CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS DE SEGURIDAD **para prevenir el secuestro de WhatsApp**

WhatsApp cuenta con millones de usuarios en todo el mundo y eso la convierte en un obje tivo atractivo para los ciberdelincuentes, quienes siguen ideando, desarrollando y aplican do métodos para robar dinero y datos. Entre los ataques más recientes que se están produ ciendo en esta app, tenemos el secuestro de WhatsApp.

Que es el secuestro de WhatsApp

Es un tipo de ciberataque cada vez más común, cuyo objetivo principal es conseguir dinero, funcionando de forma similar al ransomware; alguien consigue hacerse con el control de nuestra cuenta y para devolverla, exije que le transfiramos dinero.

La clave en este delito es hacerse del código de verificación de la víctima.

El número de la víctima puede ser es cogido de filtraciones masivas de datos personales, anteriores blancos de ataque, investigación previa, o al azar.

Cómo se lleva a cabo el secuestro

El objetivo del delincuente es hacerse del código de verificación de WhatsApp de su víctima. Para ello:

1.- En la aplicación, solicita reactivar la cuenta del número de teléfono de la cuenta que busca robar.

2.- Eso genera el envío de un código de verificación al teléfono de la víctima vía SMS.

3.- El malhechor llama o le escribe por WhatsApp a su víctima, diciéndole que le ha enviado el código por error, tratando de generar simpatía o ur gencia, y le pide que se lo envíe.

4.- Si la víctima manda el código, ya ha perdido su cuenta de WhatsApp.

Estafas y delitos tras el secuestro de la cuenta

Algunas de las formas en que los delincuentes aprovechan el secuestro de WhatsApp son:

- Extorsionar al dueño de la cuenta por un rescate. Nada garantiza que de pagar la cuenta sea devuelta, se recomienda no pagarlo.
- Suplantar al propietario de la cuenta para estafar y robar las cuentas de WhatsApp de sus contactos.

Pedir depósitos de dinero y rea lizar estafas a familiares o cono cidos de la víctima.

Usar los números de los contac tos para mandar spam, malverti sing y ataques de phishing.

Cómo prevenir estafas y el secuestro de WhatsApp

1.- Nunca compartir su código de verifi cación, contraseñas u otros datos personales.

2.- Nunca hacer click en enlaces sospe chosos o enviados por personas en las que no confíe.

3.- Desconfiar especialmente de mensa jes que lo contacten pidiendo dinero, ofreciendo descuentos u oportunida des de ganar premios, beneficios o pornografía.

4.- Si un enlace parece importante, pre guntar a quién lo envió por medios distintos a WhatsApp (por ejemplo, teléfono).

Cómo prevenir estafas y el secuestro de WhatsApp

5.- Hacer su foto de perfil en WhatsApp visible solo para contactos confirma dos.

6.- Activar verificación de dos pasos:
- Ingrese a la sección "Ajustes" de la app.
- Ingrese a la sección "Cuenta".
- Ingrese a la sección "Verifica ción en dos pasos" y luego seleccione "Activar". Intro duzca un código de 6 núme ros que funcionará como contraseña.

7.- Introduzca una dirección de correo electrónico cuando se le solicite, de forma adicional, para aumentar la seguridad.

Qué hacer si ya se fue víctima

1.- Ingresar a WhatsApp con su número de teléfono y pedir un nuevo código de verificación. Ingresarlo en What sApp hace logout al delincuente que usa su cuenta.

2.- Avisar a sus contactos que su cuenta de WhatsApp ha sido robada, y que si se contactan con ellos haciéndose pasar por usted, no deben hacer caso ni hacer clic en enlaces que les envíen.

3.- Denunciar ante las autoridades: Bri gada Investigadora del Cibercrimen de la Policía de Investigaciones. Telé fonos: +562 2 7080658 +562 2 7080659.