

Experiencia de simulación:

identificar los ataques de phishing y whaling

🕒 Descripción general

Los ataques de phishing manipulan al personal para que pongan en riesgo la seguridad aprovechándose de emociones como el miedo, el deseo de ayudar o el respeto a la autoridad. Esta actividad se enfoca en una forma de phishing específica y muy selectiva, conocida como “whaling” o “fraude del CEO”. En estos ataques, la delincuencia se hace pasar por miembros del equipo directivo, como personal a cargo de la dirección ejecutiva o financiera, para aprovecharse del sesgo de autoridad y provocar una respuesta emocional inmediata.

Hoy en día, agentes de amenazas suelen utilizar la inteligencia artificial generativa (IA) para crear correos electrónicos de phishing con logotipos exactos de las organizaciones y sin errores gramaticales. Aunque se debe seguir estando alerta a los errores evidentes de ortografía o de marca, esta sesión anima a comprender que ya no se puede confiar únicamente en estos indicios superficiales de phishing.

👤 Roles

Persona facilitadora:

controla el ritmo del ejercicio, modera los debates y garantiza la participación de todas las personas.

Participantes:

hablan abiertamente sobre sus procesos de razonamiento y responden a las situaciones presentadas siguiendo las reglas del ejercicio.

Introducción

Presente la siguiente situación: Summit View Logistics está expandiendo sus operaciones a Europa. El director ejecutivo, Marcos Suárez, ha estado viajando por México toda la semana para asegurar el arrendamiento de un almacén importante. En la organización, todo el mundo sabe que este trato es de prioridad absoluta. La directora financiera, Elena Lugones, está en un vuelo de 10 horas de regreso a la sede central y, por el momento, no hay forma de contactarla. Sofía Bertello, la responsable de cuentas por pagar, recibe un correo electrónico sospechoso.

Parte 1: anotación de señales

🕒 **Duración:** 15 minutos

Materiales:

- Cronómetro o temporizador.
- Hojas impresas con las situaciones.
- Bolígrafos o lápices.

Instrucciones:

- Divida al salón en grupos pequeños.
- Entregue las hojas impresas con los correos electrónicos y bolígrafos o lápices a cada grupo.
- Indíqueles a los grupos que subrayen los elementos que crean una falsa sensación de confianza. Por ejemplo, firmas de correo electrónico correctas, referencias a proyectos internos reales o un tono ejecutivo auténtico.
- Indíqueles a los grupos que **marquen con un círculo** las señales de advertencia en el comportamiento. Algunos ejemplos son la urgencia extrema, las exigencias de mantener la solicitud en secreto o las instrucciones de evitar los portales de pago estándar.
- Deles 15 minutos a los grupos para que lean el correo electrónico, lo analicen y hagan anotaciones.

Parte 2: debate

 **Duración:** 10 minutos

Preguntas:

- ¿Qué indicadores de confianza falsos descubrió y en qué medida influyeron en su confianza en el correo electrónico?
- ¿Que señales de advertencia específicas en el comportamiento delataron la estafa?
- ¿Cómo están diseñados esos desencadenantes del comportamiento para hacerle sentir o reaccionar de determinada manera?

Posibles respuestas o sugerencias

- Indicadores de confianza falsos: Quienes realizan ataques de phishing rastrean LinkedIn o sitios web corporativos en busca de nombres de proyectos reales para que el correo electrónico parezca auténtico.
- Señales de advertencia: En el correo electrónico de phishing, se le pide al personal que omita los procedimientos estándar. El remitente exige discreción y que la persona que supervisa al personal no se entere.
- La lección principal: Se están utilizando elementos que parecen reales o fiables para ocultar un engaño. El verdadero peligro son las señales de advertencia en el comportamiento.

Conclusión

 **Duración:** 5 minutos

Concluya el ejercicio relacionando los conceptos directamente con la realidad de su organización. Explique que detectar una señal de advertencia es solo el primer paso en la defensa; el segundo consiste en tomar las medidas adecuadas siguiendo los procedimientos de la organización.

Aproveche la oportunidad para responder las preguntas que puedan surgir sobre cómo notificar este tipo de estafas a nivel interno y sobre las herramientas, los canales y la documentación disponibles para notificar estos incidentes.

Redactar

- Bandeja de entrada
- Borradores
- Enviados
- Destacados
- Correo no deseado
- Papelera
- Archivar
- Todo el correo

- Archivar
- Correo no deseado
- Eliminar
- Más
- Responder
- Reenviar

De: Marcos Suárez <m.suarez@interno-summitviewlogistics.com>
Para: Sofía Bertello
Asunto: **URGENTE: Depósito del almacén de Ciudad de México**

Hola, Sofía:

Estoy reunido con el personal de la agencia inmobiliaria en Ciudad de México. Estamos listos para firmar el contrato de arrendamiento del almacén que comentamos en la reunión general del lunes.

Tenemos un problema importante. Otra empresa acaba de hacer una oferta por el almacén. El agente inmobiliario dijo que si no hacemos el depósito de garantía de USD 60 000 en la siguiente hora, van a arrendarle el almacén a la otra empresa.

Elena Lugones está en pleno vuelo y no puedo esperar su aprobación. El agente inmobiliario todavía no se encuentra registrado en nuestro portal y eso llevará mucho tiempo.

Necesito que proceses una transferencia directa a la cuenta cuya información adjunto a continuación. Mantengamos esto entre nosotros hasta que Elena aterrice, para que nadie entre en pánico pensando en que no se va a cerrar el trato. Avísame en cuanto esté confirmada la transferencia.

Saludos,
Marcos

Adjunto: Detalles_Transferencia_Bancaria.pdf

Indicadores de confianza falsos: la ubicación del remitente (Ciudad de México); la mención de un proyecto real (arrendamiento de un almacén / reunión general); el conocimiento del nombre de la directora financiera y su estado (Elena, está en un vuelo).

Señales de advertencia en el comportamiento: urgencia extrema (próxima hora / otra empresa lo obtendrá); omisión de procedimientos (no está registrado en el portal de proveedores); aislamiento (mantengamos esto entre nosotros).