06

Situaciones de riesgo en el entorno Web 2.0:

Suplantación de identidad, Ciberbullying, Grooming, Sexting.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ÍNDICE

I. OBJETIVOS

- **Concienciar** a los menores de que deben ser muy cuidadosos con los datos de carácter personal que desvelan al utilizar los servicios de la Web 2.0.
- **Dar a conocer los riesgos** que pueden generarse de un uso inadecuado de los datos de carácter personal en la Web 2.0.
- **Ofrecer consejos** que faciliten un uso consciente de los datos personales en la Web 2.0.
- **Saber qué hacer y a quién acudir** en caso de ser víctima de una de estas situaciones.

II. CONCEPTOS

1. RIESGOS, MENORES Y SERVICIOS WEB 2.0.

El uso de los servicios que componen la Web 2.0 (*buscadores, plataformas colaborativas, redes sociales, servicios de video online, blogs, wikis, etc.*) por parte de niños y adolescentes supone en, la mayoría de los casos, ocio, entretenimiento, relacionarse con los amigos, una forma de conocer gente y de habituarse al uso de las nuevas tecnologías, que van a ser necesarias para el desarrollo de su personalidad, de las habilidades propias en la era tecnológica y de su consolidación posterior.

Sin embargo, como cualquier adaptación a un nuevo entorno social, el uso de los servicios que componen la Web 2.0 tiene aparejados ciertos riesgos que aumentan cuando el individuo forma parte de un colectivo de especial vulnerabilidad, como es el de los menores: niños y adolescentes. A los integrantes de este colectivo se les denomina "nativos digitales" (*debido a su conocimiento del medio y sus posibilidades, pues han nacido ya con Internet*) sin embargo, su comportamiento se caracteriza principalmente por una ausencia de percepción del riesgo y una sensación de "control" sobre su vida, en la que se incluye su "vida *online*, su experiencia digital".

Estas características, llevadas a un entorno que ofrece muchas ventajas, pero en el que también aparecen riesgos, hacen necesario una adecuada información para, si no eliminar del todo, sí disminuir las situaciones negativas a las que se pueden enfrentar los niños y adolescentes y sus familias.

Los principales riesgos a los que se enfrentan los menores se pueden clasificar en riesgos de acceso a contenido inapropiado, riesgo de adicción y riesgos de acoso.

Las dos primeras situaciones de riesgo señaladas (contenidos inapropiados y adicción) no están directamente relacionadas con la privacidad de los usuarios, sino con otros elementos psicosociales de este colectivo, sin embargo, situaciones como la suplantación de identidad, el *ciberbullying, grooming, sexting*, etc., en muchas ocasiones comparten **una inadecuada gestión de la privacidad**, ya sea por descuido del usuario o por engaño de terceros.

Estas situaciones, dado el entorno tecnológico en el que se producen y la posibilidad de expansión viral de aquellos contenidos o informaciones lesivas, llegan a anular o dificultar la capacidad de reacción de las víctimas, situándolas en una posición de indefensión y vulnerabilidad.

a) Suplantación de identidad

Con la suplantación de identidad una persona se hace pasar por otra diferente. Se puede definir como **la apropiación indebida de la identidad de una persona por un tercero y la actuación de éste en su nombre**. Es una de las situaciones que se pueden producir en la utilización de los servicios de la Web 2.0. En estos casos una persona utiliza el nombre y demás datos personales de otra persona haciéndose pasar por ella. Son pues datos de carácter personal los que se utilizan.

Ejemplos de estas conductas:

- La creación de un perfil de un tercero en una red social.
- La utilización del perfil real de otra persona en una red social, previa obtención ilegitima de las claves de acceso.
- La utilización de la cuenta de correo de un tercero, previa obtención ilegítima de las claves de acceso.
- La utilización del teléfono u otro dispositivo móvil de un tercero sin su consentimiento, enviando mensajes o imágenes para que se le atribuyan a ese tercero.

Consecuencias de la suplantación de identidad.

