14/01/2026

Fraudes financieros: no cojas su llamada o perderás todos tus ahorros

Millones de personas desprevenidas de todo el mundo son estafadas a través de grupos de chat con falsos consejos financieros. detrás están organizaciones criminales que, ubicadas a miles de kilómetros, secuestran, torturan y esclavizan a sus ’peones



Todo comienza con un anuncio de apariencia inofensiva en Facebook. «Consejos gratuitos sobre acciones vía WhatsApp» lee Mia en su móvil. Encima aparece el logo de un popular neobroker. La publicidad le llama la atención. Mia (nombre falso) ya había pensado en dedicar más atención a sus inversiones financieras. Hace clic y aterriza en un grupo de WhatsApp dedicado a inversiones. Mia, de 42 años, es empleada en una tienda.

Un viernes, una mujer llamada Laura la contacta por WhatsApp. Se presenta como asistente de un renombrado gestor de fondos de cobertura. Ella y alguien a quien llama 'el profesor', dice, trabajan para una institución financiera estadounidense muy conocida.

Mia busca en Google, todo parece serio. El profesor existe, la institución financiera también. Se deja engatusar por la amable asistente y aguarda los consejos del profesor para invertir en acciones. Al chatear surge cercanía personal. «Buenos días –escribe Laura–. Necesito café urgentemente, si no se me van a cerrar los ojos». Ambas mujeres charlan sobre el día a día de Mia, sus preocupaciones, el deseo de ganar dinero...

Pronto llegan los primeros consejos de inversión. Mia descarga en su teléfono una app que Laura le ha recomendado llamada STLSTE. Invierte, al principio, unos pocos miles de euros; luego, cada vez más. En la pantalla, las ganancias mostradas se disparan.

Todo es maravilloso hasta que Mia quiere transferir sus ganancias de ensueño a su cuenta y Laura le exige otro pago. Es el momento en que Mia se da cuenta de que algo no está bien: ha caído en una estafa financiera. En realidad, el proveedor de servicios estadounidense no gestiona ningún grupo de WhatsApp para sus clientes privados. El profesor no tiene nada que ver con la estafa. En ningún momento, Mia ha comerciado con acciones, sino que solo ha transferido dinero a estafadores: unos 20.000 euros.

Ella es apenas una de varias decenas de miles de víctimas anuales de una maquinaria global de fraude que se embolsa muchos miles de millones. Solo en 2024 los estafadores en línea, los llamados scammers, se apoderaron de más de un billón de dólares en todo el mundo, según calcula la ONG Global Anti-Scam Alliance.

¿Cómo funciona el fraude?

1. **Contacto en aplicaciones:** Los estafadores contactan a las víctimas a través de Facebook, Instagram, WhatsApp y Telegram, prometiendo altos retornos en inversiones.
2. **Grupos de Whatsapp:** Si las víctimas muestran interés, los estafadores las añaden a grupos de WhatsApp con nombres similares a instituciones financieras conocidas.
3. **Instalar 'apps' fraudulentas:** Estos grupos tienen miembros falsos que comparten historias de éxito también falsas. Los estafadores piden instalar apps fraudulentas.
4. **IBAN extranjero:** En estas plataformas falsas se registran los afectados, que transfieren dinero a una falsa cuenta comercial con un IBAN extranjero.
5. **El dinero nunca se invierte:** El dinero fluye a través de canales encubiertos hacia los estafadores sin haber sido invertido nunca.
6. **Retorno ficticios:** Los timadores muestran a la víctima retornos ficticios. El estafador envía capturas de pantalla mostrando crecimientos de saldo en pocas horas.
7. **Altas comisiones:** Cuando las víctimas intentan retirar su dinero, el estafador les pide pagar impuestos, comisiones... para sacarles aún más dinero.
8. **Desaparecen sin previo aviso:** Una vez que el estafador cree que ha extraído todo el dinero posible, cortan toda comunicación y desaparecen, dejando a la víctima sin recursos.

La revista alemana Der Spiegel siguió el rastro del dinero robado e investigó plataformas dudosas y conexiones de cuentas. El equipo de investigación se topó con una red ramificada y con un centro del fraude situado en Birmania, donde batallones de scammers se sientan frente a smartphones y ordenadores con una misión: contactar con usuarios de Internet por todo el planeta y extraerles todo el dinero que puedan. Muchos de estos peones trabajan frecuentemente bajo coacción. Son también víctimas, ya que detrás de las fábricas de estafas a menudo está el crimen organizado chino. Según Naciones Unidas, estas redes criminales han secuestrado a cientos de miles de personas en el sudeste asiático para que trabajen como 'esclavos' en estas fábricas ilegales. Es decir, hacen lo que sea necesario para mantener el negocio en marcha.

