SEPTIEMBRE DE 2021 | Nº 09-2021

TIPOLOGÍA DE ESTAFAS Y ROBOS MÁS FRECUENTES EN WHATSAPP

BOLETÍN INFORMATIVO ARLC/FT/FPADM Y OTROS ILÍCITOS

FUENTE: ANTILAVADODEDINERO

Los más de 100.000 millones de mensajes de WhatsApp enviados diariamente en el mundo son la autopista perfecta para todo tipo de engaños, estafas y robos.
"Lo primero y último que hacemos al despertarnos e irnos a dormir es desbloquear nuestro smartphone y revisar WhatsApp, ya es casi un automatismo. En plena pandemia y en cuarentena algunos individuos ejecutaron este acto hasta 200 veces por día. La correlación de nuestros datos en esta aplicación con otras plataformas hermanas como Facebook e Instagram, habla de la expectativa de la industria de que nuestras conductas e información sean susceptibles de ser analizadas y monitoreadas continuamente, evidenciando que la tendencia respecto de la intensidad y continuidad en el uso de esta plataforma se incrementará inexorablemente en el futuro", explicó Gabriel Zurdo, especialista en ciberseguridad.
El problema es que ahora WhatsApp se transformó en la principal vía de acceso de los criminales, que lo usan como una forma de atacar a sus posibles víctimas. ¿Cómo reconocer un fraude en WhatsApp? ¡Siempre es urgente!

EL SERVICIO DE MENSAJERÍA PROPIEDAD DE FACEBOOK, WHATSAPP TIENE EMPLEADOS QUE SE DEDICAN SÓLO A REVISAR RIESGOS EN SU PRIVACIDAD, ES UNO DE LAS MÁS USADOS EN TODO EL MUNDO Y NUESTRO PAÍS NO ES LA EXCEPCIÓN. ARGENTINA ESTÁ EN EL QUINTO LUGAR ENTRE LOS QUE MÁS TIEMPO PASAN CONECTADO A INTERNET. CON 9 HORAS Y 40 MINUTOS, SOLAMENTE NOS SUPERAN FILIPINAS, BRASIL, COLOMBIA Y SUDÁFRICA. EL 80% DE LOS ARGENTINOS RECONOCE QUE USA WHATSAPP INTENSAMENTE (99%) PARA SUS COMUNICACIONES.

"Comparando marzo 2019 a marzo 2020 y marzo 2020 a marzo 2021 pasamos de 2.581 a recibir un total de 14.583 denuncias de estafas. El aumento, en términos porcentuales, corresponde a un 465% aproximadamente. Pasamos de 1.305 casos de fraude a 8.559, lo que representa un 58,7% aproximadamente del total de los casos. De accesos a cuentas, pasamos de 229 a 1.220", detalló Horacio Azzolin, titular de la Unidad Fiscal Especializada en Ciberdelincuencia.

ESTAFAS VIEJAS, NUEVAS Y PELIGROSAS POR WHATSAPP

Durante las últimas semanas, especialistas de la consultora de seguridad informática BTR Consulting descubrieron la proliferación de diversas técnicas, algunas nuevas y otras recicladas, de ataques vinculados a la app de mensajería:

- Espiar WhatsApp: varios sitios prometen acceder a toda la información de la cuenta de un objetivo de forma completamente gratuita. En su mayoría, los únicos pasos que se requieren para este "hackeo instantáneo" es completar algunos datos, como el número de contacto de la persona que se quiere monitorear y el sistema operativo del usuario que quiere espiar a la otra persona. El abanico de amenazas es amplio, en su mayoría buscan distribuir publicidad, pero también instalar virus y malware en los dispositivos.
- Versión falsa: circulan varias versiones no oficiales de la aplicación que exponen a los usuarios a engaños y estafas. El "mod" de WhatsApp, una versión no oficial que ofrece a los usuarios funciones adicionales, e incluye un malware peligroso que puede captar al dispositivo. Este malware puede disparar anuncios sin autorización, comprar suscripciones e interceptar mensajes.
- Robo de dinero al azar: "Hola mamá, perdí mi celular, este es mi nuevo número". La madre contestó y preguntó si era su hija, a lo que el estafador respondió que sí, claro. Al día siguiente, la 'hija' le envió un mensaje pidiéndole dinero y le explicó que cuando perdió su teléfono, perdió también su cartera y el dinero que tenía. Es importante hablar por teléfono o reunirse personalmente con el "familiar" si alguna vez recibimos un mensaje pidiendo dinero.
- Estafa de falso delivery: los estafadores simulan trabajar en empresas de delivery on-line y les piden a sus víctimas que hagan click en un link que los invita a ingresar sus datos con el propósito de confirmar información personal, bancario, de la tarjeta de crédito u otra información confidencial. Esto tiene íntima relación con el enorme crecimiento de las entregas a domicilio de todo tipo durante la pandemia de Covid-19.
- Engaños con código QR: más conocido como QRLJacking, aprovecha que los usuarios pueden ingresar a través de este tipo de códigos a la aplicación para dispositivos en los que utilizar WhatsApp Web y, de esta forma, generar uno fraudulento, pero muy similar al original. Después de que el usuario lo escanea; la sesión ya queda almacenada en el computador del criminal y puede utilizarla como quiera.
- Estafa de la emergencia familiar: el proceso inicia con un intento de conexión sospechoso o no autorizado a cuentas de Instagram o Gmail, esta mecánica incluye el robo de la lista de contactos que normalmente está sincronizada con WhatsApp. Esto es posible por vías como: haber sido víctima de phishing, tener una contraseña muy fácil de descubrir en alguna de estas plataformas; o que tanto el usuario y password de red social o cuenta de mail haya sido filtrada / expuesta y revendida en el mercado negro. Así, los ciberdelincuentes se hacen pasar por conocidos de la víctima y, haciendo uso de un argumento coyuntural, apelan a circunstancias normales en la vida de las personas: una emergencia.
- Robo/secuestro de la cuenta: se suele dar cuando un delincuente accede a la cuenta de la víctima para cometer un fraude. Debido a que el estafador está usando la cuenta real de un amigo, su petición de dinero es más creíble para la víctima, una alternativa también muy difundida es la del pedido de rescate para la devolución de la cuenta a la persona hackeada.
- El fraude por WhatsApp y el robo del buzón de voz: Otro truco habitual que incluye acceder al buzón de voz para robar el código de verificación de la app. El problema en esta situación es que muchas personas no protegen debidamente su buzón de voz. No suelen cambiar la contraseña predeterminada, que habitualmente está configurada como «1111» o «0000», o la cambian por una combinación de números predecible, como «1234».

