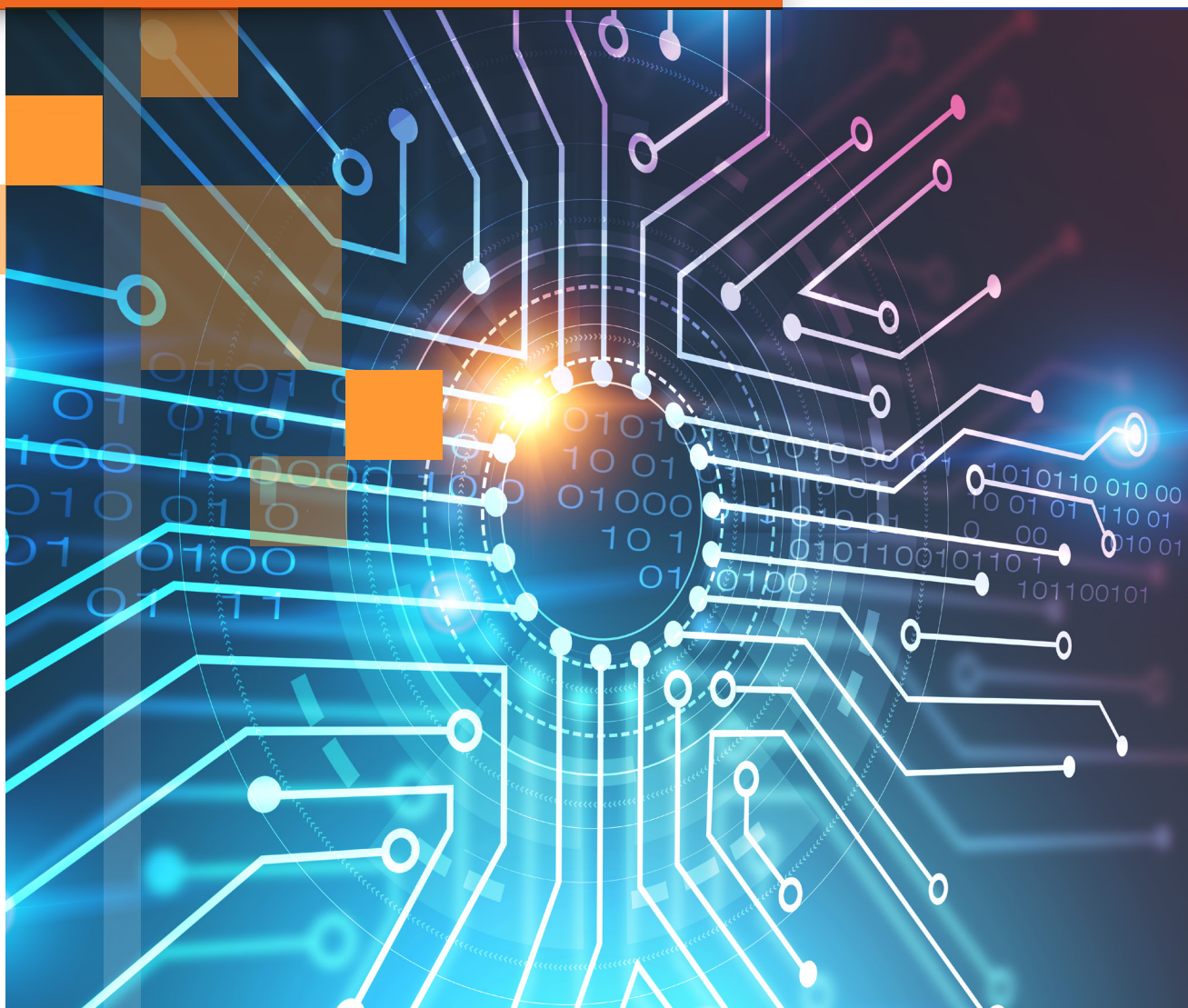
KnowBe4
Human error. Conquered.

Guía para el comprador

Plataforma de capacitación en concientización sobre seguridad y phishing simulado



Guía para el comprador:
Plataforma de capacitación en concientización sobre seguridad y phishing simulado

Índice

KnowBe4 es la plataforma integrada más grande del mundo para capacitación en concientización sobre seguridad y phishing simulado. En esta guía, encontrará información sobre lo siguiente:

- Por qué es necesaria la capacitación en concientización sobre seguridad.
- Qué ofrece la plataforma KnowBe4.
- Cuáles son las características fundamentales que deben buscarse en cualquier proveedor de capacitación en concientización sobre seguridad.

El problema constante de la ingeniería social

Sus empleados son el eslabón más débil en la seguridad de TI. La ingeniería social es la principal amenaza de seguridad para cualquier organización. El preocupante crecimiento de los ataques cibernéticos sofisticados solo empeoran el problema, ya que los ciberdelincuentes aprovechan el punto más débil: los empleados. Numerosos informes y documentos técnicos demostraron que en los últimos cinco años las organizaciones estuvieron expuestas a un aumento masivo en la cantidad de ataques cibernéticos.

Como los responsables de las amenazas se centran en sus empleados, es necesario realizar una capacitación en concientización sobre seguridad. La capacitación en concientización sobre seguridad es una forma de educación que busca brindar a los integrantes de una organización la información necesaria para protegerse a sí mismos y a los activos de su organización ante pérdidas o daños.

El objetivo de la capacitación en concientización sobre seguridad es dotar a sus empleados de los conocimientos adecuados para combatir estas amenazas. No se puede esperar que los empleados sepan por su cuenta qué amenazas existen o cómo lidiar con ellas. Es preciso enseñarles lo que sus empleadores consideran arriesgado o aceptable, qué pistas deben buscar que indiquen amenazas y cómo responder cuando las adviertan.

"Las personas acostumbran a tener una solución tecnológica [pero] la ingeniería social elude a todas las tecnologías, incluidos los firewall. La tecnología es fundamental, pero debemos observar a las personas y los procesos. La ingeniería social es una forma de piratería informática que utiliza tácticas de influencia".

— Kevin Mitnick

La estrategia de KnowBe4: el phishing, la capacitación y el análisis

KnowBe4 ayuda a decenas de miles de clientes a gestionar el problema constante de la ingeniería social. Contamos con la biblioteca de contenidos de la capacitación en concientización sobre seguridad más grande del mundo, que incluye módulos interactivos, videos, juegos, carteles y boletines informativos, para que sus empleados puedan tomar decisiones más inteligentes en materia de seguridad todos los días: esa es nuestra misión.

KnowBe4 cuenta con dos ventajas competitivas. En primer lugar, con distintas herramientas y fuentes de información, proporcionamos a la organización una buena perspectiva de su perfil de riesgo actual. Este paso, que muchas veces omiten los competidores, es necesario para seleccionar las medidas de defensa apropiadas y disminuir eficazmente el riesgo. En segundo lugar, al centrarse en la inteligencia de amenazas locales, KnowBe4 le permite prestar mayor atención a detener las amenazas específicas que su entorno recibe y que son exitosas. La mayoría de los proveedores de capacitación en concientización sobre seguridad se centran principalmente en el uso de las estadísticas de correo electrónico de phishing recopiladas a nivel mundial de todos los intentos de phishing y de los clientes, y comunican las tendencias mundiales como si fueran las que más deberían preocuparle a usted también. KnowBe4 informa sobre las tendencias mundiales emergentes; pero da a los administradores de TI el poder de ver cómo los intentos y éxitos locales de phishing difieren de los del resto del mundo y cómo responder en consecuencia.

KnowBe4 utiliza una estrategia polifacética, que comienza con conocer la postura de riesgo específica de su organización, y luego le permite aprovechar tanto el impulso global de los intentos de phishing del mundo real, como de los que han logrado superar sus defensas específicas:

Pruebas de referencia

Proporcionamos pruebas de referencia para evaluar el porcentaje de Phish-prone™ (predisposición a ser víctima de phishing) de sus usuarios a través de un ataque de phishing simulado gratuito.

Capacite a sus usuarios

Aproveche la biblioteca de contenido de la capacitación en concientización sobre seguridad más grande del mundo, que incluye módulos interactivos, videos, juegos, carteles y boletines informativos. Campañas de capacitación automatizadas con recordatorios programados por correo electrónico.

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.

Observe los resultados

Descubra la generación de informes sobre la seguridad empresarial, con estadísticas y gráficos tanto para la capacitación en concientización sobre seguridad como para el phishing, listos para que la gerencia muestre sus éxitos y áreas de mejora.

Siga leyendo esta guía para conocer nuestra gama de contenidos de capacitación y las distintas funciones disponibles en nuestra plataforma de capacitación y phishing simulado.

La biblioteca de capacitación y el contenido de phishing simulado de KnowBe4

Biblioteca de capacitación

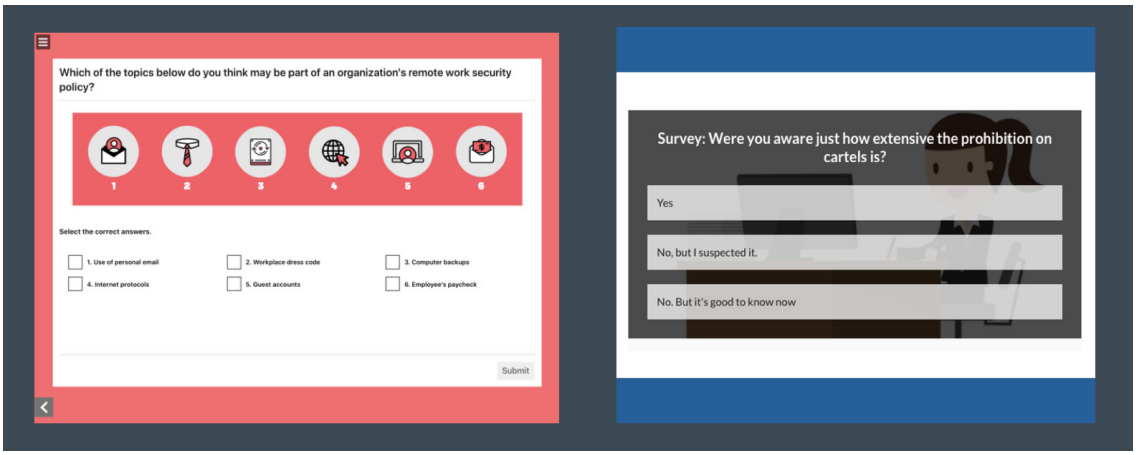
KnowBe4 ofrece la biblioteca de contenido de la capacitación en concientización sobre seguridad más grande del mundo, que se actualiza constantemente y que incluye módulos interactivos, videos, juegos, carteles y boletines informativos.

Para facilitar el acceso de los clientes a esta biblioteca de contenidos, KnowBe4 cuenta con “ModStore”. Los clientes pueden utilizar ModStore para buscar, examinar y obtener una vista previa del contenido y, según el nivel de suscripción, añadir el contenido de capacitación elegido a la biblioteca de su cuenta de KnowBe4.

Nuestras asociaciones con proveedores de contenidos de aprendizaje electrónico y concientización sobre seguridad de todo el mundo aportan una variedad y un estilo únicos a la colección para garantizar que las campañas de capacitación se mantengan actualizadas y sean relevantes e interesantes para sus usuarios. ModStore dispone de una gran variedad de contenidos sobre diferentes temas y tipos de contenidos.

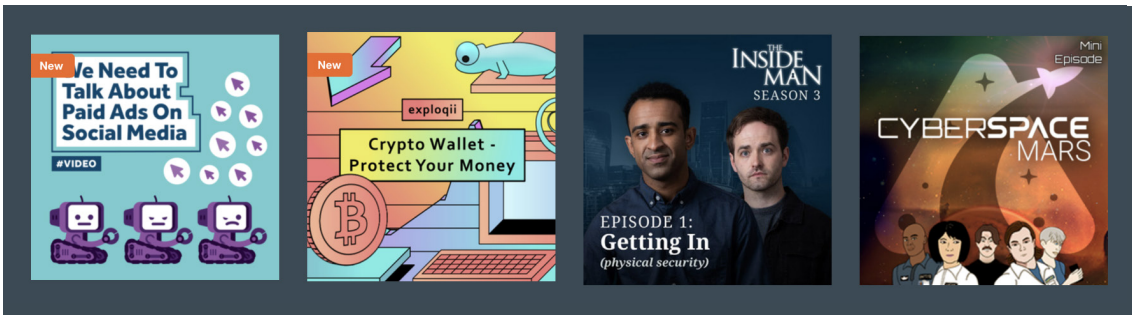
Módulos de capacitación

Los módulos de capacitación son módulos interactivos que abarcan una amplia gama de temas. Los módulos cumplen con el estándar SCORM y pueden descargarse para utilizarlos con su propio sistema de gestión de aprendizaje (Learning Management System, LMS). Cientos de módulos de capacitación se pueden comercializar.



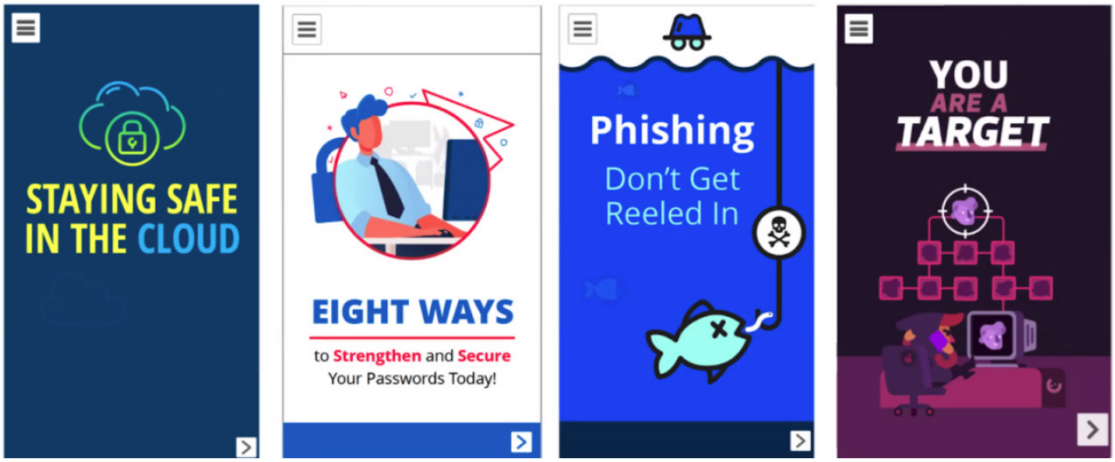
Módulos de videos

Los videos son archivos MP4 que pueden verse en el navegador o descargarse para utilizarlos con su LMS.



