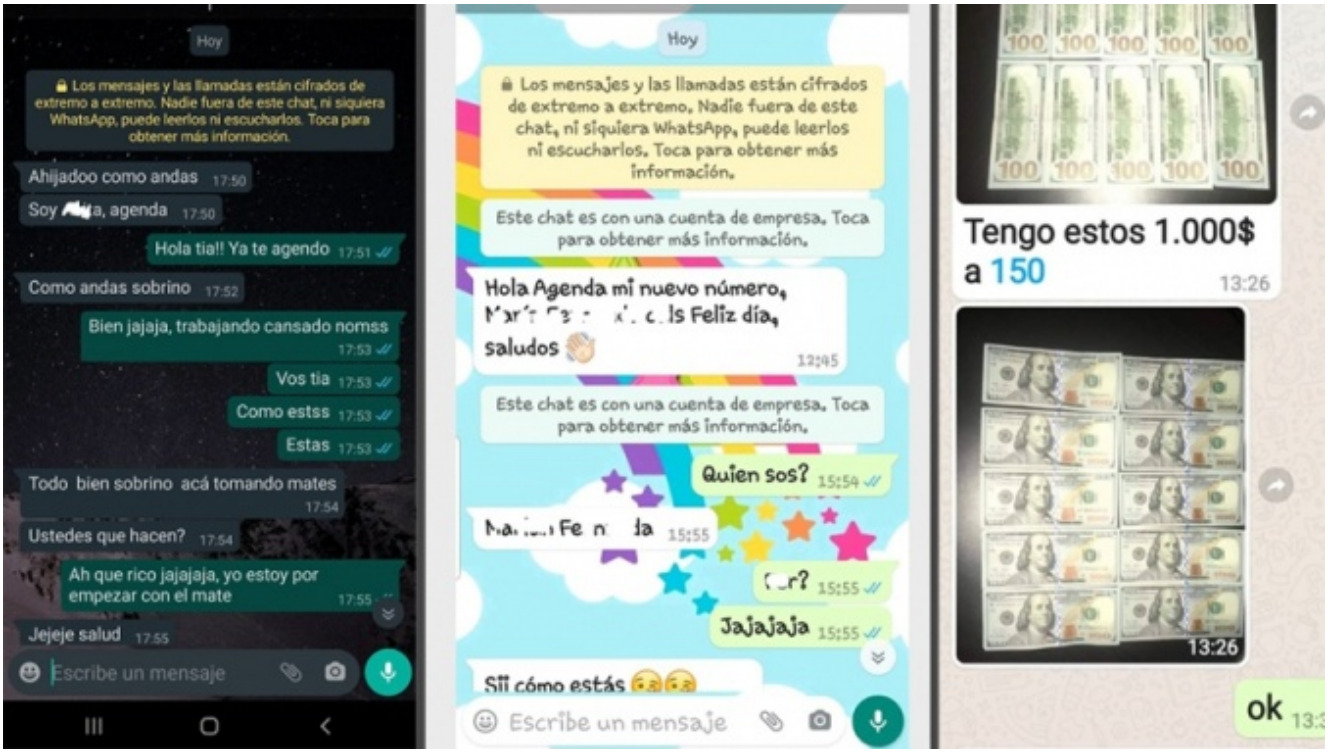
Ciberdelito: advierten sobre el robo de cuentas de WhatsApp y la nueva estafa del dólar “cara grande”

18 noviembre, 2021



El fiscal Horacio Azzolin, titular de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), alertó a través de su cuenta de Twitter sobre una nueva modalidad de fraude.

Un fiscal especializado en cibercrimen advirtió este miércoles sobre una **nueva modalidad de estafa que incluye el robo de una cuenta de WhatsApp** a partir de la cual los **delincuentes acceden a los contactos de la víctima y les ofrecen como anzuelo venderles dólares “cara grande” a cambio de una transferencia o un depósito bancario.**

La advertencia fue anunciada por el fiscal Horacio Azzolin, titular de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), a través de su cuenta de Twitter @horacioazzolin.

El fiscal señaló que desde la UFECI están viendo una serie de **“fraudes asociados a usurpación de identidad, especialmente en Whatsapp”.**

En una de las capturas de pantalla publicada por la fiscalía, se advierte una nueva estafa en la que el ciberdelincuente toma el control de la cuenta de WhatsApp de una persona, tiene todos sus contactos y le manda a familiares o amigos mensajes para ofrecer dólares “cara grande”, es decir de la serie más nueva y en contraposición de los menospreciados “cara chica”, y a un precio tentador.

