SIEMPRE ALERTA ANTE EL CIBERACOSO

Los riesgos de la web 2.0

Internet y los servicios de interactuación que ofrece como las redes sociales o los chats permiten a los menores pasar su tiempo libre en contacto directo con sus amigos y familiares. Sin embargo, la Red también se ha convertido en un lugar de libre acceso para delincuentes que buscan contactar con estas jóvenes víctimas para saciar sus más oscuros deseos. El ciberbullyng, la suplantación de identidad, el grooming o el sexting son algunos de estos tipos de acoso. Descúbrelos, identifícalos y aprende a actuar contra ellos

David Val

El uso de los servicios que componen la Web 2.0 (buscadores, plataformas colaborativas, redes sociales, servicios de vídeo online, blogs, wikis...) 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»

«Los 'nativos digitales' también tienen que aprender a usar la tecnología»

(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».

¿Cómo prevenir estas situaciones?

La Agencia Española de Protección de Datos está trabajando intensamente en concienciar sobre este tipo de abusos ya no solo a los menores, sino también a sus padres y profesores. Entre los consejos que da en su página web destacan los siguientes:

• **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. Solo un círculo estrecho de contactos sabrá quién se esconde detrás del nick, por lo que en caso de que ocurra algún tipo de acoso será más fácil localizar al agresor.

• **En la dirección de correo electrónico evita dar información que pueda identificarte,** como por ejemplo la fecha de nacimiento.

• **Usa la función de copia oculta (CCO) para mandar correos electrónicos a varias personas.** No publiques tu dirección de correo electrónico en sitios web y no participes en mensajes en cadena. Y relee todos 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 incómodas o desagradables.** Recuerda que eres tú quien controla la situación y que con un solo click puedes terminar con aquello que te 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 (que incluyan números, letras, símbolos) y recuerda que debe ser secreta.** No la compartas ni siquiera con tus amigos y cada dos o tres meses cámbiala por otra distinta.

• **Pide permiso a tus amigos si vas a publicar información o fotos donde aparezcan.** No publiques imágenes de otras personas en Internet sin autorización de quien aparece.

• **Utiliza la webcam solo con personas de confianza.** No hagas delante de ella nada que no harías en público y tápala con cinta adhesiva o gírala hacia un punto muerto cuando no la uses.

• **Si te encuentras ante una de las situaciones que analizamos en este artículo** debes pedir ayuda a un adulto de confianza (padres, familiares, profesores...) y denunciar el caso a la Policía o la Guardia Civil. También puedes recurrir a la Agencia Española de Protección de Datos si hay un uso inadecuado de datos de carácter personal. Y ante todo, no te fíes de ningún desconocido por muy buena gente que parezca.

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 riesgos señaladas no están 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 menor 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 a dificultar la capacidad de reacción de las

Cyber-Bullying.


Sexting.

«Muchos niños y adolescentes son engañados en Internet»

víctimas, situándolas en una posición de indefensión y vulnerabilidad.

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 este en su nombre. En estos casos, una persona utiliza el nombre y demás datos personales de otra persona haciéndose pasar por ella. Para ello, crean perfiles falsos en redes sociales o utilizan el perfil real de otra persona tras haber obtenido de manera ilegítima las claves de acceso. La suplantación de identidad puede originar graves consecuencias para la persona suplantada. En su nombre se pueden realizar comentarios, juicios, afirmaciones, amenazas o provocaciones que atentan gravemente contra su intimidad, honor o integridad física.

Ciberbullying o ciberacoso

Es una situación de acoso, hostigamiento, insultos, vejaciones, incluso chantaje de un menor a otro a través de redes sociales y demás medios de la Web 2.0 tales como blogs, correo electrónico o mensajería instantánea tipo Whatsapp. También se considera ciberacoso la publicación y difusión de vídeos y fotografías de terceras personas sin su consentimiento en plataformas electrónicas.

