Phishing, Vishing y la evolución de los ataques cibernéticos utilizando la Inteligencia Artificial

octubre 23, 2023

SHARE

Por: Edison Cóndor, Analista de Infraestructura del Ministerio de Relaciones Exteriores.

En la actualidad, la ciberseguridad se ha convertido en una preocupación crítica en nuestro mundo cada vez más digital. Las amenazas cibernéticas evolucionan constantemente, dos de las más persistentes son el phishing y el vishing. Sin embargo, lo que hace que estos ataques sean aún más preocupantes es cómo estos se han transformado y se han vuelto más peligrosos gracias al uso de la inteligencia artificial (IA).

El phishing y el vishing son dos tipos de ataques cibernéticos que utilizan la ingeniería social para engañar a las víctimas que revelen información personal o financiera. El phishing se realiza a través de correos electrónicos o mensajes de texto falsos que parecen provenir de fuentes legítimas, como bancos, empresas de tecnología o incluso gobiernos. El vishing en cambio, se realiza a través de llamadas telefónicas falsas que parecen provenir de empresas de servicio o algún familiar en peligro. A continuación, exploraremos cómo los ciberdelincuentes están utilizando la IA para transformar estos métodos de ataque y cómo podemos defendernos contra ellos.

Phishing: Engaño en el Ciberespacio

El phishing es una forma de ataque cibernético en la que los delincuentes intentan engañar a las personas para que revelen información confidencial, como contraseñas o datos bancarios, haciéndose pasar por una entidad confiable. Era frecuente que el phishing se realice mediante correos electrónicos fraudulentos; sin embargo, hoy en día, el phishing ha evolucionado y se ha vuelto más persuasivo y personalizado, utilizando a su favor estrategias como:

Ingeniería Social Avanzada: A través de esta, los atacantes estudian a sus víctimas y utilizando la información recopilada de las redes sociales y otros recursos públicos para crear mensajes convincentes que aumenten la probabilidad de que se lleve a cabo el engaño.

Inteligencia Artificial: Mediante la IA se automatiza la generación de correos electrónicos fraudulentos y mensajes de phishing. Esto permite a los ciberdelincuentes lanzar campañas masivas con mayor eficiencia y al mismo tiempo personalizar mensajes para que parezcan auténticos.

Vishing: El arte de la suplantación de identidad telefónica

El vishing es una variante del phishing que se lleva a cabo mediante llamadas telefónicas en lugar de correos electrónicos. Los delincuentes informáticos utilizan técnicas de ingeniería social para engañar a las personas por teléfono y obtener información confidencial o realizar estafas financieras, aprovechando los avances de la IA, los delincuentes han encontrado un camino para realizar ataques de vishing de las siguientes maneras:

Voz Sintética Avanzada: Con la IA, los atacantes pueden generar voces sintéticas extremadamente realistas, lo que les permite imitar y/o suplantar la identidad de familiares.

Escalada de Escenarios: Los ciberdelincuentes pueden usar algoritmos de IA para adaptar rápidamente sus tácticas a medida que la conversación progresa. Esto les permite ajustar sus respuestas a las reacciones de la víctima y aumentar sus posibilidades de éxito.

A medida que los ataques se vuelven más avanzados, es necesario que las personas y las organizaciones adopten medidas de seguridad más sólidas, por lo tanto, la clave es la educación que nos permita detectar amenazas cibernéticas, incluidas las tácticas de phishing y vishing.

Estrategias para evitar ataques de phishing y vishing

Verificación de Identidad: Antes de proporcionar información confidencial, verifique la identidad de la persona o entidad que la solicita, para evitar el vishing es importante que se realicen preguntas que solo la persona que conoce podría responder.

Verificación de la Fuente: Antes de hacer clic en cualquier enlace, verifique la fuente del mensaje. Compruebe la dirección de correo electrónico del remitente y la URL del sitio web.

Comprobar la seguridad del sitio web: Asegúrese de que el sitio web sea seguro. Busque un candado en la barra de direcciones (https://) y verifique si el sitio utiliza certificados SSL válidos.

Evitar caer en trampas que llamen a la humanidad de una persona: a menudo los delincuentes se escudan en situaciones de riesgo o peligro lo que podría conllevar a que las personas sean engañadas.

Privacidad de redes sociales: por medio de la Inteligencia Artificial, es posible realizar la clonación de la voz, los delincuentes usan fragmentos de videos públicos en redes sociales, por lo que se recomienda agregar a personas que en verdad conozcamos, esto bajara el riesgo de este tipo de engaño.

La inteligencia artificial ha elevado la peligrosidad de los ataques de phishing y vishing a un nuevo nivel, la capacidad de los atacantes para crear engaños personalizados por medio de mensajes y llamadas cada vez más convincentes.

La educación y prevención permiten combatir los ataques impulsados con Inteligencia Artificial. Al estar informados sobre estas técnicas y estrategias, podemos reconocer los intentos de engaño.