publimetro

Fecha: 30/05/2025 Audiencia: 382.227 Sección: OCIO Y TIEMPO LIBRE
Vpe: $4.220.660 Tirada: 84.334 Frecuencia: 0
Vpe pág: $5.467.176 Difusión: 84.334
Vpe portada: $5.467.176 Ocupación: 77,2%

fayerwayer **FW**

FOTOS: FREEPIK

Cómo evitar fraudes y suplantaciones creadas con IA

Protección. Los ciberdelincuentes clonan la voz e identidad de directivos para solicitar transferencias bancarias y defraudar a empresas y negocios

Mario Mendoza
Metro World News

En los últimos meses, la Inteligencia Artificial (IA) volvió a sorprender al mundo con nuevas tendencias virales, como la generación de imágenes, basadas en fotografías personales, audios y expedientes de empleados y directivos para cometer fraudes contra empresas y pequeños negocios.

Un reporte de la empresa WeWork Latinoamérica alertó que, aun cuando las nuevas aplicaciones muestran el lado más creativo y accesible de la IA, también evidencian lo fácil que es manipular contenido privado y cómo esta tecnología puede ser utilizada con fines malintencionados.

La firma señaló que, de acuerdo con expertos y compañías de ciberseguridad, la IA representa uno de los mayores riesgos de la actualidad, ya que los delincuentes la utilizan para crear nuevas formas de fraude y suplantaciones en entornos empresariales o corporativos.

"Los ciberdelincuentes están aprovechando estas herramientas para crear contenidos falsos altamente convincentes, como voces clonadas y videos manipulados, con el objetivo de engañar a empleados y organizaciones.

"Un ejemplo alarmante es la clonación de voz, donde, con apenas unos segundos de audio, los estafadores pueden replicar la voz de una persona para realizar solicitudes falsas de transferencias bancarias o acceso a información sensible", advirtió la empresa.

¿CÓMO EVITAR FRAUDES BASADOS EN IA CONTRA LAS EMPRESAS?

1 **Para desactivar el riesgo de fraudes corporativos,** perpetrados a través de herramientas o aplicaciones de Inteligencia Artificial, Diego Kexel, General Manager de WeWork Latinoamérica te recomienda:

2 **Verificar solicitudes por múltiples canales.** Antes de aprobar transferencias de dinero o compartir información confidencial, es fundamental confirmar la autenticidad de la solicitud mediante llamadas telefónicas directas u otros canales alternativos.

3 **Implementar protocolos de seguridad rigurosos.** Establecer procesos internos claros para la gestión de información sensible, como aprobaciones en varios niveles y autenticación multifactorial, reduce significativamente los riesgos.

4 **Capacitar continuamente a los empleados.** Educar al equipo sobre los nuevos métodos de fraude basados en IA, como el phishing avanzado y la clonación de voz, permite detectar y prevenir posibles ataques.

5 **Adoptar herramientas digitales para detección de fraudes.** Utilizar software de análisis de comportamiento y autenticación biométrica ayuda a identificar actividades sospechosas en tiempo real.

6 **Actualizar constantemente los sistemas de seguridad.** Mantener los programas y protocolos de ciberseguridad al día es clave para protegerse contra vulnerabilidades que puedan ser explotadas por ciberdelincuentes.

"La inteligencia artificial ofrece innumerables beneficios en el ámbito laboral, pero su uso responsable y seguro requiere una vigilancia constante y la adopción de prácticas preventivas.

"Con un enfoque proactivo, las compañías pueden aprovechar todo el potencial de esta tecnología sin comprometer la seguridad de su información ni la de sus colaboradores".

DIEGO KEXEL,
WeWork Latinoamérica.