Para poder diferenciar una situación de ciberacoso es importante tener en cuenta que son situaciones que se dilatan en el tiempo –no puntuales– y que no cuentan con elementos de índole sexual. Además, la víctima y la persona acosadora son menores de edades similares. Ejemplos de casos de ciberbullying son la publicación de fotos o vídeos comprometidos para avergonzar a la víctima y su difusión entre los círculos de amigos; inscribir su dirección de e-mail en webs de servicios publicitarios para ser víctima de spam y de contactos no deseados o crear rumores ofensivos o reprochables sobre la víctima.

Grooming

Es una situación de acoso y chantaje a un menor de edad por parte de 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 tiene 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 la 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 chantajear a la víctima con difundirlas una vez conseguidas o robadas las contraseñas o las libretas de direcciones electrónicas.

Tú decides en Internet

La Agencia Española de Protección de Datos ha habilitado la web www.tudecideseninternet.es, un proyecto dirigido a fomentar la concienciación de los menores en el uso adecuado y responsable de la información que publican en la Red, tanto propia como de terceros, y que configura el nuevo 'Canal Joven' de la Agencia.

La iniciativa, orientada a jóvenes de entre 10 y 15 años y desarrollada por la AEPD en colaboración con el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), proporciona una plataforma de consulta y apoyo tanto para los menores como para los educadores —padres y profesores—. En este sentido, el director de la AEPD, José Luis Rodríguez Álvarez, ha subrayado que «la formación es la vía más eficaz para que los menores puedan utilizar y disfrutar de Internet, evitando situaciones de riesgo y sin realizar conductas que pueden resultar lesivas para otros».

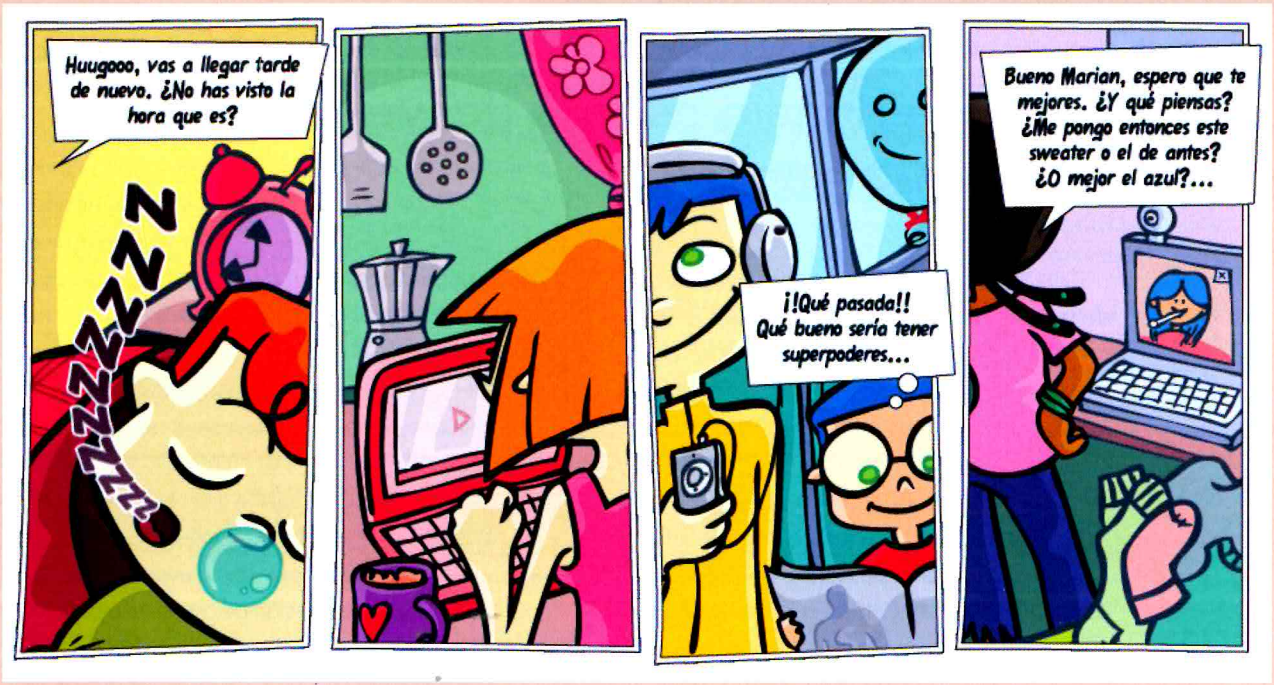
El proyecto está estructurado en dos partes: una dedicada exclusivamente a los menores, más amena y en forma de cómic, y otra destinada a educadores, con fichas didácticas para impartir en clase, recomendaciones y recursos de interés. El cómic, 'The Pandi y sus historias online', narra las aventuras de un grupo de amigos con diferentes personalidades. Según avanza la historia, los personajes se ven envueltos en situaciones relacionadas con su privacidad y la utilización de sus datos personales. En cada una de ellas los menores tendrán que responder preguntas vinculadas a estos temas, dilemas cuya contestación indicará cómo se enfrentarían a situaciones de riesgo tanto en Internet (redes sociales o mensajería instantánea) como en el mundo offline. «¿Un contacto de una red social es lo mismo que un amigo en la vida real?» o «¿Qué consecuencias puede tener el etiquetado de un amigo en una foto subida a una red social?» son algunas de las preguntas planteadas.