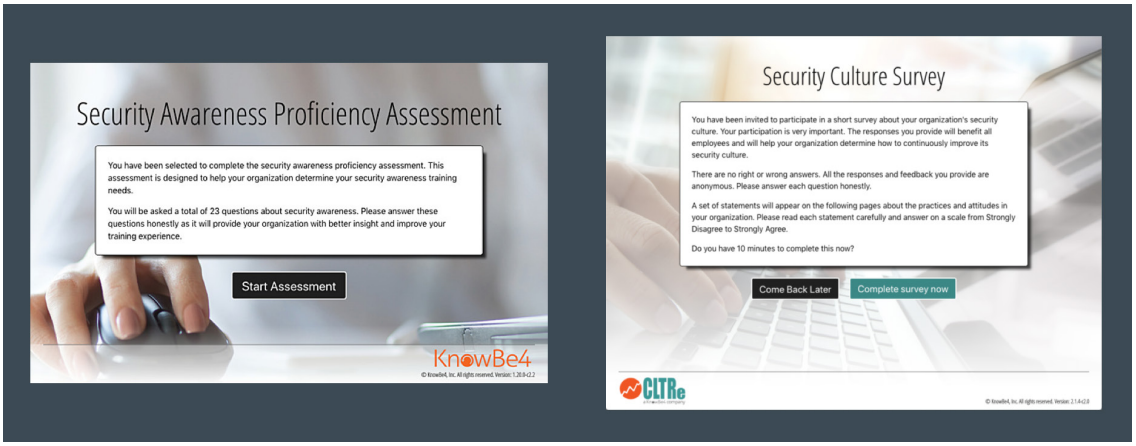
Módulos Mobile-First

Los módulos Mobile-First están optimizados para que tanto su visualización como la interacción con ellos se lleven a cabo desde un dispositivo móvil. Estos módulos no duran más de cinco minutos y están pensados para captar el interés de los usuarios, ya sea mientras se desplazan o se encuentran en regiones con poco ancho de banda. Los módulos Mobile-First se pueden comercializar y cumplen con el estándar SCORM, por lo que se pueden descargar para utilizarlos con su LMS.



Evaluaciones

Las evaluaciones permiten desglosar los puntos fuertes y débiles de su organización. Puede utilizar los resultados de la evaluación para crear un plan de capacitación en concientización sobre seguridad más específico.

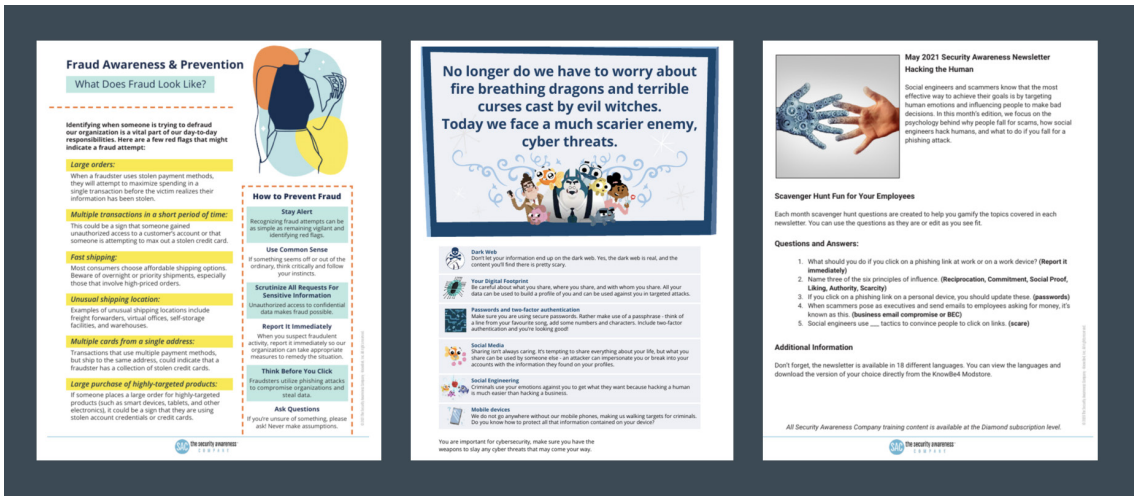


Juegos

Los juegos pueden reforzar las habilidades y la información que sus usuarios están aprendiendo de una manera nueva e interesante. Los juegos cumplen con el estándar SCORM y pueden descargarse para utilizarlos con su LMS.

Boletines informativos y documentos de seguridad

Los boletines informativos y los documentos de seguridad son archivos PDF que pueden imprimirse o compartirse de manera digital con sus usuarios. Estos documentos cubren una amplia gama de temas de ciberseguridad para ayudar a reforzar las habilidades que sus usuarios aprenden en la capacitación.



Carteles e ilustraciones

Los carteles y las ilustraciones son imágenes de alta calidad y archivos PDF que pueden imprimirse o compartirse de manera digital con sus usuarios. Le recomendamos que cuelgue carteles en su oficina o los distribuya en las oficinas que los empleados tienen en sus casas para que sirvan de recordatorio visual de que deben tener presente la seguridad en sus tareas cotidianas.

Niveles de acceso a la capacitación

Ofrecemos tres niveles de acceso a la capacitación: I, II y III, según su nivel de suscripción. El contenido de la capacitación en concientización sobre seguridad de cada nivel se ha elaborado cuidadosamente de forma que complemente el nivel anterior, y todas las suscripciones ofrecen distintos niveles de compatibilidad con varios idiomas y opciones de contenido apto para dispositivos móviles. Para ver toda nuestra biblioteca y sus constantes actualizaciones en tiempo real, regístrese para acceder a la vista previa de la capacitación de ModStore de KnowBe4.

Nivel de acceso a la capacitación I (Plata)

El nivel de acceso a la capacitación I le proporciona los elementos fundamentales necesarios para iniciar un programa de capacitación en concientización sobre seguridad. Es ideal para las organizaciones que no cuentan con una capacitación en concientización sobre seguridad y quieren comenzar al menos un programa de capacitación anual. Obtendrá módulos de capacitación y video, evaluaciones y refuerzos educativos, como documentos de seguridad y carteles. Vemos que muchos clientes comienzan con el nivel I para que sus usuarios aprendan sobre los aspectos básicos de la concientización sobre seguridad, como entender qué es la ingeniería social, y luego se dan cuenta de que están preparados para pasar al siguiente nivel de contenido de capacitación que profundiza en otros temas de ciberseguridad. Cuando la capacitación anual ya no es suficiente, y está listo para lanzar campañas de capacitación más frecuentes, los niveles de acceso a la capacitación II y III le permiten desarrollar un programa de capacitación en concientización sobre seguridad más sólido y completamente consolidado.

Nivel de acceso a la capacitación II (Oro y Platino)

La biblioteca del nivel de acceso a la capacitación II tiene como base el nivel I y se amplía para ofrecer una mayor variedad de estilos, formatos y temas en los contenidos de capacitación. El nivel II, que abarca desde la animación hasta la acción en vivo y el aprendizaje a ritmo propio, le permite ofrecer una capacitación más específica según los roles de sus usuarios, su ubicación en el mundo y el sector de su organización. Además, debido a la variedad de módulos de capacitación de cinco minutos o menos, es fácil establecer una cadencia más frecuente de campañas de capacitación que mantengan a sus usuarios interesados. Si se realizan más capacitaciones y con mayor frecuencia, será posible impulsar un cambio de comportamiento en el que la concientización sobre seguridad sea lo más importante.

Nivel de acceso a la capacitación III (Diamante)

El nivel de acceso a la capacitación III incluye todo el contenido de capacitación de los niveles I y II, más el acceso a la biblioteca más completa de contenido de la capacitación en concientización sobre seguridad. Esto mejora la capacidad de su organización para ofrecer un programa de concientización totalmente consolidado de forma continua. El nivel III contiene diversas series de video galardonadas de alta definición que relacionan las escenas de cada episodio con las prácticas recomendadas clave de ciberseguridad, lo que hace que aprender a tomar decisiones de seguridad más inteligentes a través de aplicaciones del mundo real sea divertido y atrapante. La amplia gama de temas, formatos, longitudes y estilos de diversos publicadores de contenido le permite disponer de más opciones de contenido para satisfacer las necesidades exclusivas de sus usuarios y alinearse con la cultura corporativa de su organización. Con el nivel III, puede probar diferentes estilos y formatos con diferentes segmentos de audiencia para maximizar el compromiso de los usuarios. Este nivel también le da la flexibilidad de mezclar las cosas para perfeccionar el contenido que resuena mejor en los distintos departamentos y ubicaciones regionales. Puede crear campañas de capacitación más cortas y frecuentes que faciliten la implementación de su programa de concientización durante todo el año. Retenga el interés de sus alumnos con una cadencia constante de campañas que utilicen una gran variedad de contenidos sobre las prácticas recomendadas de seguridad. Esta mezcla de contenido actualizado generará memoria muscular a lo largo del tiempo sin necesidad de utilizar la misma capacitación una y otra vez.

Publicadores de capacitación

Descubra un poco sobre cada uno de los publicadores a continuación y encuentre la mejor combinación para crear su propio programa polifacético y consolidado de capacitación en concientización sobre seguridad.

KnowBe4

El contenido interactivo de la capacitación en concientización sobre seguridad que han desarrollado KnowBe4 y Kevin Mitnick expone casos reales en los que Kevin, el hacker más famoso del mundo, lleva a los alumnos entre bastidores para que vean cómo los ciberdelincuentes hacen lo que hacen. El contenido de capacitación de KnowBe4 cuenta con la combinación adecuada de gráficos y texto para mantener a los alumnos interesados e incorporando la información. Los módulos y videos de capacitación contienen consejos y sugerencias prácticas, personajes memorables y tramas asombrosas.

The Security Awareness Company (SAC)

SAC ofrece una variedad de capacitaciones fundamentales repletas de información. El contenido se ha elaborado minuciosamente para maximizar la comprensión, la retención y el cambio de comportamiento con una línea de cursos muy completa que también incluye revisión de conocimientos, interacciones con el curso, cuestionarios, juegos, documentos y boletines informativos mensuales.

Popcorn Training

Todos aman una buena historia. Esta capacitación despierta las emociones, activa la imaginación y motiva a los alumnos a pasar a la acción. Las animaciones coloridas, los videos de acción en vivo y los cuestionarios ayudan a reforzar el aprendizaje y vienen con documentos de seguridad y carteles complementarios para afianzar los mensajes clave.

Exploqii

Capacitación en concientización sobre seguridad simplificada. Videos de capacitación rápidos y de tamaño reducido, presentados con animaciones vívidas y coloridas. Este contenido se centra en transmitir un mensaje fácil de procesar y retener.

Twist & Shout

Entretenimiento educativo sazonado con humor que seguramente será un éxito instantáneo. Estos videos inspirados en series de televisión lo reúnen todo para crear una capacitación que se sienta personal, real, agradable y con la que los alumnos se puedan identificar.

El Pescador

Las coloridas animaciones dan vida a la capacitación. Las aventuras del memorable capitán El Pescador harán que los alumnos estén atentos a los consejos de concientización sobre seguridad con una gran variedad de módulos de capacitación, videos, carteles y documentos.

CLTRe

La encuesta de cultura de la seguridad (SCS) de CLTRe proporciona un método eficaz y fácil de usar para evaluar el estado actual de su cultura de la seguridad y hacer un seguimiento de los cambios en esta a lo largo del tiempo. La encuesta de cultura de la seguridad utiliza métodos y principios científicos sociales comprobados para proporcionar resultados fiables y fundamentados que permitan a las organizaciones evaluar, construir y mejorar su cultura de la seguridad.

Universidad Saya

Los módulos de microaprendizaje de la Universidad Saya se redactan y producen originalmente de forma que representen las voces reales y el panorama socioeconómico y de amenazas en Japón con el fin de garantizar que todas las personas dispongan de información para protegerse de las amenazas globales de la ciberseguridad.

MediaPRO

Los módulos interactivos y los videos cortos garantizan que las lecciones sean atrapantes y que la información se retenga. En ellos, se cubren temas como las normativas sobre la privacidad de datos, el cumplimiento corporativo y la prevención del acoso sexual.

Capacitación de Compliance Plus

(Disponible como complemento en cualquier nivel de suscripción)

La capacitación de Compliance Plus de KnowBe4 es interactiva, relevante y atrapante; incluye escenarios simulados de la vida real para ayudar a enseñar a sus usuarios cómo reaccionar ante una situación difícil. El contenido aborda temas delicados como el acoso sexual, la diversidad y la inclusión, la discriminación y la ética empresarial. La biblioteca de Compliance Plus ofrece varios tipos de formatos multimedia y materiales de refuerzo para respaldar su programa de capacitación en materia de cumplimiento.

Contenido de phishing simulado

Nuestra amplia biblioteca de plantillas le permite utilizar la plataforma de KnowBe4 para “phishing listo para usar”. Puede ponerse en funcionamiento en menos de 30 minutos.

Plantillas de correo electrónico

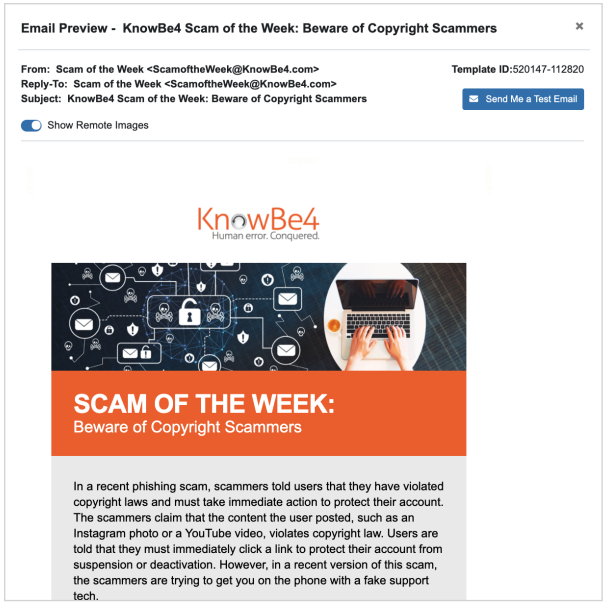
Nuestra biblioteca de plantillas en varios idiomas incluye correos electrónicos de más de 30 categorías, como por ejemplo: Banca y finanzas, redes sociales, TI, Gobierno, servicios en línea, eventos actuales, atención médica y mucho más. Además, tiene acceso a una sección comunitaria donde puede intercambiar plantillas con miles de otros clientes de KnowBe4.

