# Desarticulada una organización criminal internacional que defraudó más de 5.000.000 de euros a través de una sofisticada ciberestafa

*Actualidad España | 11-02-2023 | 14:33*


**Policia Nacional**

Agentes de la Policía Nacional, en una operación conjunta con el Servicio Secreto de EEUU, han desarticulado una organización criminal internacional asentada en Madrid especializada en la comisión de estafas online. Hay ocho personas detenidas en España y una en Miami (EEUU), de diferentes nacionalidades, presuntamente dedicadas a estafar a empresas y ciudadanos americanos. El entramado abrió más de 100 cuentas bancarias en España en las que, en menos de un año, recibieron cerca de 5.000.000 de euros de las víctimas. La investigación ha contado con el apoyo de EUROJUST, que ha sido determinante para que las autoridades policiales y judiciales de EEUU, Panamá y España trabajaran de forma conjunta. Los agentes han incautado objetos de gran valor, entre los que se encuentran relojes de alta gama tasados en 200.000 euros, y han congelado activos por más de medio millón de euros.

La investigación se inició a raíz de una denuncia presentada por un procesador de tarjetas debido a la utilización fraudulenta de dos de sus tarjetas, pertenecientes a un ciudadano estadounidense, en un lujoso establecimiento comercial de Madrid. La compra se realizó online, si bien la recogida se efectuó en el local, reclamando el titular de la tarjeta transacciones por un importe de más de 20.000 euros.

Realizadas las primeras gestiones, los agentes de la Unidad Central de Ciberdelincuencia identificaron una metodología delictiva compleja que se extendía a distintos países y múltiples víctimas y que, además, había generado millones de euros de fraude.

Mediante técnicas de ingeniería social, phishing y smishing robaban datos sensibles

Las pesquisas acreditaron que, en una primera fase, los investigados utilizaban técnicas de ingeniería social, phishing y smishing para recabar datos sensibles de víctimas potenciales ?personas físicas y empresas norteamericanas- relacionados con sus activos financieros.

Posteriormente, las telefoneaban (vishing) enmascarando las llamadas (spoofing) para obtener el resto de información necesaria para materializar las estafas mediante compras a través de internet, o realizando transferencias desde las cuentas de las víctimas a otras controladas por la

organización desde España. En ocasiones incluso se llegaron a detectar llamadas a tres, de forma que el estafador interactuaba simultáneamente con la víctima y con su entidad financiera norteamericana para aportar los códigos de verificación y autorización de las transacciones que necesitaba para ejecutar las operaciones.

Con el avance de la investigación, los agentes identificaron al líder, y principal investigado, de la organización criminal. Se trataba de un ciudadano nicaragüense, sin arraigo en España y recién llegado a nuestro país desde Panamá, con un elevado nivel de vida.

Crearon más de 100 cuentas bancarias en las que recibieron 5.000.000 de euros de las víctimas en menos de un año

En las cuentas bancarias controladas por los investigados -que han resultado ser más de 100- recibieron cerca de 5.000.000 de euros en menos de un año; si bien, fruto de la cooperación policial internacional, existen indicios que apuntan a que esas cifras pueden ser mayores (más de 200 empresas y personas estafadas y un fraude que superaría los 7.000.000 de euros). Una vez que el dinero entraba en sus cuentas, lo extraían en cajeros automáticos, lo enviaban al extranjero mediante nuevas transferencias, o bien lo convertían en criptoactivos.

El principal investigado, que hacía uso de numerosa documentación falsa para actuar con mayor impunidad, era quien controlaba de forma directa las cuentas bancarias abiertas en España. Sin embargo, él no era titular de las mismas, ya que las abría a nombre de terceras personas; unas trabajaban directamente con él, y a otras las captaba (para abrir cuentas online) normalmente entre personas con bajos recursos o indigentes.

Gran movilidad geográfica y alto nivel de vida de sus miembros

En las cuentas bancarias abiertas en nuestro país recibían los fondos fraudulentos que les permitían llevar un alto nivel de vida. En este sentido, alquilaban vehículos de alta gama, así como hoteles y viviendas en zonas residenciales exclusivas por todo el territorio nacional.

