Así se comportó el dólar esta semana (2024)

Cifras en pesos

Fuente: Investing

El Salmón Reportaje

Criminales están robando la imagen de famosos para estafar a sus víctimas

Nos adentramos en las estafas de las redes sociales para destapar la forma en la que los ciberdelincuentes usan la inteligencia artificial como herramienta de engaño.

Hoy más que nunca debemos desconfiar de lo que encontremos en internet

DIEGO OJEDA

dojeda@elespectador.com
@DiegoOjeda95

El listado es largo: Gustavo Petro, Karol G, Luis Díaz, Shakira, Sebastián Tamayo, Verónica Alcocer... Todos están apareciendo en videos promocionales que circulan en Facebook recomendando los servicios que ofrecen supuestos gurús de las finanzas como Alisson Castillo, Ángela Pérez, Daniela Reyes, entre otros nombres falsos que son usados por ciberciminales.

Para muchos su oferta puede ser tentadora, pues prometen salir de la pobreza con poco más de $200.000. "Hemos creado un programa para ayudar a todos los colombianos que quieren triunfar en la vida. Nuestros clientes se han comprado un carro, han saldado sus deudas, se han comprado una casa y han alcanzado un nuevo nivel de vida. Para participar en este programa solo debes suscribirte al canal de Telegram y escribirnos", dice en uno de los anuncios.

En la investigación que hicimos para este reportaje alcanzamos a identificar por lo menos 10 videos que repiten el mismo patrón: figuras públicas que supuestamente recomiendan los servicios financieros de alguien, la promesa de ser la respuesta a cualquier problema económico, la garantía de que se cuenta con un respaldo institucional (como el Gobierno o el Banco de la República) y el llamado a presionar un botón y suscribirse a un determinado canal de Telegram.

Cada publicación de estas puede tener miles de "me gusta", así como cientos de comentarios de personas que señalan "me interesa", "cómo hago para participar" y "dónde consigo más información". También hay otros que intentan alertar a la comunidad de que estos anuncios en realidad conducen a una estafa, pues no hay que ser experto para notar que en la realización de esos videos se usó inteligencia artificial como herramienta para poner en la boca de famosos palabras que nunca dijeron.

En realidad, la producción se ve torpe. Las palabras no concuerdan con el movimiento de los labios y los gestos que hacen las personas no se ven naturales. Aun así, la manipulación de estos videos (catalogados como *deepfakes*) es suficiente para que muchos caigan en el engaño y, de entrada, señalan un potencial camino de daños en la medida en la que las producciones ganen más nivel técnico.

Nos adentramos en esta estafa con la intención de conocer cómo operan y lo que nos encontramos fue un elaborado esquema para enredar a la gente. —Hola, saludamos a la supuesta experta financiera. —Hola, bendiciones, contesta. —Hoy, si Dios quiere, puedes llegar a ser financieramente independiente y ganar el capital para iniciar tu propio negocio. ¿Te interesa saber más?, añade a su respuesta. —Por supuesto, respondemos.

Cinco minutos después nos envían lo que parece ser un paquete predeterminado de audios en donde intentan brindar toda la información. La voz que se escucha también se siente robótica, pero puede pasar como humana. "Trabajamos en una plataforma en línea en la que ganamos dinero vendiendo divisas y acciones. El tiempo de trabajo es de dos a cuatro horas. Su beneficio es 100 % garantizado y asegurado contra pérdidas".

El intercambio entre el usteo y el tuteo se mantiene a lo largo de la conversación.

—¿Cómo se llama la plataforma?, preguntamos. —La plataforma en la que trabajo es Bitget, contesta, al referenciar un conocido exchange de criptomonedas (probablemente aprovechan su popularidad para intentar impartir confianza en la víctima).

Siguen llegando mensajes. Esta vez las notas de voz nos dicen que "las ganancias están totalmente garantizadas. En tres horas tendrás $15 millones en tu cuenta bancaria. Esta estrategia de inicio es muy simple, compramos divisas a un precio bajo y las vendemos a un precio más alto. Solo necesitas hacer un depósito de $215.000 y entonces empezaré a hacer dinero para nosotros".

