

La nueva estafa de WhatsApp que usa autos 0 km como engaño



La compañía en detección proactiva de amenazas ESET advierte acerca de **campañas fraudulentas** compartidas por el servicio de mensajería instantánea WhatsApp.

Los mensajes **hacen creer a los usuarios de la aplicación de mensajería instantánea que compañías automotrices, en celebración del aniversario 80°, están otorgando regalos gratis.**

El fraude vía WhatsApp fue detectado en **varios países de la región latinoamericana**. Y el modus operandi tiene a **Toyota y Volkswagen** como quienes supuestamente están dando «¡Regalos gratis para todos!».

El mensaje llega al usuario de la **aplicación de mensajería instantánea desde otro contacto de confianza**, quien seguramente también cayó en la trampa. Y como el requisito es reenviar el texto a «cinco grupos o 20 amigos» para así obtener el regalo, se **comparte sucesivamente**.

Al hacer clic sobre el link que llega por WhatsApp, se abrirá una página que invitará al usuario a participar en una **encuesta sobre datos personales** y la marca de autos respectivamente. Entre la información compartida, se requiere la dirección de correo electrónico y el número de teléfono.

La técnica de fraude no es nueva, sino que desde hace tiempo se viene utilizando la

excusa de regalar por un aniversario. Pero, en este caso, para hacer verosímil el engaño, al terminar la encuesta, se muestra una instancia que aparenta realizar una **fase de recopilación de la información**. Luego, el usuario podrá participar del «sorteo».



El engaño se divide en varias fases, como la aparente recopilación de información y el supuesto sorteo.

ESET

La siguiente parte del concurso consta de la elección de varias opciones y, en caso de que el usuario acierte, obtendrá el regalo. Tras un par de intentos, **«logra elegir una opción ganadora» que es nada más ni nada menos que un automóvil**. El premio puede ser la posible razón por la cual quien recibe el mensaje no dudan en reenviarlo.

“Para agregar elementos que convenzan al usuario de ser una promoción legítima, **la campaña hace uso de elementos apócrifos, como algunos comentarios de supuestos participantes que han obtenido premios similares a los ofertados o que han participado, así como un número elevado de “Me gusta” en la publicación del concurso, que podrían agregar credibilidad al engaño**”, destaca Miguel Ángel



La Ingeniería Social asociada a este engaño indica que el usuario es ganador de un automóvil.

ESET

En caso de que el usuario de WhatsApp continúe la interacción con la campaña, será dirigido a **otros sitios con más concursos**. Aunque estos requerirán, mediante el envío de un mensaje de texto, la validación de si se trata de una persona real.

Así, la persona se suscribe con su número de teléfono a servicios de mensajería premium y la campaña pasa a ser monetizada. Es decir, recibirá múltiples mensajes y, además, **la víctima del fraude será quien los pague**.



Monetización de la campaña mediante el envío de mensajes SMS.

ESET

Por último, otro riesgo para el usuario está presente en cada **interacción con el sitio que se intenta abrir** o, por otro lado, en cada **descarga de archivos**.

Fuente: Ámbito