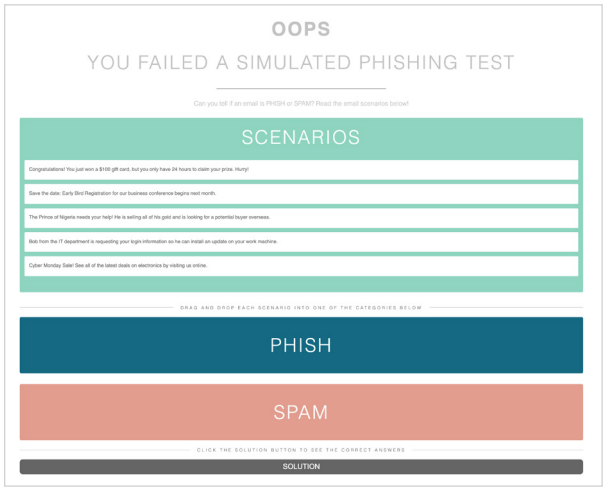
Plantillas de páginas de inicio

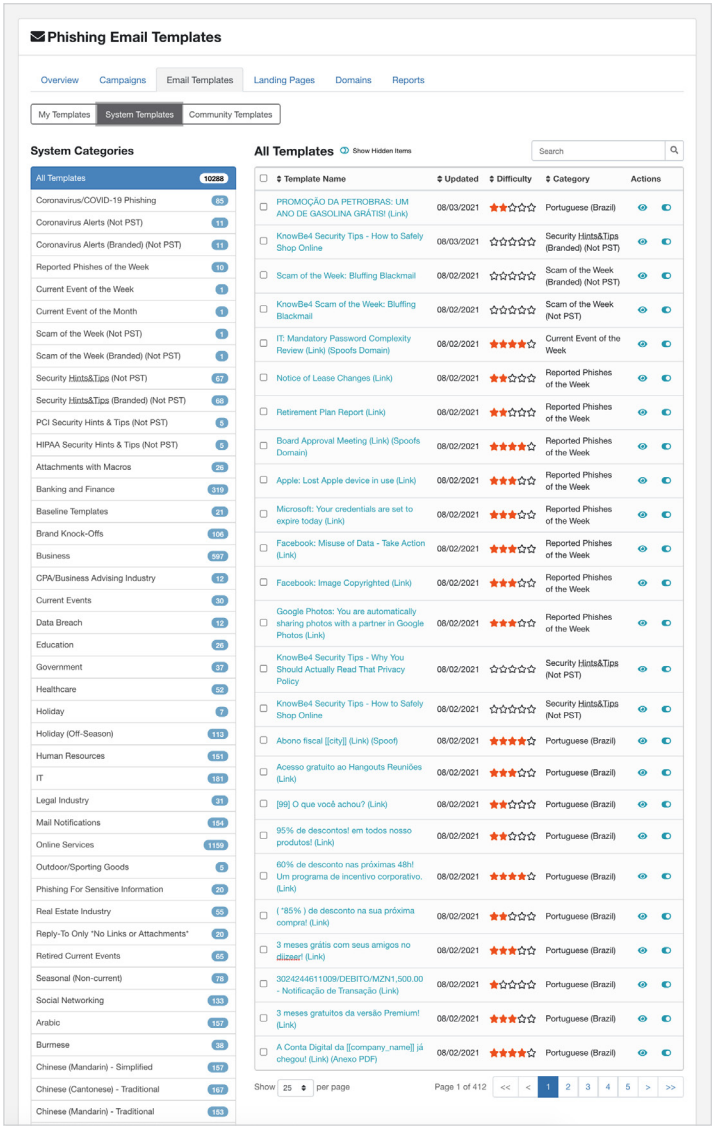
Cada plantilla de correo electrónico de phishing también puede tener su propia página de inicio personalizada, lo que permite capacitar con respecto al punto de error y las páginas de inicio que suplantan identidades para obtener información delicada específicamente. Podrá elegir entre más de 200 páginas de inicio para influir en la reacción de sus usuarios ante una prueba de phishing. Hay tres opciones para establecer qué página de inicio verán sus usuarios cuando fallen sus pruebas de phishing. Gracias a la compatibilidad con las páginas aptas para dispositivos móviles, puede 1) personalizar su página de inicio predeterminada, 2) elegir una página de inicio específica para la campaña o 3) establecer una página de inicio específica para la plantilla.

Boletines informativos

Como parte de las categorías de plantillas de phishing de KnowBe4, tiene acceso a los boletines informativos “Estafa de la semana” y “Sugerencias y consejos de seguridad” para mantener a sus usuarios al tanto de las últimas estafas de phishing y ayudar a reforzar los consejos básicos de seguridad. Puede utilizar estos boletines informativos como parte de una campaña semanal, quincenal o mensual al configurar una campaña de phishing en la consola de KnowBe4.







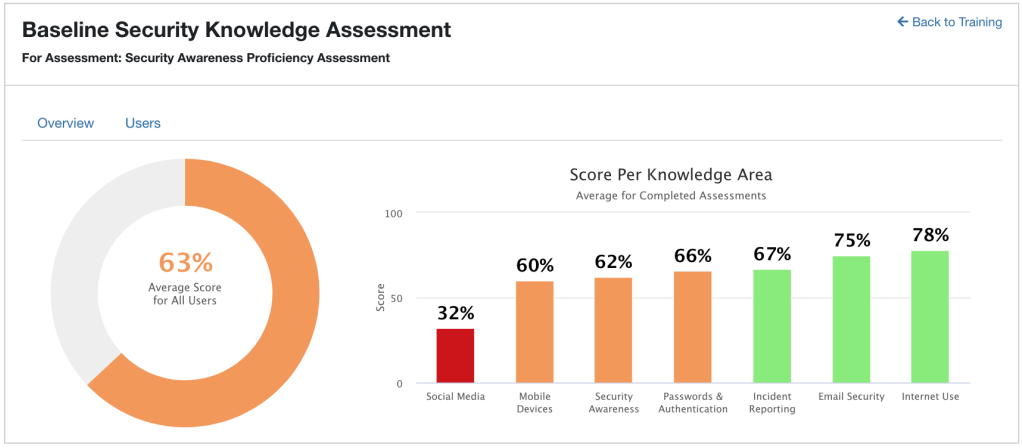
Evaluaciones

Averigüe en qué punto se encuentran sus usuarios con respecto a los conocimientos de seguridad y a la cultura de la seguridad para facilitar el establecimiento de métricas de seguridad de referencia que pueda mejorar con el tiempo.

Las evaluaciones de KnowBe4, integradas en la plataforma de KnowBe4 sin costo adicional, le permiten determinar quiénes son los usuarios que saben cuáles son las acciones más seguras a tomar ante situaciones de riesgo y cómo llevarlas a cabo. Este conocimiento le permitirá establecer un punto de referencia para la cultura de la seguridad que intenta lograr en su organización y hacer un seguimiento del éxito de sus programas de capacitación.

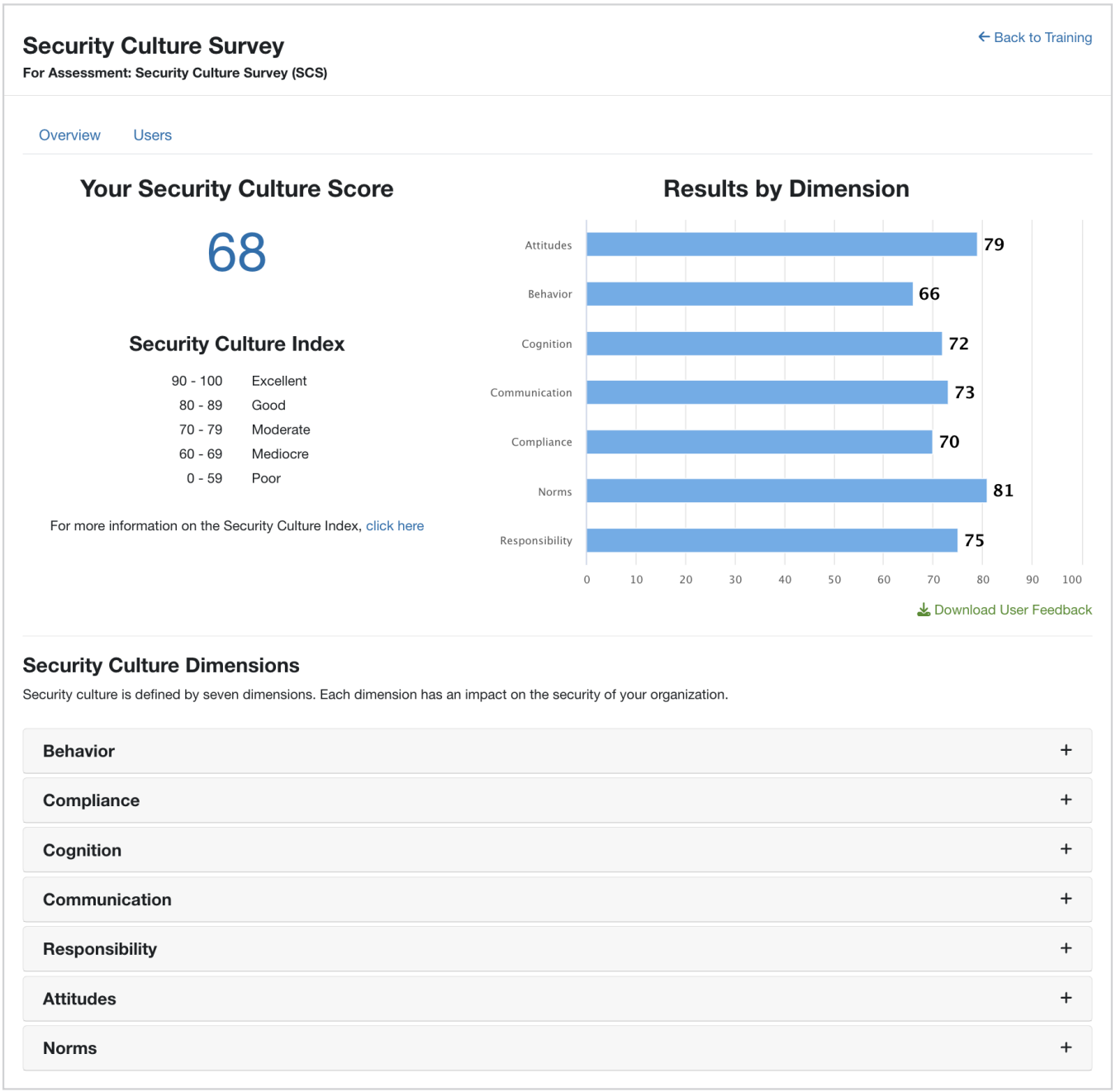
Security Awareness Proficiency Assessment (SAPA)

SAPA es una evaluación basada en las habilidades cuyo objetivo es ayudar a su organización a determinar sus necesidades de capacitación en concientización sobre seguridad al detectar las lagunas en los conocimientos de los usuarios, así como las mejoras de aprendizaje recomendadas.



Encuesta de cultura de la seguridad (SCS)

La encuesta de cultura de la seguridad analiza la opinión de sus usuarios sobre la seguridad en su organización; los aspectos psicológicos y sociales que impulsan el comportamiento social. La SCS muestra la eficacia general de su programa de cultura de la seguridad y cómo esta mejora con el tiempo.



Tanto la SAPA como la SCS se basan en la ciencia de la evaluación y le permiten medir los conocimientos y la competencia en materia de seguridad de sus usuarios, y analizar la postura general de la cultura de la seguridad de su organización.

Soporte en varios idiomas

La interfaz del alumno localizada y el contenido traducido en su totalidad para campañas de phishing y capacitación están disponibles en 35 idiomas principales para una cobertura global de sus alumnos. La consola de administración localizada está disponible en 10 idiomas.

La consola de KnowBe4

La plataforma de KnowBe4 es fácil de usar, intuitiva y potente. Está pensada para los profesionales de TI atareados que tienen otros 16 incendios que apagar. Los clientes con empresas de todos los tamaños pueden implementar la plataforma de KnowBe4 en producción al menos dos veces más rápido que nuestros competidores.

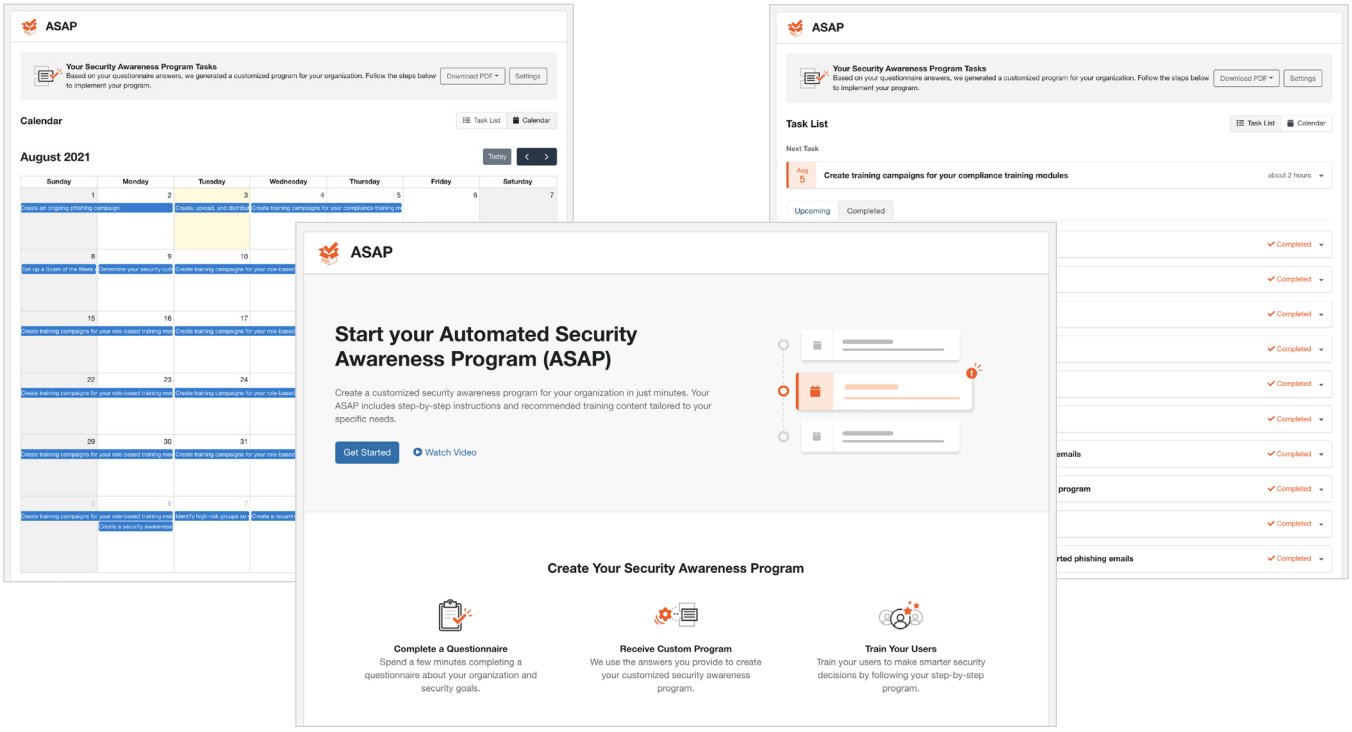
Siga leyendo para obtener más información sobre todas las funciones que ofrece la plataforma de KnowBe4.

