

Capacitación en concientización sobre seguridad y plataforma de simulación de phishing

Lo ayuda a gestionar el problema constante de la ingeniería social

Capacitación en concientización sobre seguridad de KnowBe4

Su personal está expuesto con frecuencia a ciertos ataques de phishing y ransomware que son muy sofisticados. Es fundamental que forje una cultura que dé prioridad a la seguridad mediante capacitaciones entretenidas y avaladas.

- ▶ **Realice pruebas iniciales**
Ofrecemos pruebas iniciales para evaluar el porcentaje de Phish-prone™ (predisposición para ser víctima de phishing) de sus usuarios simulando de forma gratuita un ataque de phishing.
- ▶ **Ponga a prueba a sus usuarios contra el phishing**
Implemente los mejores ataques de phishing simulados y totalmente automatizados. Miles de plantillas de uso ilimitado y plantillas de phishing de la comunidad.
- ▶ **Capacite a sus usuarios**
La biblioteca más grande del mundo con contenido de la capacitación en concientización sobre seguridad: módulos interactivos, videos, juegos, afiches y boletines informativos. Campañas de capacitación automatizadas con recordatorios programados por correo electrónico.
- ▶ **Vea los resultados**
Genere informes de nivel empresarial, que muestran estadísticas y gráficos para capacitación y phishing, listos para administrar.



Funciones de la capacitación en concientización sobre seguridad de KnowBe4

- **Uso ilimitado**

Ofrecemos tres niveles de acceso a la capacitación a través de ModStore de KnowBe4, los cuales le permiten ingresar a nuestra biblioteca de contenido de más de 1300 elementos según su nivel de suscripción. Se brinda acceso ilimitado a todas las funciones de phishing con licencias flexibles. Agregamos nuevas funciones potentes con regularidad.
- **Experiencia de aprendizaje y consola de administrador localizadas**

Puede configurar su propio idioma predeterminado en tres ajustes de localización: Idioma de la Consola de administrador, Capacitación y Phishing (suplantación de identidad). Con estas opciones de localización, puede habilitar a sus administradores para que controlen la consola de KnowBe4 en uno de los diez idiomas para elegir, además de ofrecer una experiencia de capacitación más inmersiva para sus aprendices en más de 35 idiomas.
- **Administrador de contenido**

Con el Administrador de contenido, puede personalizar sus preferencias de contenido de la capacitación sin esfuerzo. Ajuste los puntajes de aprobación, incorpore temas de marca, permita que se realicen pruebas y dígame adiós a la omisión de contenido. Disponible en todos los niveles de suscripción.
- **Contenido comercializable**

Con esta función de autoservicio, puede agregar contenido personalizado de marca al principio y al final de determinados módulos de capacitación de KnowBe4. Puede agregar los elementos de la marca de su empresa, por ejemplo, logotipo, gráficos personalizados y colores corporativos para adaptar cualquier mensaje que desee transmitirles a sus usuarios.
- **Cargue su propio contenido**

¿Quiere complementar su contenido de la capacitación en concientización sobre seguridad de KnowBe4 con la capacitación personalizada de su empresa u otro tipo de capacitación corporativa? Gracias al sólido sistema de gestión de aprendizaje (Learning Management System, LMS) de KnowBe4, puede cargar su contenido de capacitación y video de conformidad con el estándar SCORM y gestionarlo junto con el contenido de su capacitación de ModStore de KnowBe4, todo en un solo lugar, ¡y sin costo adicional!
- **Evaluaciones**

Descubra el nivel de sus usuarios tanto en conocimientos como en cultura de la seguridad para ayudar a establecer métricas de seguridad de referencia. Utilice la evaluación basada en habilidades y la encuesta de cultura de la seguridad (SCS) para medir y monitorear el conocimiento y el sentimiento de seguridad de sus usuarios, a fines de construir una cultura consciente de la seguridad a lo largo del tiempo.
- **Personalice las páginas de inicio y las plantillas de phishing**

Además de las decenas de miles de plantillas del sistema que son muy fáciles de usar, puede personalizar los escenarios según la información personal e incluir archivos adjuntos simulados para crear sus propias campañas específicas de spear phishing (suplantación de identidad específica). Cada plantilla de correo electrónico de phishing puede tener su propia página de inicio personalizada, lo que permite la educación sobre el punto de error.
- **Phish Alert Button**