La suplantación de identidad puede originar graves consecuencias para la persona suplantada. En su nombre se pueden realizar comentarios, juicios, afirmaciones, amenazas, provocaciones,… que atenten gravemente contra su intimidad, honor o integridad física.

Asimismo, puede dar lugar a la exigencia de responsabilidades civiles y penales a los autores de estas conductas.

b) Ciberbullying o Ciberacoso

Es una situación de acoso, hostigamiento, insultos, vejaciones, incluso chantaje, de un menor a otro a través de medios de los servicios de la Web 2.0 tales como blogs, correo electrónico, la mensajería instantánea, las redes sociales, la mensajería de texto a través de teléfonos o dispositivos móviles o la publicación de vídeos y fotografías en plataformas electrónicas de difusión de contenidos.

Características principales de esta forma de acoso son las siguientes:

- Que la situación de acoso se dilate en el tiempo. Quedan excluidas las acciones aisladas.
- Que no cuente con elementos de índole sexual, (aunque también podría albergar elementos de este tipo).
- Que víctimas y acosadores sean iguales, menores de edades similares.
- Que el medio utilizado para el acoso sea tecnológico.

Son ejemplos de esta forma de acoso los siguientes:

- Publicar fotos o vídeos comprometidos que puedan avergonzar a la víctima y enviárselas a su círculo de amigos.
- Inscribir la dirección de correo electrónico en Webs de servicios publicitarios para que luego sea víctima de Spam, de contactos con desconocidos,…

- Crear rumores respecto de la víctima atribuyéndole un comportamiento reprochable, ofensivo o desleal, para que reciba represalias de terceros.
- Acciones que generan acoso a partir de la suplantación de la identidad:
    - Crear un perfil falso o un blog con los datos de la víctima donde aparezcan a modo de confesiones determinados acontecimientos de la vida privada de ésta.
    - Hacer comentarios ofensivos en chats, foros, comunidades participando agresivamente de manera que las reacciones vayan posteriormente dirigidas a quien ha sufrido la usurpación de identidad.
    - Hacerse con la contraseña del perfil en una red social, y modificarla de forma que la víctima no pueda acceder, para posteriormente publicar en el muro contenidos inapropiados que deriven en algún tipo de responsabilidad.

Elementos que facilitan la aparición de estas conductas:

- La proliferación de dispositivos de teléfonos móviles, tablets, etc., con cámara de foto y vídeo y su conexión a Internet.
- La sensación de anonimato que otorga Internet a los usuarios.
- La arquitectura de participación y difusión de los servicios de la Web 2.0. La denominada reputación online es un atractivo para los acosadores. Sus "fechorías" las va a conocer todo el mundo, formándose así una reputación, en principio querida por el acosador.

De nuevo, hay que recordar que este tipo de conductas pueden dar lugar a la exigencia de responsabilidades civiles y penales.

c) Grooming

Es una situación de acoso y chantaje a un menor de edad por un adulto. Ya no estamos hablando de una situación entre menores, sino que una de las partes, el acosador, es un adulto, que se hace pasar por un menor para llegar a su víctima. Si bien puede responder a las mismas finalidades que el *ciberbullying*, lo que caracteriza al *grooming* es que este acoso tenga una intención sexual. Se puede definir como el *acoso ejercido por un adulto y se refiere a las acciones realizadas deliberadamente para establecer una relación y control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual explícito o implícito.*

En la mayoría de los casos se llega a esta situación por medio del engaño del adulto que se hace pasar por menor para aproximarse a su víctima, conseguir ser su amigo y obtener la información necesaria para el acoso. Es habitual que se trate de imágenes o informaciones comprometedoras, que van a permitir chantajearla con difundirlas una vez conseguida o robadas las contraseñas o las libretas de direcciones electrónicas.

Una vez que el acosador se hace con la contraseña y se apodera de la libreta de direcciones electrónicas dispone de los medios para lograr de la víctima los propósitos que persigue que como hemos dicho, son de carácter sexual, amenazándola a la víctima con hacer llegar a sus padres, amigos y conocidos la información que ha conseguido mediante engaño si no accede a sus deseos.

