Expansión

Publicación	Expansión Economía Digital, 1	Fecha	19/12/2024
Soporte	Prensa Escrita	País	España
Circulación	36 629	V. Comunicación	113 834 EUR (119,450 USD)
Difusión	23 452	Tamaño	904,60 cm² (84,6%)
Audiencia	132 000	V.Publicitario	12 471 EUR (13 086 USD)

economistas Consejo General

LA INTELIGENCIA ARTIFICIAL DISPARA EL FRAUDE ONLINE

¿Quién debe pagar las pérdidas de las estafas?

A medida que proliferan los fraudes en los pagos, gobiernos, bancos y empresas tecnológicas discrepan sobre quién debe cubrir las pérdidas de los consumidores. **Por Joshua Franklin, Stephen Gandel y Akila Quinio (Financial Times)**

El abogado californiano Christopher Pitet fue víctima de un fraude a principios de este año. Recibió un correo electrónico, aparentemente del abogado contrario, con instrucciones sobre dónde transferir los 59.517,50 dólares acordados en el juicio. Los envió tal y como se le había indicado en dicho email. Pero el mensaje había sido enviado por un pirata informático que había instalado un bot de vigilancia en el servidor del bufete de Pitet y había observado cómo se desarrollaban las conversaciones para llegar a un acuerdo hasta el momento en que debía efectuarse el pago. Pitet, un abogado experto en fraudes, había transferido sin saberlo el dinero directamente a la cuenta del delincuente.

Pitet se dio cuenta de que le habían engañado y se puso en contacto con Citibank, que tenía la cuenta del pirata informático. Citi se negó a ayudarle, alegando que no era culpable ni legalmente responsable de cubrir las pérdidas. El abogado demandó al banco, pero éste se mantuvo firme. Lo más inquietante para Pitet fue que Citi citaba en su correo electrónico cinco casos en los últimos dos años en los que otras personas, incluidos bufetes de abogados, habían sido estafados de forma similar, habían demandado a Citi y habían perdido. Presintiendo la derrota, retiró la demanda.

Citi declaró que el caso de Pitet "carece de fundamento jurídico y que aunque nos esforzamos por prevenir el fraude y por ayudar a los clientes a recuperar el dinero perdido, el banco no es responsable de las acciones de personas que son engañadas para que sigan instrucciones de delincuentes".

Jamie Dimon, CEO de JPMorgan, defiende que los bancos no pueden ser responsables de los pagos que los usuarios hacen "voluntariamente".

Los avances en la inteligencia artificial y la velocidad de los pagos en tiempo real han facilitado que los estafadores manipulen a personas para que les transfieran voluntariamente su dinero. Las cifras exactas son difíciles de precisar, ya que muchos casos no se denuncian por miedo a represalias o vergüenza. Pero la Comisión Federal de Comercio de Estados Unidos calcula que la magnitud de los fraudes ascendió a 158.000 millones de dólares en 2023, frente a 137.000 millones en 2022.

Los audios, los vídeos y las imágenes generados por inteligencia artificial son uno de los factores que explican ese aumento. La consultora Deloitte estima que los contenidos generados por inteligencia artificial contribuyeron a más de 12.000 millones de dólares por fraudes en Estados Unidos el año pasado y que la cifra podría alcanzar los 40.000 millones en 2027.

Responsabilidades

A medida que el problema ha ido creciendo, también lo ha hecho el debate entre los gobiernos, los bancos y las empresas tecnológicas sobre quién debe cubrir las pérdidas cuando no se puede recuperar el dinero.

El Gobierno británico ha dictaminado que los bancos son responsables de las pérdidas de hasta 85.000 libras. En Australia echan más la culpa a las empresas tecnológicas. Y en Estados Unidos la cuestión sigue sin respuesta y se está volviendo políticamente tensa. Algunos altos cargos demócratas quieren que los bancos asuman más responsabilidad y la Oficina de Protección Financiera del Consumidor está investigando Zelle, un sistema de transferencia de pagos propiedad de un consorcio de grandes bancos estadounidenses que ha sido utilizado por estafadores.

Los vídeos creados por inteligencia artificial han hecho más sencillas las estafas online

Casi el 80% de los fraudes en los pagos se originan en las redes sociales, según UK Finance

Los bancos no quieren que se les considere culpables. JPMorgan Chase ha declarado que está dispuesto a demandar a la Oficina de Protección Financiera del Consumidor en respuesta a su investigación. Su consejero delegado Jamie Dimon dijo en una reunión de banqueros en octubre que "no podemos ser responsables de cada pago que se hace voluntariamente". Los bancos intentan culpar a las empresas tecnológicas como Meta, TikTok y Snapchat, donde se originan muchas estafas.