“Querida, vos tenés a alguien que pueda comprar dólares? Necesito vender 2.500 dólares cara grande. Necesito los pesos por transferencia o depósito bancario”, son algunos de los mensajes de una captura de pantalla aportada por la fiscalía.

En otra de las imágenes, se observan dos fotografías de diez billetes de 100 dólares “azules” o de “cara grande”, con el mensaje: “Tengo estos $1.000 a 150” pesos, (la cotización es de hace unas semanas).

“Desde hace algunas semanas mucha gente está recibiendo mensajes por WhatsApp de conocidos en los que les piden plata prestada por algún problema puntual o les ofrecen comprarles dólares a buen precio”, explica Azzolin en sus tuits.

“Quienes hacen esto consiguen los contactos de la persona cuya identidad toman por diversos medios”, afirmó y allí advirtió sobre falsos mails de cuentas de correos electrónico supuestamente desactivadas o con el logo de bancos, pero explicó que ahora los estafadores roban cuentas de WhatsApp.

> *“Desde hace algunas semanas mucha gente está recibiendo mensajes por WhatsApp de conocidos en los que les piden plata prestada por algún problema puntual o les ofrecen comprarles dólares a buen precio”.*

Uno de los métodos, según Azzolin, es que **con datos ciertos y hasta con una foto de perfil que puede ser la de la víctima del robo de la identidad, envían mensajes a familiares y amigos desde una nueva línea telefónica,** con la advertencia de que lo agendes porque cambiaron el número y luego piden prestada plata u ofrecen los dólares.

“Hola ahijado, cómo andás? Soy …, agendá”, dice uno de los mensajes publicados por la fiscalía y que obtuvo como respuesta: “Hola tía, ya te agendo”, lo que demuestra que con un par de datos y poco de charla previa, ahora la persona que será estafada cree que ese conocido cambió su número de WhatsApp, cuando en realidad es todo una farsa.

“La otra variante es, en vez de usar un supuesto ‘nuevo número’, usar la cuenta de WhatsApp de la víctima que tomaron previamente”, señaló Azzolin para luego dar una serie de consejos para evitar lo que en la jerga se conoce como el “take over” de cuentas de la popular aplicación de mensajería.

Lo más importante, según la UFECI, es **nunca entregar a nadie y bajo ningún motivo el código de verificación que la plataforma WhatsApp envía por mensaje de texto (SMS).**

“Quienes atacan utilizan el código y activan la cuenta ajena en un nuevo dispositivo para luego cometer diferentes delitos”, advierte la fiscalía.

Lo que aconsejan es **“activar la ‘verificación de dos pasos, ingresando para ello desde la aplicación, a la sección ‘Cuenta’, ubicada dentro de la sección ‘Ajustes’ o ‘Configuración'”.**

“El más importante de todos, creo yo, es asociar un email a la cuenta y activar la verificación en dos pasos o segundo factor de autenticación. Y, además, NO (repito, NO) entregar los códigos de verificación para activar la cuenta a terceros, incluso aunque recibas un mensaje que aparenta ser de un conocido”, señaló Azzolin en su Twitter.

“La clave acá es la forma en la que los ‘malos’ consiguen el código de verificación que manda WhatsApp para instalar una cuenta en un nuevo dispositivo. Se lo dan las propias víctimas”, comentó el fiscal.

Y explicó que “los medios que usan para conseguirlo son, en las últimas semanas, principalmente dos”.

“El primero es alrededor de una venta por internet. El supuesto comprador le dice al vendedor que le va a mandar un código para cargar el GPS y llegar al lugar donde retira la mercadería o para transferirle el dinero”, explicó.

“El segundo –continuó-, un poco más artero en los tiempos que corren, es el código de activación de un turno para vacunarse contra el Covid-19, que le tenés que pasar al ‘operador’ que te llamó supuestamente de algún Ministerio de Salud”.

En el último mensaje de su hilo de tuits, Azzolin concluyó: **“Si tienen claro todo esto, cuidan sus claves como las llaves de su casa, no caerían nunca en este tipo de maniobras de ingeniería social, les propongo comentarles de esto a sus familiares y amigxs”.**

Consultado por Télam y a modo de conclusión, Azzolin aseguró hoy que “lo importante es que, por un lado, la gente que tiene cuentas, las proteja. Poner contraseñas robustas, activar el doble factor de identificación y no entregar las claves ni el segundo factor de autentificación, ni el código de activación a nadie”.

“Eso permite que a uno no le roben la cuenta y de esa forma no estafen a tus contactos. Y si uno recibe estos mensajes, hay que ignorarlos, no caer en esas trampas”, puntualizó.

Fuente: Télam