Automated Security Awareness Program (ASAP)

Muchos profesionales de TI no saben exactamente dónde comenzar al momento de crear un programa de cultura y capacitación en concientización sobre seguridad que funcione para su organización.

Gracias a nuestro generador de Programas en concientización sobre seguridad automatizados (Automated Security Awareness Program, ASAP) eliminamos todas las conjeturas. ASAP es una herramienta integrada en la consola que le ayudará a crear un programa en concientización sobre seguridad adaptado a su organización. Además, le mostrará los pasos necesarios para crear un programa de capacitación totalmente consolidado en tan solo unos minutos.

Tras responder a siete preguntas sobre sus objetivos y su organización, la herramienta ASAP le sugerirá y planificará un programa automáticamente. Las tareas del programa se basarán en las prácticas recomendadas para alcanzar sus objetivos de concientización sobre seguridad.



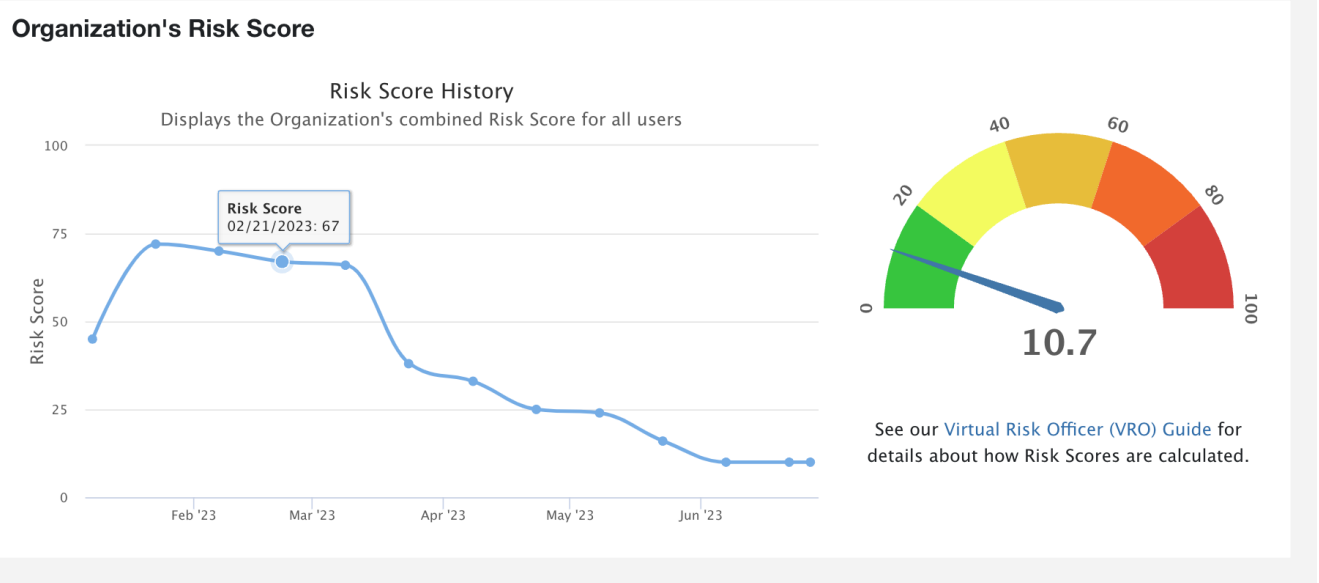
El programa incluye tareas factibles, consejos útiles, sugerencias de contenido de capacitación y un calendario de gestión de tareas. Su programa personalizado se puede gestionar completamente desde la consola de KnowBe4. También podrá exportar el programa completo como una versión detallada o de resumen breve en formato PDF, y utilizarlo para los requisitos de cumplimiento y la generación de informes para la gerencia.

Tablero de la consola

Nuestro tablero de phishing y capacitación le permite ver el puntaje de riesgo de su organización y el desempeño de sus usuarios finales de un vistazo, y hacer una comparación con compañeros de diferentes sectores mediante la evaluación comparativa del sector.

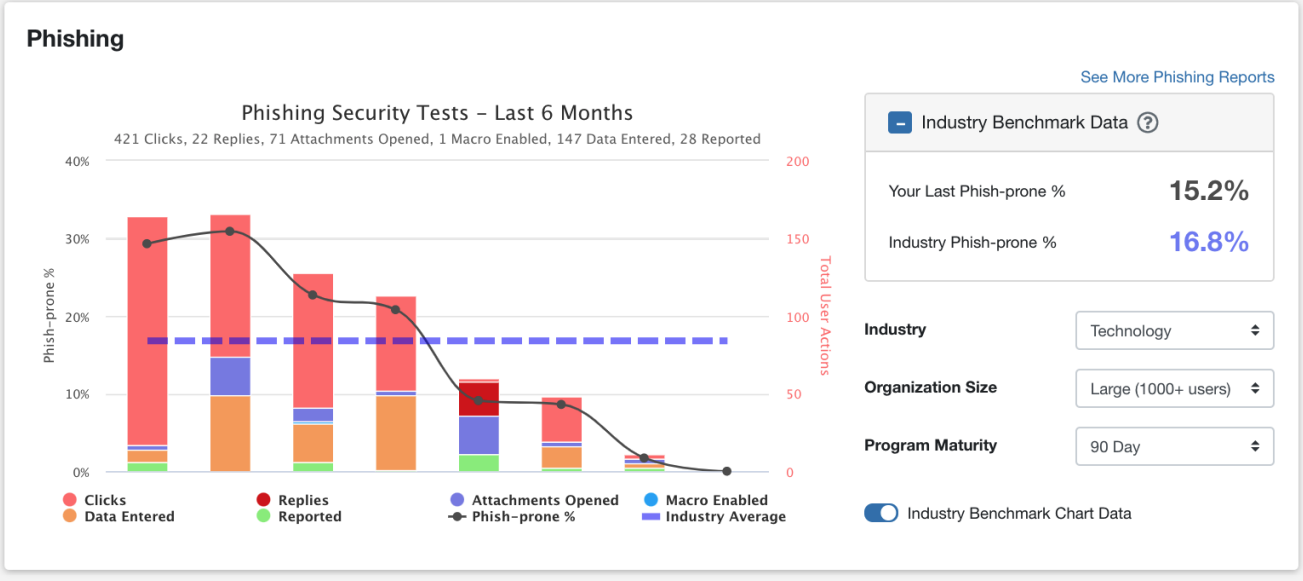
Vista del puntaje de riesgo de la organización

Vea el puntaje de riesgo general de su organización a partir de los puntajes de riesgo combinados de todos sus usuarios.



Resultados del porcentaje de Phish-prone (predisposición para ser víctima de phishing)

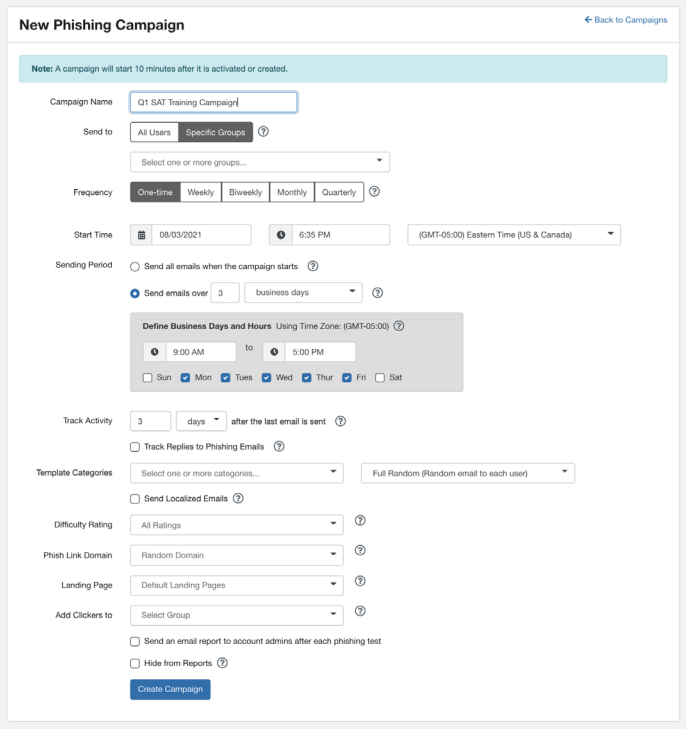
Nuestra plataforma ofrece diferentes formas de medir el progreso de sus usuarios finales en sectores similares, según los resultados del phishing y de la evaluación. Esta función del tablero le permite ver el porcentaje de Phish-prone (o cuántos usuarios son propensos hacer clic en un correo electrónico de phishing) en comparación con otros compañeros de su sector.



Plataforma de phishing simulado

KnowBe4 ofrece un novedoso enfoque para la capacitación de los usuarios sobre la amenaza del phishing, ya que le permite crear campañas de phishing que envían a sus usuarios correos electrónicos de phishing simulado. Estos ataques simulados imitan los ataques reales de phishing y enseñan a los usuarios a mantenerse alerta.

Los clientes de KnowBe4 pueden programar y enviar una cantidad ilimitada de pruebas de seguridad contra el phishing (PST) simuladas a sus usuarios durante el periodo de la suscripción. Siga leyendo para obtener más información sobre las funciones más populares de nuestra plataforma de phishing.

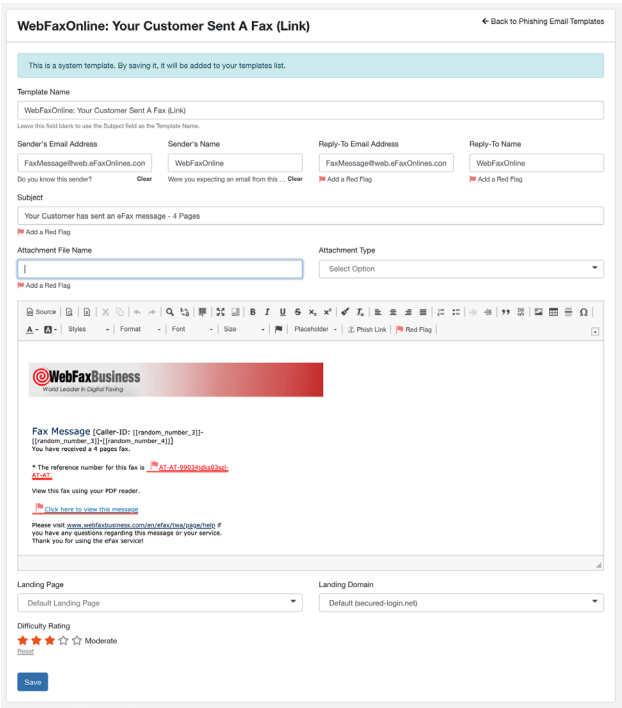


Campañas de phishing

La plataforma de KnowBe4 le permite determinar los tipos de ataques a los que son vulnerables sus usuarios, informar a estos cómo detectar las señales de alarma y calcular el porcentaje de Phish-prone (predisposición para ser víctima de phishing) de su organización. Para comenzar con su programa de capacitación, el primer paso es crear sus campañas de phishing para poner a prueba a sus usuarios y así poder determinar en qué capacitación deberán inscribirse.

Programación de pruebas de phishing

Puede programar pruebas de phishing a partir de nuestra extensa biblioteca con más de 25 000 plantillas disponibles en más de 40 idiomas o elegir de la sección de plantillas comunitarias, que los administradores han creado para compartir con sus colegas. Elija entre ataques de phishing simulado únicos, semanales, quincenales o mensuales, y vea inmediatamente cuáles empleados caen en estos ataques de ingeniería social. Además, con la exclusiva función "contra perros de pradera" de KnowBe4, puede enviar plantillas de phishing aleatorias en distintos momentos durante toda la campaña de phishing, para así imitar los ataques de phishing de la vida real y evitar que los usuarios se avisen de que se trata de una prueba de phishing.



Personalización de la plantilla de phishing

Puede personalizar cualquier plantilla del sistema además de incluir archivos adjuntos y macros simulados. Genere desde cero plantillas de correos electrónicos de phishing personalizadas o modifique nuestras plantillas actuales para enviarlas a los usuarios. Incluso puede hasta personalizar las situaciones en función de la información pública o personal, crear campañas de spear phishing (suplantación de identidad específica), que reemplaza los campos con datos personalizados.

Al poder utilizar logotipos en los correos electrónicos de phishing, podrá crear plantillas de correo electrónico de aspecto legítimo con nuestra plataforma mediante el uso de enlaces integrados en el correo electrónico que dirigen a la dirección URL original del logotipo. De este modo, el propietario del logotipo sigue hospedando la imagen y posee los derechos sobre ella.

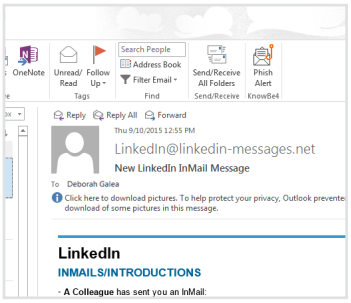
Phish Alert Button

Solo con hacer un clic, el complemento del botón Phish Alert Button de KnowBe4 le brinda a sus usuarios una forma segura de reenviar las amenazas en los correos electrónicos a un equipo de seguridad para su análisis y elimina el correo electrónico de la bandeja de entrada del usuario a fin de evitar una exposición futura. Todo eso con tan solo un clic. El botón Phish Alert Button (PAB) para Microsoft 365 le permite añadir idiomas a su instancia de PAB para mostrar automáticamente el idioma deseado según la configuración del idioma del sistema de sus usuarios.

