

## Los riesgos de usar WhatsApp

### Gmail para empresas

 [google.com/apps](http://google.com/apps)

Obtén Gmail para tu dominio con Google Apps - 30 días gratis



Los riesgos de usar WhatsApp

**ABC de España 2** / Cómoda, práctica y el estándar en la comunicación desde dispositivos móviles inteligentes. WhatsApp, aplicación de mensajería instantánea, cuenta con más de 500 millones de usuarios en todo el mundo pero, a raíz de su éxito, está en el punto de mira de los ciberdelincuentes. Aunque parezca una herramienta inocente, su uso puede contemplar algunos riesgos.

"Las numerosas vulnerabilidades encontradas la han situado como blanco perfecto para la distribución de malware y robo de datos personales. Esta situación se ha visto agravada por la escasa percepción de riesgos entre los usuarios de dispositivos móviles que apenas si toman precauciones para proteger su información", explica fuentes de InnoTec System, firma de seguridad informática de la empresa española Entelgy.

**Fallos de seguridad** Las críticas por su "pésima gestión", según los expertos de esta empresa, acerca de la seguridad de la herramienta se ampliaron tras la compra multimillonaria de Facebook. Desde sus

inicios se han ido descubriendo múltiples fallos de seguridad. El más importante, y del que se han hecho eco otras compañías, es "la falta de cifrado de sus comunicaciones", que permite dar acceso de forma inconscientes a la agenda telefónica y a los mensajes de los usuarios. Aunque la compañía desarrolladora de WhatsApp corrigió algunas de las vulnerabilidades, los expertos en seguridad insisten en que el cifrado de los mensajes sigue siendo "fácil de romper".

**Vulnerabilidades en la ubicación** Los expertos reconocen que otras vulnerabilidades relacionadas con el sistema de ubicación del usuario a través del servicio de geolocalización de WhatsApp "almacena las coordenadas geográficas y las mantiene desprotegidas". De este modo, al compartir una ubicación los datos se descargan a través de un canal no seguro, sin utilizar SSL –protocolo diseñado para permitir la transmisión de información de manera segura– y sin cifrar.

Este problema ha provocado que, según reconocen desde la compañía de seguridad, cualquier usuario, de forma anónima y sin necesidad de credenciales pueda "utilizar la infraestructura de WhatsApp para subir todo tipo de archivos o ficheros de cualquier tamaño a sus servidores (incluido los ejecutables)".

**Propagación de "malware"** Además, WhatsApp no cuenta con ningún tipo de antivirus y los contenidos se borran automáticamente en un período de 30 días. Esta situación provoca, a ojos de los especialistas, un camino sencillo para distribuir todo tipo de "malware" o realizar ataques de "phishing".

**Carencias en el proceso de alta** Desde InnoTec System han apuntado la existencia de una "grave carencia" en el proceso de alta y verificación de los usuarios. "Así, el código de activación de usuario se genera en el propio entorno de la aplicación, incluso antes de ser enviado a los servidores internos para que éstos manden el mensaje SMS, con el código, al usuario", señalan.

La posibilidad de cambiar el remitente a la hora de enviar mensajes o el acceso a las conversaciones de un usuario a través de otras aplicaciones que tienen acceso a la tarjeta MicroSD –donde se almacenan las copias de seguridad de WhatsApp– son otros de los fallos observados en los últimos meses.