Denuncian intentos de estafas masivas a través de números de Movistar y Movilnet

La delincuencia también tiene presencia en la red telefónica. Ya se ha hecho frecuente las denuncias sobre usurpación de identidad o las estafas electrónicas a través de la telefonía celular en Venezuela.

“Me acaba de llamar un tipo que dijo ser Luis Rodríguez y se identificó como trabajador de Movistar. Me dijo que era el operador 21 de la compañía y cuando entró la llamada por WhatsApp, tenía el logotipo de la empresa”; esta fue la experiencia de Magaly Reinosa*, quien a pesar de estar fuera del país recibió una llamada de un número de la compañía de telecomunicaciones de origen español.

A Reinosa le pareció extraña la llamada, ya que generalmente las compañías telefónicas no usan la red WhatsApp para contactar a sus clientes y por esta razón colgó. Además, había escuchado sobre estafas que se realizan con este modus operandi.

Carlos Benítez* también recibió una llamada de unos supuestos agentes de Movistar, que realizaban el contacto a través de un número telefónico de la estatal Movilnet.

«La persona que me llamó un día lo hizo a mi número Movistar y otro día al número Digitel y se estaba haciendo pasar por trabajador de esas dos compañías; pero yo colgué la llamada cuando me di cuenta que me llamaban de un número Movilnet. Les dije: ‘¿Me están llamando supuestamente de Movistar y estás usando un número Movilnet? Me contestaron que eso era ‘un número corporativo’ y colgué la llamada”, explicó Benítez a Efecto Cocuyo.

Muchos de estos delincuentes informáticos utilizan este modus operandi para tratar de acceder a la cuenta de WhatsApp y así poder iniciar las estafas usurpando la identidad de la víctima.

“Allí empiezan a ‘vender dólares’, por el WhatsApp, y muchas personas lamentablemente caen, porque creen que quienes les venden es una persona de confianza”, señala un funcionario policial entrevistado por Efecto Cocuyo, quien además aseguró que es un delito que se sigue cometiendo a pesar de las alertas que han hecho los órganos de seguridad y los medios de comunicación.

Benítez indicó que el número desde donde se le pretendía realizar una actividad ilícita era 04261010374, perteneciente a la compañía venezolana Movilnet.

¿Cómo estafan con mi número de WhatsApp?

En el caso de Mercedes Ruiz, los delincuentes intentaron tener acceso a su cuenta de la aplicación de mensajería instantánea WhatsApp. El pasado 9 de diciembre, la mujer recibió una llamada desde un número Movilnet; era un hombre que también se hizo pasar por operador de Movistar y le advirtió que perdería su línea si no seguía las indicaciones que le daría.

El estafador le pidió a Ruiz que le indicara un código que le iba a llegar a su teléfono y después de recibirlo tenía que apagar el teléfono celular por lo menos por 30 minuto;, esto supuestamente para no perder la línea de Movistar.

“Me dijo que la idea era evitar que fuera víctima de estafas, como muchas personas en el país”, señala.

La mujer siguió todas sus instrucciones y apagó el equipo, luego le comentó a sus hijos lo que había sucedido y estos rápidamente procedieron a encender el teléfono para saber lo que ocurría.

“Cuando encendimos el teléfono la persona llama nuevamente y con un tono invasivo, que ni te permite hablar, nos reprende por no dejar el equipo por más tiempo apagado, nos decía que iba a perder la línea”, contó uno de los hijos de Ruiz a Efecto Cocuyo.

Lo que pudieron evidenciar los hijos de la víctima fue que en el teléfono se estaba descargando una APK, que son las siglas de Android Application Package, y se trata de un archivo ejecutable que contiene todos los datos que se necesitan para instalar y hacer funcionar una aplicación Android.

La APK se llamaba GB WhatsApp y es una aplicación clon de WhatsApp, muy parecida a la original. Además de funcionar de la misma forma, permite el acceso a los contactos, incluso si no tienen la aplicación instalada.

“Nosotros le preguntamos por qué estaba hablando desde un Movilnet si se supone que era Movistar y el hombre nos dijo que esa era la línea que le había dado el Estado, algo sin sentido; luego, mi hermano le preguntó al estafador dónde mi mamá había comprado el equipo, que era superviejo, y empezó a decir cualquier dirección que obviamente nada que ver y trancamos bloqueamos el número”, dijo un familiar de Ruiz.

No solo en teléfonos

Las estafas en la red no solo se registran en teléfonos celulares, también cuando tus datos son compartidos con terceros.

Karla Rodríguez* un día fue a comprar unos productos en un reconocido supermercado del país y cuando fue a pagar con su tarjeta internacional presuntamente le copiaron los últimos cuatro dígitos.

En Venezuela es común que los cajeros de distintos negocios pidan tus datos al momento de pagar, incluso en algunos casos exigen escribir un número telefónico detrás del recibo de pago, con el que se queda la empresa.

Después de esta compra Rodríguez comenzó a recibir llamadas de números desconocidos durante un mes, pero nunca atendió las llamadas.

Luego recibió otra llamada con la que los estafadores se hicieron pasar por operadores de la empresa de cable por suscripción Simple TV.

“No me pidieron ningún dato personal, solo me dijeron mi nombre y si tenía el servicio activo; les dije que sí y ya. A los minutos me llegó la alerta de que habían pasado un consumo por 93 euros desde un comercio llamado Inisishu_Ueonhoagyulje, que está ubicado en Corea del Sur”, comenta la víctima.

Al darse cuenta que su tarjeta estaba siendo utilizada por otra persona, Rodríguez procedió a bloquearla y mientras hacia el proceso nuevamente utilizaron su tarjeta.

Tras su experiencia la joven señala que esta red de delincuentes no necesita la tarjeta física para cargarte un consumo, tampoco te llaman y piden datos personales, porque solo quieren confirmar que el número que tienen registrado es el que corresponde al titular de la tarjeta.

Por último, recomienda que no se puede ir a pasar la tarjeta internacional en comercios donde los cajeros copien los números de la tarjeta.

En mayo de este año, Movistar alertó que no estaba realizando llamadas a sus clientes solicitando datos personales y enviando códigos para la aplicación WhatsApp a través de SMS. Desde el 1 de diciembre, la cuenta de Twitter de la compañía no ha hecho ningún anuncio sobre estas denuncias.

Con información de La Nación