knowbe4

2026 Mes de la Concientización sobre la Ciberseguridad

Kit de recursos: dossier estratégico

SEMANA 1
SEMANA 2
SEMANA 3
SEMANA 4

INFORME DE LA MISIÓN:

Mes de la Concientización sobre la Ciberseguridad 2026

Su misión, si decide aceptarla: brindar a su equipo la información que necesita para mantenerse un paso adelante de la ciberdelincuencia global.

Aproveche al máximo el arsenal de herramientas, equipamiento y especialistas en ciberseguridad de este año como parte de un equipo de élite conocido como la "División de Riesgos del Personal". Como integrante de la DRP, ayudará a su personal a emprender cuatro misiones semanales, cada una centrada en una ciberamenaza específica.

Transformar a su personal en una fuerza de defensa de primera línea ahora es mucho más fácil. Hicimos el trabajo pesado con una colección gratuita de recursos.

Esta campaña lista para usar del Mes de la Concientización sobre la Ciberseguridad convierte a su personal en "agentes de operaciones encubiertas" en la lucha contra el ciberdelito. Además de módulos de capacitación gratuitos y materiales de apoyo, como afiches y documentos, incluimos cuatro fichas de personajes "especialistas", que representan las habilidades necesarias para desenvolverse en el panorama de amenazas actual. También encontrará cuatro escenarios prediseñados para ejercicios de simulación, pensados para realizarse de forma presencial o virtual y ayudar a su equipo a fortalecer su resiliencia frente a las amenazas del futuro.

Su equipamiento

Lo que incluye nuestra página web del kit:

FOR YOUR EYES ONLY

Exclusivo para usted

- **Seminario web:** Cómo proteger la incorporación de la IA en su organización.
- **Informe técnico:** Cómo proteger la fuerza laboral híbrida: la seguridad de humanos y agentes de IA en esta nueva era.
- **Cuatro documentos con escenarios para ejercicios de simulación organizados por tema.**
- **Planificador semanal web de Concientización sobre Seguridad**, que organiza todos los recursos dirigidos al personal que aparecen a continuación en temas semanales para usarlos durante octubre. Disponible aquí:

PLANIFICADOR SEMANAL

Para sus agentes

Acceda a todos los cursos y al contenido mediante los enlaces proporcionados hasta el **31 de octubre de 2026.**

- **Seis módulos gratuitos de capacitación interactiva o de video**
  - Frenesí del smishing (disponible en 35 idiomas)
  - Un ataque de ingeniería social mediante deepfakes (disponible en 35 idiomas)
  - Protección de la propiedad intelectual (disponible en 12 idiomas)
  - Contraseñas seguras, cuentas protegidas (disponible en 35 idiomas)
  - Audiocast “Hábitos a prueba de hackeos” (disponible en 12 idiomas)
  - Juego “En busca de la privacidad” (disponible en 13 idiomas)
- **Cuatro fichas/afiches de personajes especialistas de la División de Riesgos del Personal**
- **Cuatro afiches y recursos de señalización digital ideales para reforzar conceptos clave**

Introducción a la División de Riesgos del Personal

Para agentes de la DRP, la lucha constante contra maleantes ya es bastante difícil, por eso quisimos facilitar al máximo la incorporación de más agentes. Para comenzar, cada recurso está alineado con un tema general que servirá de eje para cada una de las cuatro semanas de octubre. Cada semana, considere compartir uno o más de estos tipos de contenido:

- **Video o módulo de capacitación interactivo**
- **Afiche/documento informativo**
- **Ficha del personaje especialista de la DRP**
- **Documento para ejercicio de simulación**

Más adelante en este dossier analizaremos con mayor detalle el tema de cada semana, pero este es el resumen:

- **Semana 1:** Phishing e ingeniería social
- **Semana 2:** Seguridad de la IA y deepfakes
- **Semana 3:** Seguridad de los datos y contraseñas
- **Semana 4:** Notificación de incidentes

Para visualizar cómo encaja todo, consulte nuestro Planificador de Concientización sobre Seguridad, disponible aquí:

