

Alertan sobre presuntos robos de cuentas en Whatsapp

En las últimas semanas se identificó un ciber ataque que consiste en el robo de cuentas de WhatsApp, según advierten desde la compañía de ciberseguridad Check Point.

No se trata de una modalidad nueva de robo sino que se notó una recurrencia de este tipo de engaños. Cuando un usuario cambia de equipo y quiere transferir su cuenta de WhatsApp, la compañía envía un código de autenticación por SMS al número de teléfono para que pueda introducirlo en el nuevo dispositivo y así pueda activar su cuenta allí.

Ahora bien, esto también puede ser una puerta de entrada que los ciber criminales pueden aprovechar para vulnerar la seguridad de la cuenta y adueñarse de ella.

“Lo primero que hay que saber de este ciber ataque es que el principal activo para el ciber delincuente es aprovecharse de la confianza de la víctima”, destacó el director técnico de Check Point para España y Portugal, Eusebio Nieva.

Y añadió: “La manera para llevar a cabo este ataque se basa en que, con anterioridad, este ciber criminal ha conseguido atacar a uno de los contactos de la víctima en cuestión y robarle todos los números de teléfono que tenía”.

De esta forma, el criminal consigue el número de la víctima y busca activar el WhatsApp de ese número en otro equipo que tiene en sus manos. Para eso solicita el envío del código SMS para la autenticación, tal como lo solicita la aplicación. Ese número le llegará al usuario genuino.

Entonces tiene que encontrar la forma de qué se lo dé. ¿Cómo lo hace? Apelando a su confianza. Así, el criminal se hace pasar por un contacto conocido y le escribe a la víctima solicitando dicho código que le llegó a su teléfono, alegando que se han equivocado al mandárselo y que por favor se lo dé.

“Lo imprescindible para este ciber ataque es que la víctima confíe en el número desde el cual le está hablando, porque al conocerlo se fía. Simple, pero efectivo”, subraya el directivo.

Claro que si el usuario tiene activada la autenticación en dos pasos, al ciber delincuente no le alcanzará con obtener el código de verificación que envía WhatsApp por SMS sino que

además deberá introducir ese código PIN para activar la cuenta en su dispositivo. De ahí que sea tan importante activar esta función.

Así, el ciber atacante puede enviar un SMS con un enlace que redirija a un sitio con malware o bien mandar un mensaje vía WhatsApp del tipo “mira qué interesante, descárgatelo”, también con un enlace malicioso.

Esto también puede dar pie a la infección del dispositivo móvil para tener acceso a diferentes aplicaciones y a los movimientos de la víctima o para introducir en el dispositivo un troyano bancario para robar los datos bancarios y obtener con ello un beneficio económico.

Recuperar la cuenta no es sencillo

“La única manera sería hablando con WhatsApp para informarles del robo de la cuenta y que ellos anulen automáticamente esa cuenta con ese número de teléfono”, explica el directivo citado por Portaltic.

Además, habría que notificar a las autoridades correspondientes para que se haga un monitoreo de la situación y se impida que el delincuente siga cobrándose víctimas.

Cómo cuidarse de este tipo de ataques

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

Cuando se activa esta opción, cada vez que se busque verificar la cuenta de WhatsApp en algún nuevo dispositivo, se solicitará esa clave.

Activar esta opción te protegerá, también ante futuros ataques. Es importante que, al configurar la verificación en dos pasos, ingreses también una dirección de correo electrónico para que no se bloquee la cuenta si te olvidás tu número de PIN.

¿Qué pasa si el atacante configuró un PIN de seguridad y no puede recuperar su cuenta aunque haya seguido los pasos indicados?

Si el atacante que robó la cuenta, se anticipó y configuró el segundo factor de autenticación, entonces debe esperar siete días para poder verificar tu número sin el código de verificación en dos pasos.

Independientemente de si se sabe el código de verificación en dos pasos o no, la sesión de la persona con acceso a tu cuenta se cerrará en cuanto ingreses el código de seis dígitos enviado por SMS, explican desde WhatsApp.

Pasados esos siete días, podrá verificar su número sin necesidad de introducir el PIN, pero todos los mensajes que se hayan recibido durante ese período se eliminarán y no se podrán recuperar.

Si trascurrieron más de 30 días desde que se usó WhatsApp por última vez, sin el PIN y sin verificar su número de nuevo, la cuenta será eliminada pero podrá crear una nueva, verificar su número y establecer un nuevo PIN.

Además de todo esto, puede contactarse con la plataforma para reportar este incidente escribiendo a support@whatsapp.com y mencionando en el asunto: “Pérdida/Robo: desactivar mi cuenta”.

Con información de La Verdad