Descubren nueva táctica de robo de WhatsApp

Posted on 18 de mayo de 2021 by Diario Humano

La estafa de ingeniería social roba la credencial de activación y deshabilita la contraseña personal que sirve como doble autenticación

Diario Humano | La Paz, Baja California Sur (BCS).–

Los ataques para el robo de cuentas de WhatsApp se extienden y continúan. En el pasado, hemos visto como los cibercriminales han lanzado estafas valiéndose de tácticas, como la verificación de anuncios, la invitación a una fiesta o evento VIP, y la clonación de cuentas al robar la foto de las víctimas.

La mejor manera para evitar estos tipos de fraudes solía ser la activación de la verificación de dos pasos, donde el usuario crea una contraseña personal que se solicita en el momento de la instalación de la app.

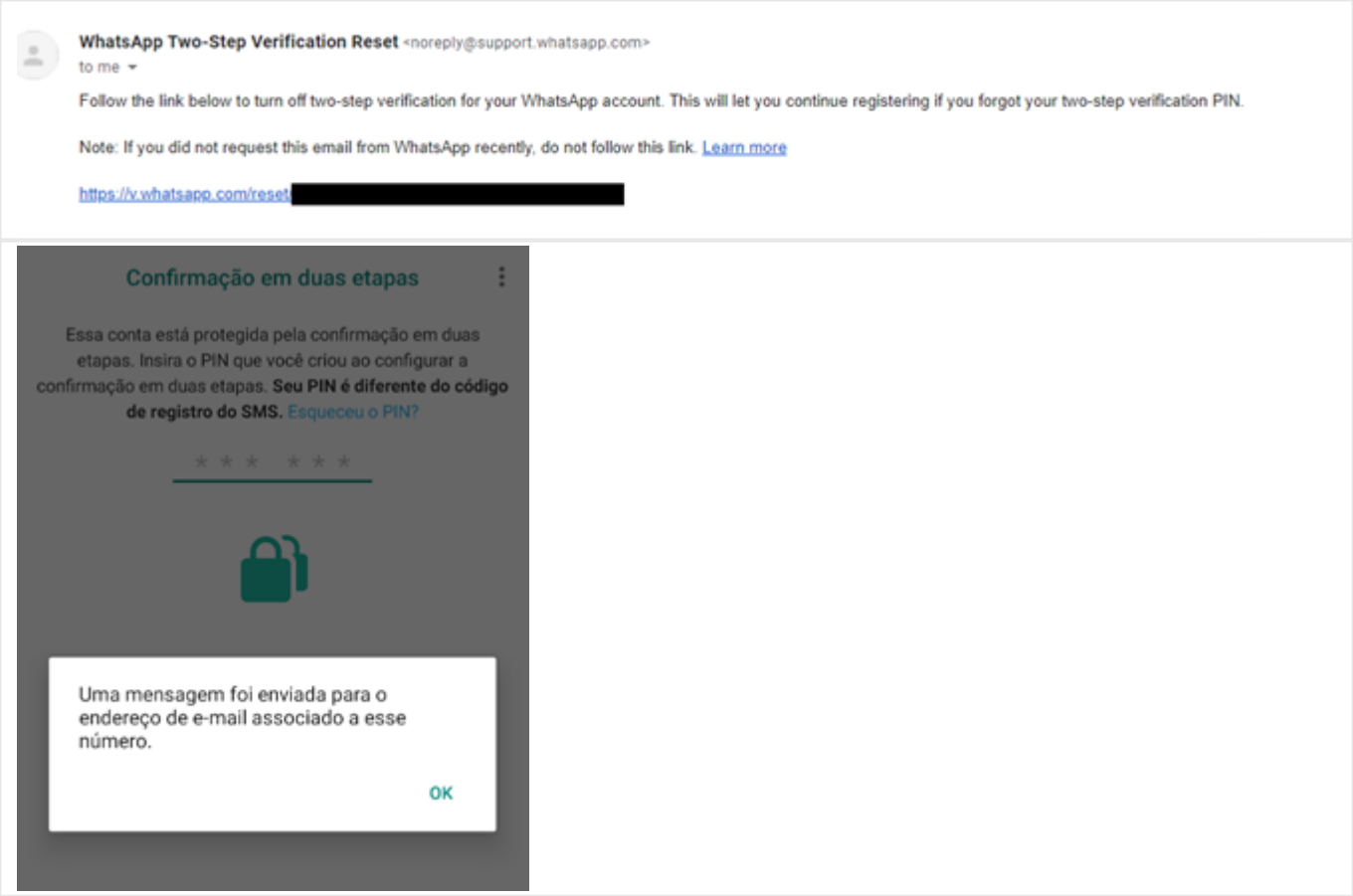
Al parecer, este recurso finalmente se popularizó, pero no para el objetivo previsto ya que analistas de Kaspersky acaban de descubrir un esquema que, a través del uso de la ingeniería social y una solicitud al área de soporte de la aplicación, burla esta protección.

