KnowBe4

IA contra IA

Cómo combatir a los ciberdelincuentes con un programa de capacitación en concientización sobre seguridad basado en IA

IA contra IA: Cómo combatir a los ciberdelincuentes con un programa de capacitación en concientización sobre seguridad basado en IA

✦ Índice

INTRODUCCIÓN

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 ciber-seguridad, 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 las formas en que los malhechores usan la IA para sus propios dispositivos. También aprenderá cómo un sólido programa de capacitación en concientización sobre seguridad (Security Awareness Training, SAT) y un programa de phishing simulado con IA en su núcleo pueden contribuir a una iniciativa integral de ciberseguridad.

EL PANORAMA CAMBIANTE DE LAS CIBERAMENAZAS BASADAS EN IA

A menos que haya estado viviendo bajo una piedra generada por DALLE-3, seguramente ya habrá visto noticias sobre las innumerables formas en que los ciberdelincuentes están utilizando la IA generativa y herramientas relacionadas para causar problemas.

La IA ya se está utilizando para facilitar las campañas de desinformación e información errónea, mejorar los ataques de ingeniería social, y automatizar los ataques multicapa y multifacéticos a escala, incluso por parte de atacantes con escasos conocimientos técnicos.

No cabe duda de que quienes lideran la seguridad de la información están prestando atención. Un informe reciente de la empresa de detección de amenazas Netacea descubrió que el 93 % de los profesionales de seguridad encuestados creen que enfrentarán ataques diarios basados en IA en los próximos seis meses. Un poco menos de dos tercios (65 %) creen que la IA ofensiva será lo habitual.

✦ Cómo la IA potencia los ataques de phishing y la ingeniería social

➔ Generación automatizada de contenido

- La IA, en particular los modelos de procesamiento del lenguaje natural, puede generar correos electrónicos de phishing convincentes que sean correctos desde el punto de vista gramatical y contextualmente relevantes. Esto dificulta que los filtros de correo no deseado (spam) tradicionales los detecten como maliciosos.

- Las investigaciones indican que los correos electrónicos de phishing generados por IA tienen tasas de éxito más altas en comparación con los creados manualmente. Por ejemplo, un estudio de la Agencia de la Unión Europea para la Ciberseguridad (European Union Agency for Cybersecurity, ENISA) descubrió que la IA puede generar mensajes de phishing muy personalizados a escala, dirigidos a personas específicas imitando su estilo de escritura.

➔ Personalización de spear phishing (suplantación de identidad específica)

- Los algoritmos de IA pueden analizar grandes cantidades de datos de las redes sociales y otras fuentes en línea para recopilar información personal sobre los objetivos. Esto permite a los ciberdelincuentes crear correos electrónicos de spear phishing personalizados y convincentes que tienen más probabilidades de engañar a los destinatarios.
- El Informe sobre investigaciones de filtraciones de datos de Verizon (Verizon's Data Breach Investigations Report) destaca cómo los ataques de ingeniería social impulsados por IA pueden utilizar información detallada sobre los intereses, las conexiones y el comportamiento de una persona para aumentar la tasa de éxito de estos ataques.

➔ Automatización de sitios de phishing

- La IA puede automatizar la creación de sitios web falsos que imitan a los legítimos. Estos sitios pueden adaptarse en tiempo real para evadir la detección y parecer más auténticos, y así aumentar las posibilidades de que los usuarios ingresen sus credenciales.
- Según un estudio publicado en la revista Computers & Security, los sitios de phishing impulsados por IA pueden cambiar dinámicamente su apariencia y comportamiento según las interacciones del usuario y los datos de inteligencia sobre amenazas para pasar desapercibidos durante más tiempo.

➔ Tecnología *deepfake*

- Los *deepfakes* generados por IA pueden crear imitaciones realistas de audio y video de personas. Los ciberdelincuentes los utilizan para hacerse pasar por personas en rangos ejecutivos o personas de confianza, y convencer a sus víctimas de que divulguen información delicada o autoricen transacciones.
- La Agencia de Seguridad de Infraestructura y Ciberseguridad (Cybersecurity and Infrastructure Security Agency, CISA) emitió advertencias sobre la posibilidad de que los *deepfakes* se utilicen en ataques de ingeniería social y destacó su creciente sofisticación y los desafíos que plantean para su detección.

