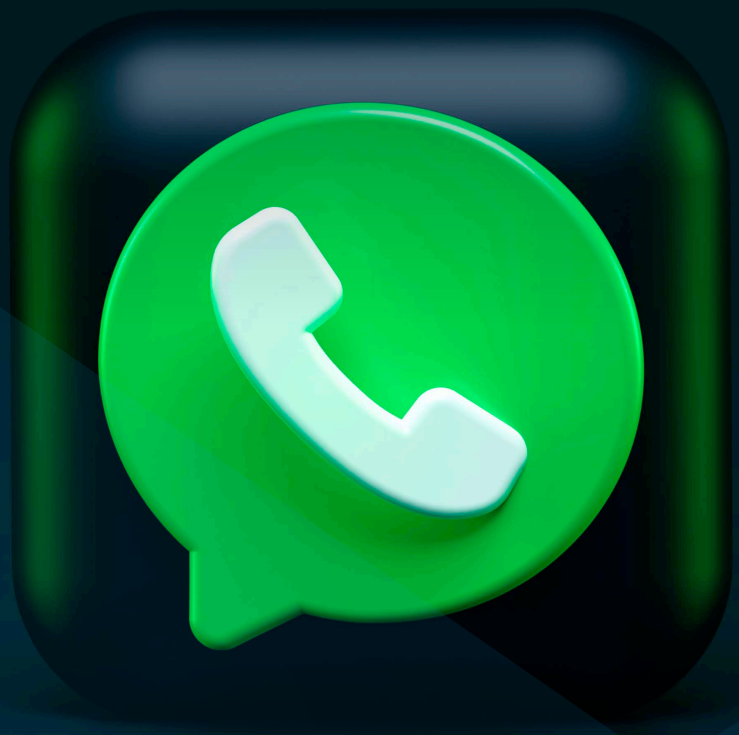
¿Cómo proteger ante un robo de WhatsApp a los tomadores de decisiones?



En estos últimos meses, estamos viendo un incremento exponencial en casos donde directivos están perdiendo acceso a su WhatsApp y con él, están extorsionando o defraudando a los contactos que tiene la cuenta.

Carlos es un directivo importante que hace un par de semanas despertó y no pudo abrir la aplicación de WhatsApp en su teléfono celular. Llevaba un par de días mandando mensajes para hacer posiblemente la mayor venta del trimestre. Mensajes con información confidencial de la empresa, propuestas y otros temas estaban en la aplicación de WhatsApp.

Justo la noche anterior, había recibido un mensaje que en ese momento no le había prestado atención: un mensaje de su jefe que decía: "te agregué como contacto de seguridad para mi cuenta de WhatsApp, para poder habilitarlo, te llegará un mensaje de SMS que necesito que me envíes para poder confirmarlo". Lo que Carlos no sabía, era que estaba enviando un código de SMS para poder activar su propia cuenta de WhatsApp en otro teléfono.

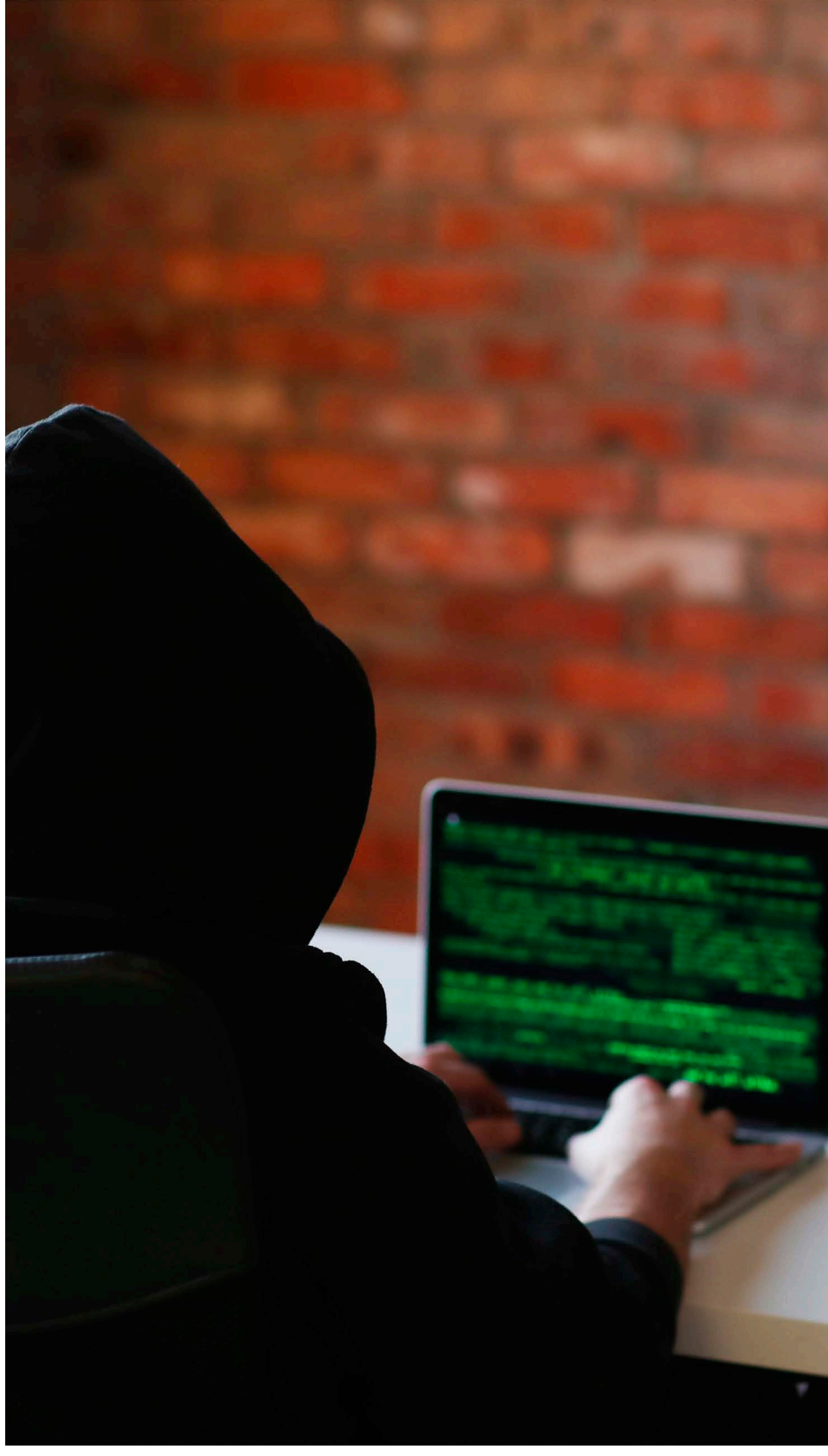
La información que uno puede encontrar en WhatsApp si es que se usa tanto para temas personales como para temas corporativos puede generar una desesperación cuando uno identifica que no puede acceder a la información. "¿Por qué usé WhatsApp para enviar esa información? ¿Y si me extorsionan? Creo que mandé una contraseña por WhatsApp" era lo único que pensaba este directivo.

