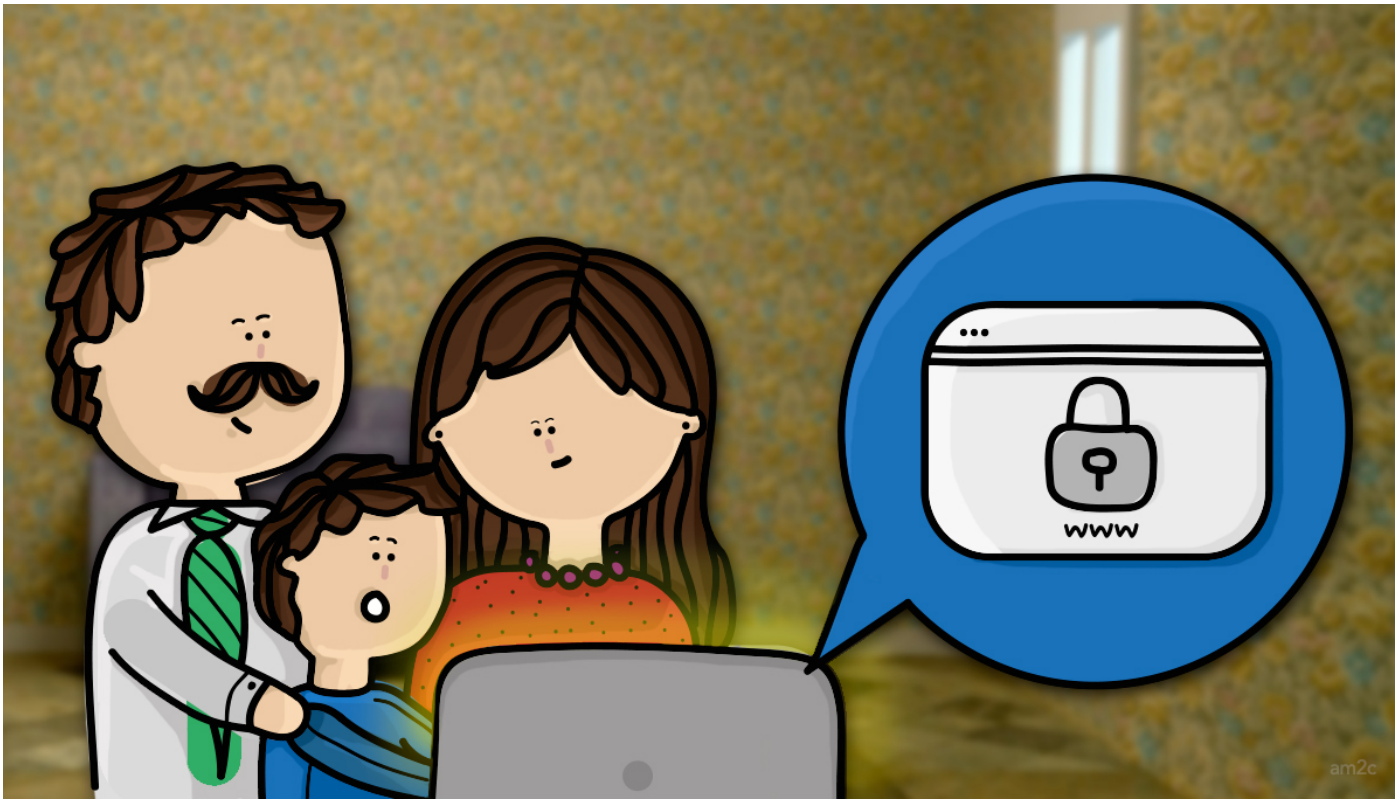
Published on *Revista .Seguridad* (http://revista.seguridad.unam.mx)

AMENAZAS Y RECOMENDACIONES PARA MENORES DE EDAD EN EL USO DE LA TECNOLOGÍA

Héctor Jesús Pérez Mancilla

sexting

numero-28



En la actualidad, vivimos en un mundo gobernado por la campaña mediática del consumo y la facilitación de las tecnologías de información. Cada día, en cualquier parte del mundo, las personas consumen diversos productos y servicios al hacer uso de nuevas tecnologías de información, sin que los usuarios se den cuenta de la gran cantidad de datos personales que son compartidos y muchas veces sin que estén conscientes de la forma en que permiten que estos sean difundidos. Los menores de edad están expuestos en este contexto.

En este artículo abarcaremos los delitos informáticos más utilizados por las diferentes organizaciones criminales y los más combatidos por las organizaciones gubernamentales y sociales.

RIESGOS

Cada día es más frecuente la tendencia de regalar a los menores de edad dispositivos electrónicos sin ninguna concientización previa o sin alguna recomendación de uso, manejo y cuidado de la información personal.

