Supuesta ‘copia de seguridad de mensajes de WhatsApp’ podría robar sus datos: así es cómo funciona

29/09/2021

La ciberdelincuencia sigue afectando de forma crítica a las personas en la web, casi siempre haciendo uso de estrategias desarrolladas por medio de elementos como enlaces maliciosos enviados al correo electrónico.

De esta forma, con ayuda de lo que se conoce como ***phishing,*** los delincuentes suplantan la identidad de personas o empresas para hacer creer a los internautas que **los links adjuntos a un e-mail pueden abrirse o descargarse sin ningún problema.**

Entonces, cuando el usuario permite la entrada del malware, el dispositivo se infecta y el ciberdelincuente logra el cometido: afectar de forma considerable el software del

aparato hasta **conseguir datos personales de la víctima con los cuales poder robarla o estafarla.**

Este es el caso de una nueva forma de suplantación y robo de información que tiene a una supuesta **‘copia de seguridad de mensajes de WhatsApp’** como protagonista.

El Instituto Nacional de Ciberseguridad de España (Incibe) publicó un informe en el que notifica la existencia de una “campaña de correos electrónicos suplantando la identidad de WhatsApp cuyo mensaje contiene un enlace que descarga un troyano en el dispositivo”.“El correo electrónico simula ser una copia de seguridad de las conversaciones de WhatsApp y el histórico de llamadas, instando al usuario a pulsar sobre el enlace para descargarlo”, añade el documento.

Ahora bien, el simple hecho de descargar el archivo no afecta de forma considerable el dispositivo en el que se ha bajado la data. Lo recomendado por los expertos es **eliminar de forma inmediata el archivo del computador, celular o tablet y borrar del todo el email que llegó al correo con el documento adjunto malicioso.**

Sin embargo, el verdadero problema radica en descargar y abrir el archivo, ya que es en ese proceso donde el malware se desata y empieza a afectar el equipo o terminal.

“Si ha descargado y ejecutado el archivo malicioso, es posible que su dispositivo se haya infectado. Para proteger su dispositivo, debe escanearlo con un antivirus actualizado”, explicó Incibe; aunque tampoco son muchas las esperanzas que quedan de evitar un daño mayor en el aparato. Mensaje recibido en el correo electrónico. Foto: Incibe

¿Cómo evitar caer en esta trampa?

Así como sucede en este ejemplo, en la mayoría de los casos la mejor “medicina” es la prevención. **No confiar demasiado y**

aprender a conocer las estrategias usadas por los ciberdelincuentes, es una buena forma de cuidar al máximo su privacidad.

Por esto es importante nunca pulsar sobre un enlace sino se está 100 % seguro de la confiabilidad del mismo. Tampoco es recomendable descargar un archivo adjunto sin antes comprobar la veracidad tanto del correo como de la información suministrada en el mensaje.

Lo mejor es ponerse en contacto con la persona o empresa citada en el e-mail (en este caso WhatsApp) y de esta manera cerciorarse de la autenticidad de los datos. Además, usted puede estar atento a la información actualizada que entregamos en Infobae para no caer en engaños.

Asimismo, se recomienda revisar de forma exhaustiva el texto y remitente del mensaje con el fin de intentar hallar irregularidades ortográficas y gramaticales, además de diferencias claras entre la dirección web original de WhatsApp y la que muestran los delincuentes en el e-mail.

“No facilite sus datos personales **(número de teléfono, nombre, apellidos, dirección o correo electrónico) o bancarios en cualquier página**. Infórmese previamente y lea los textos legales de la web para descartar un posible mal uso de sus datos”, agrega la entidad española.

Cabe recordar que por ahora la única forma que tiene WhatsApp para crear copias de seguridad es por medio de su aplicación por lo que no se debe confiar en ningún otro supuesto método que prometa cumplir con este objetivo, ni en su celular ni en su computador.

Fuente: Infobae