- Cuando el usuario hace clic en el botón Phish Alert Button en una prueba de seguridad contra el phishing simulada, se informa la acción correcta de este usuario.
- Cuando el usuario hace clic en el botón Phish Alert Button en un correo electrónico de phishing no simulado, el correo electrónico se reenvía directamente al equipo de respuesta ante incidentes.
- El texto del botón y los cuadros de diálogo para el usuario son completamente personalizables.
- Clientes compatibles: Outlook 2016, 2019, 2021 y Outlook para Microsoft 365, Exchange 2016, 2019 y 2021, Outlook en la web (Outlook.com), la aplicación Outlook Mobile (iOS y Android), Chrome 80 y posterior (Linux, OS X y Windows), cuentas de Gmail conectadas a través de Google Workspace. El complemento de Gmail es compatible con Gmail en el navegador y los clientes móviles.

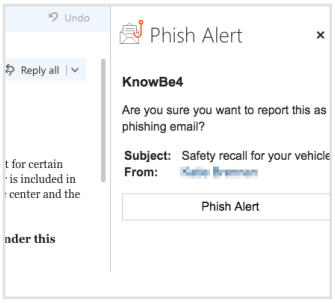
Barra de herramientas de Outlook

Agrega el botón Phish Alert Button para los usuarios



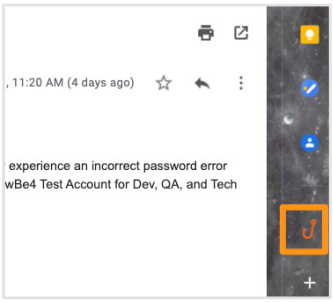
Panel de complementos de Microsoft 365

Agrega el botón Phish Alert Button para los usuarios



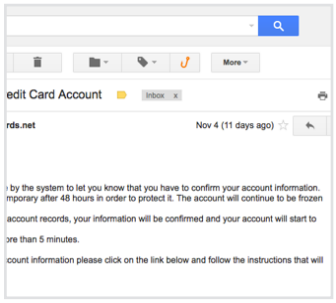
Complemento de Gmail

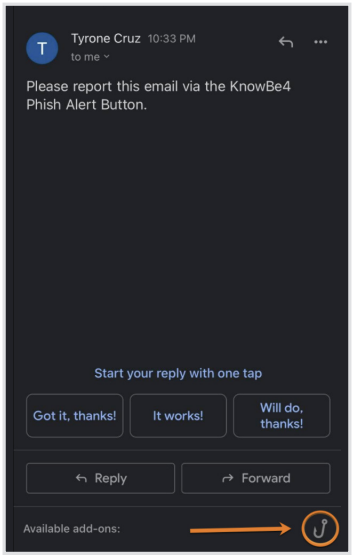
Agrega el botón Phish Alert Button para los usuarios



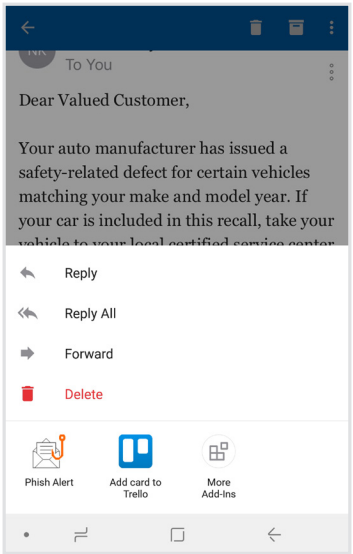
Extensión para Gmail

Agrega el botón Phish Alert Button para los usuarios

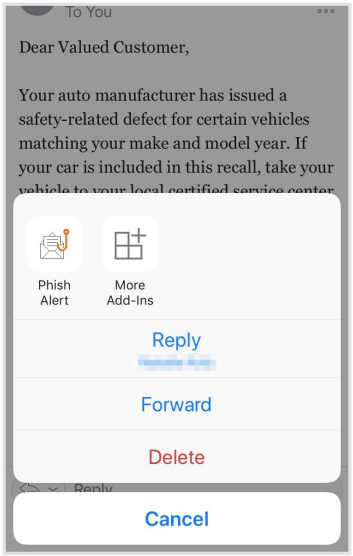




Gmail móvil (Android)



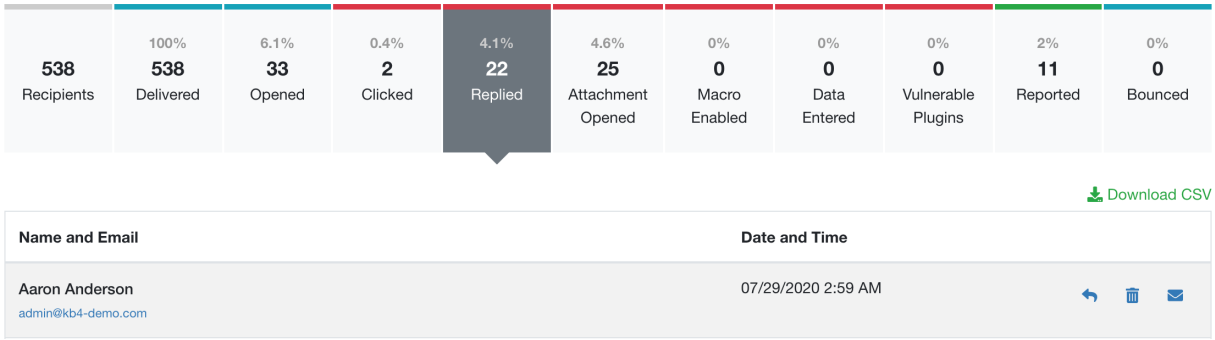
Outlook móvil (Android)



Outlook móvil (iOS)

Seguimiento de respuesta al phishing

El seguimiento de respuesta al phishing de KnowBe4 le permite hacer un seguimiento en caso de que el usuario haya respondido a un correo electrónico de phishing simulado y también puede recopilar la información de la respuesta para su revisión en la consola de KnowBe4. Tenemos disponible una categoría de plantillas de phishing simulado por el sistema que se denomina “Respuesta en línea” que se diseñó específicamente para probar si el usuario interactuará con los malhechores por su parte. No obstante, el seguimiento de respuesta al phishing también funciona con cualquiera de nuestras plantillas de phishing.



El seguimiento de respuesta al phishing es fácil de usar y está activado de forma predeterminada para las nuevas campañas de phishing a través de la opción “Realizar seguimiento de las respuestas a los correos electrónicos de phishing”.

Dominios de phishing personalizados

Dominio de phishing es el nombre que le damos a la URL que se completa en la esquina inferior izquierda de su pantalla cuando pasa el cursor del mouse por encima del enlace de un correo electrónico sospechoso. Tenemos una variedad de distintos dominios de phishing que puede seleccionar para que la URL que se completa cambie siempre, para que los usuarios finales estén atentos en todo momento. Con la suplantación de identidad de dominio ilimitada, le permitimos suplantar cualquier dirección de correo electrónico al realizar campañas de phishing simulado.

Funciones avanzadas de phishing

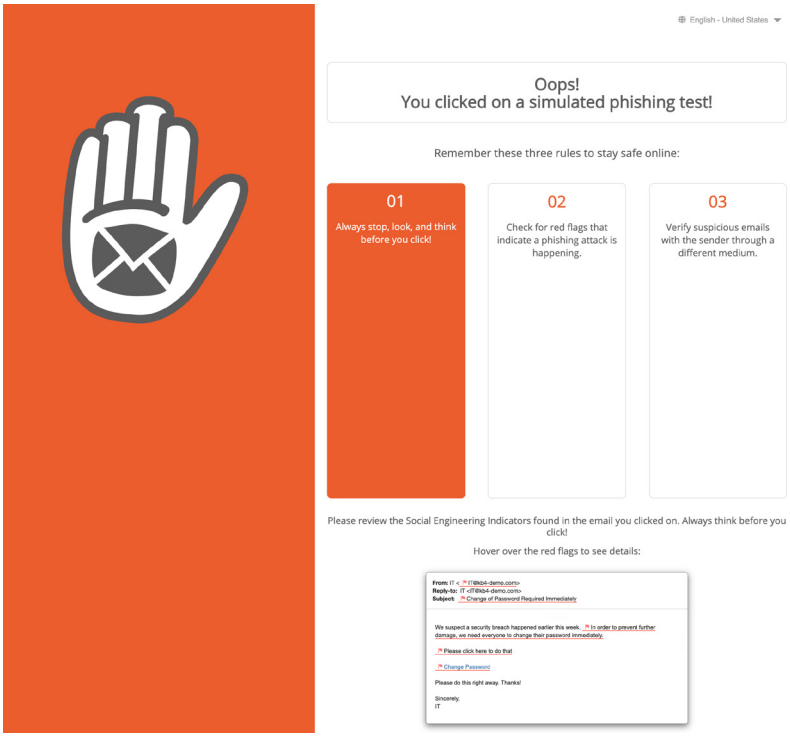
Algunos niveles de suscripción ofrecen más posibilidades de sacar el máximo partido a nuestra plataforma de phishing. Siga leyendo para obtener más información sobre estas funciones.

Indicadores de ingeniería social (SEI)

Nuestra función de Indicadores de ingeniería social (SEI) es una tecnología patentada que convierte cada correo electrónico de phishing simulado en una herramienta que el departamento de TI puede utilizar para capacitar de manera instantánea a los empleados.

Cuando un usuario hace clic en cualquiera de los correos electrónicos de phishing simulado de KnowBe4, se lo dirige a una página de inicio que incluye una copia dinámica de ese correo electrónico de phishing que muestra todas las señales de alarma. También puede personalizar cualquier correo electrónico de phishing simulado y puede crear sus propias señales de alarma.

De ese modo, los usuarios podrán ver de inmediato las trampas potenciales y aprender a detectar en el futuro los indicadores que pasaron por alto.



Prueba de memoria USB

Fácilmente podrá crear su prueba de memoria USB desde la consola de KnowBe4 y descargar archivos de Microsoft Office especiales, "que sirven de baliza". También puede cambiar el nombre de los archivos para que los empleados se sientan tentados a abrirlos. Después, coloque estos archivos en cualquier memoria USB, que puede dejar en cualquier área del sitio que sea muy transitada. Si un empleado recoge la memoria USB, la conecta a su estación de trabajo y abre el archivo, este "llamará a casa" e informará el error y datos como la hora de acceso y la dirección IP. Si un usuario además habilita los macros en el archivo, también se hará un seguimiento de datos adicionales como el nombre del usuario y de la computadora, y estos datos estarán disponibles en la consola.

Phishing con códigos QR

Puede poner a prueba a sus usuarios con códigos QR en lugar de enlaces de phishing o archivos adjuntos en los correos electrónicos. Los códigos QR, o códigos de respuesta rápida, son códigos de barras escaneables que contienen datos en un formato compacto. Si sus usuarios escanean un código de barras malicioso, podrían visitar un sitio web peligroso. Además, los enlaces maliciosos ocultos en códigos QR pueden eludir los filtros de seguridad de su organización.

Las campañas de phishing con códigos QR físicos le permiten probar cómo reaccionarán sus usuarios al encontrar un código QR inesperado. Por ejemplo, si sus usuarios ven un código QR en un afiche en un lugar conocido, es posible que lo escaneen y abran el enlace sin comprobar que es seguro. Las pruebas de seguridad contra el phishing con códigos QR pueden ayudar a preparar a sus usuarios para ataques reales de phishing con códigos QR.

Phishing basado en IA

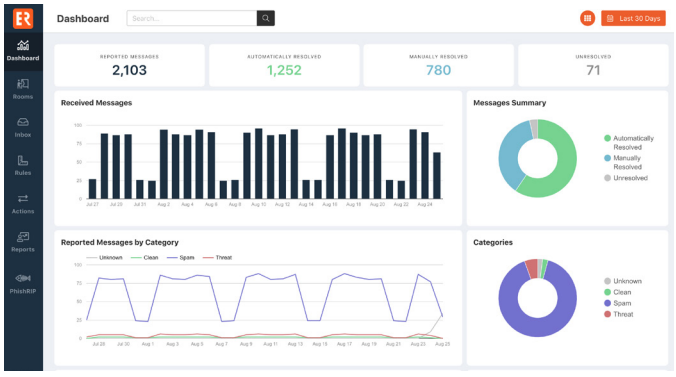
El phishing basado en IA le permite aprovechar el poder de la IA para elegir automáticamente la mejor plantilla de phishing para cada uno de sus usuarios según su capacitación e historial de phishing en particular. A partir de los datos del Agente Impulsado por Inteligencia Artificial (Artificial Intelligence Driven Agent, AIDA) de KnowBe4, un motor de recomendaciones le permite automatizar la selección dinámica de plantillas de pruebas de seguridad contra el phishing (PST) para sus usuarios.

Piénselo como su propio asistente personal de phishing (suplantación de identidad) de IA que elige automáticamente la mejor prueba de phishing para cada usuario en un momento determinado. Cuando utiliza el phishing basado en IA, básicamente crea una campaña de phishing única para cada uno de sus usuarios a fin de asegurarse de que cada uno de ellos reciba pruebas de phishing personalizadas según su nivel individual. Ofrezca a sus usuarios una experiencia más personalizada que se adapte a su nivel actual de conocimientos.

Phishing de devolución de llamada

Como administrador de la consola de KnowBe4, usted tiene la capacidad de utilizar la nueva función de simulación de Phishing de devolución de llamada. Esta herramienta le permite enviar un correo electrónico a los empleados con un número telefónico y un código. Si los empleados llaman a este número y proporcionan el código, esto ya se consideraría el primer error. Luego, si los empleados brindan información personal o confidencial, esto constituiría un error aún mayor. Esta simulación le permite evaluar si su personal sería susceptible de caer en este tipo de trampa de phishing.

PhishER Plus



PhishER Plus está disponible como complemento de producto para cualquier nivel de suscripción. Se trata de una plataforma basada en la web sencilla y fácil de usar que ayuda a su equipo de operaciones de seguridad y seguridad de la información a superar el caos de las bandejas de entrada y actuar con mayor rapidez ante las amenazas más peligrosas. PhishER Plus se desarrolló para potenciar las defensas de seguridad del correo electrónico de su organización. Además, provee una capa final adicional cuando su puerta de enlace de correo electrónico seguro y otras capas de ciberseguridad fallan. PhishER Plus permite utilizar un flujo de trabajo crítico para ayudar a sus equipos de respuesta ante incidentes a trabajar juntos para mitigar la amenaza de phishing. Además, es perfecto para todas las empresas que deseen priorizar y administrar de forma automática los mensajes potencialmente maliciosos con precisión y celeridad. Al combinar KnowBe4 y PhishER Plus en su flujo de trabajo de seguridad del correo electrónico, no solo reducirá la carga de trabajo de sus equipos de seguridad de la información y respuesta ante incidentes, y detectará más rápidamente las verdaderas amenazas, sino que también podrá mejorar el nivel de su programa de capacitación en concientización sobre seguridad.

