

Si lo llaman del Minsal para pedirle información sobre sus vacunas, cuelgue al tiro

Hackeo de WhatsApp: cómo los cibercriminales se apoderan de los contactos para pedirles dinero

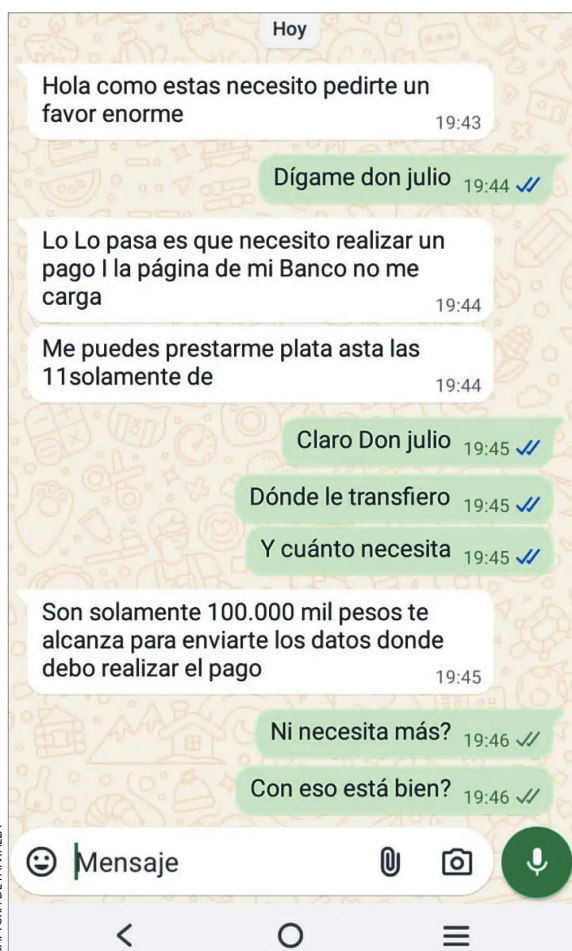
Los criminales se aprovechan de una función para trasladar la aplicación de un número de celular a otro.

ARIEL DIEGUEZ

“Me puedes prestarme plata asta las 11 solamente”. Uno de tus contactos de WhatsApp te está pidiendo “un favor enorme” y el mensaje tiene errores inocentes y sospechosos. El “solamente” pegado al 11 ya, pasa, pero el “me” no puede aparecer dos veces. “Me puedes prestar” o “préstame”, pero no las dos formas en una misma frase. Lo otro es que no tiene nada que ver “asta”, sinónimo de mástil y de cuerno, porque lo correcto es “hasta”. Esto no llega hasta aquí.

“Son solamente 100.000 mil pesos”. Si escribiste 100.000, no tiene necesidad incluir “mil”. ¿Será el autocorrector? ¿La persona que supuestamente te está enviando estos mensajes habitualmente usa estas expresiones? Si la respuesta es no, hay que desconfiar. Mucho más si en ningún momento usa tu nombre o el alias con que habitualmente se dirige a ti.

Ciberdelincuentes hackean cuentas de WhatsApp y los contactos que figuran en ella empiezan a recibir frases de este tipo.



Así es el WhatsApp de la estafa: con un sospechoso asta sin hace.

“Actualmente se ha viralizado, a través de los diferentes medios de comunicación, un nuevo método de estafa que consiste en simular ser del Ministerio de Salud, solicitando el código de verificación a través de la aplicación WhatsApp. Una vez que este código es entregado por cada una de las víctimas, comienzan a extorsionar y solicitar dinero a cada uno de los contactos que registran los dispositivos electrónicos”, explica el inspector Esteban Donoso, de la Brigada del Cibercrimen Metropolitana de la PDI.

El que llama pide información sobre las vacunas del usuario, pero en realidad va tras otro dato. “La aplicación de WhatsApp mantiene un código único e irrepetible por cada uno de los usuarios”, explica.

Gabriel Bergel, presidente de la Fundación de Ciberseguridad 8.8, explica cómo funciona el secuestro de WhatsApp. “Lo que los cibercriminales tratan de hacer es tomar el WhatsApp de otra persona y a través de él pedir plata”, cuenta.

Todo comienza con un servicio de esta aplicación a los usuarios: si por alguna razón alguien debe cambiar de teléfono o de número telefónico, puede trasladar todos sus contactos de WhatsApp, sin necesidad de volver a digitalizarlos uno por uno. Para hacerlo, en la misma aplicación hay que seguir una serie de pasos.

Los delincuentes primero escogen un número de celular auténtico, probablemente de alguna de las bases de datos que circulan por Internet. Luego abren WhatsApp en su teléfono y piden a la

aplicación trasladar el WhatsApp del número que escogieron al de ellos. Tienen que digitar el número del celular del usuario, o sea, el “antiguo”, y el del delincuente, o sea el “nuevo”.

Entonces WhatsApp envía al teléfono del usuario un código. “Cuando a uno le llega ese código, tiene la advertencia de que no hay que transferirlo, no hay que entregarlo a un tercero. Lo que hacen los cibercriminales es que inventan alguna excusa, en este caso una encuesta, y en la llamada de teléfono que le hacen a la víctima le dicen oye, necesitamos un código para validar la encuesta, para verificar tu identidad, lo que sea. Te acaba de llegar a WhatsApp. La gente no se da cuenta y termina relacionando ese código que le llegó para cambiar el número con la mentira o el engaño que le están haciendo por teléfono”, cuenta.

El usuario le dice el código al supuesto encuestador, quien lo digita en su propio teléfono y listo, se apodera del WhatsApp ajeno. El usuario lo pierde. “Los delincuentes sólo tienen acceso a los números de los contactos, no a lo que uno dijo antes por WhatsApp. Como uno guarda papá, mamá, hermano, amiga, empiezan a contactarse con ellos para pedirles plata”, explica.

El WhatsApp se puede recuperar, asegura. “Existe un procedimiento en el que WhatsApp básicamente valida tu identidad. Te van a hacer llegar un código a tu correo electrónico o a otro número, para tratar de determinar que tú eres efectivamente el dueño de esa cuenta y no el cibercriminal”, dice Bergel.