PANORAMA | Tribunales/Seguridad

Así engañaban a mayores de 65 años haciéndose pasar por empleados de seguridad bancaria

El comunicado policial no especifica que entre las víctimas o los detenidos haya residentes en Córdoba o en la Subbética; la operación, en diferentes puntos de España, ha permitido esclarecer 134 hechos delictivos y un fraude superior a 1.140.000 euros

Redacción/Priego Digital
Jueves 12 de noviembre de 2026 - 22:10



La Policía Nacional ha detenido a 43 personas por su presunta participación en una organización criminal dedicada a estafar a clientes de entidades bancarias, principalmente personas mayores de 65 años, mediante el envío de mensajes SMS y llamadas telefónicas en las que se hacían pasar por empleados de los departamentos de seguridad de sus bancos. La operación, desarrollada en diferentes puntos de España, ha permitido esclarecer 134 hechos delictivos y un fraude superior a 1.140.000 euros, según ha informado la Dirección General de la Policía.

Además de los 43 detenidos, otras 13 personas han prestado declaración en calidad de investigadas sin ser arrestadas, mientras que el conjunto de la investigación alcanza a 95 personas investigadas o presuntamente implicadas. A los detenidos se les atribuyen delitos de pertenencia a grupo criminal, estafa y blanqueo de capitales.

Mensajes que simulaban proceder del banco

El procedimiento comenzaba con el envío masivo de mensajes SMS a clientes de diferentes entidades financieras, previamente seleccionados por los presuntos estafadores. En estos mensajes se advertía de una supuesta operación fraudulenta que se estaba realizando en la cuenta bancaria y se facilitaba un número de teléfono o una dirección web para resolver la incidencia. Una de las claves del engaño era que los mensajes podían aparecer dentro de la misma conversación de SMS utilizada habitualmente por el banco, lo que aumentaba su credibilidad. Para conseguirlo, manipulaban la identificación del remitente, una técnica conocida como SMS spoofing, que permite suplantar la apariencia de un emisor legítimo.

Cuando las víctimas llamaban al número indicado o accedían a la dirección facilitada, entraban en contacto con personas que simulaban trabajar para los servicios de seguridad de su entidad. Los falsos empleados les convencían de que su dinero estaba en peligro y de que debían realizar transferencias o ingresos en otras cuentas para protegerlo. En realidad, el dinero terminaba en cuentas controladas por la organización.

Más de 45.000 euros sustraídos a una sola víctima

Los investigadores han comprobado que los presuntos estafadores disponían de información sobre determinados clientes bancarios, lo que les permitía seleccionar a personas especialmente vulnerables. La Policía señala que la mayoría de las víctimas eran mayores de 65 años, aunque no ha precisado si todas

pertenecían a ese grupo de edad. En algunos casos, los integrantes de la organización llegaron a conocer los límites de las cuentas bancarias para adaptar las transferencias a las cantidades disponibles. La investigación ha documentado situaciones en las que una sola víctima perdió más de 45.000 euros. Los presuntos estafadores también solicitaban claves bancarias o convencían a sus víctimas para compartir la pantalla del teléfono móvil, consiguiendo así información que les permitía acceder a las aplicaciones financieras.

Entre las técnicas detectadas figura una modalidad de fraude conocida como relay attack, basada en el uso de la tecnología NFC, que permite realizar pagos sin contacto. En estos casos, contactaban telefónicamente con la víctima y la convencían para instalar una aplicación falsa en su teléfono, haciéndole creer que se trataba de una herramienta oficial del banco.

Utilizaban el teléfono móvil para copiar operaciones con tarjetas bancarias

Posteriormente, le pedían acercar su tarjeta bancaria al móvil para realizar una supuesta comprobación de seguridad. La aplicación fraudulenta permitía retransmitir la comunicación de la tarjeta a otro dispositivo controlado por los presuntos estafadores, que podían utilizarla para realizar operaciones como si dispusieran físicamente de ella. La Policía Nacional advierte de que este procedimiento representa una modalidad especialmente elaborada de fraude bancario, al combinar la suplantación de identidad con herramientas tecnológicas.

Una organización con funciones repartidas

La investigación comenzó hace aproximadamente un año, después de que los agentes detectaran la existencia de grupos de mensajería privada utilizados para organizar campañas de estafas. Los integrantes de la red se distribuían diferentes funciones, desde la obtención de bases de datos de clientes hasta el contacto telefónico con las víctimas y el movimiento del dinero obtenido. Algunos se encargaban de enviar los mensajes fraudulentos y otros asumían el papel de falsos empleados bancarios. También participaban personas conocidas como mulas bancarias, que facilitaban cuentas para recibir el dinero procedente de las estafas. Según la Policía, la organización captaba para esta función a jóvenes a través de redes sociales e incluso a personas sin hogar. Posteriormente, otros integrantes retiraban el dinero en cajeros automáticos, lo transferían a nuevas cuentas o lo convertían en criptomonedas para dificultar su seguimiento.

Amenazas para evitar que las víctimas denunciaran

Los investigadores han detectado que algunos miembros de la organización llegaron a intimidar a las víctimas cuando estas descubrieron que habían sido estafadas. Para ello, enviaban mensajes amenazantes en los que incluían datos personales e incluso las direcciones de sus domicilios. El objetivo era generar miedo y evitar que acudieran a denunciar los hechos. La Policía considera que esta forma de actuar, junto con la utilización de identidades ficticias y canales privados de comunicación, revela una estructura organizada con conocimientos informáticos especializados.

Tres registros en Madrid y Cádiz

La operación policial se desarrolló en tres fases y culminó durante el pasado mes de octubre con tres registros, dos en Madrid y uno en Cádiz. Los investigadores analizaron alrededor de 400 canales y grupos de una aplicación de mensajería privada, recopilaron información sobre 300 identidades y consiguieron identificar plenamente a un centenar de personas. La investigación permanece abierta y la Policía Nacional no descarta nuevas detenciones. Por el momento, el comunicado policial no especifica que entre las víctimas o los detenidos haya personas residentes en Córdoba o en la Subbética.

Cómo evitar este tipo de estafas

La operación vuelve a poner el foco en los fraudes que utilizan la apariencia de comunicaciones bancarias auténticas para conseguir dinero o datos personales. Ante un mensaje que advierta de una supuesta operación sospechosa, conviene no llamar al teléfono ni acceder a los enlaces incluidos en el SMS, y contactar directamente con el banco a través de su aplicación oficial o de un número de teléfono comprobado. Tampoco deben facilitarse contraseñas, claves de acceso ni códigos de verificación, ni instalar aplicaciones

ni acercar tarjetas bancarias al teléfono siguiendo instrucciones de una persona que llama inesperadamente, ni realizar transferencias a supuestas cuentas de seguridad.

En caso de sospechar que se ha producido una estafa, es importante contactar inmediatamente con la entidad bancaria para intentar bloquear las operaciones y presentar la correspondiente denuncia. La Policía recuerda que un mensaje aparentemente enviado desde el número habitual del banco no garantiza que sea auténtico, ya que pueden manipular la identificación del remitente.