Es de esperarse que la delincuencia organizada, como grupos enfocados en el sector de la pedofilia, la trata de personas o en la recolección de datos personales para campañas mediáticas, también estén enterados de este tipo de vulnerabilidades en prácticas inculcadas a los menores de edad:

- Entregar información a quien les pregunte
-

Obedecer a los adultos

- No cuestionar a los adultos
- Los que son más atentos en sus respuestas, son mejor catalogados por los adultos
- Deben ser agradecidos y corresponder a los adultos por educación (Rosas, Florentina, 2010)

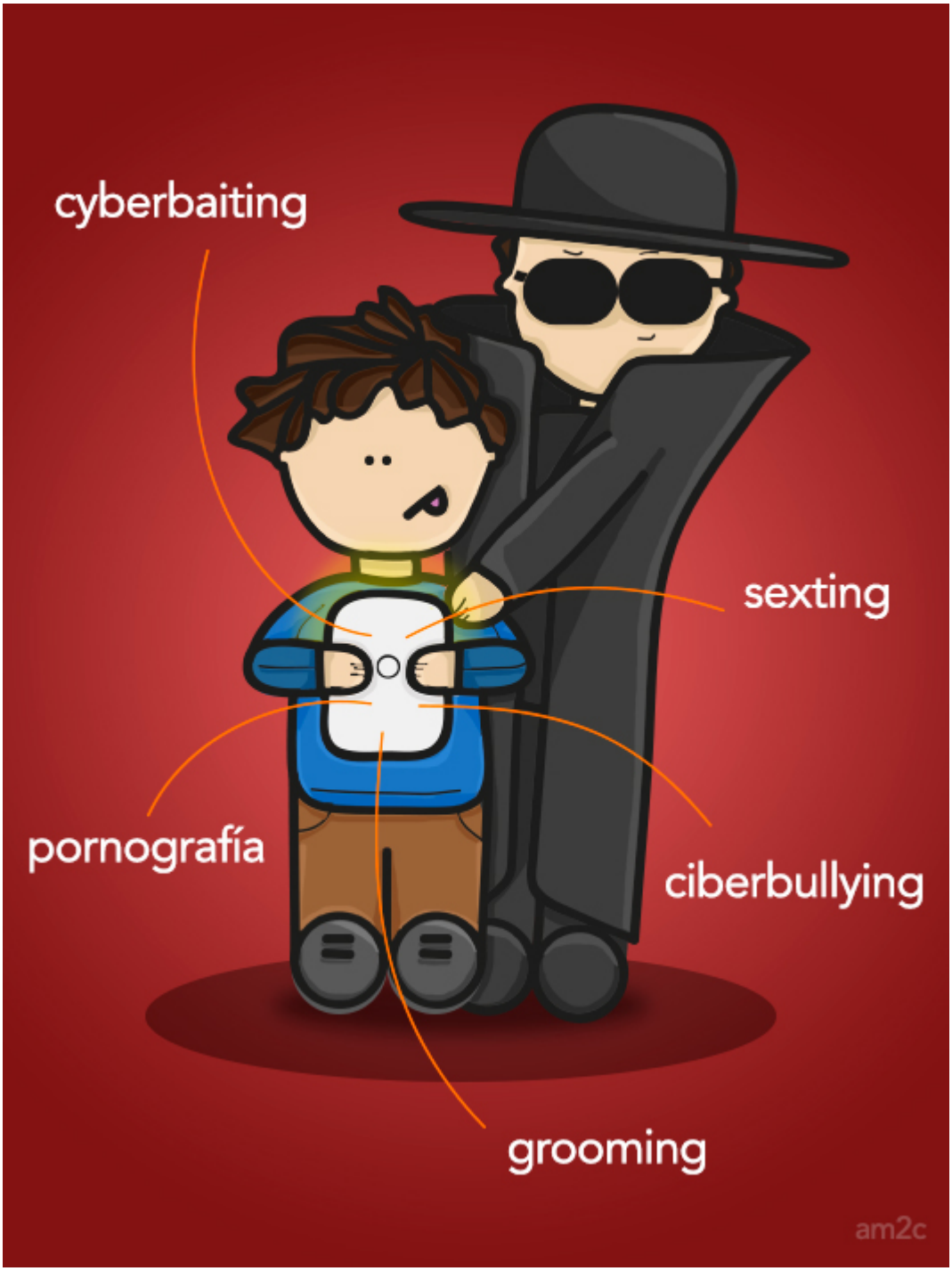
Estas vulnerabilidades son buenas costumbres que enseñan los padres o familiares a los menores y las organizaciones delictivas hacen uso de ellas, explotándolas y convirtiendo el riesgo en una amenaza latente contra los menores, porque hay una clara falta de concientización en cómo deben manejar estos la información que saben.

