Deepfakes: cómo detectar la suplantación de identidad bancaria

Recopilado por el Staff de El Inversionista

Todo gran avance conlleva un riesgo; los avances tecnológicos y la ciberseguridad nos han dado la libertad y marcado la pauta para desarrollar cambios significativos en la manera de cómo nos comunicamos, laboramos y convivimos; sin embargo, los atacantes también han tomado un papel relevante, lo cual nos incita a ser mayormente preventivos.

El conocimiento es poder; los fraudes han ido evolucionando en estos últimos años y términos como phishing, suplantación de identidad, inteligencia artificial, ingeniería social, son conceptos que han sido agregados a nuestro vocabulario, por ello mismo la tendencia para 2026 indica que los atacantes buscan aprovechar los recursos que la inteligencia artificial nos ha permitido desarrollar, hoy en día es conocido como: deepfake.

¿Qué es un deepfake y cómo funciona en el fraude bancario?

Los deepfakes, y específicamente, deepfakes bancarios, son una amenaza emergente que utiliza la Inteligencia Artificial para crear medios capaces de "clonar" apariencias de personas reales e identificables, así como la manipulación de voz y la falsificación de contenido. Los deepfakes llegan a replantear lo que implica confiar en alguien al otro lado de la pantalla, del teléfono o de cualquier dispositivo electrónico.

La terminología nace de un compuesto en inglés, "*deep*" por la rama de la inteligencia artificial deep learning (profundo aprendizaje automático, este modelo es una combinación entre la inteligencia artificial y el machine learning), el "*fake*" por considerarse falso, haciendo referencia a situaciones que nunca sucedieron, o personas que no son reales.

Los deepfakes bancarios ya han sucedido: Un empleado de una firma multinacional en Hong Kong recibió un correo electrónico supuestamente del CFO de Reino Unido, en el cual le solicitaba una "Transferencia Confidencial". El atacante convoca a una sesión en línea a la víctima y demás participantes. La víctima estaba convencida de con quién había estado en comunicación, al finalizar la reunión el atacante había logrado que la víctima realizara la transferencia de aproximadamente 25.6 millones de dólares. Los empleados confiaban tanto en las videoconferencias que no cuestionaron la identidad ni la solicitud inusual.

¿Qué salió mal?

Confianza ciega en el entorno digital. Solicitud urgente e inusual sin una verificación adicional (por teléfono por ejemplo).

Guía práctica: cómo saber si es un deepfake

Te compartimos algunas recomendaciones para que puedas estar atento a posibles casos de suplantación de identidad con IA y evites caer en uno.

Si te comparten fotos, presta atención en:

Rasgos faciales: piel sin imperfecciones, simetría poco realista, detalles en ojos y dientes.

Fondo y reflejos: válida dentro de la imagen los fondos, lo ideal es que hagan congruencia con el contexto de la conversación.

En caso de videos o videollamadas, atento en:

Parpadeo y ojos: usualmente este tipo de videos tiene parpadeos anormales (ya sean excesivos o escasos).

Sincronización labial y habla: que no haya congruencia entre lo que dice y el movimiento de los labios.

Piel y rasgos faciales: "Parece que usa filtro", la piel se nota demasiado suave, sin arrugas. Usualmente hay incoherencia en puntos clave como las orejas y el cabello.

Movimiento: el movimiento brusco es una señal, además de las posiciones de cabeza o cuerpo