14/11/26

Cerrado un canal de redes sociales que captaba cuentas bancarias para mover dinero del cibercrimen

Resumen

Tras la apariencia de vídeos cotidianos en TikTok, se ocultaba una red que ofrecía hasta 100 euros por abrir cuentas bancarias. Hay dos personas detenidas y otra investigada en Granada y Almería

Las cuentas captadas eran usadas para recibir, transferir y ocultar el dinero procedente de estafas y otros ciberdelitos

Hay al menos 162 víctimas. La investigación ha permitido recuperar 38.000 euros

Contenido

La Guardia Civil ha cerrado un canal de TikTok que buscaba captar víctimas como “mulas económicas”. Su objetivo era que creasen cuentas bancarias, para lo que supuestamente ofrecían hasta 100 euros, con el fin de recibir, transferir y ocultar dinero procedente de estafas y otros ciberdelitos. Han sido detenidas dos personas, entre ellas el administrador del perfil, y otra investigada, en Granada y Almería.

Esta investigación, de nombre “Black-Account”, ha permitido recuperar 38.000 euros y poner fin a este canal utilizado en esta red social. Hay al menos 162 víctimas afectadas. El inicio de esta operación fue gracias a la denuncia en Granada hace un año de uno de los damnificados. Desde entonces, guardias civiles del Equipo de Investigación Tecnológica EDITE han analizado gran cantidad de información de carácter financiero y tecnológico para seguir el recorrido de los fondos y destapar este sistema de captación de cuentas bancarias.

El anzuelo: un vídeo, un número de teléfono y una promesa

El método empleado es sencillo. Personas dedicadas a actividades delictivas a través de internet ofrecen dinero a cambio de que otras abran cuentas bancarias a su nombre y cedan su control, facilitando posteriormente claves y códigos de verificación para operar con ellas. Aunque estas continúan figurando a nombre de sus titulares, son otras personas quienes las utilizan para recibir, transferir y mover el dinero procedente de estafas y otros ciberdelitos, con el objetivo de dificultar el seguimiento y la identificación de sus verdaderos responsables. Basta un teléfono móvil y el alcance de las redes sociales para reclutar nuevos colaboradores.

Lo que hace especialmente peligroso este sistema no es una sola cuenta, sino su capacidad para multiplicarse. Un solo vídeo llega a miles de usuarios en muy poco tiempo y capta numerosas personas dispuestas a abrir más de una cuenta a cambio de la compensación económica que se ofrece. Cada nueva cuenta se convierte en una puerta de entrada para el dinero de las víctimas, que posteriormente es transferido entre distintas cuentas, plataformas financieras e incluso servicios de criptomonedas con la finalidad de dificultar su rastreo.

Una cuenta por 100 euros

En este caso, uno de los detenidos había creado un perfil en TikTok donde subía vídeos ofreciendo 100 euros a cambio de la creación de cuentas bancarias. Bajo la promesa de obtener dinero fácil y sin riesgos, facilitaba en los comentarios de sus vídeos un número de teléfono de contacto para aquellas personas interesadas.

El captado abría la cuenta a su nombre, superaba la verificación por vídeo con su rostro y su documento nacional de identidad (DNI) y, después, entregaba los códigos de seguridad que le llegaban por SMS. Con esta información, el control efectivo de la cuenta pasaba a manos del estafador. El titular continuaba siendo el captado, pero quien movía el dinero no.

Durante las pesquisas, la Guardia Civil ha comprobado cómo uno de los titulares bancarios investigados llegó a acumular 26 cuentas en ocho entidades distintas. Asimismo, por una sola cuenta de una entidad financiera digital llegaron a circular cerca de 80.000 euros.

La investigación continúa abierta y no se descartan nuevas detenciones.

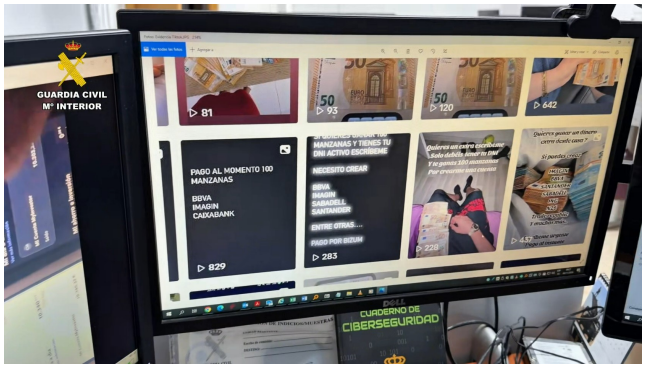
Recomendaciones de la Guardia Civil

La Guardia Civil recuerda que ninguna empresa legítima paga por utilizar cuentas bancarias de terceros. Ante ofertas de este tipo, recomienda:

- No abrir cuentas bancarias para terceras personas ni ceder el control de las cuentas de las que sea titular, aunque sea de forma temporal.
- No facilitar claves de acceso ni códigos de verificación de su banco. Quien los posea, tendrá control sobre su dinero y su identidad.
- Desconfíe promesas de dinero fácil y sin esfuerzo difundidas en redes sociales; si parecen demasiado buenas para ser cierto y suena demasiado bien, probablemente esconde un fraude.
- Las personas que cedan sus cuentas bancarias para recibir o transferir dinero procedente de actividades ilícitas pueden incurrir en responsabilidades penales.

Si ha facilitado una cuenta bancaria o datos de acceso bancario a terceros, contacte de inmediato con su entidad bancaria y presente denuncia ante la Guardia Civil o llame al 062.

Imágenes


GUARDIA CIVIL
Mº INTERIOR
81
93
120
642
PAGO AL MOMENTO 100 MANZANAS
BBVA
IMAGIN
CAIXABANK
829
NECESITO CREAR
BBVA
IMAGIN
SABADELL
SANTANDER
ENTRE OTRAS...
PAGO POR BIZUM
283
228
CUADERNO DE
CIBERSEGURIDAD