PLANIFICADOR SEMANAL

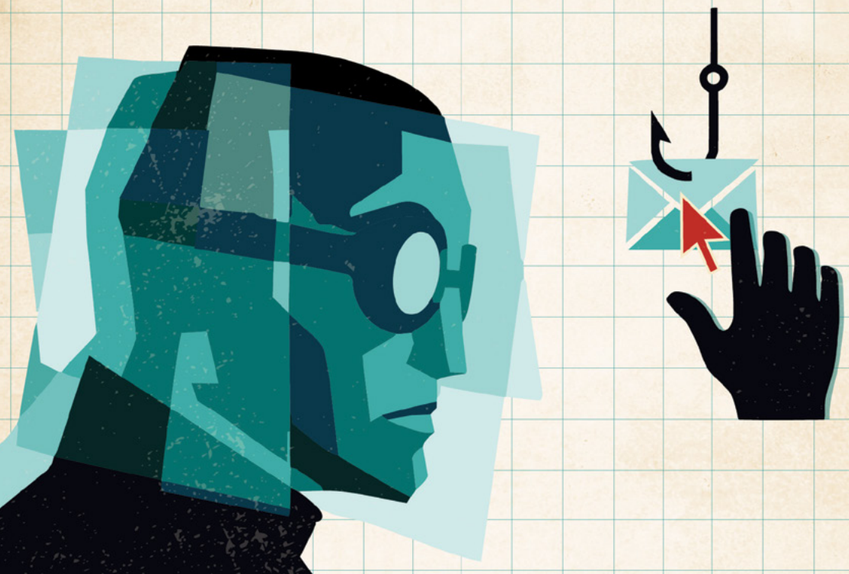
Utilice el planificador como punto único de acceso a los recursos de la DRP puestos a su disposición.

Perfiles de especialistas de la DRP

Las misiones ya están definidas. Ahora es momento de conocer al personal especialista. Presente a su personal los cuatro conjuntos de habilidades que necesitará para las operaciones cibernéticas durante el Mes de la Concientización sobre la Ciberseguridad mediante estos cuatro perfiles de especialistas. Cada uno aporta habilidades esenciales para afrontar las misiones del mes. El resto depende de su personal.

PHISHING/INGENIERÍA SOCIAL

ESPECTRO



LEMA:
CONFÍE,
PERO VERIFIQUE...
Y LUEGO
VERIFIQUE OTRA VEZ

FUNCIÓN: ESPECIALISTA EN CONTRAINTELIGENCIA

ESPECIALIDAD: DETECCIÓN DE PRETEXTING Y SOFISTICADOS ATAQUES DE INGENIERÍA SOCIAL

CONSEJO: SI UN CORREO ELECTRÓNICO CREA UNA FALSA SENSACIÓN DE URGENCIA, PROBABLEMENTE SEA UNA TRAMPA

AMENAZAS DE IA/SEGURIDAD

TECNO

LEMA:
MANTENGA SUS
HERRAMIENTAS AFILADAS
Y SU MENTE
AÚN MÁS

FUNCIÓN: ESPECIALISTA EN TECNOLOGÍA

ESPECIALIDAD: SEGURIDAD DE LA IA Y DETECCIÓN DE DEEPFAKES

CONSEJO: USE UNA PALABRA CLAVE CON SU FAMILIA O SUS COLEGAS PARA VERIFICAR LA IDENTIDAD DURANTE LLAMADAS SOSPECHOSAS “URGENTES”

SEGURIDAD DE LOS DATOS Y CONTRASEÑAS

LAVE MAESTRA

LEMA:

[CENSURADO]

FUNCIÓN: CRIPTOGRAFÍA

ESPECIALIDAD: CLAVES DE ACCESO, MFA Y CIFRADO

CONSEJO: SU CONTRASEÑA NO DEBERÍA SER UNA PALABRA; DEBERÍA SER UNA HISTORIA QUE SOLO USTED CONOZCA

PÁGINA

NOTIFICACIÓN DE INCIDENTES

VIGÍA

LEMA:

SI TODO APUNTA A UNA **VIOLACIÓN DE SEGURIDAD DE DATOS,** NO SE QUEDE CON LA DUDA:

REPÓRTELA DE INMEDIATO

FUNCIÓN: AGENTE DE CAMPO

ESPECIALIDAD: NOTIFICACIÓN DE INCIDENTES Y SEGURIDAD FÍSICA

CONSEJO: SI VE ALGO SOSPECHOSO, REPÓRTELO

PÁGINA

Integrar a todo el personal

Hemos preparado cuatro planes de lecciones completos para ayudar a guiar a su equipo mediante ejercicios de simulación de crisis de seguridad.