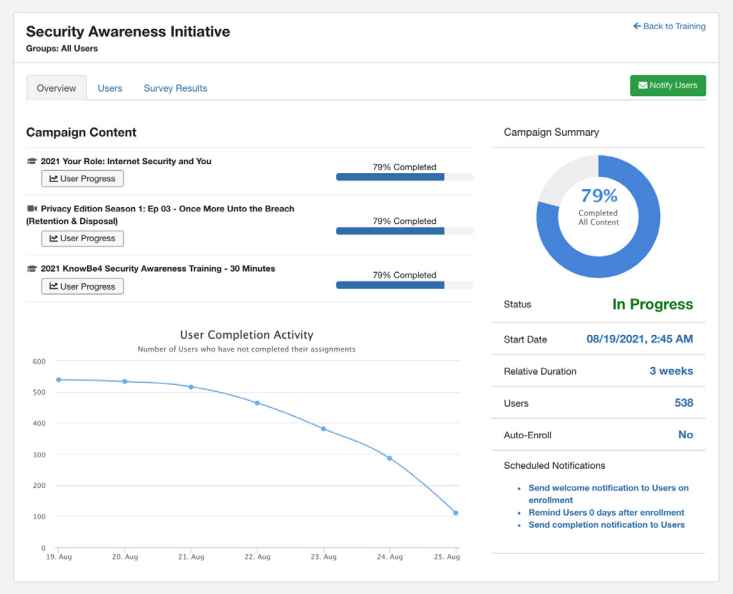
Estas son las principales ventajas de PhishER Plus:

- Libera recursos del equipo de respuesta ante incidentes para identificar y administrar el 90 % de los mensajes que son correo no deseado (spam) o correo electrónico legítimo.
- Permite ver conjuntos o grupos de mensajes según patrones que puedan ayudarlo a detectar un ataque de phishing generalizado contra su organización.
- Las entradas de la lista global de bloqueo de amenazas validadas, procedentes de más de 10 millones de usuarios capacitados, se utilizan para bloquear automáticamente los mensajes entrantes nuevos que coincidan y así evitar que lleguen a las bandejas de entrada de los usuarios. La fuente de amenazas continuamente actualizada es administrada por KnowBe4 y se sincroniza con su servidor de correo de Microsoft 365.
- PhishML™ es un módulo de aprendizaje automático de PhishER Plus que analiza cada mensaje que llega a la plataforma de PhishER Plus y le brinda información para que el proceso de priorización sea más fácil, rápido y preciso.
- Global PhishRIP es una función de cuarentena de correo electrónico que se integra con Microsoft 365 y Google Workspace para que su equipo de respuesta ante incidentes pueda hacer correcciones rápida y fácilmente. El laboratorio de investigación de amenazas de KnowBe4 valida los mensajes que coincidan con una amenaza de phishing que haya sido detectada y que otros clientes de PhishER Plus hayan eliminado de sus buzones de correo.
- PhishFlip™ es una función de PhishER Plus que toma los ataques de phishing dirigidos a la organización que han sido informados por los usuarios y los convierte automáticamente en campañas de phishing simuladas y seguras.

Plataforma de capacitación

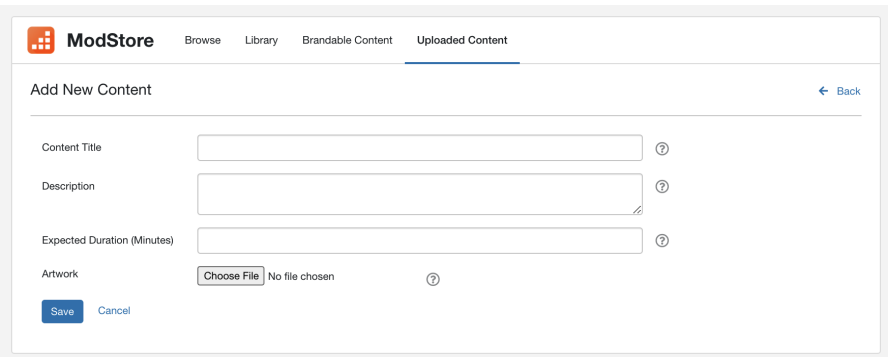
Campañas de capacitación

En la consola de KnowBe4 podrá crear rápidamente campañas permanentes o de tiempo limitado, seleccionar módulos de capacitación por grupos de usuarios, inscribir automáticamente a usuarios nuevos y automatizar correos electrónicos “de toque” para los usuarios que no completaron la capacitación. También puede editar las plantillas de notificación de capacitación, preparar las políticas para su aceptación por parte de los usuarios y ver los informes de capacitación. Las campañas de capacitación se utilizan para personalizar y gestionar el contenido de capacitación de sus usuarios dentro de nuestra experiencia de aprendizaje.



Opciones del sistema de gestión de aprendizaje

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 en el idioma que desee y gestionarlo junto con el contenido de su capacitación de ModStore de KnowBe4, todo en un solo lugar, ¡sin costo adicional!

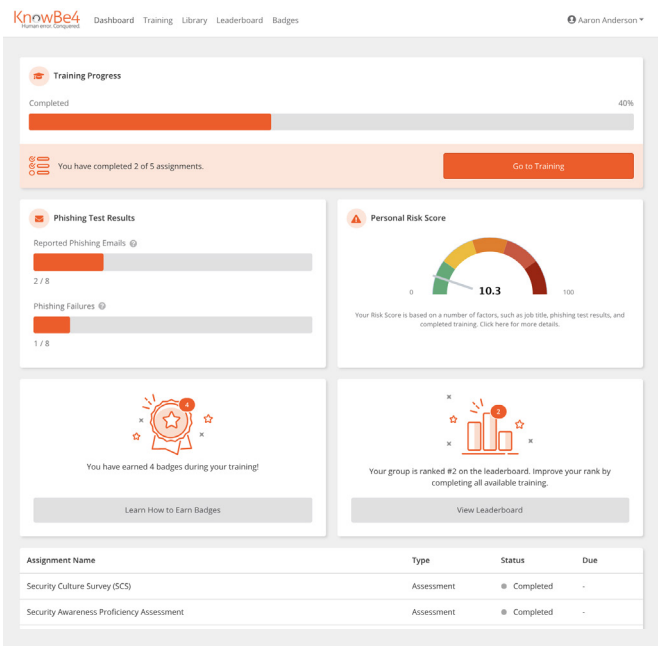


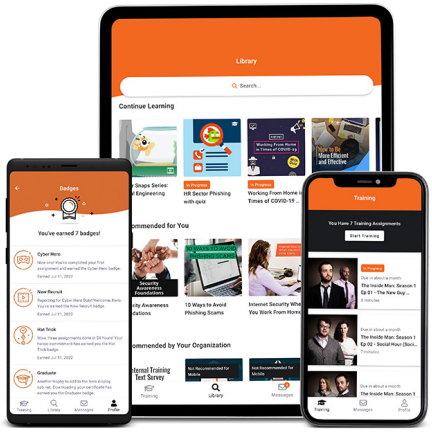
Experiencia de aprendizaje

La experiencia de aprendizaje (Learner Experience, LX) de KnowBe4 ofrece la posibilidad de personalizar y crear juegos atractivos y divertidos para su plan de capacitación en concientización sobre seguridad.

Sus usuarios podrán competir contra sus compañeros en tablas de clasificación y ganar insignias mientras aprenden a protegerse a sí mismos y a su organización de los ciberataques. También se ofrece un recorrido informativo opcional para mostrarles todo a los usuarios y hacer que se sientan cómodos en su nuevo entorno de aprendizaje.

La interfaz de LX también incluye un tablero de aprendizaje. Aquí los usuarios verán un resumen de su progreso en la capacitación, que incluye el estado de la capacitación y las fechas límite. Si lo desea, puede optar por mostrar los resultados de las pruebas de phishing de sus usuarios, el puntaje de riesgo personal y las estadísticas de la ludificación.





Aplicación de aprendizaje de KnowBe4

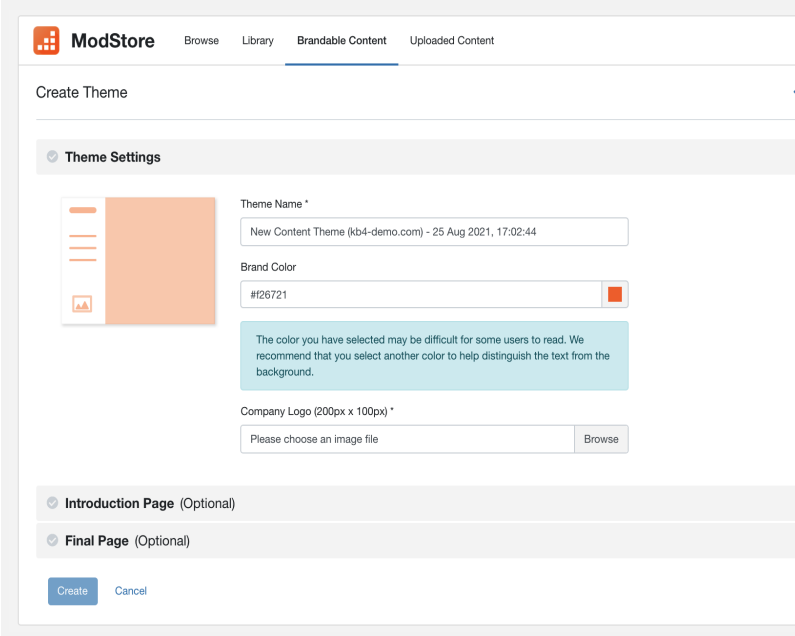
La aplicación de aprendizaje de KnowBe4 les permite a sus usuarios completar la capacitación asignada de manera práctica desde sus tabletas, teléfonos inteligentes y otros dispositivos móviles. Amplíe la protección de su superficie de ataque más grande y cubra a los empleados que normalmente no tienen acceso a un dispositivo de escritorio o portátil con una aplicación diseñada pensando tanto en el usuario como en el administrador.

La aplicación de aprendizaje de KnowBe4 se incluye con su suscripción de capacitación sin costo adicional y les ofrece a los usuarios flexibilidad y comodidad para aprender en todo momento. La aplicación, disponible para iOS y Android, admite notificaciones push para anuncios personalizados, actualizaciones sobre la capacitación asignada, así como boletines informativos de KnowBe4.

Contenido comercializable

La función de contenido comercializable le permite crear un tema de marca y aplicarlo a las campañas de capacitación activas con contenido admisible. Utilice la pestaña Contenido comercializable para establecer el color de su marca, cargar el logotipo de la empresa y añadir una introducción y una página final. Estas páginas opcionales incluyen el logotipo de su empresa, texto personalizado y una imagen que usted elija.

Utilice esta función para proporcionar un aspecto familiar a sus empleados. También tiene la posibilidad de cargar los certificados de marca de su organización en la plataforma de KnowBe4. Al final de cada módulo de capacitación, los usuarios pueden disponer de los certificados de finalización personalizados.



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 dígale adiós a la omisión de contenido. Y esta es la sorpresa: está disponible en todos los niveles de suscripción.

Capacitación recomendada de IA

ModStore de KnowBe4 aprovecha el aprendizaje automático para ofrecer sugerencias de capacitación informadas a partir de las métricas de desempeño de sus usuarios en sus campañas de pruebas de seguridad contra el phishing (PST). Según el porcentaje de Phish-prone (predisposición para ser víctima de phishing) de su organización, ModStore le ofrecerá módulos de capacitación recomendados que puede seleccionar para disminuir la tasa de clics de sus usuarios a lo largo del tiempo.

Aprendizaje opcional para los usuarios

El aprendizaje opcional le permite ofrecer a sus usuarios contenido de capacitación adicional desde su ModStore de KnowBe4. Simplemente cree campañas de capacitación específicas con el contenido de capacitación opcional que desea poner a disposición de sus usuarios para que lo seleccionen. También puede aprovechar la función de Aprendizaje opcional recomendado de IA, disponible para clientes Diamante, a fin de recomendar e implementar el contenido de capacitación adicional a sus usuarios en función de los cursos completos, sin necesidad de crear una campaña de capacitación por separado.

SecurityCoach

SecurityCoach es el primer producto de asesoramiento en seguridad en tiempo real creado para que los equipos de operaciones de seguridad y de TI puedan proteger mejor la mayor superficie de ataque de su organización: los empleados. Con la introducción de una nueva categoría de tecnología denominada “detección y respuesta humanas”, SecurityCoach podrá fortalecer su cultura de la seguridad con un asesoramiento en seguridad en tiempo real para sus usuarios, en respuesta a sus comportamientos de seguridad riesgosos.

SecurityCoach se integra con la innovadora plataforma de capacitación en concientización sobre seguridad de KnowBe4 y con su pila de seguridad actual para brindar información inmediata a sus usuarios en el momento en el que se produce un comportamiento riesgoso. SecurityCoach es un complemento opcional para los clientes de KnowBe4 con una suscripción de capacitación en concientización sobre seguridad de nivel Platino o Diamante. SecurityCoach utiliza API estándar para integrar rápida y fácilmente los productos de seguridad existentes de su organización con su consola de KnowBe4. Su pila de seguridad genera alertas que SecurityCoach luego analiza para identificar eventos relacionados con cualquier comportamiento de seguridad riesgoso por parte de sus usuarios.

Los beneficios clave de SecurityCoach incluyen los siguientes:

- Reforzar la comprensión y la retención por parte del usuario de la capacitación en seguridad, así como las políticas de seguridad establecidas con asesoramiento en tiempo real sobre comportamientos reales.
- Aprovechar su pila de seguridad actual para brindar asesoramiento en tiempo real a los usuarios riesgosos y obtener valor adicional a partir de sus inversiones actuales.
- Crear campañas personalizadas para las funciones o los usuarios de alto riesgo que los ciberdelincuentes consideran objetivos valiosos, o para las funciones o usuarios que continúan repitiendo comportamientos riesgosos.
- Rastrear e informar el comportamiento de seguridad real mejorado en su organización brindando una justificación sobre las inversiones continuas.
- Reducir los riesgos de forma cuantificable y crear una cultura de seguridad madura en menos tiempo.
- Reducir la carga de su equipo de SOC y mejorar su eficacia al disminuir los ruidos de alerta causados por los comportamientos de seguridad riesgosos y repetitivos.