Mientras tanto, son las víctimas como Pitet las que pagan el precio. El hecho de que Citibank tuviera conocimiento de múltiples incidentes similares al suyo indica una falta de voluntad para actuar, dice el abogado: "Si sabían que la gente era estafada de esta manera, ¿por qué no hicieron

Expansión

Publicación	Expansión Economía Digital, 1	Fecha	19/12/2024
Soporte	Prensa Escrita	País	España
Circulación	36 629	V. Comunicación	113 834 EUR (119,450 USD)
Difusión	23 452	Tamaño	936,49 cm² (87,6%)
Audiencia	132 000	V.Publicitario	12 786 EUR (13 417 USD)

economistas Consejo General

Australia estudia sancionar a las redes sociales y 'telecos' por no proteger suficiente al usuario

Los bancos advierten que si les obligan a reembolsar las estafas, los servicios se encarecerán

Nathaniel Gleicher, director mundial de lucha contra el fraude de Meta.

nada al respecto? Los bancos pueden y deben hacer más".

El robo de datos de más de 80 millones de particulares y empresas clientes de JPMorgan por un pirateo informático en 2014 dio lugar a que los bancos se dedicaran más a defenderse contra los delincuentes que se cuelan en sus sistemas. Y a medida que los bancos han reforzado sus defensas, los estafadores han visto que los clientes son un eslabón débil.

A medida que la práctica ha ido creciendo, también lo ha hecho la magnitud de las pérdidas por estafas de todo tipo, desde pedir dinero por promesas de amor hasta inversiones en criptomonedas. Además, las aplicaciones bancarias online y los pagos en tiempo real permiten a los delincuentes recibir inmediatamente el dinero de sus víctimas. El grupo de pagos ACI Worldwide calcula que en 2023 el 63% de estas estafas fraudulentas se realizaban a través de las redes de pago en tiempo real y que en 2028 esta cifra aumentará hasta el 80%.

En Estados Unidos, si a un consumidor le roban su tarjeta de débito o crédito, la ley federal limita su responsabilidad por cualquier cargo realizado si denuncia el robo con prontitud. Pero las normas para las transacciones fraudulentas entre cuentas son mucho menos claras. Si alguien es víctimas de un pago fraudulento, tiene pocos recursos para recuperar el dinero. Confía en que su banco se lo devuelva, pero los bancos argumentan que esto es el equivalente digital de entregar dinero en efectivo en la calle, y no su responsabilidad.

Un grupo de empresas de pagos como Mastercard, Visa y Early Warning, que gestiona Zelle, así como consultoras como Accenture, han puesto a disposición de los bancos herramientas que clasifican el riesgo de fraude de una transacción, ya sea por el tipo o el volumen del pago, en una fracción de segundo.

Los bancos pueden utilizar las puntuaciones para rechazar determinadas transacciones o justificar por qué aprobaron otras que resultaron ser fraudulentas. Pero los gobiernos y las autoridades financieras quieren más medidas.

Regulaciones

Las autoridades británicas sentaron un precedente al obligar a los bancos a reembolsar a las víctimas de fraudes. En un principio, se fijó un tope de 415.000 libras por reclamación, una cifra que los bancos y las empresas de pagos advirtieron que sería ruinosa. Presionadas por el sector y el Gobierno, las autoridades financieras acabaron rebajando esa cantidad a 85.000 libras. La norma entró en vigor en octubre.

El gobierno australiano va en una dirección diferente. Su objetivo es imponer multas a las redes sociales y a las empresas de telecomunicaciones donde se originan a menudo las estafas, así como a los bancos por no proteger a los consumidores.

En Estados Unidos, la investigación de Zelle por parte de la Oficina de Protección Financiera del Consumidor se consideró el preludio de una posible legislación. Pero se cree que Trump nombrará como director de la Oficina de Protección Financiera del Consumidor a una persona que adopte una postura menos agresiva contra las grandes empresas o que intente abolir el proyecto.

Los bancos alegan que al ampliar la responsabilidad se corre el riesgo de encarecer los servicios bancarios. Según Alison Jiménez, presidenta de Dynamic Securities Analytics, empresa asesora sobre cuestiones de delincuencia financiera, "si un banco reembolsa a un particular, esa pérdida va a redundar en comisiones más altas para los otros clientes".