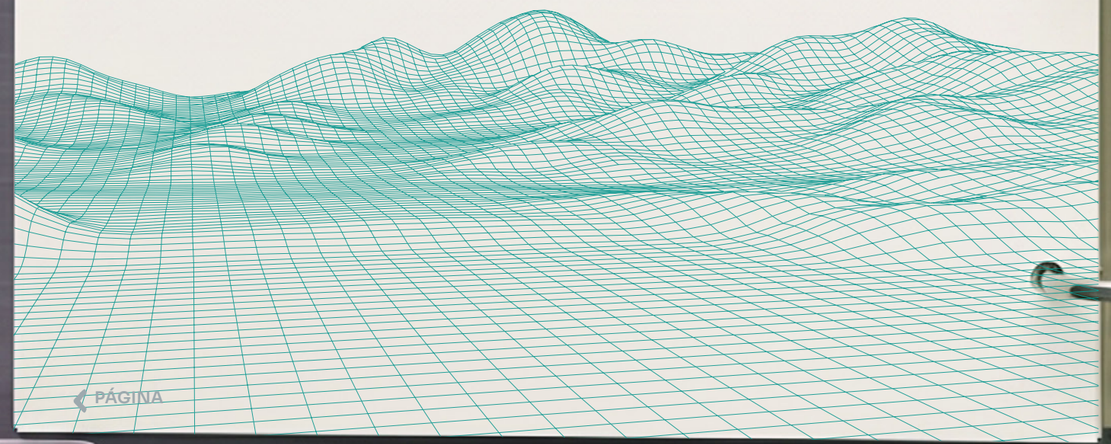
El objetivo es adaptarse a personas con cualquier nivel técnico y centrarse en la identificación de funciones, la toma de decisiones y la coordinación del equipo. Las actividades incluyen priorizar listas de verificación de respuesta y realizar simulaciones realistas de escenarios con situaciones imprevistas. Su personal aprenderá procedimientos establecidos de respuesta ante incidentes, comunicación entre distintas áreas y capacidad de adaptación durante incidentes de seguridad mediante ejercicios prácticos y sesiones estructuradas de análisis.

Estas son algunas sugerencias prácticas para aprovechar al máximo estos recursos:

1. Misión lista para usar para la gerencia:
Comparta estos recursos con las personas responsables de cada departamento junto con una nota de *Informe de la dirección*. Sugiérales que elijan el tema más relevante para su departamento y realicen una versión de *Respuesta rápida* de 30 minutos durante una reunión semanal de seguimiento ya programada.

2. Ataque informático para equipos remotos:
Si la mayor parte de su personal trabaja de forma remota, utilice las secciones *Tarjeta de escenario* de los ejercicios de simulación como preguntas de encuesta durante las reuniones generales por videoconferencia de octubre para realizar cuestionarios breves. Analicen los resultados de la semana anterior en la reunión de la semana siguiente para ver cómo le fue al equipo.

3. La misión *Elija su propia aventura* por mensajería instantánea:
Elija un día de la semana y publique una *Tarjeta de escenario* en el canal de seguridad de la información o de concientización sobre seguridad de la aplicación de mensajería interna que utilicen. Quien “Reporte el incidente” primero correctamente, y explique por qué representa un problema y qué se podría hacer al respecto en el hilo, podría ganar un premio temático u otro incentivo, según lo permita su organización.



Consejos de las mentes brillantes de la DRP: estrategias de campaña

El equipo científico y de investigación que trabaja tras bambalinas en la DRP quizá no salga mucho, pero sabe muy bien lo que hace. Quienes desarrollaron estos recursos han comprobado que las siguientes estrategias clave de campaña funcionan en organizaciones de todos los tamaños:

Piense como quien dirige la operación; actúe como agente de campo Su objetivo es cambiar comportamientos riesgosos, no solo transmitir información. Piense en cómo las mejores agencias de inteligencia del mundo construyen historias de “infiltración profunda”: utilizan múltiples puntos de contacto para reforzar un mismo mensaje. Por eso hemos autorizado suficientes recursos para aplicar un enfoque multicanal de “impacto envolvente”. Al utilizar distintos medios (videos, juegos e informes) a lo largo de la semana, reforzará los reflejos de seguridad de su personal mediante una participación constante. Así es como se transforma al personal pasivo en una sólida última línea de defensa.