¿Ganancias de casi un 7.000 % en tan solo tres horas?, esto por sí solo debería ser una señal de que se trata de un engaño de manual, pero puede que la codicia de muchos, o la desesperación financiera de otros, haga agua la boca de las víctimas, quienes terminan depositando el dinero en la cuenta de Nequi que se referencia más adelante en el chat, la cual, por cierto, está a nombre de una persona diferente al de la supuesta gurú financiera.

La estrategia está tan elaborada, que incluyen a la víctima en un chat grupal, donde fácilmente pueden estar más de 18.000 usuarios. En este se envían mensajes en los que se invita a invertir dinero, acompañados de videos en los que se ve a la inversora dándose lujos viajando por el mundo, luciendo marcas exclusivas y contando grandes cantidades de dinero (como diciendo, esta vida también puede ser tuya).

En estos grupos constantemente envían capturas de pantalla en los que, supuestamente, hay gente agradeciendo por haberles permitido salir de deudas, comprar su casa o darse esos gustos con los que siempre soñaron. Refuerzan el engaño añadiendo comprobantes de pago en Nequi, en donde se ven transferencias que superan los $12, $13, $14 o $15 millones.

Estos comprobantes también fueron revisados y encontramos que son falsos, pues la tipografía no coincide con la original, tampoco el orden de los factores de la información, entre otro tipo de inyecciones digitales que revelan la falsedad del documento. Pero, de nuevo, son retoques mínimos que pueden llegar a pasar como verdaderos ante un ojo desprevenido.

La supuesta estrategia de inversión puede variar entre los grupos de Telegram. Por ejemplo, en la conversación que tuvimos con "Daniela Reyes" se nos explicó un sistema basado en prácticas corruptas. Nos dijo que "ella" conoce árbitros de diferentes deportes, quienes a cambio de dinero le revelan los resultados que tendrán los partidos que están arreglados. Posteriormente se hacen apuestas apuntando a esos marcadores y se recogen los rendimientos. "Las ganancias están garantizadas. ¿Cuánto quieres invertir, cariño?", concluye esa conversación.

Demás está decir que el dinero que supues-

LA PREGUNTA DE LA SEMANA

¿Cuáles son las proyecciones económicas del Gobierno?

Con la presentación del Marco Fiscal de Mediano Plazo, por parte del Ministerio de Hacienda, el Gobierno reveló parte de las proyecciones macroeconómicas que tiene para lo que resta del año.

Por un lado se espera que 2024 cierre con un déficit fiscal de 5,6 %, que es el máximo que le permite la regla fiscal.

Para este año se espera que el Producto Interno Bruto (PIB) consolide un incremento de 1,7 %, lo que se traduce en un alza frente al 1,5 %que se había contemplado en el Plan Financiero, que fue presentado por el Gobierno a comienzos de este año.

Se espera que, en 2025, la economía tenga un crecimiento de 3 %. La cifra se mantendría, con algunas variaciones menores, durante la próxima década, según las estimaciones del Ministerio de Hacienda.

Asimismo, el Gobierno proyecta que el año terminará con 5,3 % de inflación y para 2025 ya deberá estar alrededor en 3 % (que es la meta del Banco de la República). El IPC debería mantenerse en ese nivel hasta 2035 (que es el horizonte que examina el Marco).

En términos de dólar, la proyección indica que la tasa de cambio acabaría en 2024 en $4.142, una mejoría frente a lo que estimaba en el Plan Financiero de principios de este año. Y para 2025 la divisa se ubicaría en $4.218.

Notificar en la tumba

MARC HOFSTETTER

A finales de 2023, cuando había discusiones sobre una licitación para la producción de pasaportes, y en medio de advertencias de la Agencia de Defensa Jurídica del Estado sobre el costo que el propio Estado habría de pagar en el futuro si se seguía una ruta conceptuada como ilegal, el entonces canciller Leyva, en un acto de desprecio por los ciudadanos contribuyentes, anotó que lo notificaran en la tumba cuando llegara esa cuenta de cobro futura por las decisiones que tomaba él ahora.

