UNIDAD 10

1. INTRODUCCIÓN

Internet se ha convertido en una revolución en la última década, haciendo realidad aspectos que hace algunos años para la mayor parte de las personas eran únicamente una cuestión de ciencia ficción. No obstante, existe una clara diferencia entre los usuarios que han "adoptado" Internet como medio de comunicación y aquellos que, primero Prensky y ahora el Berkman Center for Internet and Society, llaman "nativos digitales". Es decir, usuarios para los que no hubo una época de su vida en la que Internet tal y como la conocemos hoy en día no existía.

Éstos son, como es natural, los menores, especialmente aquellos ubicados en el rango de edad entre ocho y quince años, que constituyen no sólo aquellos que definirán el futuro de la red, sino aquellos que, por el hecho de nacer en un mundo ya conectado, consideran este hecho de manera más natural y menos extraordinaria, reduciendo al máximo la distancia que establecen entre su vida "electrónica" y su vida "física"; su identidad digital es únicamente una dimensión más de su identidad personal. Internet es una parte más de su vida social, igual que lo es ir al cine o hablar con los compañeros de clase.

Mientras que esto tiene indudablemente aspectos muy positivos para estos usuarios, les genera una dificultad añadida a la hora de aplicar patrones de comportamiento diferentes dependiendo del entorno en el que se relacionan. No hay ninguna duda de que las redes sociales, servicios de mensajería instantánea, o correo electrónico son herramientas positivas para los menores que incorporan una dimensión vital necesaria hoy en día en sus relaciones sociales, pero sobre las que es necesario educarlos para que sean conscientes de los riesgos a los que se enfrentan y dispongan de las herramientas para hacerles frente. En definitiva, al igual que una persona no se comporta del mismo modo en una cena de amigos que en una reunión de negocios, se trata de educar a los menores para que sean consciente de que enseñarle fotografías del verano a un amigo no es lo mismo que colgarlas en tu tablón de Facebook, aunque tu amigo lo sea también en Facebook.

Los principales problemas relativos a la utilización de Internet por parte de menores radican en la ingenuidad, buena fe o simple desconocimiento de lo que puede esconderse al otro lado de la red; es famosa una viñeta en la que un perro simula utilizar un ordenador mientras dice "En Internet, nadie sabe que eres un perro". La moraleja es simple: debemos desconfiar de lo que hay (o de quién hay) al otro lado de una conversación, de una página web o de un correo electrónico, ya que a ese otro lado puede haber un perro... o un delincuente.

"On the Internet, nobody knows you're a dog"
Ilustración por Peter Steiner

2. OBJETIVOS DE APRENDIZAJE

El control paterno consiste en impedir, o limitar el acceso al manejo de ciertas herramientas, o a su contenido a menores de edad. Esto se realiza mediante una serie de sistemas de bloqueo, normalmente protegidos mediante claves, bien alfanuméricas, bien mediante una combinación de teclas, que realizan los responsables legales del menor, normalmente sus padres, o los adultos responsables del uso de la correspondiente máquina. Este tipo de medidas, aunque buenas, no garantizan al cien por cien la seguridad de los menores, y es por eso que el objetivo de este curso es el de mostrar los diferentes aspectos de seguridad que se han de tener en cuenta para con los menores. Enseñar cuáles son los posibles peligros a los que se enfrentan y como evitarlos. En los últimos capítulos se muestran una serie de herramientas gratuitas de control parental y se da una lista de recomendaciones a tener en cuenta.

3. SEGURIDAD EN EL CORREO ELECTRÓNICO

El **correo electrónico** es probablemente el medio más utilizado de comunicación entre los usuarios de Internet, aunque en el espectro de población que nos centramos no tiene tanta importancia como en otros ámbitos, por lo que su nivel de amenaza no es tan elevado. Al respecto, cabe destacar que el correo electrónico, aun cuando sus ventajas son innumerables (rapidez, asincronía, facilidad de comunicación, etc.), implica algunos problemas que no sólo desconocen los menores, sino que también lo hacen los adultos.

