

Enfréntese a la IA con IA: 3 formas de usar la concientización sobre seguridad impulsada por IA para combatir a los ciberdelincuentes

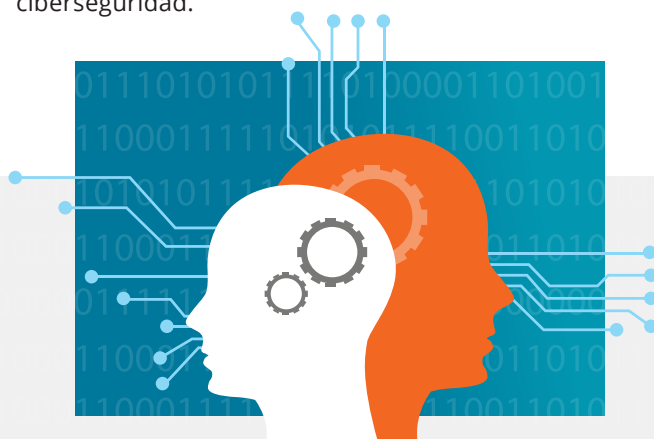
Los ciberdelincuentes están recurriendo a la IA para hacer que el mundo sea más peligroso para el resto de nosotros. Esta tecnología emergente, desde *deepfakes* hasta correos electrónicos de phishing generados por IA a gran escala, se ha convertido en un arma poderosa en los arsenales de los malhechores de todo el mundo.

Por suerte, los profesionales de la seguridad de la información como usted pueden hacer algo al respecto. Es probable que ya esté aprovechando el poder de la IA en todo su conjunto tecnológico. ¿Por qué no aprovecharlo para fortalecer su firewall humano? La ciberseguridad no solo tiene que ver con los productos de seguridad implementados, sino también con las personas que los utilizan.

En lo que respecta al elemento humano vital de la ciberseguridad, el poder de la IA se puede utilizar a su favor para brindar a los usuarios capacitación relevante y mantenerlos informados contra los ciberataques en constante cambio.

Continúe leyendo para obtener una descripción general de cómo un sólido programa de capacitación en concientización sobre seguridad (SAT, por sus siglas en inglés) y un programa de phishing simulado con IA en su núcleo pueden contribuir a una iniciativa integral de ciberseguridad.

La IA se une a los seres humanos: cómo crear una capacitación en concientización sobre seguridad más inteligente



Si bien los actores de amenazas utilizan cada vez más la IA con fines maliciosos, las herramientas de ciberseguridad se están adaptando para aprovechar el poder de la inteligencia artificial. Sin embargo, a pesar de estos avances, aún existen desafíos en materia de seguridad de la información.



La rápida evolución de la tecnología de IA requiere una vigilancia constante por parte de los usuarios.

Las medidas de seguridad tradicionales pueden ser insuficientes contra los ataques impulsados por IA, por lo que se requieren tácticas defensivas innovadoras.



La escasez de tiempo y recursos del personal de ciberseguridad agrava el desafío de mantenerse al corriente de las nuevas amenazas.

Por suerte, los nuevos avances en la concientización sobre seguridad y las estrategias de phishing simulado ofrecen esperanzas.

Estas son algunas formas clave en las que la mejora de la IA puede llevar las iniciativas de SAT existentes a un nivel superior:

Capacitación y refuerzo automatizados

La SAT mejorada con IA tiene el potencial de agilizar drásticamente el trabajo de un administrador de capacitación. Imagine un sistema de aprendizaje adaptativo impulsado por IA que asigne automáticamente capacitación a las personas en función de todos sus antecedentes de aprendizaje. Esto significa que se tienen en cuenta la eficacia de los módulos de capacitación anteriores, los resultados recientes de los ejercicios de SAT y las preferencias personales de aprendizaje, como el formato (videos, cuestionarios, animaciones, juegos) y la duración del contenido, para brindar una experiencia personalizada para cada usuario.

Este enfoque no solo reduciría tareas específicas para el administrador, también aumentaría la relevancia de la capacitación para el usuario, lo que incrementaría las posibilidades de que interactuara con el contenido y retenga lo aprendido.