Algo similar ocurre con las discusiones sobre la reforma pensional. El Gobierno envió un documento al Congreso dando su visto bueno desde el punto de vista fiscal a la reforma. Las cifras de esos cálculos debieran ser conservadoras, pero no lo son. Por ejemplo, la reforma propone que parte de las contribuciones se vayan a un fondo de ahorro que manejaría el Banco de la República. La dosis de optimismo es que sea durante la vida útil del fondo, Hacienda cree que este daría rendimientos muy superiores a los que han dado los fondos de pensiones en años recientes (y que de hecho son altos en el contexto internacional). Para ponerlo en cifras concretas, Hacienda cuenta con que esos rendimientos aportarían a las cuentas casi $200 billones.

Aun imaginando las cuentas con ese color rosa, los estimativos apuntan a que cada año, mientras no agotemos los recursos de ese fondo de ahorro, la reforma costará $3 billones y que, cuando se acabe a la vuelta de unas décadas el ahorro, esa cuenta se acercará a $30 billones por año. La única posible explicación por la cual Hacienda le da el visto bueno fiscal a ese cambio es que se está centrando en el corto plazo, apostando a que $3 billones se pueden acomodar dentro de las maltrechas cuentas del Estado. Pero, ¿y la cuenta de $30 billones por año del futuro?

El proyecto de reforma discutido comete una tremenda injusticia intergeneracional. Nos estamos aprobando unas reglas de juego pensionales caras en el presente e impagables en el futuro, heredándoles a nuestros hijos y nietos una cuenta por pagar inabordable. ¿Cómo puede el Gobierno darle luz verde fiscal a esto? ¿No debería tener en cuenta la totalidad de la senda de gastos prometida y no solo la de corto plazo? Tan claro tiene el Gobierno que esa cuenta no se podrá pagar, que la propia ministra de Trabajo ha aceptado que se requerirá un cambio de reglas a vuelta de unos años.

Gobierno y Congreso tendrían que abordar la parte difícil de la discusión, la que involucra subir la bajísima edad de pensión colombiana, igualar la de hombres y mujeres dejando prendido el bono por hijo para estas últimas y reducir el umbral de cotización a Colpensiones a 1,5 salarios mínimos. Cualquier otra decisión es ponerse a tono con el canciller y decirles a nuestros hijos y nietos que nos notifiquen en la tumba por la fiesta que financiamos, sin preguntarles, con cargo a sus ingresos.

X: @mahofste

» Este tipo de captadoras han logrado recaudar más de $4 billones en el país, de los cuales las autoridades difícilmente han recuperado $1 billón.

tamente se invierte en estos canales se pierde. Los umbrales de ganancia son tan ridículamente elevados, que no hay forma de que ese tipo de "negocios" sean sostenibles. Recuerde que de eso tan bueno no dan tanto.

También es muy probable que los rostros que aparecen en estos perfiles de Telegram, de los supuestos gurús financieros sean robados de cuentas de Instagram o recreados mediante el uso de inteligencias artificiales generativas.

¿Qué es real?

Estafas de este tipo no son noticia en internet. Lo que sí es novedad es el creciente uso de la inteligencia artificial para dar apariencia de legitimidad a los engaños (de allí el nombre de *deepfake*, que podría traducirse como mentira o falsedad profunda), en los que algunos pueden llegar a pensar: si el propio presidente de Colombia me recomienda invertir con una determinada persona, ¿por qué desconfiar?

Para entender las *deepfakes* hay que remontarnos a sus orígenes, en la industria cinematográfica. Inicialmente eran usadas (y lo siguen siendo) para pulir los gestos de los actores o incluir sus rostros en los cuerpos de los dobles de acción mediante una tecnología llamada imagen generada por computadora (CGI, por su sigla en inglés). Esta, por ejemplo, fue la que utilizaron los productores de *Rápidos y furiosos* para incluir a Paul Walker, tras su muerte, en la séptima entrega de la saga. Una tecnología que para entonces era muy costosa, pues llegó a encarecer los costos de producción del filme en unos US$50 millones.

