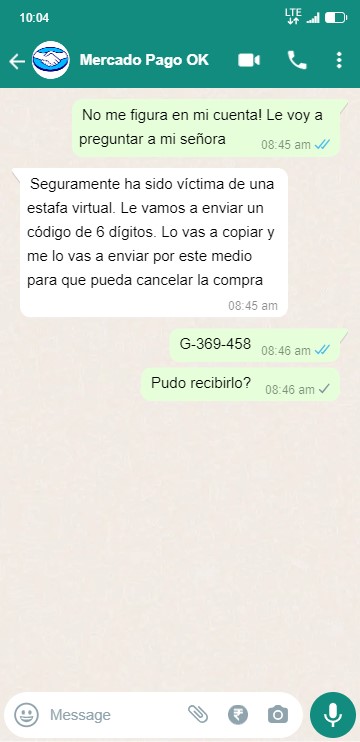
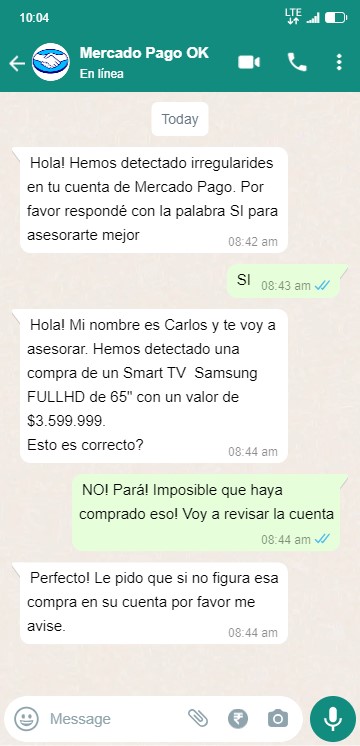
# Taller de Formación Profesional Seguridad informática

**Actividad 1:**

Analizamos las siguientes imágenes y debatimos en grupos. Anotá las respuestas.

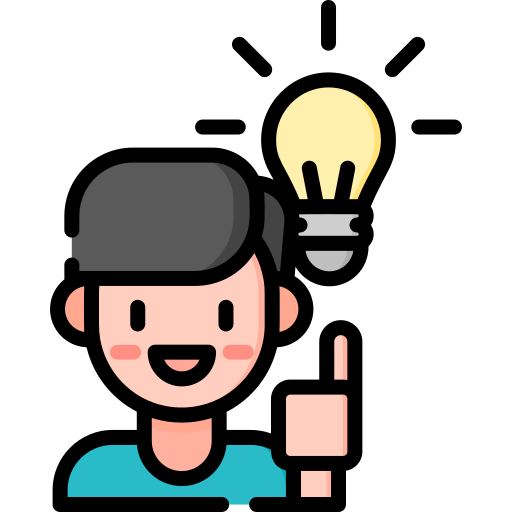


Esta es la captura de pantalla de un caso real.

* ¿Qué es lo primero que te llama la atención de los mensajes?
* Me llama la atención que ese contacto de mercado pago no tiene una cuenta de empresa ni verificada, también de que mercado pago nunca te va a pedir algún código o algún dato porque todo esta cargado en el sistema.
* ¿Hubo algún indicio o pista que te hiciera pensar que esto es falso? ¿Cómo hubieras reaccionado en tu caso?
* Si, si hubo indicios de estafa porque, para empezar mercado pago nunca te pedirá algún código de 6 digitos porque solo yo tengo acceso a ese código y es muy comprometedor enviárselo a alguien equivocado, también al pasarle el código, automáticamente deja de estar en línea y no llega el mensaje de “pudo recibirlo?”, eso da indicios de que a sido bloqueado y nos damos cuenta de que no es una cuenta verificada de mercado pago por ende es indicio de que ha sido estafado.
* ¿Dentro de qué o cuáles de tipos de amenazas identificás en este caso? Justifica tu respuesta.
* Técnicas como el Whale Phishing son solo unas de las más utilizadas por los criminales cibercriminales, aunque existen muchos otros virus y estafas de WhatsApp que es necesario conocer para prevenir.

Escaneá el siguiente QR para poder leer la noticia publicada en INFOBAE.

* ¿Qué fue lo que más te llamó la atención de esta noticia?
* Me llamo la atención que pocas veces he escuchado que hackean alguna agencia aeroespacial, me sorprende de qué Boeing siendo una multinacional tan grande pudieron hackearlos tan fácil, con un ingreso anual estimados en 2022 de 66.610.000.000 dólares. Con ese ingreso anual como no pueden tener algún método de seguridad adecuado para enfrentar estos piratas cibernéticos y estar preparado para cualquier ataque o hackeo.
* ¿Dentro de qué o cuáles de tipos de amenazas identificás en este caso? Justifica tu respuesta.
* ¿Cuáles imaginás que pueden ser los posibles errores que se han cometido para que este ataque haya podido ser ejecutado?

**Actividad 2:**

A continuación les presentamos 3 casos prácticos para evaluar en grupo y diseñar posibles soluciones.

1. **Escenario:** Imagina que estás diseñando las reglas de seguridad para la conexión Wi-Fi de tu escuela.

**Ejercicio:** Debes pensar en cómo proteger la conexión Wi-Fi para que solo los estudiantes y el personal autorizado puedan usarla. Piensa en contraseñas seguras y en cómo evitar que personas no autorizadas se conecten. También, considera cómo proteger la información que se envía y recibe por la red.

1. **Escenario:** Supón que trabajas en una empresa que crea programas de computadora y necesitas asegurar que los proyectos y la información de los clientes estén protegidos.

**Ejercicio**: Tu tarea es crear reglas para que solo las personas correctas puedan ver y trabajar en los proyectos de la empresa. También, debes pensar en cómo mantener segura la información privada de los clientes y cómo evitar que los datos importantes se pierdan o sean robados.

1. **Escenario:** Imagina que tienes una tienda en línea donde vendes cosas y necesitas asegurarte de que los datos de tus clientes estén protegidos.

**Ejercicio:** Debes pensar en cómo proteger el sitio web de tu tienda para que los hackers no puedan robar información de los clientes, como sus nombres y números de tarjetas de crédito. Considera también cómo mantener la tienda en línea funcionando correctamente para que los clientes puedan comprar sin problemas.

**Actividad 3:**

Necesitamos de tu colaboración para que toda la escuela y las familias sepan de estas vulnerabilidades, sobre todo las relacionadas a las redes sociales o correos electrónicos.

En grupo deberán crear una publicación en canva que informe y advierta sobre estos peligros cada vez más comunes en nuestra sociedad.

Podés escribir las ideas principales o realizar un diseño previo de lo que será tu publicación