Los jóvenes tienen que elegir una respuesta, a la que sucederá su correspondiente explicación sobre por qué es adecuada o no junto a la frase «Al final tú decides, pero piensa siempre las posibles consecuencias». El objeto no es que el menor sienta que un grupo de adultos le dice lo que tiene que hacer, sino ofrecerle las herramientas y los conocimientos para que decida por sí mismo.

El propósito de la AEPD con 'Tú decides' es convertirlo «en un sitio inclusivo y ameno a la vez que riguroso» en el que, por un lado, los menores se sientan reflejados y, por otro, los docentes puedan encontrar materiales útiles y precisos para involucrar a los jóvenes en su propia educación en Internet. El cómic encuentra su continuación en varias fichas didácticas para que el educador pueda utilizarlas para profundizar en los contenidos de las viñetas, y consolidar las ideas básicas y esenciales que se quieren transmitir. Para ello, cada una de las fichas contiene diferentes actividades que el educador podrá llevar a cabo con el grupo, un glosario con definiciones que aclaran la terminología específica utilizada, consejos de seguridad relacionados con los contenidos, y recursos adicionales para ampliar la información.

La importancia de la privacidad y el valor de los datos personales, su tratamiento en los distintos contextos, la identidad digital, el uso de las redes sociales, la mensajería instantánea, los problemas relacionados con la suplantación de la identidad y las situaciones de riesgo —ciberbullying, grooming y sexting— son algunas de las fichas disponibles para tratar con los alumnos. En este punto, la Agencia quiere destacar la importancia de la colaboración del INTEF para la difusión de la iniciativa tudecideseninternet.es, que alojará el contenido de las fichas en su plataforma, poniéndolo a disposición de todos los profesores. El proyecto se completa además con la apertura de un nuevo canal de comunicación específico (canaljoven@agpd.es) a través del cual menores, profesores y padres podrán plantear las cuestiones que les preocupen en relación con la utilización y protección de los datos personales de los jóvenes.

The Pandi comic de la AEPD.



«La falta de experiencia es una desventaja de los nativos digitales»

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

En este tipo de acoso cibernético suele haber tres etapas: La fase de amistad, donde el acosador toma contacto con la víctima; la fase de relación, donde se dan confesiones personales e íntimas entre el menor y el acosador que sirven para consolidar la confianza y, por último, la fase sexual, que incluye la descripción de términos específicos sexuales, grabación de imágenes, toma de fotografías e incluso intento de contacto físico.

