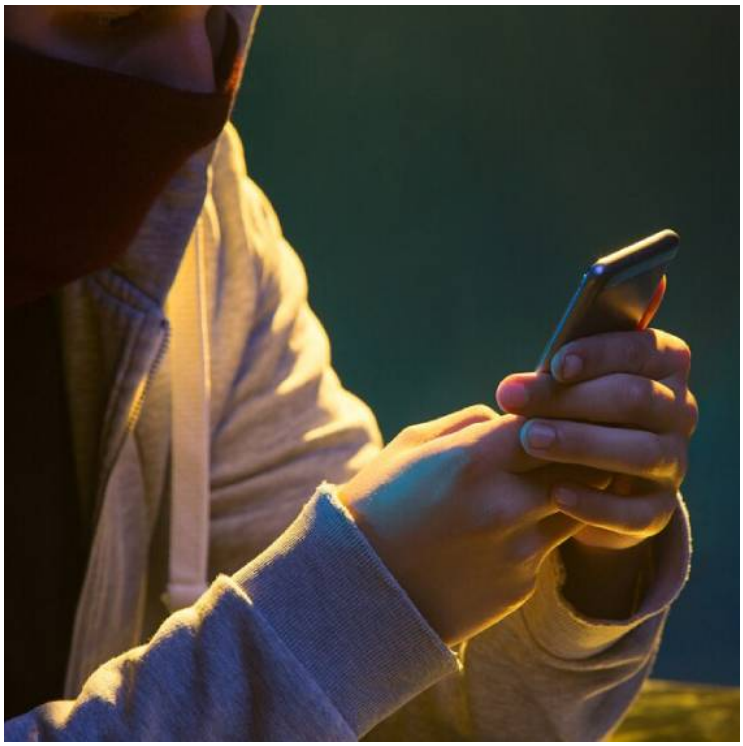
18/12/2024

Desmantelada la organización criminal que estafó más de 3 millones de euros mediante fraude telefónico

Se han llevado a cabo 29 registros simultáneos en Perú y España en los que se ha intervenido dinero, teléfonos móviles, dispositivos informáticos y documentación relativa a estas estafas



Agentes de la Policía Nacional, junto con la Policía Nacional del Perú, con la colaboración de la Agregaduría de Interior en ese país, han desmantelado la infraestructura tecnológica de una organización criminal que defraudó más de 3.000.000 de euros mediante vishing, una estafa que consiste en, a través de una llamada, suplantar la identidad de la víctima con el fin de obtener información personal y sensible de esta.

Se ha detenido a un total de 83 personas, entre las que se encuentra el líder de la organización, 35 en diferentes puntos de España -Madrid, Vigo, Barcelona, Mallorca y Salamanca- y a 48 en Perú. Se han llevado a cabo 29 entradas y registros en ambos países de manera simultánea, en las que se han intervenido dinero, teléfonos móviles, dispositivos informáticos y abundante documentación relativa a estas estafas.

La investigación se inició en agosto de 2022 al tener conocimiento de que podría existir un grupo criminal dedicado a cometer estafas mediante el procedimiento de vishing. Avanzadas las pesquisas, comprobaron que existía una estructura piramidal formada por personas de máxima confianza -familiares y amigos íntimos- con un claro reparto de funciones. En Perú se encontraba el líder de la organización, que tenía bajo su mando a tres personas que controlaban cada uno de los centros de llamadas. Estos contaban con carteles de frases motivacionales para animar a los empleados, llegando a celebrar las primeras estafas de los trabajadores de reciente incorporación. En el eslabón inferior estaban los trabajadores que se encargaban de realizar las llamadas a las potenciales víctimas estando en inmediata colaboración con los que operaban en España.

Modus operandi

Esta estafa conocida como vishing, consistía en realizar llamadas de manera masiva obteniendo la información de bases de datos y siguiendo un guión establecido para ganarse la confianza de las víctimas. Utilizando técnicas de ingeniería social, conseguían enmascarar el número de teléfono -spoofing- desde el que realizaban la llamada, logrando así que en la pantalla de los afectados apareciera el nombre y el número oficial de atención al cliente de su entidad bancaria, dando más realismo a la estafa. Todo ello lo realizaban desde los tres centros de llamadas donde trabajan unas 50 personas de manera simultánea realizando miles de llamadas diarias.