Se pueden diferenciar varias fases en esta forma de acoso:

- **Fase de amistad**. Toma de contacto con el menor de edad para conocer sus gustos, preferencias y crear una relación de amistad con el objeto de obtener su confianza.
- **Fase de relación**. La constituyen con frecuencia confesiones personales e íntimas entre el menor y el acosador. Consolida la confianza y se profundiza en la información sobre su vida, gustos y costumbres.

- **Componente sexual**. Incluye la descripción de términos específicamente sexuales y la petición a los menores de su participación en actos de naturaleza sexual, grabación de imágenes o toma de fotografías.

El *grooming* constituye un delito de los previstos en el código penal contra la libertad y la indemnidad sexual.

d) Sexting

El *sexting* consiste en la difusión o publicación de fotografías o vídeos de contenido sexual producidos por el propio remitente, utilizando para ello el teléfono móvil u otro dispositivo tecnológico.

Es importante tener en cuenta que, desde el momento en que su contenido se difunde, el autor pierde el control, pudiendo tener una difusión ilimitada (por reenvío masivo, viralidad de los contenidos en redes sociales, etc.).

Características:

- **Voluntariedad inicial**. Estos contenidos son generados por sus protagonistas o con su consentimiento.
- **Dispositivos tecnológicos.** Utilización de dispositivos tecnológicos que, al facilitar su envío a otras personas, también hacen incontrolable su uso y redifusión a partir de ese momento.
- Puede dar lugar a situaciones de ***ciberbullying***, ***sextorsion*** (chantaje en el que alguien utiliza estos contenidos para obtener algo de la víctima, amenazando con su publicación) y, dependiendo del poseedor ilegitimo de las imágenes, también puede dar lugar a ***grooming***.
- **Cesión al chantaje.** La víctima, ante la posibilidad de la difusión de imágenes sensibles que la comprometerían, puede tomar la decisión de acceder al chantaje, que normalmente consiste en seguir enviando fotografías o vídeos de carácter sexual e incluso a realizar concesiones de tipo sexual con contacto físico.
- De esta manera, el menor puede entrar en una espiral cuya salida pasa por no acceder a las pretensiones del hostigador y comunicar la situación a un adulto.

Elementos que facilitan la aparición de estas conductas:

- La atracción por la conducta transgresora propia de adolescentes.
- Falta de cultura de privacidad en los menores. No perciben amenazas para su privacidad con la publicación de contenidos en Web 2.0. Menor consciencia del riesgo y exceso de confianza, son "nativos digitales". Falta de experiencia y de perspectivas.
- Utilización incontrolada de la Webcam.
- Sustracción del dispositivo donde se alojan los videos o imágenes tanto del autor como del destinatario, ruptura de relaciones con el destinatario, etc.
- Inmediatez de las comunicaciones electrónicas.

2. CONSEJOS

- Nunca utilices tu nombre verdadero. Usa apodos o pseudónimos (*nicks*) para operar en Internet, que no pongan en entredicho la seguridad de tu vida personal. Únicamente será conocido por el círculo de contactos que saben el *nick* que empleas en Internet.
- En la dirección de correo electrónico evita dar información que pueda identificarte, por ejemplo, no incluyas el año de nacimiento.
- Usa la función de copia oculta (CCO) para mandar correos electrónicos a varias personas. No publiques la dirección de correo electrónico en sitios Web. No participes en mensajes en cadena.
- Relee los mensajes antes de enviarlos.
- Cuidado con los amigos en las redes sociales. No agregues como amigos en la Red a personas que no conozcas. Mucho cuidado con los amigos de amigos, pues pueden no ser gente verdaderamente conocida por ellos. Debes tener en cuenta que la adecuada gestión de la privacidad por un usuario no implica que sus amigos también la lleven a cabo.