Sexting

Por último, 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 o cualquier 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 las redes sociales...).

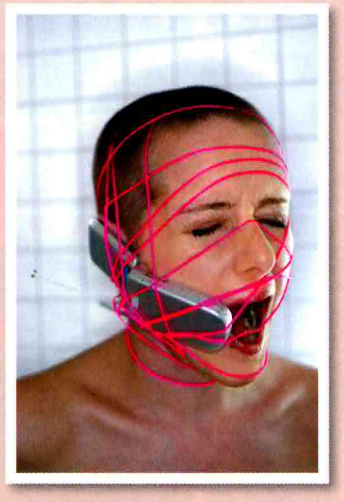
Cabe destacar que estos contenidos suelen generarse con voluntad de sus protagonistas o, al menos, con su consentimiento. Pero la utilización de los dispositivos digitales ha facilitado que este tipo de vídeos o imágenes se envíe con total descontrol y la difusión llegue a miles de personas casi sin darnos cuenta. Aun así, este tipo de acoso también puede dar lugar a situaciones de ciberbullying o de sextorsión (chantaje en el que alguien utiliza esos contenidos para obtener algo de la víctima, amenazando con su publicación) y, dependiendo del poseedor ilegítimo de las imágenes, también puede dar lugar a grooming.

Al final, la víctima, ante la presión que supone la difusión de las imágenes, 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 única salida pasa por no acceder a las pretensiones del hostigador y comunicar la situación a un adulto.

Todas estas conductas son delictivas y así están recogidas en el Código Penal como delito contra la libertad o contra la indemnidad sexual. Aun así, la atracción por la conducta transgresora propia de los adolescentes y la falta de cultura de privacidad en los menores puede dar lugar a que se conviertan en víctimas de estos tipos de acoso cibernético.

Los menores no perciben como amenazas para su privacidad la publicación de contenido erótico en la Web 2.0. Su consciencia de riesgo y exceso de confianza se debe a la falta de experiencia, de perspectiva y, especialmente, a que son «nativos digitales». *

Jóvenes y comunicación. La impronta de lo virtual



El Centro Reina Sofía sobre Adolescencia y Juventud es el responsable de este estudio que pretende abordar cómo las TIC, sobre todo a partir de la dinámica de las redes sociales, están construyendo unas formas inéditas de identificación y de interacción. Las fórmulas para contactar, para comunicarse, para reconocerse, para «estar ahí», para expresar ideas y emociones, para diferenciar lo personal de lo social, para constituir la propia autonomía, para salvaguardar la privacidad; todo está cambiando, no ya en su instrumentación o en sus dinámicas operativas sino, mucho más profundamente, en el sentido auténtico, en lo que se podría llamar la fenomenología de los elementos.

Tantas veces se escucha la expresión «nativos digitales» para referirse a adolescentes y jóvenes que han crecido en pleno auge de las tecnologías de la información y la comunicación, y a quienes, por ello, se presupone una capacidad para desenvolverse de forma natural y fácil con esas tecnologías, y tantas otras se interpreta que lo «joven» es prácticamente indisoluble de lo tecnológico, como lo es de «lo último» y «lo moderno» (frente a «lo antiguo»), que en ocasiones se pierde de vista que esos mismos jóvenes también experimentan complejos procesos de aprendizaje y socialización en torno a esas TIC.