El Programa de Inclusión y Alfabetización Digital del gobierno federal mexicano es una gran campaña que otorga tabletas inteligentes a los niños para dar un acercamiento tecnológico a las diferentes escuelas en diferentes grados escolares. Sin embargo, el único problema que se debería contraatacar es la falta de implementación de un programa de concientización para los maestros, los padres de familia y los estudiantes a los cuales se les entregan estas tecnologías, ya que corren el riesgo de revelar información y datos personales en un nivel de exposición peligrosa, que va desde conceder permisos excesivos a aplicaciones gratuitas o con costo.

Por ejemplo, existen casos bien documentados y muy conocidos (Trend Micro, 2011) de aplicaciones que solicitan acceso a muchas características cuando el único recurso al que deberían acceder en un dispositivo móvil como un smartphone o una tableta es a la linterna, pero se le asignan permisos excesivos tales como la localización, acceso a la cámara fotográfica y de video, a los contactos y a las modificaciones al sistema del dispositivo; el usuario, con la finalidad de utilizar la aplicación, accede a la concesión de los permisos sin una previa concientización. Cualquier persona, no necesariamente un niño, proporcionará los permisos con tal de obtener y utilizar la aplicación en ese momento.

El otorgar tantos permisos a una aplicación podrá permitir el uso y difusión de la información del dispositivo electrónico, más allá de la toma de imágenes, en ocasiones en las que el usuario no esté utilizando la cámara fotográfica de su dispositivo. Una fotografía de un menor de edad desnudo en el mercado negro no puede valer más allá de un dólar americano y un video en la misma situación no valdrá más allá de cinco dólares americanos (García, Colmenares, 2015), pero la problemática a combatir es que las fotografías y los videos se convertirán en parte de bibliotecas con un amplio repertorio que diferentes organizaciones criminales comercializarán en todo el mundo, propagando los datos, las imágenes y los videos de los menores, pudiendo haber prevenido la captura de estos con una correcta concientización por parte de los padres, los maestros y los adultos.

Los delitos informáticos más utilizados por organizaciones criminales son:



- Sexting: es el uso de dispositivos móviles y computadoras para el intercambio de mensajes o contenido sexual. Este contenido debe considerarse inapropiado en el momento en que el canal de conversación es abordado por menores de edad y existe una revelación inadecuada de la información por parte de algún integrante del canal de conversación.

- Ciberbullying: acoso, amenazas y agresión son algunos de los componentes de este delito a través de Internet. Esta situación entre menores de edad semejante es más compleja por la

impotencia que experimentan los jóvenes al no poder ejercer ninguna acción o tener miedo a lo que puedan realizar los padres de familia al conocer la situación.

- Grooming: es la acción de desnudar a menores de edad por medio de engaños y recopilar sus imágenes por una *webcam*. La mayoría de los atacantes que realizan este delito son adultos adoptando la falsa identidad de menores (utilizando el factor psicológico de confianza denominado “factor espejo”), ganando la confianza del menor simulando tener su edad, problemas y gustos similares. Ahora, con el uso de los dispositivos móviles se ha incrementado el *grooming* ya que, con la utilización de estos mismos, no existe la supervisión o vigilancia continua de los padres o un adulto responsable. En muchas ocasiones, ya no se requiere la interacción directa del atacante al poder establecer una interacción por medio de aplicaciones maliciosas, programadas para la recolección de imágenes.

- Pornografía: aunque en algunos países es un entretenimiento legal, siempre y cuando los participantes o actores sean considerados mayores de edad y las relaciones sexuales se lleven a cabo con consentimiento, la pornografía de menores de edad es muy recurrente y existe la distribución de este material sin autorización.

- Ciberbaiting: Esta práctica es una forma de ciberbullying, con la diferencia de que son los menores quienes acosan a sus maestros por medio de Internet. En estas prácticas se burlan de los docentes, los violentan verbalmente y humillan públicamente.

CONTRAMEDIDAS A LOS DELITOS INFORMÁTICOS

La prevención concreta al sexting es indicar a los menores de edad que la información que se proporciona por medio de dispositivos móviles, equipos de cómputo o a través de la distribución a pedimento de contenido es sensible y podría poner en riesgo su integridad o afectar su imagen.

Para el ciberbullying la forma de prevención es a través de la concientización sobre el uso correcto de los dispositivos móviles con los menores, así como el abordar a tiempo el acoso verbal y físico que es muy frecuente en los centros de estudio, evitando que el acoso se convierta en formas físicas de agresión.

El grooming es inversamente proporcional a la supervisión de padres de familia, por lo que se debe vigilar la instalación de aplicaciones en los dispositivos móviles de los menores y monitorear recurrentemente a los contactos en redes sociales.