Una oferta difícil de rechazar

Phelipe de Moura Ferreira, de 27 años, fue forzado a la criminalidad. Durante tres meses trabajó en un edificio de oficinas azul junto a un río fronterizo con Tailandia. Conversaba en inglés por WhatsApp con personas de todo el mundo. Con ayuda de un software de traducción y de ChatGPT, su 'oficina' se dirigía a víctimas de Francia, Ucrania, Alemania... Les quitaba mucho dinero, pero lo hacía contra su propia voluntad. Estaba secuestrado.

Natural de São Paulo (Brasil), y de circunstancias humildes, en noviembre de 2024 Ferreira recibió a través de Telegram una oferta de trabajo como empleado de un call center en Tailandia. Horarios flexibles, dos mil dólares al mes, un billete de avión... Sonaba tentador.

Cuando aterrizó en Bangkok, recuerda, vino a buscarlo un conductor armado que, lejos de llevarlo a la sede de una empresa de call center, lo condujo a través de la frontera hacia una Birmania destrozada por la guerra civil. Allí, en un terreno amurallado al sur de la ciudad de Myawaddy, le quitaron el pasaporte y el móvil para ser recluido en una especie de prisión. «Teníamos que dormir ocho personas en una habitación pequeña, fría y sucia. En el exterior había guardias», rememora.

Debía realizar estafas para sus 'jefes', así los llama. Era un lugar con oficinas de espacio abierto, cada una especializada en un tipo diferente de fraude financiero. En el departamento de Ferreira, que estima en varios cientos de personas, trabajaban expertos en los denominados love scams. Primero despertaban esperanzas de relaciones románticas en sus víctimas, para luego convencerlas

de que les entregaran altas sumas de dinero. En la oficina de al lado hacían comercio de criptomonedas.

Quien se negaba a trabajar en la fábrica de estafas o no tenía éxito era castigado, revela Ferreira. Con descargas eléctricas, con latigazos... Cuando un compañero de cautiverio intentó contactar con su familia en línea, fue descubierto. «Lo encerraron durante días en una habitación oscura y lo golpearon una y otra vez», describe.

A pesar de las intimidaciones, Ferreira corrió el riesgo de contactar a su padre a través de Facebook: «Escribí que necesitaba ayuda. Que no estaba en Tailandia, sino retenido en Birmania. Que aquí no hacemos trabajo legal y que nos castigan cada día».

El padre contactó con la Policía brasileña, que lo puso en contacto con The Exodus Road, una ONG que actúa contra la trata de personas. «Proporcionamos a las fuerzas de seguridad locales toda la información disponible sobre Ferreira para posibilitar su liberación», dice Cintia Meirelles de Azevedo, directora para Brasil de la organización. Hubo negociaciones con los operadores de la fábrica de estafas, supuestamente relacionados con la mafia china. De Azevedo confirma que Ferreira fue retenido en el complejo y forzado a las estafas.

Gracias a esa operación, fueron liberados más de 300 prisioneros, incluido Ferreira, que regresó a São Paulo, donde vive con sus dos hermanos y sus padres. «Birmania fue mi infierno», sentencia.

No está claro, sin embargo, que las autoridades hayan desarticulado la red criminal para la que Ferreira fue forzado a trabajar. Cuando una fábrica cierra en algún lugar, suele surgir en otra una nueva.

Un negocio redondo

Las ofertas de captación de los scammers aterrizan a menudo en plataformas como Facebook o Instagram. Los anuncios fraudulentos habrían «aumentado considerablemente» en los canales de redes sociales del consorcio Meta desde principios de 2025, informa el banco Trade Republic. Según sus propias declaraciones, el proveedor de servicios financieros reporta mensualmente entre diez mil y veinte mil nuncios fraudulentos a la empresa matriz de Facebook.

Meta no quiso responder a las preguntas de los periodistas. Un portavoz subraya que la compañía elimina todos los anuncios fraudulentos con ayuda de «tecnologías avanzadas y equipos de revisión capacitados» tan pronto como estos son descubiertos.