Sume personas colaboradoras de todas las áreas
Ninguna operación de inteligencia tiene éxito de manera aislada. Para construir una cultura de la seguridad verdaderamente resiliente, necesita incorporar personas colaboradoras más allá del perímetro de TI. Aproveche octubre para activar a “agentes durmientes” de RR. HH., Asuntos Legales y Marketing. Muéstreles que desempeñan un papel fundamental en la DRP. Cuando los mensajes sobre seguridad provienen de una persona de confianza dentro de su propio departamento, y no solo del personal de TI, es mucho más probable que se integren.

Priorice la información crítica para la misión
No ponga en riesgo a sus agentes proporcionándoles demasiada información “crítica para la misión”. Si comparte demasiada información al mismo tiempo, podrían saturarse y empezar a ojear rápidamente los informes solo para vaciar la bandeja. En su lugar, identifique las dos o tres vulnerabilidades más críticas de su organización y concentre allí sus esfuerzos. Los temas semanales de la misión —phishing, seguridad de la IA, contraseñas y notificación de incidentes— están diseñados para formar agentes integrales. Concéntrese en la misión actual, asegure el objetivo y deje la información más avanzada para futuras operaciones.

Aunque los recursos de este kit no sustituyen un programa integral de capacitación en concientización sobre seguridad, están diseñados para compartirse e implementarse fácilmente, de manera que tengan el mayor impacto posible en su personal.

Desglose de las misiones

A continuación encontrará el contenido organizado por semana, con sugerencias sobre qué recursos incluir y el texto correspondiente para los correos electrónicos.

A esta altura, esperamos que ya tenga algunas ideas o estrategias sobre cómo abordar el mes. Independientemente de cómo organice su campaña, le recomendamos enviar un correo electrónico introductorio el 1 de octubre, o incluso durante la última semana de septiembre.

Este es un ejemplo de texto:

Línea de asunto sugerida:
[INICIO DE LA MISIÓN] **Su incorporación a la División de Riesgos del Personal**

MES DE LA CONCIENTIZACIÓN SOBRE LA CIBERSEGURIDAD 2026 | **INICIO DE LA MISIÓN**

knowbe4

División de Riesgos del Personal: Informe inicial

Buenos días, agentes:

En el mundo de alto riesgo del ciberespionaje global, ustedes son el objetivo principal y nuestra línea de defensa más sólida.

Solo los equipos de agentes más alerta y con mejor preparación pueden resistir la ola de deepfakes creados con IA, sofisticados ataques de ingeniería social y la guerra en las sombras digitales que acecha en cada rincón de nuestra red.

El terreno es peligroso y no deberían operar de de manera aislada. Por suerte, hemos autorizado una serie de sesiones informativas para asegurarnos de que esté todo listo para la misión que les espera.

LA MISIÓN:

Este octubre celebramos el Mes de la Concientización sobre la Ciberseguridad incorporando a cada integrante de nuestro equipo a la División de Riesgos del Personal (DRP). Durante todo el mes, cuatro especialistas les brindarán informes; cada especialista representa un pilar fundamental de nuestra cultura de la seguridad.

Prepárense para una misión de cuatro semanas en la que cada etapa representa un nuevo nivel de conocimientos por dominar.

Manténganse alerta este mes con **[Inserte aquí las actividades o los temas planificados. Use las ideas de esta guía como inspiración.]**

Si tienen alguna pregunta, comuníquense con **[inserte el nombre de la persona de contacto]**.

El primer informe será el lunes. Permanezcan alerta, agentes. ¡Buena suerte!

SEMANA 1

Phishing e ingeniería social

Los equipos de espías más sofisticados no irrumpen; convencen a las personas para entrar. Esta semana se centra en las sutiles señales de alarma de la ingeniería social que los filtros técnicos podrían pasar por alto y en cómo identificarlas.

Este es un resumen de los recursos para esta semana:

Módulo de capacitación: Frenesí del smishing

En este módulo de siete minutos se presentan los peligros del smishing, es decir, el phishing mediante mensajes de texto, y muestra cómo su personal puede evitar convertirse en una víctima más de este tipo de ciberataque.

