# Nota informativa

## La policía nacional alerta de una nueva modalidad de fraude bancario mediante SMS y llamadas telefónicas

**En caso de duda sobre la autenticidad de la llamada recibida hay que colgar y llamar directamente al número de contacto del banco**

Madrid, 27 de agosto de 2021. Agentes de la Policía Nacional han detectado una elaborada modalidad de fraude bancario en la que se combina el uso de SMS falsos –que simulan enviados por el banco de la víctima- y posteriores llamadas telefónicas de supuestos empleados de la entidad para perfeccionar la estafa.

El modus operandi comienza con la recepción de SMS en el que la víctima recibe una alerta, al parecer de su entidad financiera, con el siguiente texto: “Hemos detectado intentos de acceso sospechosos a su cuenta. Debe activar su sistema de seguridad web o bien su cuenta quedará bloqueada”. Los mensajes pueden presentar ciertas variaciones, pero siempre incluyen un enlace para que la víctima pueda acceder directamente a su banco. Sin embargo, ese enlace en realidad conduce a una página falsa donde le solicitan los datos bancarios y personales, así como el usuario y contraseña de acceso a su banca online y un teléfono de contacto. Además, advierten a sus víctimas que recibirán una llamada para realizar las verificaciones de seguridad oportunas.

Una vez que los datos están en su poder, los ciberdelincuentes llaman a sus víctimas haciéndose pasar por empleados de su entidad. En algunos casos, la llamada puede mostrar un número de teléfono legítimo del banco, aunque realmente se trata de una “máscara” que oculta el número de teléfono desde el que realmente se emite la llamada. En esta llamada informan a la víctima de que existen movimientos sospechosos en su cuenta. Para resolver esa situación y retroceder las supuestas operaciones fraudulentas le solicita las claves de firma electrónica con las que opera habitualmente. Mientras hablan, y para dar mayor credibilidad al engaño, pueden emitir nuevos SMS informado de las supuestas gestiones que están realizando o simular que transfieren las llamadas a otros departamentos. Con este elaborado proceso, los delincuentes consiguen tener acceso total a la banca online de sus víctimas y pueden realizar pagos y transferencias mientras mantienen la comunicación con los estafados, a los que solicitan las claves necesarias para autorizar las operaciones.

### Recomendaciones para evitar fraudes online

No facilitar las claves secretas ni datos personales a través de ningún canal. Las entidades financieras pueden comunicarse con sus clientes en caso de ser necesaria alguna verificación, pero en ningún caso van a solicitar claves secretas, datos bancarios ni firmar retrocesiones de operaciones. En caso de dudar sobre la autenticidad de la llamada es mejor colgar y ser nosotros mimos los que iniciemos una nueva comunicación con nuestro banco a través del número de contacto empleado habitualmente.

Ser especialmente cauto con los SMS o correos que recibimos y prestar atención a los enlaces que puedan incluir, ya que en los casos de fraude nunca redirige a la página oficial de la entidad bancaria. Estos SMS, habitualmente, contienen faltas de ortografía o frases carentes de sentido.

No acceder a servicios online que requieran intercambio de información privada o realizar trámites bancarios desde dispositivos públicos o que estén conectados a redes wifi públicas.

En caso de recibir un SMS estas características es muy importante no facilitar ningún dato ni hacer click en los enlaces que contiene o descargar archivos adjuntos. La mejor opción para preservar nuestra seguridad es ignorarlo, eliminarlo y en caso de duda, contactar con el servicio de atención al cliente de nuestra entidad bancaria.

>>> Folleto. Productos falsificados.