El fraude comienza con una llamada a la víctima, donde los delincuentes se hacen pasar por representantes de alguna institución sanitaria y piden realizar una encuesta sobre el Covid-19.

Al finalizar las preguntas, el defraudador le pide a la víctima compartir el código que le será enviado a su celular para registrar su participación en la encuesta y evitar que la institución lo vuelva a llamar.

Toda la puesta en escena tiene un objetivo claro: hacer que la víctima comparta el código de seis números que se envía vía SMS, el cual en realidad es el código que la app envía para poder activar la aplicación en un teléfono nuevo.

Si la víctima no presta atención al mensaje y entrega el código, su cuenta podría ser robada.



La novedad de la estafa surge cuando el estafador se encuentra con que la cuenta de la víctima tiene habilitada la doble autenticación. Cuando esto sucede, el defraudador vuelve a llamar a la víctima, pero esta vez se hace pasar por el equipo de soporte de la aplicación de mensajería con el pretexto

de que se ha identificado actividad maliciosa en la cuenta. La víctima recibe instrucciones de revisar su correo electrónico y buscar el mensaje con el enlace que le permitirá registrarse de nuevo en la doble autenticación.

Sin embargo, al hacer clic en el enlace, la protección de doble factor se deshabilita lo que les permite a los delincuentes, quienes ya cuentan con el código de activación temporario, robar la cuenta de la víctima.

Lo que más sorprendió a los expertos de Kaspersky es que la víctima recibe un mensaje de correo electrónico legítimo de WhatsApp titulado “Restablecimiento de la verificación de dos pasos” con un enlace que deshabilita esta protección. Al descubrir esto, **Fabio Assolini, investigador senior de seguridad en Kaspersky**, señala que la ingeniería social de los delincuentes ha alcanzado un nuevo nivel.

“La única forma de que las personas se protejan de esta nueva estafa es sospechar o saber de antemano de que existe”, explica **Assolini.** *“Desde el punto de vista de la seguridad, el proceso de autenticación debe ser mejorado, ya que, de lo contrario, las estafas de robo de cuentas seguirán aumentando. Además, el diseño de la aplicación permite que la estafa deshabilite la autenticación de doble factor. Si, en vez, el enlace enviado llevara al usuario a la página de WhatsApp para ahí restablecer la contraseña de doble factor, los delincuentes no podrían instalar las cuentas en su dispositivo”,* concluye.

Para evitar ser víctima, Kaspersky recomienda:

• Habilite la autenticación de doble factor (código de seis dígitos) en

WhatsApp. Para crearlo, siga los pasos a continuación:
o Vaya al menú y elija “configuración” en la esquina superior derecha
o Ingrese a la opción “Configuración”
o Luego haga clic en “Cuenta”
o Seleccione “verificación de dos pasos”
o Cree un código de seis dígitos, el cual será su código de doble autenticación.

• Solicite que su número de teléfono sea eliminado de listas de aplicaciones que identifican llamadas. Los estafadores pueden utilizar estas listas para encontrar su número a partir de su nombre.

• Nunca desactive la autenticación de doble factor, a menos que olvide la contraseña y necesite cambiarla.

Para más información y consejos, visite el blog de Kaspersky.