Su personal aprenderá lo siguiente:

- **Cómo la ciberdelincuencia puede utilizar la ingeniería social mediante mensajes de texto.**
- **Qué suele implicar un ataque de smishing.**

ACCEDER AL RECURSO

Recurso para ejercicio de simulación: Desenmascarar los ataques de phishing y whaling

Este ejercicio de simulación permite que el personal aprenda a identificar y responder a sofisticados ataques de phishing y whaling. Las personas participantes analizan un correo electrónico simulado de fraude de la dirección ejecutiva para distinguir entre indicadores falsos de confianza generados por IA y verdaderas señales de alerta en el comportamiento. Está diseñado para que el personal de cualquier nivel practique el pensamiento crítico y la aplicación de los procedimientos oficiales de su organización.

Dos recursos descargables

- **No muerda el anzuelo: reporte todos los intentos de phishing.** Afiche con un recordatorio sobre las señales más comunes de un correo electrónico de phishing y qué hacer si sospecha que un mensaje podría ser phishing.
- **Su función en la seguridad de Internet.** Infografía que recuerda al personal cuáles son las tácticas de ciberdelito más comunes y cómo evitarlas.

RECURSOS DE LA SEMANA 1

Compartir el contenido

Este es un ejemplo de texto de correo electrónico del especialista Espectro para compartir el módulo de capacitación de esta semana:

Línea de asunto sugerida:
[MISIÓN DE LA SEMANA 1] **Interceptar la amenaza del "smishing"**

knowbe4

Cómo interceptar la amenaza del "smishing"

MES DE LA CONCIENTIZACIÓN SOBRE LA CIBERSEGURIDAD 2026 | **MISIÓN DE LA SEMANA 1**

Buenos días, agentes:

Habla el especialista con nombre clave **Espectro**.

Nuestros dispositivos móviles son ahora los principales objetivos de las interferencias externas. La parte enemiga ha pasado de su bandeja de entrada a su bolsillo.

LA MISIÓN:
Complete el informe "Frenesí del smishing". Este módulo de capacitación presenta los peligros del smishing, o phishing mediante mensajes de texto, y le muestra cómo evitar convertirse en una víctima más de este tipo de ciberataque.

Aprenderá lo siguiente:

- **Cómo la ciberdelincuencia puede utilizar la ingeniería social mediante mensajes de texto.**
- **Qué suele implicar un ataque de smishing.**

Acceda aquí (https://training.knowbe4.com/modstore/view/af44ce18-ea58-47c9-a352-fb1f277ec903)

Si tiene alguna pregunta, envíe un comunicado a **[Inserte el nombre de la persona de contacto]**.

Tenga cuidado. Esté alerta a los próximos informes de este mes.

Espectro. Cambio y fuera.

PÁGINA

SEMANA 2

La IA y los deepfakes

Adéntrese en el lado más oscuro de la IA para enseñar a su personal cómo maleantes utilizan herramientas de IA generativa para crear clones y guiones perfectos. Sus agentes deben confiar en su recurso más valioso: su capacidad de pensamiento crítico para verificar qué es real.

Este es un resumen de los recursos para esta semana:

Módulo de video: Un ataque de ingeniería social mediante deepfakes

Este módulo de video de seis minutos presenta a integrantes del elenco de la popular serie de concientización sobre seguridad "The Inside Man", quienes muestran cómo la ciberdelincuencia utiliza la clonación de voz mediante IA y la tecnología de deepfakes en video para hacerse pasar por personas que usted podría conocer.

Su personal aprenderá lo siguiente:

- **Cómo la ciberdelincuencia puede utilizar los deepfakes y la ingeniería social para vulnerar las defensas de una organización mediante solicitudes simples.**
- **Señales de alarma a las que debe prestar atención para protegerse y proteger a su organización de sofisticados ataques con deepfakes.**

ACCEDER AL RECURSO

Módulo de capacitación: Protección de la propiedad intelectual

En este módulo de capacitación de 10 minutos, disponible en la Biblioteca Compliance Plus de KnowBe4, se explica la importancia de la propiedad intelectual, o PI.

Su personal aprenderá lo siguiente:

- **Qué es la PI y por qué es tan valiosa.**
- **Cómo proteger la PI contra el robo, la infracción y la divulgación accidental, incluso mediante el uso de inteligencia artificial.**

ACCEDER AL RECURSO

Recurso para ejercicio de simulación: El desafío de los prompts de IA

Este ejercicio de simulación prepara al personal para identificar los riesgos del uso de prompts inseguros en el lugar de trabajo. Las personas participantes analizarán prompts de IA para determinar cuáles son seguros y cuáles ponen en riesgo los datos privados. Diseñado para que el personal de cualquier nivel practique el pensamiento crítico y el cumplimiento de las políticas de su organización.

