LITORALPRESS

Fecha: 08-07-2024
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo B
Tipo: Noticia general
Título: La tecnología de inteligencia artificial está ayudando a los estafadores a ser más listos que usted, y su banco

Pág. : 6
Cm2: 849,4

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Los fraudes ahora apuntan a grupos mucho más grandes:

La tecnología de inteligencia artificial está ayudando a los estafadores a ser más listos que usted, y su banco

Su "sexto sentido" no es digno rival para la nueva ola de timadores.

DALVIN BROWN Y KATHERINE HAMILTON
THE WALL STREET JOURNAL

La inteligencia artificial (IA) está haciendo que los estafadores sean más difíciles de detectar.

Ya quedaron atrás los mensajes mal redactados que alertaban fácilmente a las autoridades como también a la policía especializada. Los tipos malos ahora son mejores redactores y conversadores más convincentes, que pueden mantener una conversación sin revelar que son un robot, dicen investigadores de banco y de tecnología que dedican sus jornadas a rastrear los esquemas más recientes.

ChatGPT y otros instrumentos de IA pueden incluso permitir que los estafadores creen una imitación de su voz e identidad. En los últimos años, los delincuentes han utilizado un *software* basado en IA para hacerse pasar por altos ejecutivos y pedir transferencias bancarias.

"Su sexto sentido ya no le va a impedir que sea víctima", señaló Matt O'Neill, exagente del Servicio Secreto y cofundador de la firma de ciberseguridad 5OH Consulting.

En estos casos recientes, los fraudes a menudo son similares a las antiguas estafas. Pero la IA ha hecho posible que los timadores apunten a grupos mucho más grandes y utilicen más información personal para convencer de que la estafa es real.

PERJUICIO
La cifra real de pérdidas por estafas podría estar cerca de los US$ 200 mil millones.

Los funcionarios a cargo de la prevención de fraudes afirman que estas tácticas a menudo son más difíciles de detectar porque evitan los indicadores tradicionales de estafas, como enlaces maliciosos y mala redacción y gramática. Los delincuentes hoy en día falsifican licencias de conducir y otros documentos de identificación en un intento por abrir nuevas cuentas bancarias, y agregan rostros y gráficas generados por computadora para que pasen por los procesos de verificación de identidad. Todos estos métodos son difíciles de impedir, aseguran los funcionarios.

JPMorgan Chase ha empezado a utilizar modelos grandes de lenguaje para validar los pagos, lo que ayuda a combatir el fraude. Carisma Ramsey Fields, vicepresidenta de comunicaciones externas de JPMorgan Chase, señaló que el banco también ha intensificado sus esfuerzos para instruir a los clientes sobre las estafas.

Y aunque los bancos detengan algunos fraudes, la última línea de defensa siempre será usted. Estos funcionarios de seguridad aconsejan no compartir jamás información financiera o personal a menos que esté seguro de quién es el receptor. Si paga, utilice una tarjeta de crédito porque ofrece la mayor protección.

"Si alguien le dice que pague con criptomoneda, efectivo, oro, transferencia bancaria o una aplicación de pago, probablemente es una estafa", indicó Lois Greisman, directora asociada de la Comisión Federal de Comercio (FTC).

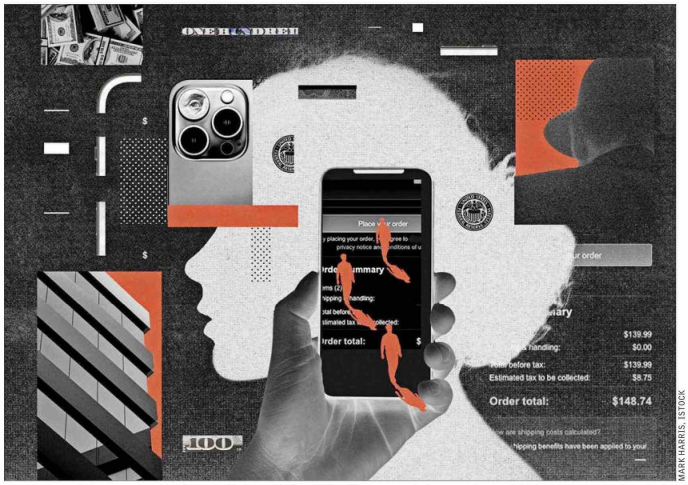
Selección de objetivo personalizada

Con la IA como un cómplice, los delincuentes están consiguiendo más dinero de las víctimas de todas las edades. Las personas reportaron pérdidas récord de US$ 10 mil millones debido a estafas en 2023, frente a los US$ 9 mil millones el año anterior, según la FTC. Puesto que esta entidad calcula que solo un 5% de las víctimas de fraude informa de sus pérdidas, la cifra real podría estar más cerca de los US$ 200 mil millones.

Joey Rosati, quien es dueño de una pequeña firma de criptomonedas, jamás pensó que podría ser víctima de una estafa hasta que un hombre que él creía que era un oficial de policía lo llamó en mayo.

El hombre le dijo a Rosati que había faltado a su designación como jurado. Parecía saber todo sobre él, lo que incluía su número de Seguro Social y que recién se había cambiado de casa. Rosati siguió la instrucción del oficial de dirigirse a la comisaría en Hillsborough County, Florida; lo que no parecía que fuera algo que sugeriría un estafador.

