

¿Qué tan compleja es su contraseña? ¿Cuánto tiempo tardó en romperse? ¿Cuál es la contraseña más segura que puedes recordar y escribir? ¿Cuántos años se te ocurrieron?

IA traducida en una computadora

KENT SCHOOL DISTRICT
EQUITY | EXCELLENCE | COMMUNITY

Un desafío de phishing

Objetivo: Aprender qué es el phishing y practicar la identificación de los tipos de indicadores de phishing

¿Qué es el phishing?

Definición: **Phishing**
Una forma digital de ingeniería social que utiliza correos electrónicos de apariencia auténtica, pero falsos, para solicitar información de los usuarios o dirigirlos a un sitio web falso que solicita información.

¿Cómo se identifica un correo electrónico de phishing?

- ¿Conoces al remitente? ¿Es alguien de quien esperabas un mensaje o alguien con quien te comunicas regularmente?
- Compruebe si hay errores tipográficos y mire los enlaces antes de hacer clic
- Lea el saludo y la firma
- ¿Parece que el asunto dentro del mensaje está fuera de lugar? Si eres cauteloso, confía en tu instinto y no hagas clic en ningún enlace, archivo adjunto ni respondas al remitente.

Actividad

1. Revise y piense en las formas de identificar las estafas de phishing.
2. Con los consejos anteriores, vea si puede identificar los tres indicadores de phishing en el correo electrónico de la página siguiente.
3. Discuta con los demás las formas en que puede recordar estar atento al phishing y evitar caer en estas estafas.

¿Sabías que una vez que hayas identificado un correo electrónico de phishing, es inteligente eliminarlo, para no volver a caer en él más tarde?

IA traducida en una computadora

Un desafío de phishing

¿Puedes encontrar los 3 problemas principales con este correo electrónico de phishing? ¿Puedes encontrar más?

Hello You Have New Vmail

SN

stuart.fletcher New-Call <sf@prizemons.com>

To Nombra tu

Reply | Reply All | Forward

Fri 9/29/2023 2:26 PM

Follow up. Completed on Friday, September 29, 2023.

If there are problems with how this message is displayed, click here to view it in a web browser.

Microsoft Outlook

Hello,

You have new voicemail message in your mailbox.

This mail was sent to: Su.nombre@kent.k12.wa.us

Preview or Download Voice Message

Sincerely,

Microsoft Customer Care

Microsoft | Support | Privacy Policy

Copyright © 2020 Microsoft .Inc

Microsoft Outlook WebApp

OWA

Respuesta: Los 3 problemas principales

Hello ,

un saludo genérico y un error gramatical para el nombre

From: Stuart.fletcher New-Call <sf@prizemons.com>

El nombre para mostrar falsificado oculta el remitente y el correo electrónico de respuesta.

Sincerely,

Microsoft Customer Care

El mensaje incluye algunos detalles sobre el remitente o su información de contacto.

IA traducida en una computadora

¿Quién es un MFA?

Objetivo: aprender qué es la autenticación multifactor (MFA) y poder identificar elementos que se pueden utilizar para MFA.

¿Qué es la autenticación multifactor?

Definición: **autenticación multifactor**
La combinación de algo que tienes (tiene propiedades físicas), algo que sabes (secreto almacenado/recordado mentalmente) y/o algo que eres (biometría). Normalmente se utiliza para autenticar a un individuo en un recurso protegido (ubicación física, datos, fondos).

¿Qué puede ser un artículo de MFA?

- **Algo que tienes + algo que sabes – Tarjeta de acceso físico + código PIN.**
- **Algo que eres + algo que sabes - Biometría facial y código PIN.**
- **Algo que eres + algo que tienes – Tarjeta de acceso físico + escaneo de retina.**

Actividad

¿Puedes identificar varias combinaciones de MFA? Marca las siguientes combinaciones con Verdadero o Falso.

1. Número de PIN y tarjeta de cajero automático..... Verdadero o Falso
2. Reconocimiento facial y de huellas dactilares..... Verdadero o Falso
3. Credencial con nombre y contraseña..... Verdadero o Falso
4. Reconocimiento facial y número PIN ..... Verdadero o Falso
5. Preguntas personales y nombre de usuario..... Verdadero o Falso
6. Contraseña de Email ..... Verdadero o Falso
7. Contraseña y número PIN ..... Verdadero o Falso
8. Llavero, código de acceso y escaneo de huellas dactilares ..... Verdadero o Falso

Clave de respuestas: 1. T, 2. F, 3. T, 4. T, 5. F, 6. F, 7. F, 8. T

¿Qué dispositivos o servicios tienes que usan MFA? ¿Discute con otras personas cómo MFA puede mantener segura su información?