Con los anuncios publicitarios fraudulentos, Meta ganó el año pasado unos 16.000 millones de dólares. Así lo sugiere, al menos, una evaluación de documentos internos por parte de la agencia de noticias Reuters.

Pero el verdadero corazón de la estafa son las plataformas comerciales falsificadas: sitios web y apps que parecen tan profesionales que no todos reconocen el engaño de inmediato. Aquí no se realiza ningún comercio bursátil real, los saldos de cuentas y las ganancias los escriben los propios timadores.

Las autoridades registran en la actualidad una auténtica inundación de plataformas falsas en internet. Además, el uso de inteligencia artificial permite generar nuevas plataformas de fraude con poco esfuerzo, como en una cadena de montaje, lo que permite a los estafadores alcanzar a cada vez más víctimas potenciales.

La artimaña funciona así: los estafadores compran apps legítimas que ya están publicadas en Google Play Store y que originalmente ofrecían contenidos diferentes. Por ejemplo, la aplicación de timo STLSTE fue antes dos apps de música. Los estafadores cambiaron el logo, el nombre y todo el contenido para convertirlas en plataformas de estafa.

¿Por qué hacen esto? Porque estas aplicaciones ya tienen el visto bueno de Google. Al comprar una app legítima, evitan el proceso de verificación y parecen más confiables ante las víctimas. Siguiendo las huellas digitales de la estafa de STLSTE, los investigadores descubrieron una red de al menos 26 plataformas y apps fraudulentas conectadas entre sí. Muchas utilizaban herramientas de desarrollo y almacenamiento en la nube procedentes de China.

En la lucha contra estas redes delictivas, las autoridades tienen sus límites. Cuando se denuncia una app fraudulenta, Google tarda semanas en eliminarla de la Play Store. Y, cuando finalmente actúa, parece que lo hace a medias. En el caso de la red STLSTE, Google no eliminó todas las apps relacionadas de inmediato. Varias permanecieron disponibles para su descarga a pesar de las

pruebas evidentes: tenían los mismos nombres de desarrollador y direcciones de correo electrónico idénticas. Mientras tanto, los estafadores siguen operando y captando nuevas víctimas.

Google asegura «actuar de forma consecuente contra aplicaciones que infringen nuestras directrices», informa por escrito. La compañía habría bloqueado solo en 2024 la publicación de 2,36 millones de apps debido a infracciones y cerrado más de 158.000 cuentas de desarrolladores maliciosos. Además, a partir de 2026, todas las apps de Android deberán ser registradas por desarrolladores verificados.

Es una carrera entre las autoridades que investigan, cuyos medios son limitados, y estafadores bien organizados que siempre desarrollan nuevos métodos. Pero la pregunta decisiva permanece: ¿dónde acaba al final el dinero robado?

Mia, la víctima, revela que solo las pérdidas sufridas por los miembros de su grupo de chat ascienden a varios millones de euros. Si detrás de su caso están scammers de una de las fábricas del sudeste asiático, no se sabe. Como casi siempre, las autoridades no han podido identificar a ningún perpetrador. Pero esta vez han dejado huellas. El dinero de Mia no aterrizó en una cartera de criptomonedas anónima, sino en una cuenta bancaria, con IBAN y nombre.

Una madeja internacional

Der Spiegel obtuvo justificantes de transferencias de varios perjudicados en la misma estafa. Muchos están supuestamente dirigidos a Easy Payment & Finance, una institución financiera con sede en Madrid que ofrece a clientes empresariales «servicios bancarios de marca blanca»; es decir, pone a su disposición su infraestructura bancaria. A los perjudicados se les hizo creer que con el registro de la app abrirían una «cuenta comercial» en dicha entidad. Los scammers promocionaban a Easy Payment & Finance como socio. La institución financiera no respondió a las preguntas de los reporteros. El Banco de España explica que Easy Payment & Finance es una «institución de pago debidamente autorizada y registrada». Sin embargo, no quiso pronunciarse más sobre casos individuales.

El rastro del dinero se pierde en una maraña de proveedores, cuentas virtuales y leyes internacionales. Para las víctimas, al final, apenas hay respuestas, ninguna justicia. Mia se ha dirigido a la supervisión bancaria española, incluso ha contactado con Interpol. Pero su dinero sigue desaparecido. Exactamente igual que Laura, la amable asistente.

Fuente: https://www.abc.es/

LINK DE LA NOTICIA