La IA puede ser la última novedad, pero no representa un vector de ataque totalmente nuevo. Los atacantes seguirán utilizando phishing generado por IA para provocar respuestas emocionales (solo que muchas más). Las víctimas asustadas cometerán errores al transferir dinero o introducir malware en los sistemas. En última instancia, la defensa será la misma: es decir, prestar atención a las señales habituales de una estrategia de ingeniería social.

Con estas similitudes tácticas fundamentales en la forma en que se siguen produciendo los ataques, el poder de la IA resulta vital para defenderse de ellos.

LA IA PARA EL BIEN: LOS ROBOTS DE NUESTRO LADO

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 IA.

Un área clave es la seguridad inteligente del correo electrónico. Los filtros de correo electrónico tradicionales se basan, en gran medida, en el análisis de los archivos adjuntos y en la búsqueda de firmas de malware conocidas. La seguridad del correo electrónico impulsada por IA va más allá de esto. Puede analizar el contenido en sí de los correos electrónicos y examinar patrones sutiles y la semántica para identificar intentos sofisticados de ingeniería social.

La IA y el aprendizaje automático también desempeñan un papel importante en la supervisión, el análisis y la detección de ciberamenazas en tiempo real en toda una organización. Los algoritmos de IA pueden procesar y correlacionar continuamente grandes cantidades de datos procedentes del tráfico de red, los terminales, los servicios en la nube, etcétera. Esto significa que la detección con IA puede identificar señales tempranas de amenazas y proporcionar alertas en tiempo real, lo que agiliza la respuesta ante incidentes.

No obstante, la parte técnica es solo un aspecto de la lucha contra la ciberdelincuencia. La IA puede y debe utilizarse para fortalecer la superficie de ataque humana.

LA IA SE UNE A LOS SERES HUMANOS: CÓMO CREAR UNA CAPACITACIÓN EN CONCIENTIZACIÓN SOBRE SEGURIDAD MÁS INTELIGENTE

A pesar de los avances de la IA, 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.

La SAT mejorada con IA tiene el potencial de agilizar drásticamente el trabajo de un administrador de capacitación.

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 cada uno reciba 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.

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.

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 conjunto 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.

MÁS INFORMACIÓN →

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

Recursos adicionales

Prueba de seguridad contra el phishing (PST) gratuita
Descubra qué porcentaje de su personal tiene predisposición para ser víctimas de phishing (Phish-prone) con la prueba de seguridad contra el phishing (PST) gratuita.

Vista previa de capacitación gratuita
Vea nuestra biblioteca completa de contenido de concientización sobre seguridad; navegue, busque por título, categoría, idioma o contenido.

Programa en concientización sobre seguridad automatizado gratuito
Cree un programa en concientización sobre seguridad personalizado para su organización.

Phish Alert Button gratuito
Ahora su personal tiene una forma segura de denunciar los ataques de phishing con un solo clic.

Domain Spoof Test gratuita
Descubra si los hackers pueden falsificar una dirección de correo electrónico de su propio dominio.

Acerca de KnowBe4

KnowBe4 capacita a su personal para que todos los días puedan tomar decisiones de seguridad más acertadas. Decenas de miles de organizaciones en todo el mundo confían en la plataforma KnowBe4 para fortalecer su cultura de seguridad y reducir el riesgo humano. KnowBe4 desarrolla una capa humana de defensa para que las organizaciones puedan reforzar el comportamiento de los usuarios a través de capacitaciones de vanguardia sobre cumplimiento y concientización sobre seguridad.

La implementación de KnowBe4 se traduce en usuarios que están alerta y se preocupan por el daño que causan el phishing, el ransomware y otras amenazas de ingeniería social. La plataforma incluye un paquete completo de capacitaciones sobre concientización y cumplimiento, asesoramiento en tiempo real para los usuarios, ingeniería social simulada por IA y defensa colectiva contra el phishing.

Con contenido en más de 35 idiomas, KnowBe4 ofrece la biblioteca más grande del mundo con contenido interesante que siempre está actualizado con el fin de reforzar su firewall humano.

Para obtener más información, visite www.KnowBe4.com.

KnowBe4

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

07E06K01