El correo electrónico es, por defecto, un medio eminentemente inseguro para el envío de información. Su contenido se transmite por la red en texto claro (sin codificar), salvo que se utilice algún medio de firma y cifrado digital.

Si visualizamos mentalmente Internet, la red está compuesta por una serie de elementos centrales que reciben los datos y los distribuyen hacia el destino apropiado ("encaminadores", o "enrutadores" en su traducción literal del inglés "routers"), y otros elementos "periféricos" que constituyen los usuarios finales (es decir, los ordenadores o los móviles etc..). Asimismo, debe tenerse en cuenta que, a menudo no existe una similitud entre aspectos geográficos del mundo real y el "virtual"; es obvio que para ir de Valencia a Madrid en un medio de transporte carece de sentido atravesar Paris o Londres, pero eso no se aplica a los datos informáticos. Un correo electrónico enviado a otro usuario que se encuentra en Madrid puede implicar que los datos que contiene atraviesen una docena de sistemas ubicados en Francia, Alemania e Italia, alguno de cuyos sistemas puede haber sido "comprometido" y los datos que recibe ser grabados o modificados.

El correo electrónico es, en aspectos de autenticidad, un medio inseguro. Esto quiere decir que el hecho de que A reciba un correo de B no siempre implica que ese correo haya sido enviado efectivamente por B; resulta relativamente sencillo para un usuario experimentado modificar los campos de un correo para hacer creer al destinatario que el emisor del correo es alguien que no es. Aunque la implicación de este hecho para los menores es pequeña, es un aspecto que hay que tener en cuenta.

Prácticamente todo usuario de Internet ha recibido un correo que forma parte de una cadena. Más allá de la molestia que suponen estas cadenas de correos, de la pérdida de tiempo que suponen para muchos usuarios y de la sobrecarga de los servidores de envío y recepción que implican, su principal riesgo reside en el uso que se le da al campo del destinatario (Para:) o copia (Cc:). Es frecuente recibir correos de este tipo cuyos emisores lo envían a unas cuantas docenas de usuarios y ni siquiera han eliminado las direcciones que contiene el cuerpo del correo, lo que implica que el correo recibido puede contener con facilidad un centenar o más de direcciones de correo electrónico. Estas cadenas son utilizadas por personas malintencionadas para construir bases de datos a las que enviar no sólo correo basura (que incrementa la pérdida de tiempo y la sobrecarga indicada previamente), sino también e-mails conteniendo cualquier tipo de malware (véase el capitulo destinado al Malware).

El phishing (ver el capítulo de Malware y el de Delitos) puede considerarse como una composición de correo electrónico y entorno web. El más habitual está orientado a conseguir credenciales bancarias pero no es el único. Existen también versiones menos perjudiciales desde el punto de vista financiero, pero que pueden implicar otro tipo de riesgos y problemas para el menor. Un ejemplo de esto podría ser el envío de un correo a un usuario describiendo un medio para averiguar qué "amigos" del MSN le tienen bloqueado. Dicho correo le redirecciona a una página web que le solicita que introduzca su usuario y contraseña de MSN. Como es obvio, el engaño consiste en que no existe dicha funcionalidad. Y lo que se consigue es que el usuario haya introducido sus credenciales de acceso a su correo de Hotmail y cuenta de MSN, donde puede existir información sensible del menor: fotografías, conversaciones, intimidades, etc. Aunque dicha información es habitualmente utilizada para la construcción de bases de datos de spam, no hay que descartar la posibilidad de que se utilice para chantajear al menor, o para hacer un uso indebido de sus datos personales.

Debe tenerse en cuenta que un porcentaje no despreciable de los usuarios que reciben un correo de un desconocido con un programa anexado, intentará abrirlo, lo que puede suponer automáticamente la infección del equipo, y de nuevo, puede implicar la instalación de software que facilite el control del equipo por parte de un tercero, quien puede llevar a cabo chantaje, intimidación abuso o robo de datos. En este punto, el menor debe ser consciente que no debe abrir los ficheros adjuntos de correos de emisores desconocidos, por muy interesantes que éstos aparenten ser.