Los agentes acreditaron una gran movilidad geográfica de los miembros de la organización. Detectaron numerosos viajes por parte de la pareja del principal investigado y sus familiares desde EEUU hasta distintas ciudades españolas -Madrid, Barcelona, Mallorca, Ibiza y Málaga- con el fin de realizar un ?turismo comercial?. Asimismo, observaron que viajaban por las principales capitales europeas -como Ámsterdam, París o Londres- donde adquirían productos de moda y joyería de gran valor y abrían cuentas bancarias.

Investigación conjunta con el Servicio Secreto de EEUU apoyada por EUROJUST

La investigación -que ha sido llevada a cabo por expertos en la lucha contra la ciberdelincencia de la Policía Nacional junto al Servicio Secreto de Estados Unidos a través de la Oficina de Enlace de la Embajada de EEUU en Madrid- ha permitido identificar a las víctimas en EEUU y relacionarlas con las actividades delictivas realizadas desde España.

Además, el apoyo de EUROJUST ha sido determinante para que las autoridades policiales y judiciales de EEUU, Panamá y España trabajaran de forma conjunta y se pudieran realizar registros simultáneos en Miami y Madrid.

La operación ha permitido la completa desarticulación de la organización criminal, con la

detención de todos sus miembros ?ocho en Madrid y uno en Miami- y la incautación de numerosos objetos de cuantioso valor. Por otra parte, los agentes también han bloqueado 74 cuentas bancarias, congelando activos por más de 500.000 euros. En el domicilio registrado localizaron una zona donde almacenaban la mercancía adquirida de forma fraudulenta o a través de los fondos provenientes de las estafas, de tal forma que parecía una tienda de artículos de lujo.

Fruto de los registros realizados, los agentes han intervenido 9 relojes de alta gama -algunos de ellos tasados por las marcadas en cerca de 200.000 euros-, numerosas joyas, 44 teléfonos móviles, 4 ordenadores portátiles y 3 de sobremesa, 3 tablets y 3 monitores. Además, también localizaron sacos de ropa y zapatillas de distintas marcas de lujo, abundante documentación y tarjetas bancarias, una pistola de aire comprimido y 8 pasaportes y documentos de identidad falsos.

#UnoDeCadaCincoDelitos: la campaña del Ministerio del Interior contra la ciberdelincuencia

Esta misma semana el Ministerio del Interior ha puesto en marcha una campaña para hacer frente al incremento de la cibercriminalidad registrada en España. Hoy, uno de cada cinco delitos en España se comete en la red.

En 2022 se produjeron un total 375.506 ciberdelitos, un 72% más que los registrados en 2019, incremento que se eleva hasta el 352% si la comparación se realiza respecto a 2015.

El objetivo de esta campaña es la concienciación y sensibilización ciudadana sobre los tipos de ciberdelitos más comunes, apelando a la necesidad de autoprotección, generar una predisposición a denunciar, e incrementar la confianza ciudadana en las Fuerzas y Cuerpos de Seguridad del Estado como primer instrumento público de lucha contra la cibercriminalidad. Para ello, se ha creado la siguiente página web https://unodecadacincodelitos.com/

Consejos de la Policía Nacional para no ser víctima de los ciberdelincuentes:

Comprobar el emisor de los mensajes o llamadas recibidas. Existen foros donde se puede consultar si existen estafas relacionadas con los números de teléfono que están intentando ponerse en contacto con nosotros.

No aportar datos personales sin cerciorarse de que se trata de la entidad en cuestión. Nuestra entidad bancaria, compañía telefónica o empresa de suministros ya dispone de estos datos, por tanto, nunca nos los va a pedir.

No facilitar nunca información de tarjetas, documentos de identidad, declaración de la renta, nóminas, nombres de usuario, claves y contraseñas.

No aceptar, en ningún caso, las condiciones que ofrezcan en una misma llamada o comunicación. Solicitar que nos remitan la documentación para su estudio o emplazar a que nos realicen una segunda llamada para que podamos hacer comprobaciones.

No clicar en los enlaces de los mensajes de texto que nos envíen y, en el caso de las cuentas bancarias, acceder siempre a través de la aplicación que nos facilitan las entidades financieras, compañías telefónicas o empresas de suministro.

Desconfiar si el interlocutor nos pone continuamente en espera, cada vez que le aportamos un dato que previamente nos ha solicitado, porque puede estar realizando una ?llamada a tres? para autorizar una transferencia de fondos en ese mismo momento.

Autor: Redacción