- Cambia el color de tu WhatsApp: muchos recibieron el mensaje que dice “cambia el color del WhatsApp: activa nuevos colores de WhatsApp, este nuevo color me encanta”. Cuando los usuarios abren el enlace para cambiar el color de su aplicación, lo que realmente están haciendo es descargar un virus en el smartphone el cuál permanece invisible, pero está a la accediendo y re-enviando información del dispositivo en el que está instalado.
- HOAX “falsedad articulada”: Se trata de mensajes en forma de texto, imágenes o vídeos en distintas redes sociales con contenido falso o engañoso y atrayente, que generalmente incluye un link a una URL supuestamente de “la marca” que llamó la atención del usuario, en realidad el link está distorsionado sutilmente. El comportamiento del HOAX luego se torna dinámico, es decir: no siempre hace lo mismo, su patrón cambia con el claro objetivo de minimizar la posibilidad de ser detectado e identificado.
- “Te mandé un código por error”: En este caso puntual los usuarios afectados reciben un mensaje que aparece en pantalla con el número de uno de los contactos de su agenda. Otra opción es que los delincuentes se hagan pasar por el soporte técnico de la compañía. Lo que hacen es simple: solicitar el reenvío de un código de seguridad, de seis dígitos, que el usuario recibió por SMS. Con estos números se apoderan de la cuenta de WhatsApp y pueden usarla para realizar otras estafas.

“La clave acá es la forma en la que los criminales consiguen el código de verificación que manda WhatsApp para instalar una cuenta en un nuevo dispositivo: se lo dan las propias víctimas”, detalló el fiscal sobre este último método, la llave de entrada para diversos tipos de estafas.

“Las aplicaciones y redes sociales no son en sí mismas peligrosas; el problema es que los ciberdelincuentes aprenden cada vez más velozmente a utilizar mejores métodos para engañarnos. La clave en temas de ciberseguridad tiene que ver con la necesidad de educar y concientizar a las personas no solo para evitar riesgos en el presente, sino a futuro. Dejar de utilizar WhatsApp no es el método ideal para evitar los peligros del mundo on-line, sino estar alertas e informarnos sobre el correcto uso de la tecnología”, concluyó Zurdo, CEO de BTR Consulting.

CONSEJOS PARA PREVENIR FRAUDES POR WHATSAPP

- Si recibes un mensaje de alguien pidiéndote dinero, primero comprueba si el número es correcto. Si uno de tus amigos o conocidos de repente tiene un número nuevo y te pide dinero, deberías encontrarlo, como mínimo, sospechoso.
- Date la oportunidad de pensar un momento y comprueba el lenguaje y el estilo de la comunicación del mensaje. ¿Es distinto y/o peor de lo habitual? Si es así, es posible que estés tratando con una estafa por WhatsApp.
- Intenta llamar al número de la persona que te pide dinero. Si es un estafador, ¡probablemente quedará en evidencia!
- Si el estafador no atiende, intentá llamar al antiguo número que tengas de tu amigo o conocido, o contactalo por una vía distinta (por ejemplo, por correo electrónico, SMS, etc.) para verificar la historia.
- No dejes que el estafador te presione. Piensa con lógica y manten la calma. Si alguien te pide dinero para cubrir urgentemente, duda, sobre todo si se trata de pagar la electricidad o un impuesto, unas horas más no cambian la situación.
- Si tienes dudas, pregunta al estafador algo que solo tu amigo o conocido pueda conocer.
- Asegura tu casilla/buzón de voz con un código personalizado que solo tu conozcas.
- Si alguien te pide que envíes un código de verificación, nunca lo envíes sin preguntar. Busca siempre contactar con la persona con la que crees que estás hablando a través de una vía distinta. Esto es importante si la persona que está pidiendo el código de verificación es alguien desconocido.
- Configura la “autenticación de dos pasos” en WhatsApp. Una vez configurada, si instalas WhatsApp en un nuevo dispositivo, WhatsApp solicitará el código de seis dígitos que has establecido, así como la verificación que te envíen. Esto puede hacer que el robo de tu cuenta sea más dificultoso.