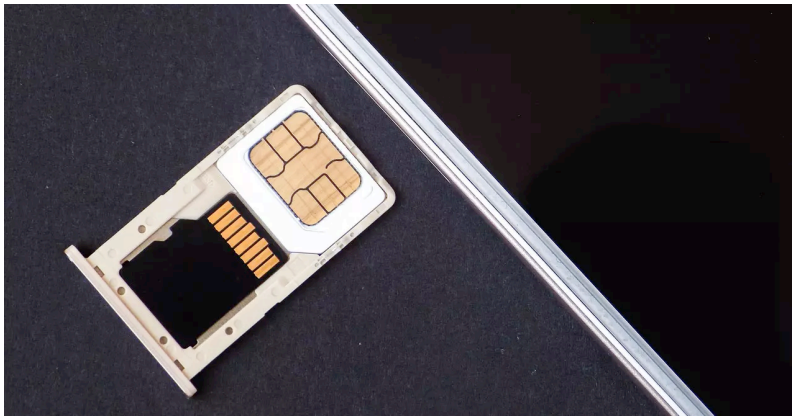
OVATION
AMERICAS

Boletín Junio 2022

Compruebe si su tarjeta SIM ha sido clonada siguiendo estos pasos:

Señales de que su tarjeta SIM ha sido clonada



Los hackers podrían clonar su tarjeta SIM sin que usted se dé cuenta.

Para hacer esto, pueden usar ingeniería social y hacerse pasar por su identidad. Este es un problema serio, ya que podrían actuar en su nombre, recibir códigos 2FA para iniciar sesión en sus cuentas, hacer llamadas o enviar mensajes de texto, etc. Hay algunas banderas rojas que pueden indicar que su tarjeta móvil ha sido clonada o, al menos, que hay algo extraño.

Este tipo de ataque se conoce como intercambio de tarjetas SIM. Básicamente, se trata de un ciberdelincuente capaz de clonar tu tarjeta móvil. Siempre utilizarás una estrategia para lograrlo, ya sea engañando a la compañía telefónica o al propio usuario. Afortunadamente, este no es un problema común, ya que existen importantes medidas de seguridad. Sin embargo, es conveniente saber qué signos puede haber y así evitar problemas.

No recibes llamadas

Una de estas señales es que no está recibiendo llamadas. Incluso intentas llamarte desde otro móvil, dar una señal pero no recibes nada en el móvil. Hay algo extraño y empiezas a sospechar que es posible que no tengas el control de tu tarjeta SIM y que alguien puede haberla clonado sin que te des cuenta. Este problema es sin duda uno de los más comunes. Tal vez recibiste una llamada extraña, alertándote de un supuesto problema, y eso es en realidad lo que desencadenó el robo de tu tarjeta. A partir de ahí, ya no podrá recibir llamadas.

Los SMS no llegan

Algo similar ocurre con los SMS. Los hackers, de hecho, tienen como objetivo clonar tarjetas móviles precisamente para obtener el control de los mensajes de texto. De esta forma, podrán recibir códigos de autenticación de dos factores, por ejemplo, y acceder a cuentas bancarias, redes sociales, etc. Si ves que un SMS no te está llegando, si compruebas que debe llegar y además ves que tampoco estás recibiendo llamadas, es sin duda una señal de que algo está pasando. Esto no siempre significa que sea un ataque de intercambio de SIM, pero es una posibilidad.

Ha perdido la conexión

Otra señal que vas a tener es si ves que has perdido la conexión. Intentas conectarte una y otra vez, estás en una zona con cobertura, pero sin embargo ves que no funciona. Es como si no tuvieras una tarjeta SIM insertada y tu teléfono móvil no recibiera ninguna señal de ningún tipo y no tuvieras llamadas, mensajes de texto o Internet. Si bien esto puede suceder por muchas razones, como fallas en la línea, una cobertura única deficiente o incluso problemas con la tarjeta SIM dañada, la verdad es que también podría deberse a la clonación de tarjetas móviles.

Tu teléfono tiene una ubicación diferente

Si revisas la ubicación de tu teléfono y parece que estabas en otro lugar, como si tu línea móvil estuviera en otra ciudad o país, es una

clara señal de que tu tarjeta ha sido clonada sin que te des cuenta. Esto es algo que debería alertarlo y tomar medidas inmediatas, como llamar a la compañía telefónica. Lo normal es que quien clone tu tarjeta SIM esté en otro lugar físico. Básicamente, lo que vas a hacer con un ataque de intercambio de SIM es suplantar y recibir una tarjeta física como si fueras tú. No será alguien que tengas cerca, por lo que ver que la ubicación ha cambiado es una buena señal.

Recibes mensajes extraños

También puede comenzar a recibir mensajes extraños, que no entiende muy bien por qué. Puede ser que el propio hacker te envíe instrucciones para supuestamente resolver un problema con la línea. Esto es lo que podría permitirle clonar tu tarjeta, por lo que nunca debes caer en este tipo de trampa. Del mismo modo, es posible que esta clonación ya haya tenido lugar y que comience a recibir correos electrónicos extraños, ya sea del atacante o de otros servicios que utilice o utilice en su nombre. Esta es otra causa de alerta. En resumen, como puedes ver, estas señales te ayudarán a saber que tu tarjeta SIM ha sido clonada. Es fundamental evitar ataques que utilicen la tarjeta SIM. Siempre debes mantener el sentido común, tener los dispositivos protegidos y actualizados.

Sigamos aprendiendo y manteniéndonos al día sobre temas de privacidad y seguridad para darnos la mejor oportunidad de evitar hackeos y estafas costosas.

Para comentarios, información o para saber cómo minimizar su exposición a los datos, no dude en ponerse en contacto con nosotros en la siguiente dirección:

info@ovationamericas.com o visite nuestro sitio web en: www.ovationamericas.com

OVATION
AMERICAS