Si deseamos evaluar si los menores están protegidos contra estos ataques o delitos o, aún mejor, si deseamos saber si nuestros hijos son o no generadores de estos delitos, debemos de poder contestar las siguientes preguntas:

- ¿Sabemos qué hacen nuestros hijos con sus dispositivos electrónicos?
- ¿Para qué los utilizan?
- ¿Qué usos les dan a las características de los dispositivos?

- ¿Sabemos el contenido de los dispositivos de nuestros hijos?
- ¿Sabemos qué redes sociales consultan?
- ¿Cómo obtuvieron el acceso a las redes sociales?
- ¿Quiénes son sus amigos o contactos en sus redes sociales?
- ¿Quiénes son sus contactos en su dispositivo móvil?

- ¿Cuidamos sus datos personales?
- ¿Qué información personal tienen autorizado entregar?
- ¿Han compartido imágenes o información de ellos en forma que les dé pena contar?

- ¿Sabemos que no incurren en algún delito a través de sus dispositivos electrónicos?
- ¿Sabemos si son generadores de ciberbaiting, sexting y ciberbullying?

CONCLUSIONES

Entre las recomendaciones que deben darse a los padres de familia, maestros y personas que interactúan de alguna forma con menores de edad o niños que hacen uso de dispositivos móviles se encuentran:

1. La responsabilidad de un dispositivo electrónico no termina con la entrega o regalo de uno, esta apenas comienza y debe darse un seguimiento constante de su uso correcto.
2. Enseñar al menor a utilizar el dispositivo adecuadamente e indicarle para qué fue diseñado, con el fin de evitar un mal uso del smartphone o tableta que conlleve al menor a un delito cibernético.
3. Concientizar al menor para que no proporcione información a personas desconocidas o que conoció en alguna red social.
4. Educar al menor de edad a no compartir imágenes o fotografías de sí mismos en ninguna red social. Enseñarles a que las personas pueden compartir fotografías de él o ella siempre y cuando no involucren imágenes deshonrosas o que lo hagan sentir en un estado incómodo.
5. Los padres pueden realizar una revisión periódica de los dispositivos electrónicos del menor de edad, como las computadoras, los teléfonos inteligentes y las tabletas, a las listas de contactos, a

los accesos a redes sociales, el uso de la cámara fotográfica y la geolocalización del dispositivo en las aplicaciones y las fotografías tomadas.

6. Concientizar de forma constante sobre los delitos más comunes a los que están expuestos, cómo cuidarse de estos y cómo no generar los mismos.

7. Formar grupos integrados por padres de familia, maestros y autoridades en los cuales se puedan concientizar sobre los delitos a los que están expuestos los menores de edad.

8. Mantener un contacto constante con autoridades especializadas en temas de ciberdelincuencia enfocados a menores de edad, para que apoyen en el desarrollo correcto de un programa de vigilancia permanente a maestros y alumnos. Aunado a esto, seguir cualquier comunicado de fuentes confiables sobre amenazas y vulnerabilidades detectadas en dispositivos electrónicos y aplicaciones que nos afecten de forma directa.

9. Tener una comunicación clara, sincera y abierta entre padres, maestros y menores de edad para atender cualquier duda o interés.

10. El más importante es que la responsabilidad de la educación no es únicamente de los maestros y directivos escolares, conlleva un compromiso de todos los adultos involucrados en la sana convivencia en el medio del menor de edad. Ellos deben de atribuirse y asumir la responsabilidad y compromiso del buen uso de los dispositivos móviles y de cómputo a los cuales tenga acceso.

REFERENCIAS

- García, J.C., Colmenares, L.E. (Abril-Junio 2015). Pornografía y explotación sexual infantil, efectos sociales y la tecnología. Pornography and child explotation. *Revista Visión criminológica-criminalística*. *Año 2 número 10 Abril-Junio 2015.* Recuperado de: http://revista.cleu.edu.mx/new/descargas/1503/Art%C3%ADculo2_pornograf%C3%ADa_infantil.pdf
- Rosas, RF.; Florentina, R. (2010). Aspectos Generales y Jurídicos de la Pederastia. Recuperado de: http://reposital.cuaed.unam.mx:8080/jspui/bitstream/123456789/880/1/Pederastia.pdf
- Trend Micro. (2011). *Cuando las aplicaciones de Android piden más de lo que necesitan*. Recuperado de: http://www.trendmicro.es/media/br/ebook-when-android-apps-want-more-es.pdf

Si quieres saber más, consulta:

- Redes sociales en la escuela
- Reputación en línea
- Criminalística aplicada en la seguridad de tecnologías de información y comunicaciones