Privacidad en redes sociales: Lo que no te están contando. Parte II

En esta segunda entrada sobre privacidad en redes sociales, vamos a tratar las actividades de riesgo que se dan habitualmente en redes sociales y de las que cualquiera puede ser víctima.

Ahora que ya hemos hablado de lo que pasa con nuestros datos cuando compartimos información en redes sociales y de qué hacen empresas como Google o Facebook con ellos, es el momento de considerar cuáles son los datos más susceptibles de crear situaciones de riesgo para nuestra privacidad.

Es importante tener en cuenta que, aunque estas actividades sean peligrosas y puedan evolucionar en delitos, no todas ellas son delitos *per se*.

Estas cinco actividades son las que consideramos de alto riesgo en redes sociales, ya que todas ellas implican la exposición de información personal a terceros.

SEXTING

GROOMING

CIBERBULLYING

HACKING

PHISHING

Sexting
Consiste en el envío de mensajes con contenido pornográfico a través de redes sociales.
El principal peligro está en la posibilidad de que esa foto sea obtenida por terceros.
También puede llevar a situaciones embarazosas.
Es importante conocer al destinatario de los mensajes antes de enviarlo para evitar algunos de estos peligros

Grooming
Es un conjunto de conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la confianza de un menor de edad creando una conexión emocional con el mismo con el fin de disminuir sus inhibiciones y poder abusar de él.

Ciberbullying
también denominado acoso virtual, se realiza a través de redes sociales o medios de comunicación digitales para acosar a una persona mediante ataques personales y/o divulgación de información confidencial o falsa entre otro medios.
Implica un daño recurrente y repetitivo infligido a través de los medios electrónicos

Hacking
En términos generales el Hacking incluye actividades orientadas a romper la seguridad de ordenadores y/o servidores.
En el caso de hacking de redes sociales consiste en hacerse con la información entregada por los usuarios en sus perfiles de redes sociales, por lo que una de las medidas de seguridad más importantes es controlar qué y cuánto se comparte en ellas.
Los hackers clonan perfiles de Facebook o twitter y diseñan juegos o pasatiempos con el fin de hacerse con más información e incluso contraseñas.

Phishing
Es un método que los ciberdelincuentes utilizan para engañar a las víctimas y conseguir que revelen información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias.
Generalmente los delincuentes se hacen pasar por otras personas o entidades (como bancos) por medio de mensajes de correo electrónico u otras redes sociales como facebook e intentan que parezca una comunicación confiable y legítima y el usuario responda con sus contraseñas e informaciones confidenciales.

Recomendaciones de seguridad:
- ✓ Cambiar periódicamente la contraseña.
- ✓ Utilizar contraseñas de acceso diferentes para cada red social
- ✓ Establecer contraseñas que no sean correlativas o con variantes obvias unas de otras
- ✓ Emplear siempre la página oficial de cada red social para entrar en ella, ya que circulan accesos que simulan serlo pero en realidad están pensados para hacerse con la contraseña.

Ahora ya sabéis qué significan las actividades de riesgo en las redes sociales y cuáles son los riesgos que conllevan. Recordad que lo más importante es tener un control total sobre la cantidad y la calidad de la información que se comparte en internet y a través de redes sociales.