LITORALPRESS

Fecha: 15-11-2024
Medio: El Mercurio
Supl. : El Mercurio - FINANZAS & TECNOLOGÍA
Tipo: Noticia general
Título: **Falta acelerar preparación de las empresas ante nuevas formas de fraudes de identidad**

Pág. : 3
Cm2: 368,5

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

ANTE EL AVANCE TECNOLÓGICO:

Falta acelerar preparación de las empresas ante nuevas formas de fraudes de identidad

Entre las amenazas que han surgido están las "selfies sintéticas", consistentes en la suplantación de imágenes de personas reales creadas con inteligencia artificial.

NOEMÍ MIRANDA G.

En una reunión por videollamada entre altos ejecutivos de una empresa transnacional, todo parecía transcurrir con normalidad: el gerente de Finanzas, cuya oficina se encontraba en Reino Unido, solicitó al ejecutivo de la filial de Hong-Kong la transferencia de US$ 25 millones. Los demás asistentes —todos con sus cámaras prendidas— aprobaron la transacción. Horas después, cuando el ejecutivo informó a la gerencia general sobre la operación, se encendieron todas las alertas. Tras extensos peritajes, la policía de Hong-Kong descubrió que ninguna de las personas presentes en la videollamada eran reales, sino que se trataba de recreaciones digitales de los rostros y las voces de los ejecutivos, tecnología conocida como *deepfake*.

41% de 350 empresas encuestadas a nivel global carecen de estrategias sólidas de verificación de identidad.

La estafa —reportada por CNN en febrero pasado, manteniendo el anonimato de la empresa— es solo un caso entre muchos en que se usan tecnologías emergentes, como la IA generativa, para cometer delitos. Y no solo en las finanzas. Ante el aumento de los ataques de *bots* en redes sociales previo a las elecciones en EE.UU., la empresa de ciberseguridad AU10TIX alertó sobre la rapidez con que avanzan las técnicas de suplantación de identidad, como las "selfies sintéticas" (imágenes falsas de personas reales hechas con IA) que ya han logrado eludir sofisticados sistemas de verificación.

Baja madurez

Ante este panorama, se podría pensar que se ha agilizado la adopción de tecnología para proteger a las empresas y a las personas. La realidad es otra: la consultora especializada Sailpoint encuestó en julio de este año a más de 350 líderes en ciberseguridad a nivel global, descubriendo que el 41% de las compañías se encuentran en el nivel más bajo de madurez en verificación digital de identidad, careciendo tanto de estrategias como de tecnologías.

Parte del problema puede deberse a la necesidad de responder en distintos frentes. Un sondeo hecho por Forbes y la empresa Arculus a 200 líderes de empresas en Estados Unidos mostró que el 65% incrementará en 2025 el presupuesto destinado a *call centers* para el reseteo de contraseñas o verificación de identidad, pese a que el 69% cree que métodos automáticos ahorrarían tiempo y recursos.

En mejor pie

Nuestro país se encuentra hoy en un buen pie para hacer frente a estos desafíos y, en opinión de Tomás Pintor, director del Diplomado Fintech de la Universidad Adolfo Ibáñez y socio de Bitlaw, se está avanzando más rápido que antes: "La ola regulatoria en materia digital no deja espacio para otra cosa. La Ley Marco de Ciberseguridad, la Ley Fintech y la nueva Ley de Protección de Datos Personales obligan a las empresas a comenzar a tomar como prioridad la seguridad de la información". Estas normativas, agrega, permitirán a las *fintech* locales —nativas en lo digital y con muy buenos sistemas— adecuarse a un estándar de cumplimiento. "Hay varios prestadores de servicios con herramientas automatizadas para el *onboarding* (registro) de clientes financieros, lo que podría verse potenciado con herramientas como las que disponga el Sistema de Finanzas Abiertas, que a través de APIs permitirá un enrolamiento de clientes más rápido y seguro", explica el experto.

Para Alfie Ulloa, presidente de Chile Telcos, el fraude por suplantación es el gran problema a atacar en materia de verificación de identidad: "Cada industria y empresa debe tener sus propias medidas para validar que son sus clientes los que están haciendo las transacciones. Los sistemas de verificación, si bien pueden apoyarse en mecanismos adicionales (una *app* en reemplazo del *token* o la tarjeta de coordenadas), tienen que ser bien analizados y, por sobre todo, responder rápidamente a nuevas formas de vulneración".

La experiencia de los consumidores

Un estudio a nivel global realizado por la empresa de verificación financiera TransUnion reveló la experiencia de los usuarios en términos de intentos de fraude.

49% de los usuarios fueron blanco de estafas por correo electrónico, sitios web, llamadas telefónicas o mensajes de texto, y el 9% fue víctima de fraude.

51% no reconoció el fraude potencial, ni se dio cuenta de que estaba siendo objeto de una estafa.

37% de los que sí reconocieron la estafa indicaron que se trató de *smishing* (fraude mediante mensaje de texto u otra vía de comunicación en el que se solicita entregar datos personales, o acceder a un beneficio, entre otros).

34% reconoció haber recibido *phishing* (correos electrónicos que parecen pertenecer a instituciones de confianza y que pueden vulnerar los datos de ingreso a esas plataformas).

33% dijo haber sido objetivo o víctima de *vishing* (llamadas telefónicas que parecen provenir de empresas confiables, como el banco del usuario, para alertar de una potencial estafa y pedir los datos de acceso a las cuentas de las personas).

Chile: El tipo de estafa más frecuente sigue siendo el *smishing*. Entre los contenidos de los mensajes de texto maliciosos está la necesidad de que la víctima verifique su identidad para recibir una encomienda, información de que ha recibido un bono o premio o la necesidad de restablecer una clave.

Durante el primer trimestre de 2024, el fraude digital más frecuente en nuestro país fue la falsificación de perfil en comunidades, foros y sitios de citas, que aumentó 22% respecto del mismo periodo de 2023.