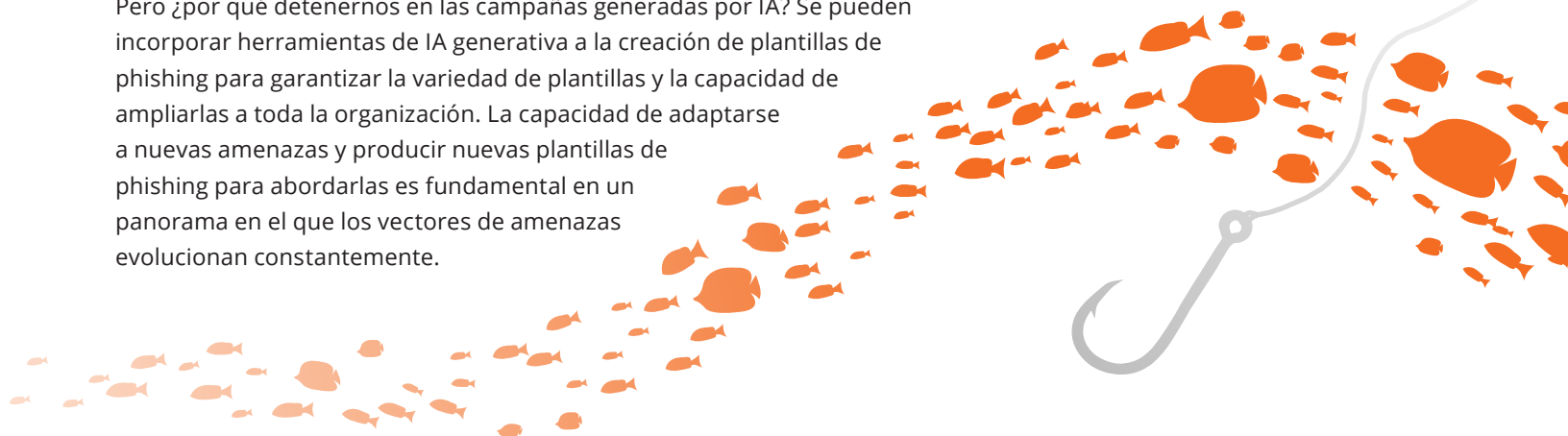
Una vez impartida la capacitación primaria, la IA también se puede utilizar para generar automáticamente cuestionarios de capacitación a fin de reforzar el contenido aprendido. Se podrían crear cuestionarios a partir del propio contenido de la capacitación o de las políticas organizacionales, y la IA generativa se encargaría de gran parte del trabajo pesado. El objetivo: reiterar los puntos clave y garantizar que la información sobre políticas se enseñe a los usuarios finales y no solo se muestre.

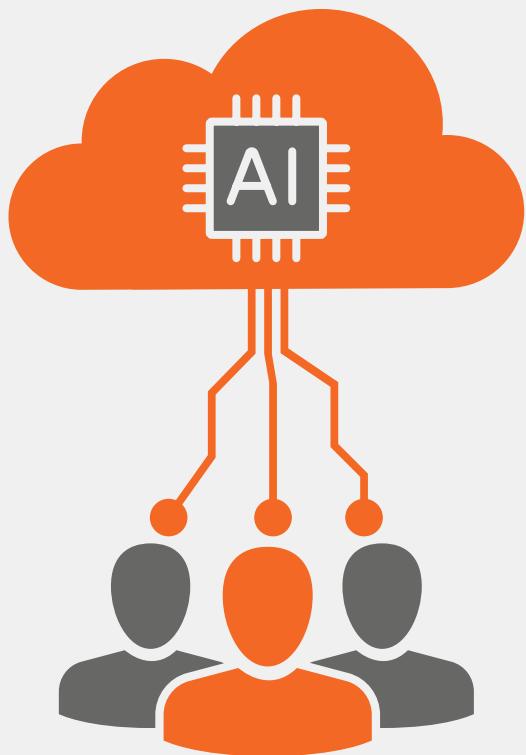


Campañas de phishing simuladas optimizadas

Un motor de recomendaciones impulsado por IA podría ser su propio asistente de phishing de IA que elige automáticamente la mejor prueba de phishing para cada usuario en ese momento. Imagine crear campañas de phishing únicas para cada uno de sus usuarios a fin de asegurarse de que reciban pruebas de phishing simuladas personalizadas según su nivel individual.

Pero ¿por qué detenernos en las campañas generadas por IA? Se pueden incorporar herramientas de IA generativa a la creación de plantillas de phishing para garantizar la variedad de plantillas y la capacidad de ampliarlas a toda la organización. La capacidad de adaptarse a nuevas amenazas y producir nuevas plantillas de phishing para abordarlas es fundamental en un panorama en el que los vectores de amenazas evolucionan constantemente.





La IA se une a la inteligencia colectiva

Un elemento clave de un programa de SAT sólido es la capacidad de los usuarios de denunciar tanto los correos electrónicos de phishing simulados como los reales que llegan a sus bandejas de entrada. Sus usuarios quieren ayudar en esta batalla de la ciberseguridad, y usted debe tener las herramientas que les permitan defender su entorno de forma proactiva.

Este trabajo colectivo impulsado por los usuarios les permite denunciar estas campañas de phishing más rápido que con los métodos convencionales. En combinación con una herramienta de seguridad de correo electrónico impulsada por IA, el trabajo colectivo ayuda a que la IA sea más inteligente al permitir que los usuarios y los equipos de seguridad identifiquen, examinen y recopilen datos (en este caso, correos electrónicos sospechosos y maliciosos) en grandes cantidades.

De esta manera, la inteligencia sobre amenazas de phishing respaldada por análisis basado en IA está equipada para proteger a su organización de nuevos ataques de phishing. Este método ayudará a garantizar un tiempo de respuesta proactivo y más rápido ante la última ola de ataques de phishing contra su organización.

Conclusión: la IA ya está aquí

El impacto de la IA en la sociedad ya no es teórico. Está ocurriendo ahora mismo. La elección no es *si* incorporarla a sus iniciativas de ciberseguridad y SAT, sino *cuándo*.

Las organizaciones deben combatir el fuego con fuego. Al aprovechar el poder de la IA en los programas de capacitación en concientización sobre seguridad, las empresas pueden gestionar su riesgo humano y mantenerse un paso adelante de los ciberdelincuentes.

En última instancia, invertir en una concientización sobre seguridad mejorada con IA es una estrategia fundamental para mantener una cultura de seguridad sólida y protegerse contra las formidables amenazas cibernéticas del presente y del futuro.

Explore el enfoque de KnowBe4 para la concientización sobre seguridad impulsada por IA

Obtenga más información