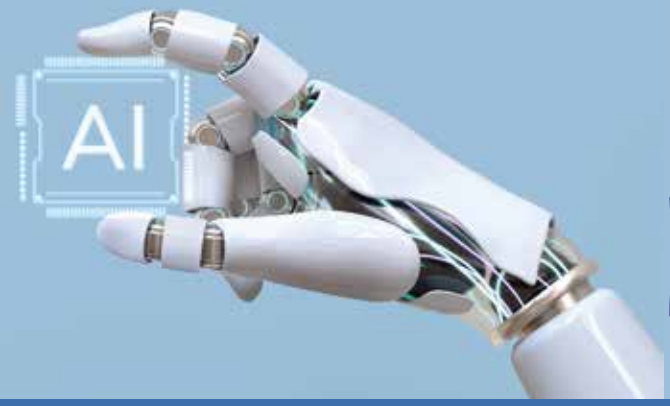
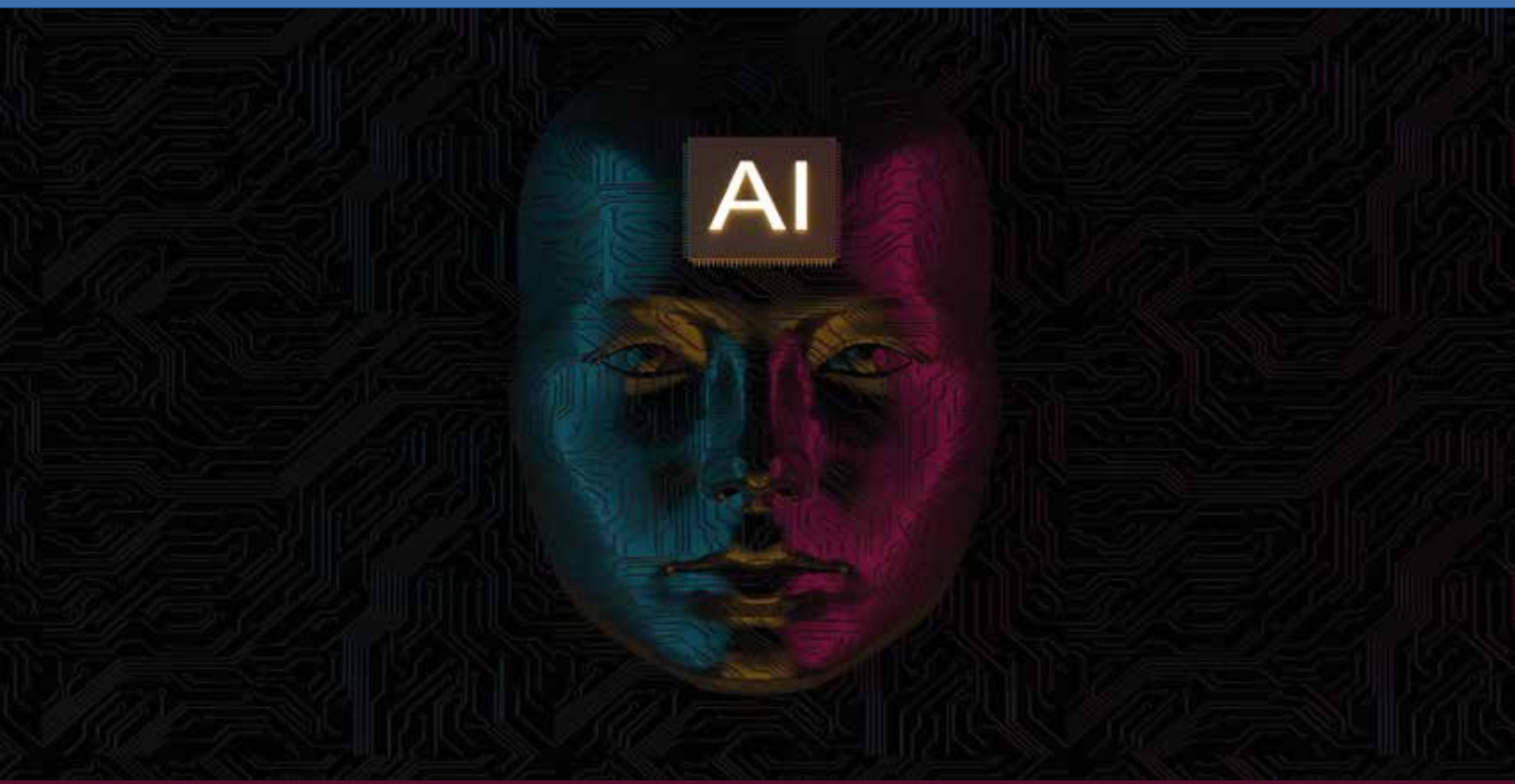
Abril - Junio



Universidad de Santander
UDES
VIGILADA MINEDUCACIÓN | SNIES 2832
ACREDITACIÓN INSTITUCIONAL ALTA CALIDAD UDES MIN EDUCACIÓN

BOLETÍN Nº 18

Inteligencia Artificial utilizada en Ciberataques



El ciberdelito ha evolucionado rápidamente gracias a la IA.

¿Qué es la Inteligencia Artificial?

