Publicado en Madrid el 09/07/2020

Preocupante aumento de ciberriesgos en las aplicaciones de citas

La empresa de ciberseguridad S2 Grupo ha advertido de que el auge de las apps de citas ha impulsado la presencia en ellas de ciberdelincuentes que buscan principalmente robar fotografías o vídoes, extorsionar o conseguir algún tipo de beneficio económico. En este sentido, la compañía ha elaborado un listado con las cico principales ciberamenazas en estos entornos digitales

“Si antes era raro ligar por Internet, ahora casi que es extraño no hacerlo. Y, por supuesto, no hay ningún problema en esto. Sólo tenemos que tener presente que en cualquier ámbito donde se implanta la tecnología, hay posibilidad de que se cuele la ciberdelincuencia. Y esto requiere, que utilicemos estas aplicaciones de citas con responsabilidad, sabiendo que todo aquello que compartamos o publiquemos en ellas podría convertirse en información de dominio público. Entre el sexting y la sextorsión sólo hay un paso”, ha explicado José Rosell, socio-director de S2 Grupo.

“Estas aplicaciones no sólo las usan las personas que quieren tener una cita. Son también utilizadas con otros fines como puede ser conseguir fotografías o, incluso, extorsionar a las víctimas. Otros llegan a conseguir una relación de confianza y de vínculo con una persona para que, cuando ésta baja la guardia, conseguir algún beneficio económico o directamente pedirle dinero”, ha alertado Miguel A. Juan, socio-director de S2 Grupo

Estos son algunos de los ciberriesgos más comunes en las aplicaciones de citas:

Pasar del sexting a la sextorsión.- Si bien el primer contacto suele ser a través de mensajes de texto en las propias apps, en seguida se suele pasar a comunicarse a través de otras plataformas como Whatsapp, Instagram o Snapchat. El objetivo suele ser enviar fotos o vídeos subidos de tono, el conocido “sexting” o, como dicen los jóvenes, “hacer nudes”. Desde S2 Grupo se ha señalado que esta es una práctica de elevado riesgo tanto si se realiza con alguien de confianza (en el futuro no se sabe qué relación se tendrá) y, todavía más, con un desconocido. “Debemos tener en cuenta que muchos perfiles son falsos y se han creado precisamente para obtener fotos de este tipo y, luego, chantajear de alguna forma. Así se pasa del sexting a la sextorsión”, ha señalado José Rosell.

La propia cita con un desconocido.- Mas allá de poder ser víctimas de una estafa o chantaje económico, uno de los peligros más graves es que el supuesto agresor quiera quedar en persona con la víctima. Por ello, se recomienda no dar información personas, no enviar fotografías y, si hay cita, hacerlo en un lugar público.

No verificar la “realidad” de la persona.- Es muy importante utilizar aplicaciones como Tineye.com o Google Images para comprobar que las imágenes de la persona con la que se esetá hablando son reales y verificar que no corresponden a un perfil falso.

Ganarse la confianza para pedir dinero.- Ésta práctica también es una de las más frecuentes. Consiste en crear una gran relación de intimidad y, cuando ya está lograda la confianza, aludir a una enfermedad, problema del pasado o similar, para lo que se requiere dinero y, entonces, se le pide a la víctima. Por supuesto, siempre se le argumenta que se le devolverá, pero no es así y suele desaparecer.

Distribución de malware.- “No debemos olvidar de que muchas veces los ciberdelincuentes se esconden bajo perfiles atractivos para ser ellos los que, con la excusa de enviar fotos, colar malware que infecte los equipos de las víctimas o instalen programas espía, por ejemplo, para conocer sus contraseñas, datos bancarios, conversaciones, etc.”, apostilla Miguel A. Juan.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Sociedad E-Commerce Ciberseguridad Dispositivos móviles