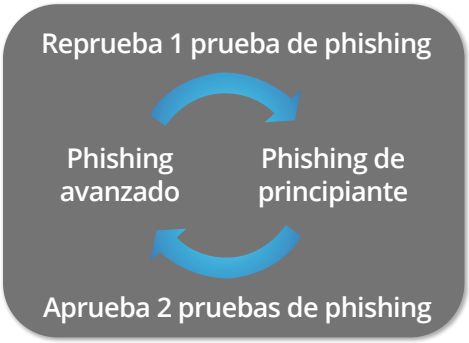
Gestión de usuarios

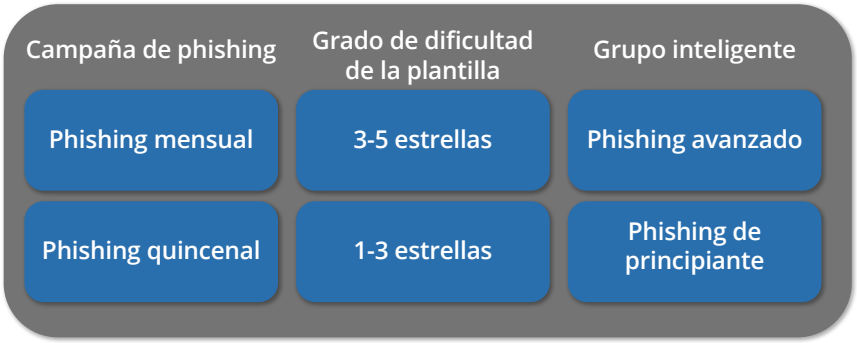
Aprovisionamiento de usuarios a través de la integración de Active Directory o SCIM

KnowBe4 facilita la administración de usuarios con la Integración de Active Directory (ADI) o la Integración de SCIM para proveedores de identidad, como Okta, OneLogin o Microsoft Entra ID. Las integraciones de ADI y SCIM le permiten cargar o sincronizar los datos de los usuarios con su consola de KnowBe4 y ahorrar tiempo al eliminar la necesidad de administrar manualmente los cambios de usuarios.

Grupos inteligentes

Con los Grupos inteligentes podrá activar el piloto automático con respecto al phishing, la capacitación y la generación de informes. Automatice la ruta que los empleados deben seguir para tomar decisiones de seguridad más inteligentes. Nuestra función de grupos inteligentes, disponible para los clientes Platino y Diamante, le permite realizar campañas de phishing dinámicas mediante la creación de grupos a partir de los criterios que usted escoja. Los usuarios se agregan y eliminan dinámicamente de los grupos inteligentes según esos criterios. Las campañas se consideran dinámicas porque sus usuarios se someten a pruebas con mayor o menor frecuencia, según sea necesario, en función de su rendimiento en las campañas de phishing. Recomendamos utilizar esta función para las pruebas de phishing, las campañas de capacitación y la generación de informes exclusivos. Gracias a la potente función de grupos inteligentes, podrá utilizar el comportamiento de cada empleado y los atributos del usuario para personalizar las campañas de phishing, las asignaciones de capacitación, el aprendizaje de medidas correctivas y la generación de informes.





Podrá crear campañas de phishing y capacitación del tipo “establecerlas y olvidarse” para que pueda responder instantáneamente a cualquier clic de phishing con una capacitación sobre medidas correctivas o notificar automáticamente a los empleados nuevos de la capacitación de incorporación, y mucho más. Elija entre cinco tipos de criterios clave por grupo inteligente y después incorpore los desencadenantes, las condiciones y las acciones para enviar los correos electrónicos de phishing o capacitación correctos al empleado correcto en el momento correcto.

Lo mejor de todo es que usted tiene la posibilidad de filtrar y extraer los informes en función de los diferentes criterios que se utilizan en las normas de sus grupos inteligentes. Por ejemplo, probablemente desee filtrar los criterios específicos de los “eventos de phishing” y crear un informe que muestre qué usuarios están mejorando o no como resultado de las pruebas de phishing que se han llevado a cabo, lo cual le permite asignar campañas de capacitación sobre medidas correctivas o pruebas avanzadas de phishing para este grupo inteligente.

Roles de seguridad

La función de roles de seguridad de KnowBe4 puede utilizarse para otorgar acceso granular a toda la consola de KnowBe4. Cada rol de seguridad es completamente personalizable a fin de facilitar la creación de roles exactos que resulten necesarios para su organización.

Debido a que los roles no son simplemente un conjunto de permisos predefinidos, es posible crear el modelo de permiso exacto que se adapte a sus necesidades. A continuación, podrá encontrar algunas situaciones frecuentes en las que los roles de seguridad le permitirán al administrador de la consola brindar acceso a los usuarios únicamente a las partes de la consola de KnowBe4 que necesitan para obtener sus resultados:

- Auditores que necesitan revisar el historial de capacitación.
- Departamentos de RR. HH. que desean ver resultados individuales de los usuarios.
- Grupos de capacitación que desean revisar el contenido de la capacitación antes de implementarla.

Generación de informes

La plataforma de capacitación en concientización sobre seguridad de KnowBe4 ofrece una amplia gama de informes que permiten conocer la eficacia de su programa de capacitación en concientización sobre seguridad. Todos los informes disponibles en su consola pueden descargarse como archivos CSV o PDF, según el tipo de informe. Obtenga más información sobre las distintas categorías y tipos de informes aquí.

La generación de informes a nivel ejecutivo y empresarial ofrece visibilidad sobre el rendimiento de toda su organización en materia de concientización sobre seguridad, con información sobre los datos correlacionados de capacitación y simulación de phishing durante cualquier periodo especificado. Incluso puede guardar los informes para verlos en otro momento o enviar los informes guardados a otros usuarios. También puede optar por programar la generación y el envío de informes con una frecuencia determinada, por ejemplo, cada trimestre. Saque provecho de las API de informes para crear informes propios y personalizados que se integren con otros sistemas de inteligencia de negocios. En el caso de que gestione varias cuentas de KnowBe4, los informes de seguimiento facilitan seleccionar informes y comparar los resultados en conjunto entre las cuentas o las oficinas de distintas ubicaciones.

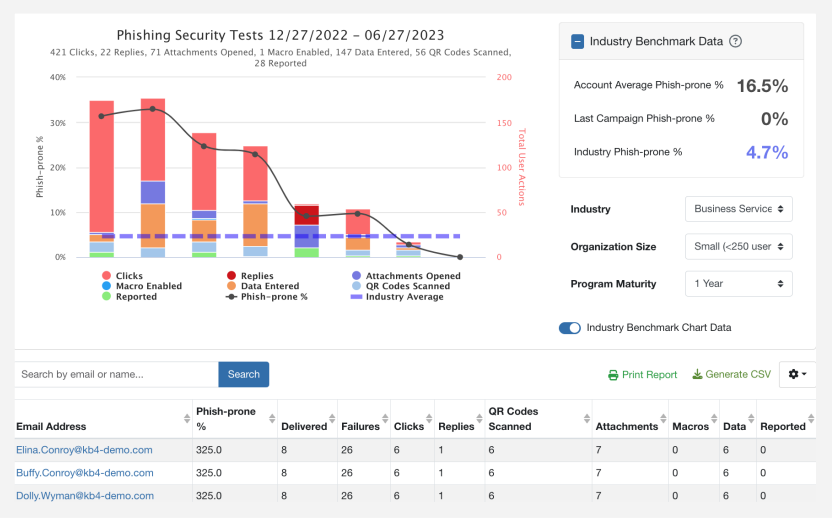
El **tablero** de su consola contiene el puntaje de riesgo de la organización y los informes de phishing. Estos informes proporcionan información general sobre el porcentaje de Phish-prone (predisposición para ser víctima de phishing) de su organización al momento de realizar la campaña de phishing y sobre las acciones de sus usuarios durante las campañas. Al pasar el cursor sobre los puntos de la tabla, obtendrá más información sobre las campañas de phishing específicas, la cantidad de usuarios a los que se envió cada prueba y las acciones de los usuarios.

Siga leyendo para obtener más información sobre la variedad de funciones de generación de informes disponibles.

Informes de phishing

La sección de informes de phishing de la consola de KnowBe4 le da acceso a informes que son útiles para totalizar las acciones de los usuarios en varias campañas (por ejemplo, ¿cuántas veces hizo clic cada usuario en un enlace de phishing?).

Su informe puede filtrarse según un rango de fechas específico, determinadas campañas y campañas enviadas a determinados usuarios. También puede comparar los errores, los correos electrónicos de phishing denunciados (correos electrónicos denunciados mediante el botón Phish Alert Button) o comparar los resultados por grupos.



Informes de capacitación

La sección de informes de capacitación de la consola de KnowBe4 le da acceso a informes que muestran qué usuarios se han conectado al menos una vez y un informe de qué usuarios no se han conectado nunca. Asimismo, puede crear informes a partir de cursos específicos ofrecidos en la consola. Este informe puede filtrarse de modo que incluya a todos los usuarios o a determinados grupos. Además, puede tener una fecha de inicio o de finalización determinada; también tiene la opción de incluir a los usuarios archivados.

Estos informes pueden proporcionar la siguiente información sobre sus usuarios:

- Usuarios que han comenzado sus cursos dentro del rango de fechas indicado.
- Usuarios que se inscribieron dentro de un rango de fechas determinado, pero que no han comenzado sus cursos.
- Usuarios que comenzaron sus cursos dentro de un rango de fechas determinado, pero que no los han terminado.
- Usuarios que se inscribieron dentro de un rango de fechas determinado, pero que no han comenzado ni terminado sus cursos.

- Usuarios que finalizaron sus cursos dentro del rango de fechas determinado.
- Usuarios que se inscribieron dentro de un rango de fechas determinado, pero que no han aceptado sus políticas asociadas al curso.
- Usuarios que han aceptado las políticas asociadas a su curso en el intervalo de fechas determinado.

Email Exposure Check (EEC) Pro

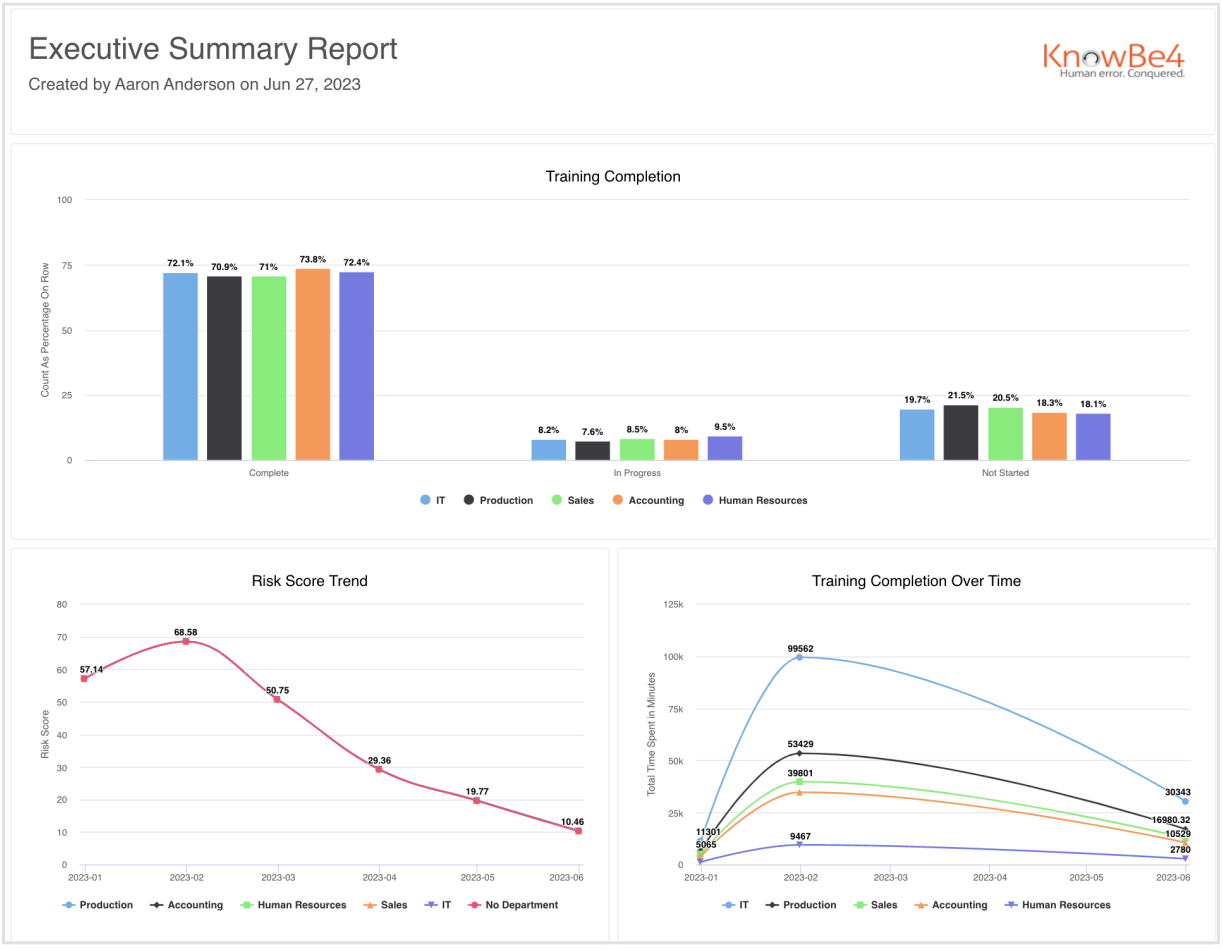
La herramienta Email Exposure Check (EEC) Pro, disponible en los niveles de suscripción Oro y superiores, detecta a los usuarios de riesgo de su organización al rastrear la información de redes sociales de la empresa y, ahora, miles de bases de datos de violaciones de seguridad.

Los usuarios se colocan en un grupo de distribución de riesgos después de que la herramienta EEC Pro haya recopilado los datos de las búsquedas que realiza. Las ubicaciones de los grupos, **Riesgo muy alto**, **Riesgo alto** y **Riesgo medio**, se basan en la cantidad de datos recopilados sobre ese usuario específico.

