¿Cómo se realizan los hackeos de WhatsApp y qué hacer para evitarlos?

13/03/2020

Los ciberdelincuentes pueden robarte el acceso a tu cuenta si no tomás algunas precauciones esenciales, como activar el segundo factor de autenticación.

Los ciberdelincuentes pueden valerse de diferentes técnicas para robarte el acceso a tu cuenta de WhatsApp. Y una vez que lo logran, además de quedarte sin poder usar tu perfil, la información que tengas almacenada en esa plataforma como tus conversaciones podrían caer en otras manos.

Una de las formas en que eso puede ocurrir es que un ciberdelincuente, que sepa tu número de WhatsApp, busque verificar esa cuenta en otro dispositivo. Claro que si lo hace, esa cuenta dejará de estar disponible en tu celular.

Pero para que esto ocurra, el sistema pide un código de verificación que llega por SMS o llamada de voz. Y si te llegara un mensaje así te darías cuenta que hay algo raro pero podría ocurrir que el usuario que busca hackear tu cuenta, al momento de solicitar iniciar sesión de tu WhatsApp en su celular, pida recibir el código por voz y si no atendés ese llamado con el código, quedará grabado en el contestador.

“Si se solicita que el mensaje llegue por mensaje de voz y el

usuario (el verdadero propietario de la cuenta) no atiende porque está en el cine o durmiendo, por ejemplo, el código quedará guardado en el contestador de su móvil. Y en muchos casos la clave para acceder al contestador de voz que se tiene por default es muy fácil de deducir. Así que si el usuario no modificó este password, el atacante podría fácilmente acceder al código de verificación para así iniciar sesión en WhatsApp desde su smartphone", explicó Luis Lubeck, analista de seguridad de Eset, en diálogo con Infobae.

Cabe recordar que es posible acceder al contestador del celular desde un teléfono fijo, de ahí que un atacante pueda recurrir a esta técnica con facilidad. Una vez que se ingresó al contestador de este modo, se le pedirá la clave de acceso al contestador que, tal como ya se mencionó si no se modificó y es la que se tiene por default es fácilmente identificable.

En otros casos, los criminales se valen de otros métodos, basados en engaños y otras formas de ingeniería social para lograr que sea el mismo propietario de la cuenta el que brinde, sin darse cuenta, el código de verificación. "En algunos casos se envía un SMS a través de un contacto del usuario que haya sido previamente hackeado con un mensaje que dice, por ejemplo: ´te llegó un código por error a tu celular pero en realidad es para mí, ¿me lo podrás dar por favor?´. Como te llega el mensaje por parte de un conocido, confiás y le das el código, sin pensar", subraya Lubeck.

Una vez que el atacante logró, por el método que sea, tomar el control de la cuenta de WhatsApp, activa el segundo factor de autenticación para blindar la cuenta y recuperar el acceso se vuelve muy difícil. Para hacer un reclamo de este tipo hay que contactarse directamente con la plataforma y comprobar la

identidad y que lo que uno dice es verdad es bastante complejo.

Aquí, las medidas de precaución recomendadas recomendadas para evitar caer en este tipo de trampas:

1. Activá la verificación en dos pasos ingresando a WhatsApp en en la sección “Cuenta”, ubicada dentro de la sección “Ajustes” o “Configuración” -dependiendo del modelo de dispositivo.

2. En caso de recibir un mensaje en el que se brinde un código de verificación, evitá compartirlo con terceros por cualquier medio. No importa si te lo solicita un supuesto amigo o conocido: todo puede ser un engaño.

3. Recordá que la plataforma no le piden información a sus usuarios por medio de mensajes -SMS, WhatsApp u otros servicios de mensajería- ni a través de llamadas telefónicas.

4. Si recibís un mensaje de WhatsApp proveniente de un usuario desconocido, es aconsejable bloquear y reportar al usuario a través de las opciones que aparecerán en pantalla.

5. Verificá habitualmente en qué dispositivos se encuentran abiertas sesiones de WhatsApp Web, y evitá abrir sesiones en dispositivos de uso compartido.

6. En caso de ser víctima de una maniobra de este tipo, avisale a tus contactos y denunciá lo ocurrido antes las autoridades correspondientes.

Fuente: Infobae