PÁGINA

Dos recursos descargables/de señalización digital

- **¿Real o falso? Identifique los deepfakes.** Afiche que recuerda la importancia de utilizar las pistas del contexto y el pensamiento crítico para ayudar a identificar deepfakes en el mundo real.
- **El phishing se vuelve más inteligente: Cómo la IA está cambiando las estafas en línea.** Infografía que explica cómo la IA hace que las estafas de phishing sean más difíciles de detectar.

RECURSOS DE LA SEMANA 2

Compartir el contenido

Este es un ejemplo de texto de correo electrónico del personaje especialista Tecno para compartir el recurso destacado que sugerimos para esta semana: el módulo "Un ataque de ingeniería social mediante deepfakes".

Línea de asunto sugerida:
[MISIÓN DE LA SEMANA 2] **Cómo detectar un deepfake**

knowbe4

Cómo detectar un deepfake

MES DE LA CONCIENTIZACIÓN SOBRE LA CIBERSEGURIDAD 2026 | **MISIÓN DE LA SEMANA 2**

Buenos días, agentes:

Especialista **Tecno**, reportándose.

Me molesta mucho ver que los avances en la tecnología de IA se utilicen para hacer el mal. Maleantes utilizan lo último en IA para clonar voces y crear deepfakes en video con los que se hacen pasar por colegas y personal de liderazgo. Cualquier persona a la que puedan duplicar para obtener el acceso y los datos que necesitan para llevar a cabo sus propias y perversas misiones se convierte en un objetivo.

LA MISIÓN:

Complete el informe en video *Un ataque de ingeniería social mediante deepfakes*. En este módulo se presenta información esencial de especialistas de "The Inside Man", quienes muestran cómo la ciberdelincuencia utiliza la clonación de voz mediante IA y la tecnología de deepfakes en video para hacerse pasar por personas que usted conoce.

Aprenderá lo siguiente:

- **Cómo la ciberdelincuencia puede utilizar los deepfakes y la ingeniería social para vulnerar las defensas de una organización mediante solicitudes simples.**
- **Señales de alarma a las que debe prestar atención para protegerse y proteger a su organización de sofisticados ataques con deepfakes.**

Acceda aquí (https://training.knowbe4.com/modstore/view/0451be1f-0531-4724-a664-21f109be6308)

Si tiene alguna pregunta, comuníquese con **[inserte el nombre de la persona de contacto]**.

Mantenga sus herramientas afiladas y su mente aún más. Esté alerta a los próximos informes de este mes.

Tecno, fuera.

SEMANA 3

Seguridad de los datos y contraseñas

Los datos delicados son una moneda de cambio en el mundo actual, y las personas maleantes están dispuestas a hacer cualquier cosa para obtenerlos. Asegúrese de que sus agentes conozcan el valor de aquello que protegen y lo que está en juego si esa información se ve comprometida. Esta semana se centra en el uso de administradores de contraseñas y la autenticación multifactor (MFA, por sus siglas en inglés) para garantizar que, incluso si se compromete su agente, los datos de la organización permanezcan cifrados.

Este es un resumen de los recursos para esta semana:

Módulo de capacitación para dispositivos móviles: Contraseñas seguras, cuentas protegidas

En este módulo de cinco minutos, diseñado para usarse en dispositivos móviles, se explica la importancia de las contraseñas seguras y las frases de contraseña en la vida laboral y personal de las personas usuarias.

Su personal aprenderá lo siguiente:

- **Consejos para crear contraseñas seguras y sólidas, y usar frases de contraseña de manera eficaz.**
- **Cómo evitar errores de seguridad comunes que dejan las cuentas vulnerables.**
- **Prácticas recomendadas para proteger las contraseñas y las frases de contraseña.**

ACCEDER AL RECURSO

Recurso para ejercicio de simulación: El juego de descifrar contraseñas

En este ejercicio de simulación, se pone al personal en el papel de hacker para que experimente cómo se vulneran las contraseñas débiles. Las personas participantes examinarán publicaciones en redes sociales e intentarán adivinar las contraseñas de quienes las poseen únicamente a partir de la información compartida en línea. Este ejercicio demuestra cómo la combinación de compartir demasiada información en línea y tener prácticas deficientes de creación de contraseñas facilita que maleantes vulneren las cuentas mediante ataques de fuerza bruta.

