Los fraudes por WhatsApp, ¿mitos o realidad?

Las últimas alertas por estafas en redes tienen que ver con este sistema de mensajería instantánea, pero no se producen a través de él

En los últimos meses, el servicio de mensajería WhatsApp ha sido protagonista de diversos bulos. La historia comienza en el móvil de una persona que recibe un mensaje de uno de sus contactos, que a su vez dice haberlo recibido de otro, y se extiende entre su grupo cobrando verosimilitud. La mayor parte de las veces alertan de peligros, pero también aluden a protestas u oportunidades de negocio. En ocasiones, es tal su difusión que hasta se han conocido fraudes recientes cometidos a través de esta red de mensajería, transmitiendo la sensación de que el delincuente puede colarse entre nuestros contactos. Sin embargo, las estafas han tenido lugar por un cauce paralelo y no dentro de WhatsApp.

La ingenuidad del usuario

A medida que los teléfonos móviles se hacen más sofisticados, su nivel de seguridad se hace más débil, ya que aceptan programas complejos, como lo son muchos de los desarrollos de software malicioso que han operado durante largo tiempo en los ordenadores: gusanos, troyanos, espías, bloqueadores del sistema, etc. El objetivo es el mismo en ambas plataformas: obtener información de manera ilegal para reportar a los cibercriminales un beneficio económico.

No todos los sistemas operativos están igual de protegidos ante el software malicioso. Android, por aceptar descargas de programas de plataformas no oficiales, es más propenso a ataques. Sin embargo, todos registran el mismo punto débil: la ingenuidad del usuario. El delincuente lo sabe y lo explota en su provecho. Para ello, juega con sentimientos como el miedo, la codicia o la curiosidad, con el fin de obtener de la víctima una información que le permita distraer su dinero.

El ingenio de los estafadores no tiene límite y han desarrollado numerosas estrategias para tener nuestros datos bancarios, obligarnos a transferirles una cantidad monetaria, la suscripción involuntaria a los SMS Premium... Precisamente, esta última modalidad es la que se ha utilizado en los últimos casos de estafas relacionadas con WhatsApp.

WhatsApp, una red cerrada

La polémica en torno a la seguridad de este sistema de mensajería instantánea ha hecho correr ríos de tinta en el pasado, aunque el servicio ha respondido siempre con mejoras en su plataforma. Sin embargo, hasta ahora nunca se ha hablado de la posibilidad de estafas por mensajes de personas que no estén en nuestra lista de contactos. WhatsApp es una red cerrada, donde solo se comunican usuarios que se tienen en su agenda de teléfonos.

Ahora bien, puede llegarnos un mensaje desde un número desconocido (que la plataforma no identifique), pero el sentido común debe llevarnos a rechazarlo siempre y a no aceptar la transferencia de archivos, aunque estos solo pueden ser multimedia (imagen, audio o video).

Es fundamental, sobre todo, evitar abrir enlaces compartidos en este sistema de mensajería instantánea enviados por teléfonos desconocidos, ya que es por esta vía por donde nos suele llegar la estafa, al abrir en el navegador del móvil páginas de *phishing*. Tampoco debemos fiarnos de mensajes que nos lleguen por SMS haciendo referencia a WhatsApp, porque al responderlos podemos estar inscribiéndonos en un servicio de SMS Premium, donde nos cobren entre 0,35 y más de siete euros por cada mensaje enviado. Esta es la estrategia utilizada en los más recientes fraudes. De todos modos, es importante constatar que ni el caso del *phishing* ni el de los SMS Premium tienen lugar dentro de WhatsApp.

¿Espiar a los contactos?

Tal vez el caso más espectacular de fraude relacionado con este sistema de mensajería sea el de un joven de Murcia que promocionaba en las redes sociales -accedió de forma ilícita a 11.000 perfiles de Facebook- un programa en descarga para espiar a los contactos de WhatsApp; es decir que el supuesto software permitía conocer todos los mensajes que el espiado intercambiara con otras personas.

Miles de usuarios accedieron a la página desde la que en principio se descargaba el programa a su móvil. Para ello, dicho programa debía tener nuestro número y nuestra contraseña en el servicio. Sin embargo, no se producía una descarga real y sí una inscripción del teléfono en un servicio SMS Premium que cargaba los costes al usuario y en beneficio del estafador.

La mayoría de los usuarios se daban cuenta de inmediato de la estafa, pero apenas se denunció porque implicaba reconocer que se había intentado descargar un programa de espionaje, un hecho ilegal. De este modo, el joven llegó a recaudar más de 40.000 euros a través de sus víctimas, hasta que le detuvo la policía.

Otro caso similar es el de mensajes de textos recibidos en algunos móviles desde el número 25568 con el siguiente texto: *"Te estoy escribiendo por wasap. Dime si te llegan mis mensajes. Me agregaste el otro día?"* o *"Será un fallo de mi móvil con el wassap. Xp no paro de enviarte la foto! La has visto? Pensé k podría agregarte al face o wassap. O verte en smsduo Q hago??"*. Algunos usuarios respondieron al SMS sin saber que se trataba de un servicio Premium, con la consiguiente sobrecarga en su factura telefónica.

¿Cómo actuar?

Para evitar fraudes de este tipo, conviene seguir una serie de pautas:

- No responder nunca a mensajes desde teléfonos que no se identifiquen con un contacto de nuestra agenda, ni dentro de WhatsApp, o servicios similares, ni por SMS.
- No abrir archivos multimedia de estos mensajes por precaución. Aunque en los móviles la descarga de software solo se realiza desde las tiendas de aplicaciones, en el caso del sistema operativo Android pueden producirse desde terceras plataformas que desconozcamos.
- Evitar la apertura de los enlaces que nos pasen y, sobre todo, no dejar datos personales en las páginas a las que nos llevan.
- Si caemos en la estafa, debemos ponernos en contacto con nuestro operador, para que no nos carguen el coste del servicio premium. La Ley de Competencia Desleal nos ampara.
- Denunciar el caso en los servicios de protección del consumidor de nuestra comunidad, así como en la Oficina de Atención al Usuario de Telecomunicaciones del Ministerio de Industria. //