76 detenidos por estafar mediante SMS fraudulentos simulando ser una conocida entidad bancaria

Actualidad España | 27-04-2023 | 20:21

Guardia Civil

La Guardia Civil ha detenido a un total de 76 personas por estafar mediante el envío masivo de SMS fraudulentos en nombre de una conocida entidad bancaria.

En la primera fase de la operación, los agentes detuvieron a un total de 30 personas en las provincias de Barcelona, Lleida, Tarragona, Girona, Zaragoza, Valencia y Madrid. En una segunda y tercera fase, la Guardia Civil ha detenido a un total de 46 personas en Barcelona, Girona y Tarragona, de las cuales cuatro eran ?captadores de mulas?.

Con la excusa de una supuesta incidencia en su cuenta bancaria, los estafadores ofrecían la posibilidad de resolverla accediendo -a través de un enlace- a la web que resultaba ser falsa. A continuación, obtenían el usuario y la contraseña de acceso a la banca digital de la víctima. Con las claves de acceso a su cuenta, los delincuentes realizaban las transferencias bancarias fraudulentas.

Las investigaciones han permitido obtener información sobre más de 350 cuentas bancarias beneficiarias de las cantidades transferidas ilícitamente con un montante total defraudado superior a un millón de euros.

De toda la información obtenida, los investigadores han analizado más de 500.000 registros de direcciones IP utilizadas por los autores de los hechos durante las fechas de comisión de las estafas.

Evolución de la técnica delictiva

En todos los casos, los perjudicados eran clientes del mismo banco sobre los que se empleaba el mismo modus operandi que con el tiempo fue evolucionando y perfeccionándose.

En ellos se combinaban técnicas de engaño como el phishing y el smishing, con los que, a través del envío de emails o SMS fraudulentos con apariencia de una fuente de confianza, pretendían obtener las credenciales de acceso de sus víctimas.

A estas técnicas se unió después otra conocida como vishing, en la que los ciberdelincuentes efectúan una llamada en tiempo real a la víctima y en la que, haciéndose pasar por un trabajador de la entidad bancaria, le advierten de movimientos sospechosos en su cuenta.

Una vez ganada la confianza, solicitaban a las víctimas las claves de acceso recibidas en sus móviles, que en realidad eran códigos para autorizar transferencias a través de una conocida aplicación de envío de dinero instantáneo.

La sofisticación en el proceso del engaño fue en aumento, ya que en la pantalla del teléfono móvil de la víctima solía aparecer el logotipo de la propia entidad bancaria y sus números reales de teléfonos, algo que solo se consigue utilizando técnicas de spoofing.

Mulas económicas

Para los investigadores, la mayoría de los detenidos ejercían funciones de ?mulas económicas?, reclutadas ?captadores?, quienes buscaban a personas en situación de vulnerabilidad. A cambio de pequeñas comisiones, obtenían las numeraciones de sus cuentas bancarias o bien lograban que abriesen cuentas online en diferentes entidades.

Los ?captadores?, ocupan un escalón superior a las ?mulas?, siendo personas que a su vez han sido embaucadas por los componentes de otro nivel superior y que, a modo de estafa piramidal, obtenían comisiones por cada una de las ?mulas? que reclutaban.

Autor: Redacción