Una necesidad de alfabetización digital sobre códigos cambiantes, que articula elementos que oscilan entre la dependencia y el reconocimiento, y en torno a la cual se establece una auténtica educación sentimental. Procesos de maduración en el uso de las redes sociales y las nuevas tecnologías, que además son asumidos como esenciales por sus propios protagonistas. Desde lógicas que aparentemente surgen del entorno laboral y formativo (hay que saber desenvolverse tecnológicamente para no quedarse fuera de la carrera competitiva, y hay que saber gestionar un yo laboral en torno a las redes sociales y las TIC), pero que inundan todos los aspectos de la vida: la mejor gestión del yo, el mejor aprovechamiento de las oportunidades, los mejores procesos de socialización, pasan por la adecuada integración con las nuevas tecnologías. Tal idea sobrevuela el imaginario colectivo, y a partir de la misma debemos ser conscientes de la manera en que sus implicaciones se ponen en juego en las relaciones que entablan los y las jóvenes, con los pares y con la sociedad en su conjunto.

En primer lugar, porque el reconocimiento general de las nuevas tecnologías y las redes sociales como el lugar en el que hay que estar, procura nuevos procesos de integración y exclusión entre adolescentes y jóvenes. Por un lado porque quien no esté ni use redes sociales quedará abocado al olvido de un grupo de pares que se autogestiona y organiza a partir de las posibilidades y facilidades que ofrece la tecnología.

Por otro lado, porque los propios usuarios y usuarias articulan de tal forma sus relaciones, sus estrategias de comunicación y sus rutinas en torno a las redes sociales, que la temporal ausencia (se estropea el ordenador o el móvil, o simplemente te lo olvidas en casa) provoca lo que se llega a sentir como verdadera «incomunicación», desde el momento en el que se asume que el grupo y los pares siguen comunicándose y relacionándose, y uno queda fuera de todas las cosas que pueden pasar o están pasando. Además, estar eventualmente fuera acentuará la ausencia del otro, de los amigos y demás relaciones, siempre presentes gracias a las redes sociales.

En segundo lugar, porque esas lógicas de la mejor gestión del yo empapan casi todos los aspectos de su vida alrededor de las nuevas tecnologías. Así, no estar integrado en las redes sociales, incluso no estarlo en tiempo real, se interpreta como perder oportunidades, no aprovechar las posibilidades que te brinda el desarrollo tecnológico que define el tiempo presente, y que no sólo te hace la vida más cómoda y práctica, sino que en sí mismo determina buena parte del sentido de las relaciones personales (estar fuera de las redes sociales como estar fuera de tu tiempo, por tanto). Lógica que, en última instancia, acepta que hay que estar «por si acaso», y que a partir de esa misma idea justifica, por ejemplo, los procesos de acumulación de contactos, aún a sabiendas de que buena parte de esos contactos «agregados» nunca o casi nunca serán «usados», o incluso corresponden a personas que apenas se conocen o con las cuales es complicado establecer un nexo de unión personal.

A partir de la asunción de que la tecnología te hace la vida más fácil y te abre nuevos horizontes, adolescentes y jóvenes asumen con naturalidad el hecho de aprovechar las oportunidades que ofrecen las redes sociales para mostrar una parte de uno mismo que facilita algunos procesos de la comunicación y las relaciones, y además permite a personas más tímidas o inseguras participar del juego: elimina la vergüenza, democratiza el flirteo, permite la transmisión reflexionada y orientada de mensajes, posibilita establecer relaciones en las que es posible mantener cierto «control» de la comunicación, etc.

A partir de la naturalización de la presencia de las redes sociales en los procesos y estrategias de relación y comunicación entre jóvenes (y no tan jóvenes), los y las usuarios/as habituales asumen, de manera explícita e implícita, estar participando de un juego (relevante a la postre, pero generalmente observado desde el entretenimiento y la diversión) en el que todo participante es conocedor de las reglas, los pros y los contras. Es decir, que pese a que nadie niega que aprovecharse y disfrutar de las ventajas de las TICs plantea algunas contrapartidas no tan beneficiosas, el clima general entre jóvenes usuarios y usuarias descansa en la percepción de «controlar» la situación, precisamente porque desde el principio creen ser conscientes de las contrapartidas... y aceptan participar porque les compensa.