Aumentan hackeos a redes sociales y robo de identidad; esto puedes hacer para protegerte

Por: RAFAEL MAYA. 06/02/2024

“Muchas gracias por tus bendiciones, recibí tu **mensaje** por ***Messenger***”, le dijo Karina vía ***WhatsApp*** a Raúl, quien sorprendido le respondió que él no le había enviado nada y mucho menos con la palabra “bendiciones”, al no ser una persona religiosa. Horas después, otro amigo le preguntó: “¿te comunicaste conmigo por ***Messenger***? ¿fuiste tú o alguien **intentó extorsionarme**?”.

Más desconcertado todavía, Raúl se dio cuenta de que su perfil de ***Messenger*** había sido ***hackeado***. Empezó a comunicarse con sus contactos para advertirles que no hicieran caso de **mensajes** supuestamente enviados desde su cuenta de ***Facebook***, en los que les pedía **dinero** para hacerles llegar un **paquete desde el extranjero**, donde supuestamente él se encontraba.

Aunque a Raúl no lo pretendieron **estafar** directamente, sí fue **víctima de suplantación de identidad** para que **ciberdelincuentes** intentaran cometer **ilícitos** haciéndose pasar por él en sus **redes sociales**. Se trata, según se ha reportado, de modalidades de **fraude o estafa** a través de **los celulares y las redes sociales**, las cuales han cobrado auge en meses recientes con un número considerable de **víctimas**.

“Se han incrementado los ataques cibernéticos, principalmente vía ***WhatsApp***, donde se **secuestra** y después se utiliza esa línea que era de una persona para luego realizar intentos de **fraude**, **extorsión** y **suplantación de identidad**”, nos explicó Mario Isla, director de **ciberseguridad** en *Tutum Tech*, empresa que brinda servicios de **consultoría tecnológica**.

El también licenciado en Informática por la Universidad La Salle advirtió que en meses recientes “se han incrementado mucho las **afectaciones vía redes sociales**, porque también ha crecido mucho el volumen de personas que las utilizan en su día a día”.

“Su envío se entregó”

“Hola, su envío se entregó en el punto de entrega. Vea dónde puede recoger su paquete aquí…”, decía el ***SMS*** que Raúl recibió en su **celular** desde el número +523114183846. El **mensaje** venía acompañado de un **link** con la supuesta información de dónde recoger el envío. Ahí comenzó su pesadilla…

Justamente en días previos, un amigo le había enviado por correo a Raúl un paquete con ropa y discos compactos. El joven estuvo pendiente del cartero, pero nunca llegó. Así que cuando recibió el ***SMS***, confió en que era un aviso oficial de Correos de México y dio clic en el **link**, pero ¡oh sorpresa! la liga no llevaba a ningún **sitio web**. Sin embargo, los **ciberdelincuentes** ya habían robado su información y la de sus contactos.

Días después, Raúl fue a la oficina postal más cercana para preguntar por el paquete. Enseñó el ***SMS*** y le aclararon que Correos de México no envía ese tipo de mensajes, por lo que seguramente se trataba de un **“fraude”**.

Desde entonces, algunos de sus contactos le avisaron a Raúl de los “**mensajes** extraños” que estaban recibiendo desde su cuenta de ***Messenger*** (con foto de perfil incluida), en los que les pedía **dinero** para supuestamente mandar un **paquete**, o también les solicitaba sus **datos personales** para hacerles un envío “desde el extranjero”.

A uno de sus amigos hasta le llamaron al **celular** y le escribieron por ***WhatsApp*** para decirle que eran de una “empresa de paquetería” y que necesitaban un pago extra, pues el **paquete** que supuestamente enviaba Raúl había rebasado el peso permitido. Según su contacto, el sujeto que le llamó tenía acento sudamericano.

Sobre este **intento de estafa**, Mario Isla nos explicó que esta modalidad “puede ser relativamente nueva”, pero aclaró que **la suplantación de identidad y los fraudes** son “tan viejos como lo que hacían los grandes mercaderes cuando ponían agua al vino para engañar y tener más ganancias”.

De acuerdo con un estudio reciente de la consultora *Dinamic*, los **fraudes** por ***WhatsApp*** afectaron a 51.3 millones de usuarios en México tan solo en la segunda mitad de 2023. La CDMX es la entidad con más casos, seguida del Estado de

México, Baja California Sur y Guanajuato.

Asimismo, el *Consejo Ciudadano para la Seguridad y Justicia de la Ciudad de México* ha reportado que los **robos de identidad** se elevaron 218% de enero a octubre de 2023, en comparación con las **denuncias** presentadas en el mismo periodo de 2022.

¿Quién podrá defendernos?

Para proteger nuestras **redes sociales** y servicios de **mensajería instantánea** de los **ataques cibernéticos**, el maestro en **tecnologías de la información** Mario Isla nos recomendó activar en ***Facebook***, ***Instagram*** o ***X*** lo que se conoce como el "doble factor de autenticación" para acceder a nuestras cuentas.

"No solo debemos utilizar usuario y contraseña, sino además un factor adicional como una **confirmación vía correo electrónico**, el envío de un **código de seguridad a teléfonos móviles**, o la implementación de un **dato biométrico**", precisó el especialista.

Aunque Isla reconoció que en cuestión de **ciberseguridad** "nunca va a existir el factor de protección al 100%, pues siempre habrá algún **riesgo** que los **ciberatacantes** puedan aprovechar", sí se pueden tomar medidas para no ser **víctimas** de estos **delincuentes**.

"En *Tutum Tech* tenemos una guía de qué hacer ante el ***hackeo*** de cuentas. Lo primero es mantener la calma; segundo, buscar a los contactos cercanos por un medio distinto a la **red social** vulnerada para informarles que la plataforma no está bajo nuestro control, y que ignoren los **mensajes** que reciban para evitar posibles **fraudes o extorsiones**", nos precisó el experto.

Isla, quien tiene 19 años de experiencia como consultor en temas de **tecnología**, compartió el número +16505434800, que es la línea con la que cuenta ***Meta*** para que las y los usuarios denuncien mediante llamada o **mensaje** los casos de **suplantación de identidad** en ***WhatsApp***, ***Facebook*** e ***Instagram***.

"Se les pedirán pruebas de identidad y se hará la gestión para recuperar las cuentas afectadas", concluyó el director de **ciberseguridad** de *Tutum Tech*. ¿Has sido víctima o conoces a alguien afectado por **ciberdelincuentes**? Sigue estas sencillas

medidas, compártelas y protégete.

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: Cuestione

Fecha de creación
2024/02/06