Ya entrada la mañana, uno de sus contactos le llamó por teléfono para confirmar si todo estaba bien, que ya estaba por realizar la transferencia bancaria para poder enviarle el dinero que necesita. Carlos no había enviado este mensaje, era un mensaje que un tercero había enviado al tener acceso a la cuenta de Carlos. A otro contacto, lo extorsionó.

A estas alturas espero que hayas logrado identificar algunos problemas del actuar de Carlos, que lamentablemente son más comunes que nada. El no tener claro el tipo de información que se comparte por medio de los mensajeros instantáneos, como es el caso de Whatsapp, el confiar ciegamente de un contacto que le pide realizar acciones que en otros casos no se harían y la repercusión que esto conlleva.

Trataré de traer paz a tu conciencia y explicar un par de cosas para poder entender esta situación. Los ciberatacantes, o más bien simples estafadores, se valen de poder tener contactos para intentar tener acceso a sus cuentas. Salen a pescar, como en el caso del phishing, para que, al lograrlo en un porcentaje pequeño de todos los intentos, puedan obtener un beneficio económico.

Lograron obtener un número de teléfono celular, en este momento de forma irrelevante, y lograron por medio de engaños el obtener el código SMS de verificación para activar la cuenta en otro dispositivo. La cuenta de WhatsApp no tenía activada la doble autenticación que requeriría al configurar la cuenta en otro dispositivo, colocar un código de 6 dígitos. Con esta doble autenticación no podrían usar tu propia cuenta en otro dispositivo. Extorsionarán y defraudarán para después tener una base de datos de teléfonos para replicar en cada uno de ellos este proceso. Fue así que llegaron al jefe de Carlos y después con Carlos, ayudados de que en el nombre configurado en el Whatsapp decía claramente “Carlos”.



No tendrán acceso a tus conversaciones anteriores ni a los nombres de los contactos, a menos de que tengan acceso a la cuenta de la nube donde se hacen los respaldos (iCloud o Google Drive), por lo que es también recomendable activar la doble autenticación en esos servicios y que las contraseñas entre ellos sean diferentes. Pero si tendrán acceso a tu foto, nombre, estado, chats individuales abiertos y la configuración de la cuenta.

También tendrán acceso a los grupos, por lo que ese será el punto donde intentarán mandar mensajes individuales a los miembros de los grupos, especialmente los que tengan nombres que tengan que ver con familia o personas cercanas que caerían más fácil en estas estafas. Les pedirán dinero y después buscarán hacer lo mismo: obtener su cuenta de WhatsApp para replicar el ataque.

Ahora, ¿Qué hacer si ya me pasó y no tenía activada la doble autenticación?
El proceso es simple, mas no inmediato.

Es necesario reinstalar la aplicación de Whatsapp en el dispositivo y hay que enviar un email a support@ whatsapp.com (sin el espacio) explicando lo que sucedió.

En cuanto tengas acceso a la cuenta, es muy importante activar la doble autenticación para que no vuelva a suceder.

Ya que estamos en este punto, es recomendable también configurar la privacidad de la cuenta para que solo tus contactos puedan ver tu foto, nombre y estado para evitar que alguien use estos datos para crear una cuenta similar con un número diferente de teléfono y se haga pasar por ti o para que sepan el nombre de cada contacto.

Debemos ser responsables de la seguridad de estos mensajeros instantáneos y su seguridad. Más si se usan en un entorno corporativo. ¿Compartes información de la empresa por Whatsapp?

Fuente de información: www.forbes.com.mx
Autor: Andrés Velazquez