Instituto Nacional
de Tecnologías
de la Comunicación

La utilización segura de la mensajería instantánea por parte de los adolescentes

Nos resulta sorprendente que nuestros hijos pasen las horas muertas pegados al ordenador, cuando lo más que hacemos nosotros es mirar el correo, leer el periódico y quizá, consultar el tiempo que hará esta semana… Les vemos reír, enfadarse e incluso hablar con la pantalla. Y pensaríamos que sufren algún tipo de trastorno si no fuera por la existencia de los servicios de mensajería instantánea, cuarta actividad más popular en la web en opinión del 65% de los usuarios españoles[1].

Según un estudio[2] sobre los usuarios de **mensajería instantánea** y sus comportamientos, el perfil de los internautas no se corresponde con el tópico de *freak*[3] informático con problemas en cuestiones de habilidades sociales, sino todo lo contrario: define a una persona altamente social y segura de sí misma, a quien le gusta salir, organizar y asistir a eventos con su familia y amigos. Así, la mensajería instantánea se confirma como un medio de interacción social.

La mensajería instantánea es un servicio a medio camino entre las salas de chat y el correo electrónico; se diferencia del primer servicio en que la comunicación se establece únicamente con las personas admitidas en la lista de contactos y del segundo, en que las conversaciones se mantienen en tiempo real. Por regla general, estos programas son gratuitos y compatibles con cualquier otro aún siendo de diferentes fabricantes gracias a que ambos utilizan los mismos protocolos de comunicación y pueden estar activos todo el tiempo que deseemos, siempre y cuando tengamos conexión a Internet.

El programa permite escribir un mensaje, acompañado de emoticones[4], y enviarlo a uno o a varios destinatarios con quienes queremos establecer la comunicación. Además, la mayoría de estos servicios ofrecen un "aviso de presencia", que indica cuándo se conectan nuestros contactos o en qué estado se encuentran, si están disponibles para tener una conversación, si están ausentes... Actualmente, algunos de los servicios de estos programas ofrecen la posibilidad de dejar un mensaje a una persona aunque no esté conectada para que lo lea en el momento en que acceda al servicio; es como el contestador o el buzón de voz de los teléfonos.

[1] Según el estudio *Mediascope*, publicado por la Asociación Europea de Publicidad Interactiva (EIAA).

[2] Estudio realizado por Microsoft en 13 países en el año 2005 y cuyos resultados se publicaron en febrero del 2006.

[3] Del inglés *freak*, que significa raro, extravagante, estrafalario o fanático; es un término usado en el idioma español para referirse a la persona interesada u obsesionada al menos con un tema, afición o hobby en concreto.

[4] Iconos, dibujos representativos que expresan estados de ánimo, acciones… Pueden ser dinámicos o estáticos.

En los primeros programas de mensajería instantánea, cada letra se enviaba a medida que se iba escribiendo el texto y así, las correcciones de las erratas también se veían en tiempo real. Esto daba a las conversaciones mayor sensación de conversación telefónica y no tanto de intercambio de texto. En los programas actuales, habitualmente, se envía cada frase de texto al terminarse de escribir (de hecho, hay que aceptar el envío del mensaje).

En las últimas versiones de los programas se han insertado una serie de nuevas funcionalidades, como la posibilidad de establecer conversaciones telefónicas, compartir archivos o programas, enviar ficheros… Los programas más utilizados son Yahoo! Messenger, MNS Messenger (actualmente denominado Windows Live Messenger), AMI (de AOL) y Google Talk.

Según un estudio realizado por Nielsen/NetRatings en junio de 2007 a jóvenes de entre 12 y 17 años, el 90% de los mismos acude a la Red para comunicarse con su entorno de manera ágil e instantánea. Algunas de las razones del auge de los servicios de mensajería instantánea son la confidencialidad o privacidad en la utilización de estos servicios y la inmediatez.

Tabla 1: Ventajas e inconvenientes de la mensajería instantánea

Ventajas	Inconvenientes
Servicio gratuito; sólo se paga la factura de conexión a Internet	Se necesita un ordenador
Fácil de usar	La movilidad de utilización está restringida
Permite establecer más de una conversación al mismo tiempo	Posibilidad de ser molestado con *spim*[5]
La conversaciones son privadas y confidenciales	
Permite realizar otras actividades al mismo tiempo	
Permite intercambiar archivos	

Fuente: INTECO

Pero el uso de la mensajería instantánea también conlleva ciertas amenazas, derivadas tanto de los usuarios como del propio servicio.

Respecto a aquellas procedentes de los usuarios, se hace referencia fundamentalmente a los abusos que pueden cometerse en la Red. Y es que la evolución en la tecnología y

[5] *Spim: spam* por mensajería instantánea (*spam*: correo basura; mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor). Fuente: Wikipedia.

su acercamiento a los menores no ha desembocado tanto en nuevos delitos, sino en nuevas formas de cometerlo.

Los acosadores en línea son directos y van rápidamente a la cuestión que les interesa; es decir, después de saludar a su víctima, se dirigen a ella con preguntas muy directas de índole sexual. Este tipo de acosadores son, pese a todo, los menos peligrosos, pues los propios adolescentes los identifican rápidamente y se deshacen de ellos. Son los pedófilos "seductores" los que encierran en sí un grave problema, pues se camuflan y se hacen pasar por adolescentes para hacerse con la confianza del menor antes de llevar a cabo su abuso. Normalmente, los acosadores entran en contacto con el menor en un chat y después le proponen continuar la conversación a través de mensajería instantánea para que no sea tan fría. Y aquí comienza la forma más utilizada de chantaje a menores por Internet, conocida como *grooming*[6].