Dos recursos descargables/de señalización digital

- **Las contraseñas seguras protegen su tranquilidad en línea.** Afiche centrado en la importancia de las contraseñas seguras.
- **Datos delicados: Manténgalos en secreto. Manténgalos protegidos.** Infografía que explica los aspectos fundamentales para mantener segura la información delicada y por qué es importante hacerlo

RECURSOS DE LA SEMANA 3

Compartir el contenido

Este es un ejemplo de texto de correo electrónico *del* personaje especialista Llave Maestra para compartir el módulo de capacitación de esta semana:

Línea de asunto sugerida:
[MISIÓN DE LA SEMANA 3] **Cómo proteger la bóveda**

Buenos días, agentes:

Especialista **Llave Maestra**, reportándose desde... una ubicación bajo llave.

Un secreto es tan seguro como la cerradura que lo protege. Volvemos a los aspectos fundamentales con los protocolos adecuados para el uso de contraseñas. Que pueda parecer información para principiantes no significa que sea menos importante. Nuestras bóvedas más complejas no sirven de nada si las dejamos abiertas.

LA MISIÓN:

Complete el módulo de capacitación para dispositivos móviles "Contraseñas seguras, cuentas protegidas". Descubra por qué las frases de contraseña son más seguras que las contraseñas comunes y cómo evitar los errores más frecuentes que dejan nuestro perímetro desprotegido.

Aprenderá lo siguiente:

- **Consejos para crear contraseñas seguras y sólidas, y usar frases de contraseña de manera eficaz.**
- **Cómo evitar errores de seguridad comunes que dejan las cuentas vulnerables.**
- **Prácticas recomendadas para proteger las contraseñas y las frases de contraseña.**

Acceda aquí (https://training.knowbe4.com/modstore/view/c0ee0966-ff3a-4fc2-93bb-2a632811140b)

Si tiene alguna pregunta, envíe una comunicación cifrada a **[inserte el nombre de la persona de contacto]**.

Como dice quien más admiro en el mundo de la magia: Manténgalo en secreto. Manténgalo a salvo.

LM

SEMANA 4

Notificación de incidentes

En la División de Riesgos del Personal, mantener los oídos bien atentos es una parte fundamental de cualquier operación. No hay agente que pueda completar una misión por su cuenta, por lo que es fundamental que su personal comprenda la importancia de informar al equipo cuando algo no parece estar del todo bien. En esta semana, se garantiza que cada agente sepa exactamente cómo pedir refuerzos cuando detecten algo sospechoso.

Este es un resumen de los recursos para esta semana:

Audiocast "Hábitos a prueba de hackeos": Notificación de incidentes

Este audiocast de 15 minutos, dividido en módulos de cinco y diez minutos, analiza la importancia de notificar las amenazas de seguridad.

Su personal aprenderá lo siguiente:

- **Los posibles obstáculos que pueden surgir al notificar una amenaza de seguridad.**
- **Por qué notificar incidentes es un paso fundamental para combatir el ciberdelito.**
- **Un proceso de toma de decisiones que pueden utilizar para analizar situaciones y elegir acciones seguras.**

ACCEDER A LA PARTE 1

ACCEDER A LA PARTE 2

Juego "En busca de la privacidad"

Este juego interactivo de 15 minutos mejorará la comprensión de su personal sobre las leyes internacionales de privacidad de datos mediante una desafiante aventura alrededor del mundo que fortalecerá sus conocimientos sobre cumplimiento.

Su personal aprenderá lo siguiente:

- **La importancia de las regulaciones sobre privacidad de los datos.**
- **Diferentes enfoques regionales e internacionales sobre la privacidad de los datos.**

ACCEDER AL RECURSO

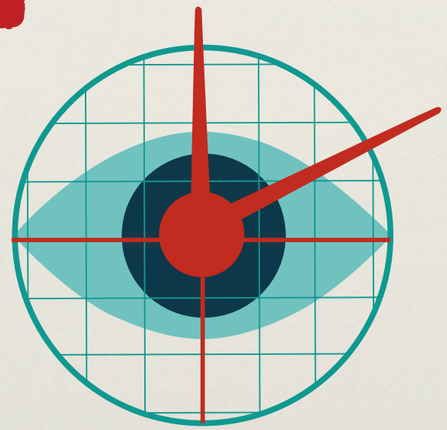
Recurso para ejercicio de simulación: Respuesta ante incidentes