- Abandona páginas web, chats o foros donde se den situaciones incomodas o desagradables. Recuerda que SON LOS USUARIOS LOS QUE CONTROLAN LA SITUACIÓN y que con un solo click pueden terminar con aquello que les incomoda.
- No facilites datos personales si no sabes a quién y para qué se necesitan. Nunca des tus datos a desconocidos. Sé muy cuidadoso con la información privada que facilitas, incluida la información sobre tu familia o amigos.
- Utiliza contraseñas difíciles de adivinar adivinar (que incluyan números, letras, símbolos) y recuerda que debe ser secreta. No debes compartirla con amigos.
- Pide permiso a otros si se va a facilitar su información. No publiques imágenes de otros en Internet sin su autorización.
- Utiliza la webcam sólo con personas de confianza. No hagas delante de ella nada que no hicieras en público. Tápala cuando no la uses o gírala hacia un punto muerto.
- Si te encuentras ante una de las situaciones que hemos visto DEBES PEDIR AYUDA a UN ADULTO DE CONFIANZA (padres, familiares, educadores,….) y DENUNCIAR EL CASO a las autoridades (Cuerpo Nacional de Policía, Guardia Civil, Agencia Española de Protección de Datos –si hay uso inadecuado de datos de carácter personal–,…).

3. PARA SABER MÁS

- Protégeles – portal del menor

  http://www.protegeles.com/
- Fundación ALIA2

  http://www.alia2.org/index.php/es/

III. ACTIVIDADES

1. SUPLANTACIÓN DE IDENTIDAD.

El profesor propondrá a los chicos y chicas que se inventen un correo que sea "atractivo" en el que se suplante la identidad de un conocido y tenga un objetivo "malicioso".

2. CIBERBULLYING

El educador pedirá a los chicos y chicas que piensen en ejemplos de ciberbullying y qué se podría hacer si uno es víctima o sabe que están acosando a un conocido.

Los chicos y chicas pueden elaborar un cartel en el que informe a los demás sobre lo que es el ciberbullying y además incluir algunos consejos.

El profesor podrá pasar el vídeo de Amanda Todd (subtitulado en español, dependiendo de la madurez de los alumnos)

http://www.youtube.com/watch?v=NaVoR51D1sU

3. GROOMING

El profesor lee la siguiente historia:

"Vanesa hace un año estuvo jugando a un juego en la Red. Era un juego en línea y un día uno de los jugadores contactó con ella. Estuvieron chateando y finalmente el jugador convenció a Vanesa para que conectara la webcam y posara de manera sexy para él. Vanesa…"

Ahora los alumnos, en grupos de dos o tres, deberán continuar la historia. Al finalizar se leerán y debatirán los finales.

Es importante que los menores sepan que el *grooming* es un delito, que está castigado con prisión

4. SEXTING

Ya hemos comentado lo rápido que se traslada la información a través de las nuevas tecnologías de la información y comunicación, por ello, hay que considerar que cualquier imagen con contenido sexual que salga de un teléfono móvil, tiene una alta probabilidad de que sea difundida por la Red de manera muy rápida y extensa.

Por tanto, la práctica del sexting tiene una serie de riesgos importantes, ¿Cuáles podrían ser?

a. Exposición a pedófilos y acosadores sexuales

Un menor que se hace una foto en determinadas actitudes puede sugerir precocidad sexual a la persona a quien le llega la foto y verse expuesto a abusos o chantajes de tipo sexual por parte de un adulto (grooming, sextorsión).

b. Ciberbullying

Un menor que ve que se distribuye de manera masiva y sin control una foto suya o un video de carácter sexual puede sentirse humillado y acosado.

c. Responsabilidad civil/penal

Un menor tiene que conocer que la Constitución y las Leyes protegen la imagen de una persona y que su distribución puede dar lugar a incurrir en responsabilidad, pues la Ley también se aplica a los menores de edad.

Vamos a ver ahora los siguientes vídeos de Pantallas Amigas:

Se accede a ellos a través de la página de www.sexting.es

Los vídeos son:

- "No lo produzcas"
- "No lo retransmitas"
- "No lo provoques"