En el trayecto, a Rosati se le pidió que transfiriera US$ 4.500 para pagar la multa antes de llegar. Fue entonces cuando se dio cuenta de que era una estafa y colgó.



MARK HARRIS, ISTOCK

Los consumidores pagaron a los estafadores US$ 1.400 millones en criptomonedas en 2023, un aumento de más del 250% en relación a 2019, según datos de la FTC.

"No soy un joven sin educación, inmaduro. Tengo mi cabeza bien puesta", expresó Rosati. "Pero eran perfectos".

Los ataques de ingeniería social como la estafa de la designación como jurado se han vuelto más sofisticados con la IA. Los timadores utilizan instrumentos de IA para descubrir detalles sobre objetivos en las redes sociales y las filtraciones de datos, señalan expertos en ciberseguridad. La IA puede ayudarlos a adaptar sus esquemas en tiempo real generando mensajes personalizados que imiten en forma convincente a individuos de confianza, persuadiendo a los objetivos de que envíen dinero o entreguen información sensible.

El perfil en LinkedIn de David Wenyu exhibía un mensaje "abierto a trabajar" cuando recibió un correo electrónico en mayo en que le ofrecían una oportunidad laboral. Parecía ser de SmartLight Analytics, una compañía legítima, y llegaba seis meses después de que había perdido su trabajo.

Aceptó la oferta, aun cuando notó que la dirección del correo electrónico era ligeramente diferente de las que aparecían en el sitio web de la empresa. La compañía le emitió un cheque para que comprara en un sitio web específico el equipo necesario para trabajar desde casa. Cuando le indicaron que comprara los suministros antes de que el dinero apareciera en su cuenta, supo que era una estafa.

"Emocionalmente estaba demasiado desesperado, así es que ignoré esas señales de alerta", manifestó Wenyu.

En un estudio de abril entre 600 funcionarios de manejo de fraudes en bancos e instituciones financieras que llevó a cabo la compañía de *software* bancario Biocatch, el 70% indicó que los delincuentes eran más hábiles en el uso de la IA para delitos financieros que los bancos en utilizarla para la prevención. Kimberly Sutherland, vicepresidenta de estrategia de fraude e identidad en LexisNexis Risk Solutions, afirmó que ha habido un aumento evidente en los intentos de fraude que parecen estar relacionados con IA en 2024.

Riesgos de contraseña, amplificados

Los delincuentes solían tener que adivinar o robar contraseñas a través de ataques de *'phishing'* o filtraciones de datos, a menudo apuntando a cuentas de alto valor una por una. Ahora, los estafadores pueden cotejar y probar rápidamente contraseñas reutilizadas en las plataformas. Pueden emplear sistemas de IA para escribir un código que automatizaría diversos aspectos de sus tácticas, explicó O'Neill.

Si los estafadores obtienen su correo electrónico y una contraseña que utiliza comúnmente debido a una filtración de datos de una compañía tecnológica, los instrumentos de IA pueden verificar rápidamente si las mismas credenciales desbloquean sus cuentas de banco, de redes sociales o de compras.

Ser más astuto que las estafas

Las instituciones financieras están tomando nuevas medidas —y utilizando ellas mismas la IA— para proteger su dinero y sus datos.

Los bancos monitorean cómo introduce sus credenciales, ya sea que tienda a usar su mano izquierda o derecha cuando la desliza en la aplicación, y la dirección IP de su dispositivo para crear un perfil sobre usted. Si un intento de inicio de operación no iguala su comportamiento habitual, se detecta, y tal vez le pidan que proporcione más información antes de proceder.

Pueden indicar cuándo lo están forzando a que complete información, debido a los cambios en su cadencia de escritura. Si los dígitos se copian y pegan, si la verificación de voz es demasiado perfecta, o si el mensaje de texto está espaciado en forma demasiado pareja y es gramaticalmente correcto, eso es una señal de alerta, indicó Jim Taylor, jefe de producto de RSA Security, una firma con tecnología de detección de fraude a la que recurren Wells Fargo, Citibank y otras instituciones.

Autodefensa

Los consumidores pagaron a los estafadores US$ 1.400 millones en criptomonedas en 2023, un aumento de más del 250% en relación a 2019, según datos de la FTC.

Como resultado, funcionarios de seguridad sugieren que active una autenticación de dos factores, así recibe un mensaje de texto o correo electrónico cada vez que alguien trate de iniciar operaciones en una de sus cuentas. Si algo se siente raro durante un potencial intercambio de dinero, haga una pausa.

Hacer una pausa en una situación potencialmente fraudulenta también es importante sicológicamente. Muchos estafadores tratan de crear una falsa urgencia o confundir a las víctimas para manipularlas. Si toda la información sobre una transacción o cuenta proviene de una sola persona, eso es una señal de alerta. Obtenga una segunda opinión de un contacto de confianza.

"Si le va a afectar mucho si lo pierde, valídelo", dijo O'Neill, el exagente del Servicio Secreto.

Artículo traducido del inglés por "El Mercurio".