La inteligencia artificial (IA) es una rama de la informática que desarrolla programas capaces de emular procesos propios de la inteligencia humana. Es decir, las máquinas pueden analizar el entorno y realizar determinadas acciones de manera más o menos autónoma con el fin de lograr objetivos concretos.

El ciberdelito ha evolucionado rápidamente gracias a la IA.

Hoy en día, los ciberdelincuentes atacan a ciudadanos y empresas de todo el mundo con técnicas sofisticadas y estafas difíciles de detectar que pueden engañar incluso a altos ejecutivos experimentados.

Fuente: https://www.inbest.cloud/comunidad/ciberataques-con-ia-la-nueva-era-de-la-ciberdelincuencia

¿Cómo funciona un ciberataque con IA?

Los ciberdelincuentes pueden utilizar la IA para automatizar tareas, como la búsqueda de vulnerabilidades en los sistemas informáticos o la creación de correos electrónicos de phishing personalizados.

La IA también puede utilizarse para analizar grandes cantidades de datos y así identificar patrones que podrían indicar un ataque en curso.

¿Cuáles son los principales riesgos?

Mayor sofisticación: Los ataques con IA pueden ser más difíciles de detectar y prevenir que los ataques tradicionales.

Mayor velocidad: La IA permite a los ciberdelincuentes lanzar ataques a gran escala de forma rápida y eficiente.

Mayor impacto: Los ataques con IA pueden tener un impacto devastador en las empresas y los gobiernos, ya que pueden provocar la pérdida de datos sensibles, la interrupción de servicios críticos e incluso daños físicos.

Fuente: https://www.inbest.cloud/comunidad/ciberataques-con-ia-la-nueva-era-de-la-ciberdelincuencia

Ejemplos de Ciberataques Impulsados con IA

El insólito robo millonario que engañó a un empleado: usó un filtro con la cara de su jefe

Una compañía de Hong Kong ha vivido un terrible suceso que ha dado la vuelta al mundo.

Y es que uno de sus empleados ha sido víctima de una estafa mediante videollamada en la que se utilizaban deepfakes y con la que los hackers consiguieron hacerse con 25 millones de euros.

El empleado de la multinacional durante una semana realizó varias videollamadas con el CFO de la compañía y otros directivos.

En las videoconferencias, un directivo le pidió que realizara varias transferencias en total 15 y a diversas cuentas por un valor total de 200 millones de dólares de Hong Kong, que al cambio son unos 25 millones de euros. El empleado hizo justo lo que le habían pedido, terminó transfiriendo el dinero, aunque el problema era que tanto el CFO como el resto de directivos de la compañía en realidad eran deepfakes.

Los deepfakes no son realmente nuevos. Se tratan de archivos de vídeo, imagen o voz que han sido manipulados mediante un software de inteligencia artificial (IA) de modo que parecen reales y auténticos.

Fuente:https://www.elespanol.com/omicrono/software/20240205/insolito-robo-millonario-engano-empleado-usando-filtro-cara-persona/830417023_0.html

¿Qué tipos de ciberataques se realizan?

Los ciberdelincuentes son conscientes de que la IA es muy útil para perpetrar sus ataques.

A continuación, te mostramos algunos vectores de ataque que pueden ser empleados con Inteligencia Artificial:

Phishing o Spear-Phishing

Con la ayuda de la IA, los ciberdelincuentes suplantan la identidad de empresas en correos electrónicos muy persuasivos, animando al usuario a facilitar información personal, a clicar en enlaces o a descargar archivos adjuntos que pueden contener software malicioso.

Los ciberdelincuentes, con la ayuda de la IA, pueden imitar la redacción de correos electrónicos suplantando a otras personas de la misma empresa o simular una página web de un servicio y que parezca el original.

Suplantación de identidad

También pueden hacerse pasar por otra persona o compañía a través de otros canales, como WhatsApp, mensajes SMS y llamadas telefónicas, utilizando herramientas de clonación de voz en el último caso.

Fuente: https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/ciberataques-inteligencia-artificial.html

¿Qué medidas debes tomar?

Revisa siempre el remitente de los mensajes antes de contestar o clicar en los enlaces de un correo. Recuerda que algunas herramientas de IA pueden escribir igual o de manera similar a personas o empresas.

Por regla general, no proporciones datos sensibles o confidenciales en la página web a la que te intenta redirigir un enlace incluido en un SMS o email. Tampoco descargues aplicaciones a través de estos canales; recuerda hacerlo siempre desde los mercados oficiales.

No compartas las contraseñas, ya que son únicas e intransferibles, y no las introduzcas en herramientas de Inteligencia Artificial.

Crea una cultura de ciberseguridad, sé consciente de los riesgos que puede ocasionar un mal uso de las IAs y transmite esos conocimientos a tu entorno más cercano y profesional.

Fuente: https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/ciberataques-inteligencia-artificial.html

CONTÁCTANOS

Si presentas dudas o detectas alguna situación sospechosa puedes comunicarte con el subproceso de seguridad informática UDES:

Bucaramanga
seguridadinformatica@udes.edu.co
Teléfono (607) 6516500 ext. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
Teléfono: (605) 5730073 ext. 129

Cúcuta
wpena@udes.edu.co
Teléfono: (607) 5748717 ext. 4196