Sextorsión, grooming y otros peligros de las RRSS

Las Redes Sociales (RRSS) han ido ocupando nuestro espacio vital casi sin darnos cuenta. Y ciertamente son muy útiles en muchos casos. Pero también hay que ser conscientes de sus peligros y de lo bien que aprovechan sus debilidades los ciberdelincuentes. En este artículo les explicamos algunos de los últimos casos detectados, como el grooming o la sextorsión.

Sextorsión, grooming y otros peligros de las RRSS

Seguramente el rey de las aplicaciones sea **WhatsApp**. Sus datos no dejan lugar a dudas: Más de 2 mil millones de personas en más de 180 países usan WhatsApp. Una aplicación gratuita, que posibilita el contacto con amigos, familiares, compañeros de trabajo, crear grupos de todo tipo... Pero el rey no ha estado nunca exento de críticas ni de acusaciones de poca transparencia. Por eso los ciberdelincuentes ya se han ocupado de encontrar las rendijas de seguridad para idear en su lado oscuro.

Hace relativamente poco WhatsApp ha incorporado **la opción de enviar fotos y vídeos que desaparecen de los mensajes enviados nada mas ser visualizados por el destinatario**. «Visualización única» es el nombre de esta opción que otras plataformas como Telegram ya habían implantado. Pensada en principio para aumentar la seguridad de los usuarios, los ciberdelincuentes han visto rápidamente que la opción permite hacer capturas de pantalla. Y eso puede usarse con fines delictivos. El más conocido es la extorsión por motivos sexuales, un delito que la Secretaría de Estado de Seguridad reconoce que ha aumentado un 46% desde el año 2018.

En esta misma línea delictiva encontramos el ***grooming***, que es el acoso y abuso sexual de menores por parte de adultos. Esta práctica es mucho más común en **TikTok**, la red social preferida por los adolescentes en este momento. Crear un perfil falso, fingir ser un menor o un *influence*r es pan comido para los delincuentes que generan un vínculo de confianza que les lleva a solicitar contenidos sexuales. A partir de aquí, con la captura de WhatsApp o con los contenidos de TikTok, **el criminal hace chantaje para no divulgar estos contenidos.** Puede pedir dinero o favores como enviar nuevos contenidos sexuales.

Instagram también se ha convertido en un problema, porque se pueden hacer ataques bajo demanda. En este caso también se aprovechan de los sistemas de protección de Instagram y **a cambio de un pago se puede inhabilitar cuentas de otros usuarios.** El *modus operandi* es sencillo: desde foros clandestinos se publicitan trabajos para inhabilitar cuentas particulares de Instagram. Las ofertas de servicios para inhabilitar cuentas suelen ser baratas, lo que facilita la extorsión a todo tipo de usuarios. Además, a este tipo de ciberdelito se le añade el proceso contrario: pagar por restaurar una cuenta eliminada.

Es fácil imaginar que los ciberdelincuentes capaces de usar las RRSS para estos hechos delictivos también lo tienen fácil para copiar, usurpar, falsificar o robar producto físico o digital. Posteriormente chantajear a los verdaderos propietarios de esos productos, que además verán mermada muy seriamente su reputación online. Todos estos problemas pueden solucionarse o anticipándose a ellos con los servicios que ofrece ProMonitor y que pueden ver **AQUÍ.**

En la web de **Panda Security**, una empresa especializada en la creación de productos de seguridad, pueden leer un interesante artículo donde se explica el

significado de sexting y sextorsión.

También encontrarán mucha información en la web **PantallasAmigas.net**. Se trata de una iniciativa de la **Fundación Edex**, una organización no lucrativa dedicada al desarrollo positivo de menores y adolescentes. Pantallas Amigas nació en el año 2004 con la misión de la promoción del uso seguro y saludable de Internet y otras TIC, así como el fomento de la ciudadanía digital responsable en la infancia y la adolescencia.

Imagen principal: Gerd Altmann en Pixabay