IA traducida en una computadora

KENT SCHOOL DISTRICT
EQUITY | EXCELLENCE | COMMUNITY

Estar cifrado o no estar cifrado

Objetivo: Aprender qué es el cifrado de sitios web y poder identificar si los sitios web están cifrados.

¿Qué es el cifrado de sitios?

Definición: **cifrado de sitios web**
HTTPS (Protocolo seguro de transferencia de hipertexto) es una forma especial de mantener seguros los mensajes cuando habla con un sitio web. Es como un código secreto que mantiene tus palabras a salvo. Cuando envía mensajes al sitio web, se convierten en un código secreto para protegerlos. Y cuando el sitio web le responde, también utiliza un código secreto para mantener las cosas seguras.

¿Cómo puede saber que su sitio está cifrado?

Puede saber si un sitio web utiliza HTTPS mirando un pequeño candado en la barra de direcciones en la parte superior de la pantalla, justo a la izquierda de donde está el nombre del sitio web. Si ve el candado, significa que sus mensajes están seguros. Pero si no hay ningún candado o si el candado tiene una línea roja, significa que tus mensajes no están seguros, ¡así que ten cuidado!

Actividad

Búsqueda del tesoro de cifrado de sitios web. Vea si sus lugares favoritos son lugares seguros para compartir su información. Tómese el tiempo para explorar lo siguiente y encontrar HTTPS o el

- [ ] Cifrado encontrado en tus redes sociales favoritas
- [ ] Cifrado encontrado en su sitio de juegos favorito
- [ ] Cifrado encontrado en su acceso a correo electrónico en línea
- [ ] Cifrado encontrado en un sitio de aprendizaje en línea
- [ ] Cifrado encontrado en su sitio web de transmisión de video favorito
- [ ] Cifrado encontrado en su motor de búsqueda favorito

¿Descubrió un lugar que visita con frecuencia que no estaba cifrado? ¿Discuta con otras personas por qué el cifrado de sitios web es importante antes de compartir su información?

IA traducida en una computadora

Ingeniería social

Objetivo: Aprender qué es la Ingeniería Social y poder identificar las principales características de un ataque de Ingeniería Social.

¿Qué es la ingeniería social?

Definición: **Ingeniería Social**
Usar una técnica de manipulación para engañar a una persona para que revele información confidencial, obtenga acceso no autorizado o cometa fraude utilizando su reputación para obtener confianza falsa por parte de su organización.

¿Cuáles son las características de un ataque de ingeniería social?

Los ingenieros sociales se aprovechan de sus pensamientos y emociones. Rasgos de un ataque de ingeniero social:

#1 Emoción de alta tendencia: es más probable que tomes una decisión irracional o arriesgada cuando te sientes emocional (enojado, asustado, emocionado, etc.)
#2 Urgencia: Sus ataques estarán redactados para obligarte a sentir que debes tomar una decisión desinformada. decisión.
#3 Confianza: intentarán parecer una fuente confiable o un amigo

Actividad

¿Puedes identificar qué rasgo utilizan los siguientes ataques de ingeniería social? Etiquete cada uno con el número de rasgo. **1 = Emoción 2 = Urgencia 3 = Confianza**

_____ Texto de un número desconocido diciendo que se ha perdido un paquete y que necesitan su información para confirmar el envío de otro.

_____ Una ventana emergente en línea que dice que ganó un premio único en la vida, pero debe reclamarlo dentro de los 15 minutos completando cierta información personal.

_____ Ve una ventana emergente en línea que advierte que su computadora ha sido infectada y, para solucionarlo, debe descargar un software antimalware específico.

_____ Tu mejor amigo te envía un correo electrónico pidiéndote que revises un enlace extraño que te lleva a fotos de un viaje reciente.

Clave de respuestas: 1, 3, 2, 3

¿Se te ocurre un ataque de ingeniería social que utilice los tres rasgos? ¿Discuta con otras personas sobre qué formas puede prepararse y evitar ataques de ingeniería social?

IA traducida en una computadora