Informes avanzados

Los informes avanzados proporcionan métricas procesables e información sobre la eficacia de su capacitación en concientización sobre seguridad. Los informes avanzados permiten crear muchos tipos de informes según las necesidades de su organización. Esta función viene con una colección de más de 60 informes integrados con información que proporciona una visión holística de toda su organización a lo largo del tiempo. Además, amplía considerablemente los informes detallados instantáneos sobre una serie de indicadores clave de la capacitación de concientización.

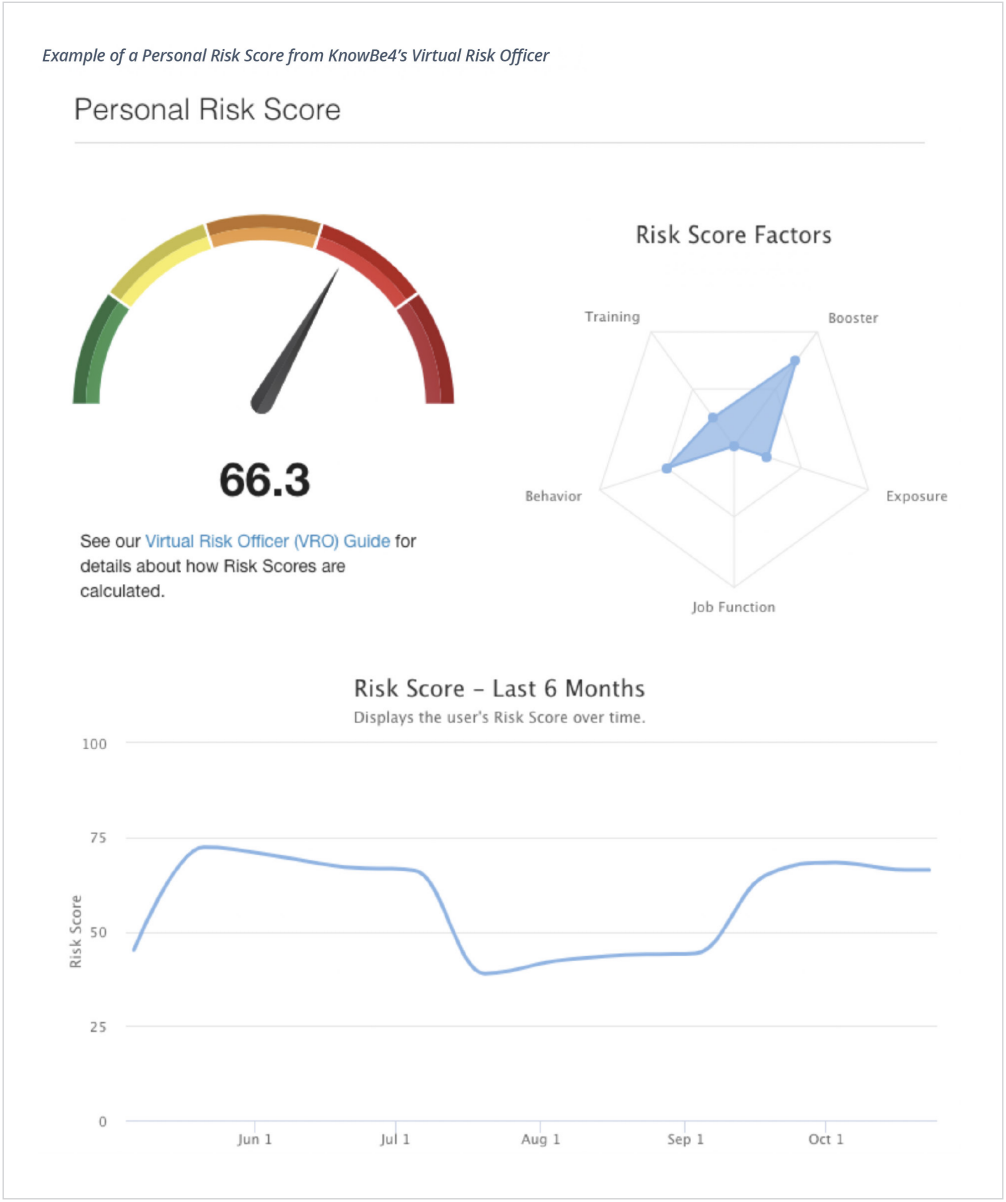
Además, con los **Informes ejecutivos**, puede crear y entregar informes personalizados a nivel ejecutivo que proporcionan información para ayudar a tomar decisiones basadas en datos sobre su programa.



Virtual Risk Officer

La funcionalidad de Virtual Risk Officer (VRO) le permite detectar el riesgo a nivel del usuario, del grupo y de la organización, y tomar decisiones basadas en datos en lo que respecta a su plan de concientización sobre seguridad. Con VRO, puede supervisar la situación de sus empleados y su organización a lo largo del tiempo en lo referente al riesgo de los usuarios.

Example of a Personal Risk Score from KnowBe4's Virtual Risk Officer



API flexibles

En los niveles de suscripción Platino y superiores, KnowBe4 ofrece dos API sólidas que ofrecen más opciones para el análisis de la actividad de los usuarios y la generación de informes.

- Las API de informes le permiten extraer datos de su consola de KnowBe4 para generar informes. Las API permiten solicitar datos de phishing, capacitación, usuarios y grupos.
- La API de eventos de usuario le permite integrar fácilmente los datos de los eventos relacionados con la seguridad de sus usuarios o de las actividades de capacitación que se realizan en otras plataformas de terceros y transferirlos a su consola de KnowBe4. Agregue estos eventos a las líneas de tiempo de sus usuarios, elija utilizarlos para aumentar los puntajes de riesgo de sus usuarios para ayudarlo a adaptar el contenido específico para otras campañas de phishing o capacitación.

Password IQ

Disponible en el nivel de suscripción Diamante, PasswordIQ supervisa continuamente su organización en busca de cualquier vulnerabilidad de contraseñas detectada en su Active Directory. Comprueba si sus usuarios utilizan actualmente contraseñas compartidas, débiles o que aparecen en violaciones de seguridad de datos de dominio público para que pueda establecer una base de referencia de los problemas de contraseñas y gestionar mejor el problema continuo del riesgo de contraseñas entre sus usuarios.

Niveles de suscripción

Nivel Plata: El nivel de acceso a la capacitación I incluye la capacitación en concientización sobre seguridad de Kevin Mitnick en el módulo completo de 45 minutos y la versión ejecutiva de 15 minutos. Además, incluye pruebas ilimitadas de phishing simulado, evaluaciones, la aplicación de aprendizaje de KnowBe4, capacitación recomendada de IA y generación de informes sobre la seguridad de la empresa mientras dure la suscripción.

Nivel Oro: Incluye todas las funciones del nivel Plata más el contenido del nivel de acceso a la capacitación II que también incluye los módulos de capacitación de KnowBe4. El nivel Oro también incluye informes Email Exposure Check (EEC) mensuales.

Nivel Platino: Incluye todas las funciones de los niveles Plata y Oro. El nivel Platino también incluye nuestras funciones avanzadas de phishing: grupos inteligentes, API de informes, API de eventos de usuario, funciones de seguridad e indicadores de ingeniería social (SEI) en la página de inicio.

Nivel Diamante: Incluye todas las funciones de los niveles Plata, Oro y Platino más el nivel de acceso a la capacitación III, lo que le da acceso completo a nuestra biblioteca de contenido con más de 1300 elementos, entre los que se incluyen módulos interactivos, videos, juegos, afiches y boletines informativos relacionados con la capacitación en concientización sobre seguridad. Además, podrá aprovechar nuestra función Phishing basado en IA para personalizar las pruebas de phishing por usuario, activar el aprendizaje opcional recomendado por IA para sus usuarios y utilizar PasswordIQ para supervisar continuamente su organización en busca de cualquier vulnerabilidad de contraseña detectada en su Active Directory.

Compliance Plus: Está disponible como complemento opcional en todos los niveles de suscripción. La capacitación de Compliance Plus es interactiva, relevante y atrapante. Incluye escenarios simulados de la vida real para ayudar a enseñar a sus usuarios cómo accionar ante una situación difícil. El contenido aborda temas delicados como el acoso sexual, la diversidad y la inclusión, la discriminación y la ética empresarial. La biblioteca de Compliance Plus ofrece varios tipos de formatos multimedia y materiales de refuerzo para respaldar su programa de capacitación en materia de cumplimiento.

PhishER Plus: Está disponible como producto independiente o como complemento opcional en todos los niveles de suscripción. PhishER Plus es una plataforma liviana de SOAR que analiza y prioriza de manera automática los mensajes de correo electrónico que hayan sido informados, a fin de detectar y poner en cuarentena los correos maliciosos en toda la organización. Además, convierte los correos electrónicos de phishing del mundo real en oportunidades de capacitación, a modo de campañas de phishing simuladas. Gracias a sus funciones de lista de bloqueo y PhishRIP global, detecta amenazas de origen colectivo y validadas por inteligencia artificial a fin de bloquear y eliminar de manera proactiva los ataques activos de phishing que hayan eludido los filtros del correo electrónico ANTES de que el usuario quede expuesto. Con PhishER Plus, obtendrá grandes ahorros en presupuesto y tiempo del equipo de seguridad de la información, ya que podrá reducir el volumen de esfuerzos de remediación que gestiona su centro de operaciones de seguridad.

SecurityCoach: Disponible como un complemento opcional para los clientes de KnowBe4 con una suscripción de capacitación en concientización sobre seguridad de nivel Platino o Diamante. SecurityCoach es el primer producto de asesoramiento en seguridad en tiempo real creado para que los equipos de operaciones de seguridad y de TI puedan proteger mejor la mayor superficie de ataque de su organización: los empleados. Con la introducción de una nueva categoría de tecnología denominada “detección y respuesta humanas”, SecurityCoach podrá fortalecer su cultura de la seguridad con un asesoramiento en seguridad en tiempo real para sus usuarios, en respuesta a sus comportamientos de seguridad riesgosos.

“El eslabón más débil de la seguridad de la información es la ingeniería social”.

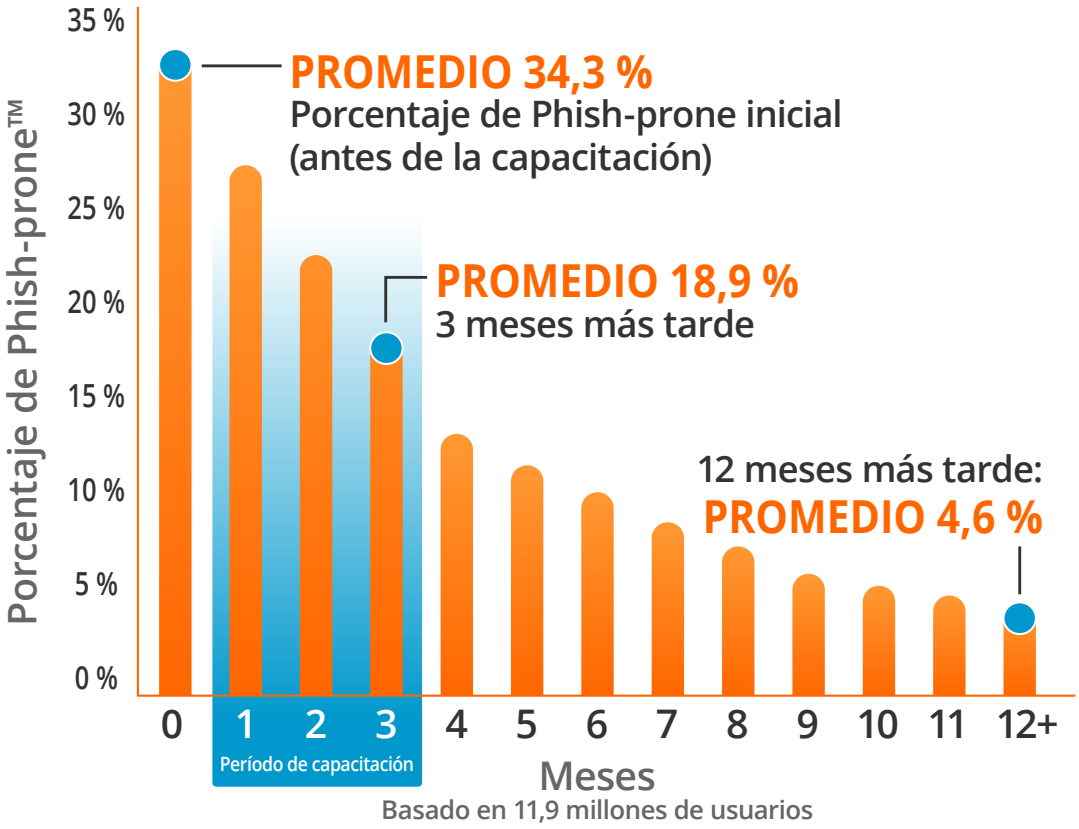
– Kevin Mitnick, “El hacker más famoso del mundo”, consultor de seguridad de TI

Prueba visible de que el sistema KnowBe4 funciona

Cuando invierte en la capacitación en concientización sobre seguridad y en las pruebas de seguridad contra el phishing, ve el valor y el retorno de la inversión rápidamente.

Los resultados del Informe de evaluación comparativa del sector de phishing de KnowBe4 de 2024 muestran claramente dónde comenzaron los porcentajes de Phish-prone (predisposición para ser víctima de phishing) y dónde terminaron después de al menos 12 meses de pruebas periódicas y capacitación en concientización sobre seguridad.

El porcentaje de Phish-prone inicial de referencia del sector resultó ser un preocupante 34,3 %. Por suerte, los datos mostraron que este 34,3 % puede reducirse casi a la mitad, a un 18,9 %, en los 90 días siguientes a la implementación de la nueva capacitación en concientización sobre seguridad. Los resultados de un año muestran que, si se siguen estas prácticas recomendadas, el porcentaje de Phish-prone final puede reducirse a un promedio de 4,6 %.



Fuente: Informe de evaluación comparativa de phishing por industria de KnowBe4 de 2024

Nota: El PPP inicial se calcula en función de todos los usuarios evaluados. Estos usuarios no habían recibido ninguna capacitación con la consola de KnowBe4 antes de la evaluación. Los períodos posteriores reflejan los porcentajes de Phish-prone (predisposición para ser víctima de phishing) para el subconjunto de usuarios que recibieron capacitación con la consola de KnowBe4.

KnowBe4
Human error. Conquered.

KnowBe4 Brazil | Av. Ibirapuera, 2315, Indianópolis, CEP 04029-200 | São Paulo-SP | Tel: +55 (0800) 761-2668 | www.KnowBe4.com | Sales@KnowBe4.com