Los estafadores seguían un guion durante sus llamadas, con el que conseguían que las víctimas cayeran en la trampa. Se presentaban alegando que eran del Departamento de Prevención y Fraude, «El motivo de mi llamada informativa es porque nos ha saltado una alerta de seguridad. Verificamos que en estos momentos hay un retiro pendiente de 280 euros a través de la operativa efectivo móvil». Una vez captada la atención del cliente les explicaban que, «Es muy probable que esta persona haya vulnerado sus datos y este teniendo acceso a su cuenta en estos momentos, de igual manera vamos a proceder a elevar un atestado policial a nombre de esta persona para que se puedan hacer las investigaciones pertinentes». Posteriormente la persona que realizaba la llamada le preguntaba al estafado sobre el posible origen del «fraude», dando varias opciones al cliente, «¿Perdió o prestó su tarjeta?», «¿Compartió datos bancarios? ¿O algún familiar tiene acceso a su app?», «¿Le ha llegado un mensaje de actualización por una app que no recuerda haber instalado?» y «¿Suele responder llamadas con contenido vacío? Llamadas que cuando contesta cuelgan o dejan en espera». Una vez la víctima del fraude les daba una respuesta los estafadores le informaban de que con su autorización realizarán un atestado policial para que se hagan las investigaciones correspondientes.

Una vez les hacían creer que tenían un cargo fraudulento y que su cuenta estaba bloqueada, les indicaban los pasos a seguir en la aplicación de su banco -utilizando para ello los manuales de usuario que les facilitaban los líderes de la organización- simulando que el código que recibirían en sus teléfonos móviles les permitiría desbloquear su cuenta. El engaño finaliza una vez que ese código era facilitado por la víctima a su interlocutor quien, de manera inmediata, lo enviaba a los otros miembros de la organización ubicados en España. Estos se encontraban en modo alerta en calles en las que se existían sucursales de entidades bancarias próximas para la retirada de efectivo del cajero utilizando dicho código. Una vez tenían el dinero en su poder, se apropiaban de un porcentaje que oscilaba entre el 20 y el 30%, transfiriendo el resto a la organización en Perú por medio de empresas dedicadas al envío de efectivo a otros países.

Claves para comunicarse

Los empleados de España se repartían por diferentes ciudades para dificultar así cualquier investigación policial posterior. De esta forma, utilizaban claves secretas con sus compañeros de los centros de llamadas para informarles de las entidades que tenían a la vista mediante unos códigos de colores en función de las sucursales en cuestión.

Una vez los investigadores lograron identificar a los miembros de esta organización, con la colaboración de la Agregaduría de Interior en Perú, establecieron un dispositivo policial formado por más de un centenar de agentes para la localización de todos ellos. De esta forma, se realizaron 29 entradas simultáneas en España y en Perú, logrando la detención de 83 personas como presuntos responsables de los delitos de estafa agravada, blanqueo de capitales y pertenencia a organización criminal. Durante el operativo en Perú, que contó con la presencia de agentes de la Policía Nacional española, se desmantelaron tres call center desde los que operaba la organización, descubriendo in fraganti como operaban 50 trabajadores de la estructura criminal.

Además se ha intervenido dinero, teléfonos móviles, dispositivos informáticos, así como documentación relativa a estas estafas. Actualmente la investigación continúa abierta puesto que no se descartan nuevas detenciones o la aparición de más víctimas.

La Policía Nacional aconseja

No aportar nunca datos personales ni bancarios sin cerciorarse de que se trata de la empresa o la entidad en cuestión. Además, nuestra entidad bancaria ya dispone de estos datos, por tanto, nunca nos los van a pedir.

Recordar que ninguna empresa privada o institución pública utiliza este método para solicitar datos personales a sus clientes.

No facilitar nunca información de tarjetas, documentos de identidad, nombres de usuarios, códigos y contraseñas.

Ante cualquier duda sobre si la identidad del interlocutor es realmente la de nuestra entidad bancaria, cortar inmediatamente la comunicación y llamar al teléfono de atención al cliente que podemos encontrar tanto en las páginas oficiales como en la propia aplicación.

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

LINK DE LA NOTICIA