El Consejo Ciudadano para la Seguridad y Justicia (CCPSJ) de México informó que en los primeros dos meses del año el número de hackeos en WhatsApp se incrementó en un 672%, en comparación con el mismo periodo de 2023.

Entre enero y febrero del año pasado se registraron 18 robos de cuentas, mientras que en los primeros dos meses de 2024 el número ascendió a 139, según Salvador Guerrero Chiprés, presidente del CCPSJ, en una entrevista con Expansión. Los ciberdelincuentes buscan engañar a los usuarios para que realicen depósitos de diferentes sumas de dinero.

> *"El 42% de las veces las cantidades solicitadas son menores a 3 mil pesos, el 39% de los casos piden entre 3 mil y 5 mil pesos; un 7% solicita entre 15 mil y 30 mil pesos y otro 7% más de 30 mil pesos",* detalló Guerrero.

El presidente del CCPSJ explicó que el hackeo de cuentas en WhatsApp es una estrategia criminal diseñada para que no se denuncie. Si cada célula delictiva de tres personas engaña diariamente a 20 usuarios por 3 mil pesos, generan 60 mil pesos al día. Está estructurado para que el daño sea pequeño y las personas afectadas no busquen justicia.

¿Cómo hackean las cuentas?

Utilizan desde llamadas telefónicas haciéndose pasar por familiares o amigos en apuros, hasta mensajes diciendo que ganaron un sorteo. Actualmente, *"emplean técnicas o vectores de ataque mediante ingeniería social, que es la evolución de todas las técnicas de extorsión y chantaje existentes",* comentó Nicolas Segura, ingeniero de preventa de la empresa de ciberseguridad Octapus.io.

Los delincuentes suelen llamar a las personas y pedir un código. Cuando el usuario proporciona ese código, les da acceso a su cuenta de WhatsApp, permitiéndoles contactar a los contactos de la agenda y pedir dinero o solicitar préstamos en su nombre.

Siete de cada diez latinoamericanos conocen los virus. Sin embargo, entre el 56% y el 77%,

respectivamente, no están familiarizados con los mensajes maliciosos ni los programas que bloquean o cifran datos y exigen un rescate, según una encuesta de la firma de ciberseguridad Kaspersky.

Según Salvador Guerrero, la gente rara vez denuncia, por lo que no se conoce ni una "millonésima parte" de los delitos cometidos bajo esta modalidad. El presidente del CCPSJ explicó que es posible impugnar el pago de la deuda debido a que hubo dolo al establecer alguna modificación arbitraria en tu contra. Además, se puede abrir una carpeta de investigación con los datos y capturas de pantalla para actuar contra la cobranza ilegítima, que es el delito más común después de la extorsión.

¿Cómo protegerse?

Si sospechas de una llamada, cuelga y contacta directamente a la empresa o servicio desde el cual te están llamando. Los bancos y tiendas tienen múltiples formas de comunicación. Tampoco es recomendable abrir enlaces o proporcionar datos solicitados durante una llamada.

> *«No abras ninguna cuenta o mensaje no solicitado, desconfía de cualquier bien o servicio que esté un 30% por debajo del precio de mercado",* sugirió Salvador Guerrero.

El Consejo Ciudadano para la Seguridad y Justicia gestiona la app No + extorsiones, que tiene una base de datos de números telefónicos dedicados a la extorsión. Además, el consejo cuenta con el número de atención 55 5533 5533.