Los bancos piden a las compañías de telecomunicaciones y a las redes sociales que asuman una mayor responsabilidad. Casi el 80% de los fraudes en los pagos se inician en las redes, según el organismo UK Finance. La banca coopera mucho porque sabe que será responsable de alguna manera si no lo hace. En cambio, muchas redes y empresas de telecomunicaciones no cooperan en absoluto porque no tienen una espada de Damocles sobre ellas.

Bancos, políticos y reguladores argumentan que las empresas de redes sociales no hacen lo suficiente para impedir los fraudes. Hacerlas responsables les daría un incentivo para detectar y eliminar los contenidos fraudulentos.

Antes de las elecciones generales de julio, el Partido Laborista británico había elaborado planes para obligar a las empresas tecnológicas a compartir con los bancos la responsabilidad por las pérdidas derivadas del fraude. Ahora, la ministra de economía Rachel Reeves ha pedido a las empresas de redes sociales y telecomunicaciones que le informen sobre los avances en la prevención del fraude antes de marzo, con la amenaza velada de adoptar nuevas medidas si no actúan.

Multas

Nathaniel Gleicher, director mundial de lucha contra el fraude de Meta, propietaria de Facebook, declaró a *Financial Times* en octubre que la plataforma ya está tomando medidas contra el fraude porque quiere crear una comunidad "segura" para sus usuarios y no ser multada por el organismo regulador británico de medios de comunicación Ofcom. Según la Ley de Seguridad Online de Reino Unido, las empresas de redes sociales están obligadas a retirar los anuncios fraudulentos y se exponen a multas si no lo hacen. Facebook, X y Match Group, propietaria de la aplicación de citas Tinder, son también signatarias del Tratado contra el Fraude en Internet, un acuerdo voluntario elaborado el año pasado entre las empresas tecnológicas y el Gobierno británico para reducir el fraude.

Mientras bancos, políticos y otros debaten quién tiene la responsabilidad, los métodos de los estafadores son cada vez más sofisticados. La inteligencia artificial les permite generar correos electrónicos, anuncios y mensajes más personalizados y cada vez más eficaces para engañar a sus objetivos, afirma Michael Jabbara, ejecutivo del equipo de lucha contra el fraude en los pagos de Visa.

Anna Rowe, fundadora de Catch the Catfish, un grupo de defensa de la seguridad en las citas online, afirma que los *deepfakes* empezaron a aparecer en este campo en 2022 y se han vuelto cada vez más sofisticados: "Los estafadores que intentan seducir a sus víctimas son ahora capaces de hacer video llamadas en las que superponen imágenes de los rostros de otras personas sobre los suyos o incluso ponerse gafas. Están evolucionando muy deprisa".

Reality Defender es una de las cada vez más numerosas empresas que ofrecen a bancos y otras entidades herramientas para detectar *deepfakes* y evitar fraudes. Su consejero delegado Ben Colman asegura que es muy fácil hacer *deepfakes* de audio y vídeo y que su software puede detectar rápidamente audios o vídeos generados por inteligencia artificial que engañan a la mayoría de las personas.

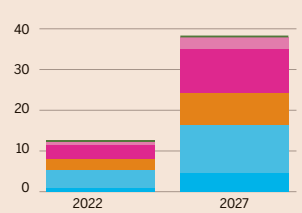
La compañía está financiada por las consultoras Accenture y Booz Allen Hamilton. Por el momento sólo ofrece sus herramientas a grandes entidades como los bancos, pero está trabajando en una versión de su software que podría descargarse de una tienda de aplicaciones, lo que permitiría a cualquiera con un teléfono móvil escanear los mensajes que recibe para ver si son falsos. Pero hasta entonces Colman afirma que el consumidor medio sigue siendo vulnerable a estos fraudes cada vez más sofisticados.

A medida que más personas caigan en estas trampas, los llamamientos a la acción en Estados Unidos aumentarán. "Las cifras son demasiado grandes para ignorarlas. Todo el mundo ha sufrido un fraude o una estafa, bien sea un demócrata o un republicano radical", afirma John Breyault, de la Liga Nacional de Consumidores del país.

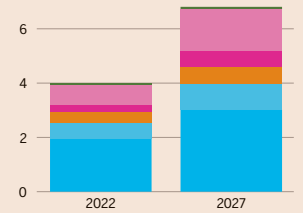
LOS PAGOS INSTANTÁNEOS FACILITAN LOS FRAUDES ONLINE

EEUU · R. Unido · India · Brasil · Australia · Arabia Saudí

Pagos inmediatos
En billones de dólares.



Pagos fraudulentos autorizados
En miles de millones de dólares.



Expansión

Fuente: ACI Worldwide