Este tipo de abuso se caracteriza por el robo de la contraseña de acceso del menor al servicio de mensajería instantánea. El delincuente se adueña de la identidad del adolescente en el servicio y de sus contactos y le chantajea, pidiéndole que acceda a sus peticiones a cambio de no mandar a sus contactos imágenes tomadas a través de la cámara web del menor, previamente robada. El acosador cada vez consigue más porque tiene a la víctima a su merced; además, cuentan con la ventaja del pudor que les da a los menores confesar que han accedido a este tipo de chantajes.

Pero el *grooming* no es el único tipo de abuso al que son vulnerables los menores. Otro caso es el *e-bullying*, acoso entre estudiantes o profesores con afán de mofa y burla, lo que también puede ocasionar graves trastornos al niño que lo sufre. Quizá sea el peligro más conocido por su íntima relación con el *bullying*, con la única diferencia de que el primero se realiza en la Red y el segundo cara a cara.

En cuanto a las amenazas generadas por el propio servicio de mensajería instantánea, se deben a las vulnerabilidades propias del servicio. El hecho de que los proveedores de mensajería instantánea den con cada nueva versión una serie de posibilidades más allá del simple mensaje (archivos compartidos, videoconferencia…) está directamente relacionado con el aumento de las amenazas a las que ha de enfrentarse el servicio. Además, el uso creciente de estos programas los hace estar en el punto de mira de los *hackers*, que los utilizan como vía para el *phishing*[7] y el *pharming*[8] enviando mensajes de

[6] *Grooming*: cualquier acción que tenga por objetivo minar y socavar moral y psicológicamente a una persona, a fin de conseguir su control a nivel emocional. Si bien esta actividad puede producirse en cualquier instancia, es particularmente grave en los casos en los que una persona lleva a cabo este tipo de coacciones y presiones emocionales en contra de un menor, con el objeto de obtener algún tipo de favor sexual. Fuente: INTECO. [En línea] Disponible en www.observatorio.inteco.es

[7] *Phishing*: es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta. Fuente: INTECO. [En línea] Disponible en www.observatorio.inteco.es

manera indiscriminada a miles de usuarios, quienes acaban por descargar o ejecutar programas maliciosos que infectan sus ordenadores.

Recomendaciones de INTECO a los usuarios

Actualmente, el **Observatorio de la Seguridad de la Información** de INTECO está llevando a cabo diferentes estudios relacionados con la seguridad de los menores en Internet:

1) **Estudio sobre los hábitos de seguridad en el uso de las TIC y acceso a contenidos por niños y adolescentes y e-confianza de padres y tutores**. Este documento abordará dos frentes:

   - El estudio y análisis de los usos, hábitos, acceso a contenidos, conocimientos y percepción de seguridad de los menores respecto a las TIC, en especial Internet, así como los conocimientos, consciencia, percepción, implicación sobre la seguridad y e-confianza de los padres respecto del uso de las tecnologías por parte de sus hijos.

   - La elaboración de una guía práctica con consejos para un uso seguro y adecuado de las nuevas tecnologías y sus servicios (Internet, telefonía, videojuegos, etcétera).

2) **Estudio sobre la seguridad de las plataformas educativas**. En dicho estudio, se diseñará y desarrollará un informe sobre la seguridad de los contenidos y servicios integrados en las plataformas educativas, a partir del análisis de información disponible en la materia y de casos de éxito en los ámbitos nacional e internacional, además de entrevistas a expertos, con el objetivo de definir qué estándares de seguridad son necesarios para su desarrollo.

Por otro lado, tal y como se ha presentado anteriormente, resulta necesario ofrecer a los usuarios una serie de consejos para evitar que los menores sean víctimas de ciber-acoso o de *grooming* o accedan a contenidos ilícitos e inapropiados a través de Internet. En esa línea, INTECO hace a todos los usuarios las siguientes recomendaciones:

1) Aprenda a utilizar las nuevas tecnologías para poder saber qué hace su hijo mientras está en Internet y tener una idea sobre los peligros a los que se puede llegar a enfrentar.

[8] *Pharming*: explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio. Fuente: Wikipedia [En línea] Disponible en http://es.wikipedia.org/

2) Eduque a sus hijos en el uso seguro de Internet. Por ejemplo, enséñele a ignorar el *spam* y a no abrir archivos procedentes de desconocidos; explíquele que es posible que a través de uno de estos archivos alguien le robe sus contraseñas de acceso.

3) Establezca el ordenador en un lugar común de la casa.

4) Las cámaras web no son imprescindibles. Restrinja su uso entre los más pequeños.

5) Hable con su hijo sobre las páginas que visita en Internet, con quién habla y sobre qué temas.

6) Conciencie a su hijo de la importancia de no agregar desconocidos a sus contactos y de la importancia de no revelar datos personales.

7) Incúlquele la importancia de no enviar fotos ni vídeos a desconocidos.

8) Hable con su hijo acerca de los contactos que establece en Internet.

9) Háblele de los riesgos a los que se puede enfrentar desde el ordenador. Insista en que el hecho de que no tenga contacto directo con quien está al otro lado no significa que no pueda hacerle daño, y en que a veces no basta con apagar el ordenador.

10) En caso de que su hijo sea víctima de *grooming*, póngase en contacto con la policía y denuncie el caso[9].

[9] Diríjase a la Brigada de Investigación Tecnológica de la Policía (denuncias.pornografia.infantil@policia.es; 915 82 27 53) y a la Brigada de Delitos Telemáticos de la Guardia Civil (delitostelematicos@guardiacivil.org).