¿Qué es el spoofing y cómo afecta a WhatsApp?

Imagina que un día recibes un mensaje de un compañero de trabajo o un familiar cercano a través de WhatsApp. Todo parece normal, hasta que descubres que no era esa persona quien te enviaba los mensajes, sino un ciberdelincuente que había tomado el control de su cuenta. Este escenario, que puede sonar casi imposible, es cada vez más común, y se lleva a cabo mediante una técnica conocida como spoofing.

El spoofing, tanto en el ámbito del correo electrónico como en aplicaciones móviles, es una técnica de suplantación de identidad que pone en peligro la privacidad y seguridad de los usuarios. En el caso de WhatsApp, esta amenaza ha crecido considerablemente, tal como lo advierten los expertos en seguridad de Panda Security y ESET, quienes alertan sobre las múltiples formas en las que los ciberdelincuentes pueden tomar el control de una cuenta de WhatsApp.

Qué es el spoofing y cómo afecta a las cuentas de WhatsApp

El spoofing es una técnica utilizada por los atacantes para falsificar la identidad de una persona o entidad con el objetivo de engañar a sus víctimas. En el contexto de WhatsApp, el spoofing se refiere a la suplantación de la cuenta de un usuario, permitiendo que el ciberdelincuente acceda a la aplicación en nombre de la víctima. De esta manera, el atacante puede leer mensajes, intervenir conversaciones y enviar mensajes a los contactos de la víctima, sin que esta se dé cuenta de lo que está ocurriendo.

Una de las formas más comunes en que los ciberdelincuentes pueden robar una cuenta de WhatsApp es mediante la técnica de QRLJacking (Quick Response Code Login Jacking), un tipo de ataque de ingeniería social que explota la función de iniciar sesión a través de códigos QR.

Este vector de ataque afecta a las aplicaciones que utilizan códigos QR para iniciar sesión, como WhatsApp Web o la versión de escritorio de la aplicación.

Cómo roban las cuentas de WhatsApp

El QRLJacking funciona de la siguiente manera: el ciberdelincuente genera un código QR falso que aparenta ser el auténtico de WhatsApp Web. Luego, mediante técnicas de ingeniería social, induce a la víctima a escanear este código, haciéndole creer que está accediendo a una página o servicio legítimo. Una vez que la víctima escanea el código, el atacante obtiene acceso a su cuenta y puede iniciar sesión en su propio dispositivo.

Este ataque suele pasar desapercibido para la víctima, ya que sigue teniendo acceso a su cuenta desde su propio teléfono. Sin embargo, el ciberdelincuente tiene ahora el control total de la cuenta desde otro dispositivo, lo que le permite enviar mensajes, leer conversaciones y hasta intervenir en conversaciones en tiempo real. Según ESET, este tipo de ataques puede ser difícil de detectar, lo que lo hace especialmente peligroso.

Existen varias formas en que los ciberdelincuentes pueden tomar control de una cuenta de WhatsApp. Además del QRLJacking, una de las más comunes es la clonación de la SIM o eSIM del teléfono de la víctima. Al duplicar la tarjeta SIM, el ciberdelincuente puede registrar el número de teléfono de la víctima en otro dispositivo, tomar el control de la cuenta de WhatsApp y comenzar a enviar mensajes suplantando su identidad.

Otra técnica común es a través de mensajes SMS de phishing. En este tipo de ataque, los ciberdelincuentes envían un mensaje a la víctima haciéndose pasar por un contacto de confianza y solicitándole que comparta un código de verificación o que siga un enlace malicioso. Al hacer esto, la víctima entrega el control de su cuenta al atacante.

Una vez que los ciberdelincuentes toman el control de la cuenta, pueden utilizarla para enviar mensajes maliciosos o enlaces de phishing a todos los contactos de la víctima. Esto no solo afecta a la privacidad del usuario, sino que también pone en riesgo a todos los que se encuentran en su lista de contactos.

Cómo evitar ser víctima de spoofing en WhatsApp

Afortunadamente, hay medidas que los usuarios pueden tomar para protegerse del spoofing en WhatsApp. Una de las más importantes es activar la verificación en dos pasos. Este sistema de

seguridad añade una capa adicional de protección al requerir un PIN de seis dígitos cada vez que se registra el número de teléfono en un nuevo dispositivo.

El proceso para habilitar la verificación en dos pasos es sencillo:

Abre WhatsApp y entra en Ajustes.

Entra en la sección de Cuenta.

Selecciona la opción de Verificación en dos pasos.

Activa la verificación y establece un PIN de seis dígitos.

Además, es recomendable introducir una dirección de correo electrónico válida al activar la verificación en dos pasos. Esto permite recuperar la cuenta en caso de que se olvide el PIN, ya que WhatsApp puede enviar un enlace de recuperación al correo proporcionado.

Otra recomendación es nunca escanear un código QR que no provenga de una fuente confiable. Si se recibe un código QR por correo, mensaje o a través de un sitio web sospechoso, lo más seguro es ignorarlo y utilizar únicamente los códigos proporcionados por el sitio oficial de WhatsApp Web o la aplicación oficial.

Con información de Infobae