Estafadores se aprovechan de la ansiedad por vacunarse para robar cuentas de WhatsApp

18/07/2021

Las estafas por WhatsApp están a la orden del día. El modus operandi suele ser siempre el mismo (o parecido), lo que cambian son las **excusas** para lograr convencer al usuario que otorgue información privada o confidencial. En este caso, la excusa de la cual se están valiendo los estafadores es la **vacuna**. Por medio de un simple artilugio logran **convencer a los usuarios para que les den un dato clave que les hace perder el acceso a su cuenta de WhatsApp.**

En estos días comenzaron a circular diferentes relatos de usuarios que cuentan que reciben un supuesto llamado desde el Gobierno de la Ciudad para para obtener la segunda dosis de la vacuna contra el COVID-19. **Les dicen que los van a reempadronar y que para eso necesitan un código que les llega por SMS.**

El código en cuestión es el número para activar el WhatsApp en otro dispositivo. Muchos usuarios, ante el apuro por resolver el trámite, lo otorgan sin mirar de qué se trata y así terminan **perdiendo el acceso a su servicio de mensajería.**

A continuación, los cibercriminales activan la cuenta de WhatsApp en un **nuevo dispositivo** y empiezan a enviar mensajes a todos los contactos de la víctima **solicitándoles dinero o generando otro tipos de engaños.**

¿Cómo protegerse de estas estafas? La primera gran precaución es saber que **ni desde el Gobierno de la Ciudad ni de ninguna**

otra entidad se requiere brindar un código para empadronarse. El sistema de inscripción implica entrar al sitio oficial del Gobierno de la Ciudad y completar un formulario online. Luego el turno se confirma por medio de mail o mensaje de WhatsApp. A su vez, los ciudadanos de CABA pueden escribirle a **Boti**, el sistema automatizado, para consultar por sus turnos.

En el resto de las jurisdicciones del país el sistema de inscripción es más o menos similar: el empadronamiento requiere la inscripción online o a lo sumo llamar a un número telefónico dedicado específicamente para estos casos. En algunos casos, donde se están dando las vacunas sin turno basta con ir a las dependencias indicadas, directamente con DNI.

En cuanto a este o cualquier otro tipo de engaños en los cuales se solicite un **código** o **token** se debe dudar de antemano y **evitar dar este tipo de información.** Lo mismo vale para los mensajes que llegan con adjuntos o links donde se solicita incluir información confidencial como claves y datos de inicio de sesión.

Cómo proteger tu cuenta de WhatsApp

1. Activar el segundo factor de autenticación. Esta es una medida de seguridad clave para proteger la cuenta de posibles robos. Cuando se emplea esta opción, aún cuando el atacante logre obtener el código de activación para usar la cuenta en otro dispositivo se le requerirá esta clave de acceso que se configura del siguiente modo: ingresar a **Ajustes/Cuenta/Verificación en dos pasos.**

Otras medidas de precaución que debe saber siempre el usuario es que **no debe brindar su código de verificación a terceros**. Hay que recordar que la plataforma no le pide información a sus usuarios por medio de mensajes -SMS, WhatsApp u otros servicios de mensajería- ni a través de llamadas telefónicas.

Es vital activar la verificación en dos pasos de WhatsApp

Si se recibe un mensaje de WhatsApp proveniente de un **usuario desconocido** solicitando datos confidenciales de este tipo, es aconsejable **bloquear** y **reportar** al usuario a través de las opciones que aparecerán en pantalla. También es aconsejable verificar habitualmente en qué dispositivos se encuentran abiertas sesiones de WhatsApp Web, y evitar abrir sesiones en dispositivos de uso compartido.

2. Reportar usuarios que puedan resultar sospechosos o molestos. Es posible bloquear un usuario por el motivo que sea, ingresando al chat, luego en Ajustes/Más y seleccionado allí bloquear. Pero hay un paso más para hacer en caso de que se trate de un contacto que esté enviando mensajes molestos, amenazantes o inoportunos por el motivo que sea. En esos casos directamente se puede optar por **Reportar** que es otra de las herramientas disponibles en el apartado mencionado. Hay que tener en cuenta que al usar esta opción, se enviará a WhatsApp los mensajes más recientes de esta persona a modo de sostén de la denuncia que se está realizando. De hecho al presionar **Reportar** se verá una leyenda que indica esto para que el usuario esté al tanto de la situación.

3. Evitar reenviar contenido sin saber si se trata de algo que legítimo y verificado. Siempre confirmar con fuentes fiables los datos que se comparten porque sino se contribuye a viralizar desinformación y posibles engaños. Cabe recordar que la aplicación incluyó una herramienta hace un tiempo que indica si un mensaje fue reenviado ya varias veces para alertar al usuario de que se trata de cadenas de WhatsApp lo cual no necesariamente implica que sea información fiable.

Fuente: Infobae