Con el uso de la inteligencia artificial, esta no solo ha ido optimizando los tiempos de producción en las escenas donde se emplea CGI, sino que también ha abaratado sus costos al punto de hacerla más "asequible" para la población en general. Como lo resume Daniel Molina, vicepresidente de iProov para América Latina (empresa que se dedica a la verificación biométrica), "hoy cualquiera puede crear un *deepfake* con lo que cuesta un plato de Crepes & Waffles. Es una locura".

Es más, el desarrollo de estas tecnologías permite que hoy ni siquiera los estafadores tengan que poner la cara, pues pueden manipular la de otros o crear unas propias, mediante el uso de inteligencias artificiales.

Aunque actualmente las aplicaciones para "falsear la realidad" son limitadas (y aun así la gente cae), el desarrollo que pudieran tener a futuro estas herramientas podría llegar a un punto en el que se obtengan resultados extremadamente pulidos que desdibujen cada vez más la línea entre lo real y lo falso en las redes sociales.

Alto grado de impunidad

El problema con estas estafas es que, por funcionar de manera digital, pueden llegar a gozar de un elevado grado de impunidad. El ejemplo más grande es que el video que usa la imagen del presidente Gustavo Petro (que fue alertado por la misma cuenta de Facebook de Presidencia de la República el pasado 29 de mayo) sigue circulando y, potencialmente, defraudando a la gente.

Según el Ministerio de las TIC, con base en el protocolo establecido por el Equipo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert), este video ya fue reportado. "Se solicitó la respectiva validación y suspensión de la publicación, copiando a la Agencia de Ciberseguridad e Infraestructura de Estados Unidos (CISA) para su apoyo con la gestión del caso", precisa. Aun con toda esta institucionalidad, el seudónimo de Alisson Castillo sigue celebrando estafas.

Más allá de la impunidad en la que operan los ciberdelincuentes, llama la atención que las mismas redes sociales funcionan como vehículo para que éstos lleguen a sus víctimas, pues todos los videos identificados en esta investigación se están distribuyendo como contenido patrocinado en Facebook. Es decir, los estafadores le pagan a las empresas, como Meta, para que en esencia publiciten sus amenazas.

Contactamos a Meta, que señaló que las estafas están prohibidas en sus políticas, incluyendo las que se promuevan en anuncios publicitarios. "Este tipo de abuso daña la experiencia de nuestra comunidad, por lo que suprimimos todo contenido cuyo objetivo es engañar o representar de forma engañosa deliberadamente, así como aprovecharse de los demás para conseguir dinero o bienes de cualquier otro modo. Como parte de este compromiso, Meta ha desarrollado herramientas en línea para ayudar a las personas a proteger sus cuentas y reportar abusos", aseguró la compañía.

Evite morder el anzuelo

El gerente de Red Team de NeoSecure by SEK, Feliz Lauzmen, asegura que, por lo general, los estafadores apuntan a uno de dos sentimientos que puede tener la víctima. Por un lado está la codicia, mientras que por el otro está el miedo, en estafas en las que se intimida a la persona a tomar una decisión apresurada para evitar supuestas consecuencias negativas.

Es importante entender que estos delincuentes intentan trabajar con la psicología de los usuarios, por lo que la principal recomendación ante cualquier anuncio, oferta o mensaje de este tipo es desconfiar.

Por su parte, el consultor de ciberseguridad de Control Risks Adalberto José García aconseja no revelar información confidencial a extraños, no hacer clic en enlaces ni descargar imágenes o archivos no solicitados o de desconocidos, así como no enviar dinero o hacer transferencias a alguien de dudosa procedencia en internet.

Si logra identificar uno de estos videos en redes sociales, presione el menú de opciones y denúncielo, ya que así le ayudará al algoritmo a localizar este contenido dañino.

Cifras entregadas a **El Espectador** por el superintendente de Sociedades, Billy Escobar, muestran que las cibercaptadoras están en auge por estos días, las cuales han llegado a recibir dineros del público que superan los $4 billones, de los cuales a duras penas se ha logrado recuperar $1 billón para las víctimas.

Si bien la inteligencia artificial tiene infinidad de usos benéficos, casos como estos nos demuestran que su manipulación también puede ser malintencionada. Hoy más que nunca debemos interactuar con extrema cautela en internet, como lo demuestran este tipo de estafas.