Este completo plan de lecciones sobre respuesta ante incidentes guía al personal de la organización mediante ejercicios de simulación de crisis de seguridad. Las actividades se adaptan a participantes de cualquier nivel técnico y se centran en la identificación de funciones, la toma de decisiones y la coordinación del equipo. Las actividades incluyen priorizar listas de verificación de respuesta y realizar simulaciones realistas de escenarios con situaciones imprevistas. Las personas participantes aprenderán procedimientos establecidos de respuesta ante incidentes, comunicación entre distintas áreas y capacidad de adaptación durante incidentes de seguridad mediante ejercicios prácticos y sesiones estructuradas de análisis.

Dos recursos descargables/de señalización digital

- **Un reporte, protección compartida.** Afiche que destaca la importancia de reportar rápidamente los correos electrónicos sospechosos para proteger información personal, colegas y datos de la clientela.
- **Phishing, seguridad física y violaciones de seguridad de datos.** Infografía que le recuerda al personal por qué reportar de inmediato las inquietudes relacionadas con la seguridad evita que los problemas pequeños se conviertan en incidentes graves.

RECURSOS DE LA SEMANA 4



Compartir el contenido

Este es un ejemplo de texto de correo electrónico de la especialista Vigía para compartir el audiocast y el módulo del juego de esta semana:

Línea de asunto sugerida:
[MISIÓN DE LA SEMANA 4] **Mantenga informado al equipo**

knowbe4

Mantenga informado al equipo

MES DE LA CONCIENTIZACIÓN SOBRE LA CIBERSEGURIDAD 2026 | MISIÓN DE LA SEMANA 4

Buenos días, agentes:

Vigía reportándose con un último informe y resumen de situación.

Nuestras misiones solo tienen éxito si la DRP sabe qué está ocurriendo sobre el terreno y en el mundo real.

Reportar incidentes no es delatar. Es transmitir información esencial para que nuestros equipos puedan proteger el perímetro y mantener a raya a maleantes.

Su cuarto y último informe tiene dos partes:

LA MISIÓN:

Escuche: Hábitos a prueba de hackeos: notificación. Domine un proceso fundamental de toma de decisiones en seguridad de la información para analizar amenazas en tiempo real.

Acceda a la Parte 1 (https://training.knowbe4.com/modstore/view/ad7bb017-916b-442f-b1e7-4f96bf6b202f)

Juegue: En busca de la privacidad. Viaje por el mundo (de forma virtual) y ponga a prueba sus conocimientos sobre las prácticas internacionales de privacidad de datos para conocer mejor qué está en juego cuando se producen incidentes de una posible violación de seguridad de datos.

Acceda a la Parte 2 (https://training.knowbe4.com/modstore/view/a5ec90a8-956b-4675-8c63-c336812752e7)

Si tiene alguna pregunta, comuníquese con **[inserte el nombre de la persona de contacto]**.

Aquí Vigía. Me despido en nombre de todo el equipo de la DRP.

INFORME FINAL DE LA MISIÓN:

Mantenga el riesgo del personal siempre presente

El equipo de liderazgo de la DRP espera que este dossier de la misión y los recursos proporcionados le hayan ayudado a brindar a su personal las habilidades y las herramientas necesarias para hacer frente a ciberamenazas de todo tipo.

Establecer y mantener una sólida cultura de la seguridad es una misión permanente. Lograr un cambio real y positivo en el comportamiento requiere una estrategia que transforme la mayor superficie de ataque de su organización —su personal— en su principal fortaleza y, de ese modo, reduzca el riesgo del personal.

Considere estos recursos como un complemento de un enfoque integral de concientización sobre seguridad y capacitación. Si desea saber cómo KnowBe4 puede ayudarle a dar el siguiente paso, contáctenos.

Para acceder a más recursos e información para usted y su personal durante el Mes de la Concientización sobre la Ciberseguridad, no deje de seguir y mencionar a @KnowBe4 en las redes sociales. Utilice las etiquetas #CyberAware y #CyberSecMonth para mantenerse al tanto durante todo el Mes de la Concientización sobre la Ciberseguridad.

knowbe4