Si crees que alguien robó tu cuenta de WhatsApp, los pasos a seguir son:

- Envía un correo electrónico a **support@whatsapp.com** que contenga tu número telefónico completo (que incluya código de país y área), describe lo que sucedió.
- Notifica a tus familiares y amigos ya que el atacante podría hacerse pasar por ti en tus chats individuales y grupales.

Con estos sencillos pasos evita ser víctima del robo de tu cuenta.

Referencias

En Internet

- https://noticieros.televisa.com/videos/hackeo-a-whatsapp-la-paparrucha-del-dia/
- https://latam.kaspersky.com/blog/robo-de-cuentas-en-whatsapp-al-burlar-la-doble-autenticacion/21962/
- https://faq.whatsapp.com/general/account-and-profile/stolen-accounts/?lang=es_pe

SEDENA

SECRETARÍA DE LA DEFENSA NACIONAL

RECOMENDACIONES DE SEGURIDAD PARA UTILIZAR WHATSAPP.

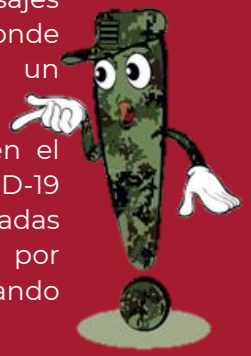
Objetivo del robo de cuentas de WhatsApp

El robo de cuentas es un modus operandi utilizado para extorsionar o defraudar a los contactos de las víctimas y obtener otros números para realizar lo mismo.

¿Cómo es posible el robo de las cuentas?

Las formas en que los ciberdelincuentes pueden robar la cuenta son muy diversas:

Algunos cibercriminales pueden robar tu cuenta a través de cadenas de texto sospechosas, o enviándote mensajes para anunciar concursos, donde aseguran que podrías ganarte un premio.



También se ha detectado que en el contexto de la pandemia de COVID-19 los cibercriminales realizan llamadas telefónicas haciéndose pasar por personal de salud realizando encuestas.

Al término de las preguntas el delincuente solicita un código que la víctima recibirá vía SMS supuestamente para registrar su participación y evitar lo vuelvan a llamar.

En realidad, el código es el que WhatsApp envía para poder activar la aplicación en un teléfono nuevo con la cuenta de su víctima.

Los cibercriminales también se hacen pasar por personal de soporte técnico de la aplicación realizando el procedimiento descrito.

Técnicas empleadas para burlar la verificación en dos pasos.

La verificación en dos pasos se ha convertido en una de las medidas de protección de cuentas más utilizadas actualmente, aunque se trata de un método que claramente refuerza la seguridad de nuestros perfiles en redes sociales, los cibercriminales han ingeniado métodos para lograr vulnerarla.

Una forma que aprovechan los cibercriminales para obtener los códigos consiste en solicitarlos mediante **SMS**. Para ello, realizan un intercambio de la tarjeta SIM "Sim Swapping" (duplicación o suplantación de la tarjeta SIM) comunicándose con la empresa proveedora de telefonía de la víctima, para convencerlos de que ellos son los propietarios de la línea y pedir que el número se cambie a otro dispositivo.

Los cibercriminales publican aplicaciones maliciosas con permisos para acceder a los SMS en el dispositivo lo que les permitiría visualizar los códigos de verificación y robar la cuenta de la víctima, la mayoría de las aplicaciones maliciosas se encuentran en sitios no oficiales, pero no se descarta que también se encuentren en Google Play o AppleStore.

Recomendaciones

Para evitar ser víctima de ciberdelincuentes en WhatsApp, lleva a cabo las siguientes acciones:

A. Habilita la autenticación de doble factor (código de seis dígitos) en WhatsApp, siguiendo los pasos de configuración en la aplicación.

B. No abras tu cuenta en equipos compartidos y verifica de manera frecuente en qué dispositivos aparecen las sesiones iniciadas de WhatsApp Web.

C. La aplicación nunca solicita a los usuarios información por llamadas, mensajes de WhatsApp o mensajes de texto (SMS).

D. Al momento que tenga que recibir algún código de verificación, evite compartirlo con más personas incluso amigos o familiares.

E. Siempre que recibas mensajes de texto de números desconocidos, bloquéalos sin responder ni dar información personal.

F. Cierra todas las sesiones abiertas en WhatsApp Web, esta suele ser una fuente de filtración de información y usurpación en el sistema de mensajería.

G. Solicita que tu número de teléfono sea eliminado de listas de aplicaciones que identifican llamadas, los estafadores pueden utilizar estas listas para encontrar tu número a partir de tu nombre.