El complemento Phish Alert Button (Botón de alerta de phishing) de KnowBe4 les brinda a sus usuarios una forma segura de reenviar las amenazas de correo electrónico al equipo de seguridad para que puedan analizarlas, y elimina el correo electrónico de la bandeja de entrada del usuario para evitar la exposición futura. ¡Y todo con un solo clic!
- **Indicadores de ingeniería social (SEI)**

La tecnología patentada convierte cada correo electrónico de phishing simulado en una herramienta que puede utilizar el departamento de TI para capacitar de forma dinámica a los empleados mostrándoles al instante las señales de alarma ocultas que pasaron por alto en ese correo electrónico.
- **Recomendaciones para la capacitación y phishing basados en IA**

Aproveche el poder de la inteligencia artificial (IA) para ofrecer a sus usuarios una experiencia más personalizada que se adapte a su nivel actual de conocimientos. Utilice el phishing basado en IA a fin de elegir automáticamente la mejor plantilla de phishing para cada uno de sus usuarios según su historial de phishing y capacitación en particular. Gracias a las recomendaciones de capacitación basada en IA, ModStore de KnowBe4 ofrece contenido de capacitación personalizado según el porcentaje general de Phish-prone™ de su organización.

Funciones de la capacitación en concientización sobre seguridad de KnowBe4 (continuación)

- **Gestión de usuarios**
La integración de Active Directory o SCIM de KnowBe4 le permite cargar fácilmente los datos de cada usuario y ahorrar tiempo al eliminar la necesidad de administrar manualmente los cambios del usuario. También puede aprovechar la función de Grupos inteligentes para personalizar y automatizar sus campañas de phishing, asignaciones de capacitación y aprendizaje correctivo según el comportamiento de su personal y los atributos del usuario.
- **Función de Informes avanzados**
Más de 60 informes incorporados con vistas integrales e información detallada acerca de sus indicadores clave de capacitación sobre concienciación a lo largo del tiempo. Aproveche las API de generación de informes para extraer datos de su consola de KnowBe4. Además, con los Informes ejecutivos, puede crear y entregar informes personalizados a nivel ejecutivo que proporcionan información para ayudar a tomar decisiones basadas en datos sobre su programa.
- **Virtual Risk Officer™**
La innovadora funcionalidad Virtual Risk Officer (VRO) utiliza el aprendizaje automático para ayudarlo a predecir e identificar el riesgo a nivel del usuario, el grupo y la organización. Este modelo de aprendizaje continuo le permite tomar decisiones basadas en datos cuando se trata de su programa en concientización sobre seguridad.
- **Phishing de devolución de llamada**
Como administrador, puede usar la función de Phishing de devolución de llamada en su consola de KnowBe4 y ejecutar una campaña de simulación de phishing de devolución de llamada para ver si su personal caería en la trampa. Se envía un correo electrónico a su bandeja de entrada, con un número telefónico y un código. Si marcan el número, se les pedirá el código.
- **PhishER Plus™**
PhishER Plus es una plataforma liviana de respuesta ante incidentes que analiza y prioriza de manera automática los mensajes de correo electrónico que hayan sido reportados, a fin de detectar y poner en cuarentena los correos maliciosos en toda su organización. Además, PhishFlip convierte los correos electrónicos de phishing del mundo real en oportunidades de capacitación, a modo de campañas de phishing simuladas.

PhishER Plus suma una lista de bloqueo de origen colectivo y validada por IA a las capacidades de PhishRIP para bloquear y eliminar de forma proactiva los ataques de phishing activos que han eludido los filtros de correo electrónico ANTES de que los usuarios se expongan a ellos. Ahorra un importante tiempo y presupuesto al equipo de Seguridad de la Información mediante la reducción del volumen de esfuerzos correctivos que gestiona su equipo del SOC.

¿Sabía que el 88 % de las violaciones de seguridad de datos ocurren debido a un error humano?

Obtenga su prueba de seguridad contra el phishing (PST) gratuita y descubra qué porcentaje de su personal tiene predisposición para ser víctima de phishing (Phish-prone)