4. SEGURIDAD EN NAVEGACIÓN WEB

Compitiendo con el correo electrónico, la web es el servicio estrella de Internet, en especial tras la aparición de la web 2.0, donde el usuario no es ya un mero espectador sino que dispone de todos los medios para convertirse en un componente activo de la web.

Dejando las redes sociales para un punto posterior, la principal figura a destacar en este caso son los blogs (bitácoras), cuyo crecimiento en los últimos años ha sido exponencial. Un blog no es otra cosa que un espacio web tradicional donde los contenidos se cuelgan de manera secuencial a modo de diario personal, y donde se reflejan opiniones, fotografías y vivencias de la persona. En el caso de los menores, es fácil que éstos utilicen el blog para comunicarse con otros usuarios tanto de su esfera social local como global, y que éste contenga información sensible tanto desde el punto de vista de la protección del menor como desde el punto de vista de la intimidad.

El menor debe ser consciente de la importancia, visibilidad y perdurabilidad de cualquier contenido que "cuelga" en Internet. Aunque publicar una confidencia pueda parecer una buena idea en un determinado momento, quizá una semana después esa "entrada" o "post" ya no sea tan buena idea, por sus implicaciones para el propio autor o para terceras personas. No hay que olvidar en ningún momento que cualquier cosa que un usuario pone en Internet se convierte en eterno, y su control escapa al propio autor. El menor debe saber, que una fotografía colgada en un blog deja de estar bajo su control, ya que es posible copiarla y colgarla en otro blog, en una red social, enviarla por correo o guardarla en el ordenador de cualquier usuario.

Al igual que no le damos nuestra dirección postal ni teléfono móvil a cualquiera, tampoco debemos hacerlo en Internet (ni en un blog ni en cualquier otro medio). Aunque parezca que nuestros visitantes son los amigos de siempre, en realidad puede que no sea así. Otras muchas personas, curiosos, amigos de otros amigos, o personas con las que no nos llevamos bien, pueden acceder a nuestro espacio personal y por tanto a nuestros datos personales. Los problemas de privacidad que puede acarrear un blog donde el menor da detalles de sus amistades, lugares frecuentados, horarios... son algo a tener muy en cuenta por los propios menores, pero especialmente por los padres: es necesario estar muy atento a la utilización de nuestros datos en Internet, por ejemplo, a la hora de registrarse en webs no confiables que nos pueden llegar a solicitar hasta el teléfono, la dirección de nuestra casa o determinada información sobre nuestros hábitos.

De la misma forma que ningún padre abandonaría a sus hijos en el centro de una gran ciudad, a merced de todo tipo de delitos, es muy importante no abandonar "digitalmente" a los menores; aunque en ocasiones nos resulte cómodo que nuestros hijos conecten a Internet, y a primera vista parezca inofensivo, debemos tener siempre presente que en la red hay gente buena y mala, contenidos apropiados e inapropiados, excelentes amigos y delincuentes... exactamente igual que en la vida real.

5. SEGURIDAD EN MENSAJERÍA INSTANTÁNEA

La mensajería instantánea es, junto con las redes sociales, el principal medio de comunicación de los menores en Internet. Este medio permite una comunicación inmediata y síncrona, además de proporcionar múltiples funcionalidades de intercambio de información, tanto de ficheros como de conexión a la WebCam del interlocutor. Aunque existen multitud de protocolos y programas de mensajería instantánea, sin duda el más utilizado en la actualidad por los menores es Microsoft Messenger (MSN); en cualquier caso, los problemas comentados en el presente punto son extrapolables a cualquier sistema de mensajería.

El principal problema relativo a la utilización de sistemas de mensajería instantánea en los menores y en general, en el uso de Internet por parte de éstos, es la ingenuidad y el desconocimiento de lo que puede esconderse en una inocente conversación; la primera regla de oro es no admitir a cualquiera que nos añada como amigo ya que, a priori, no sabemos quién está detrás de una dirección de correo. Para una persona malintencionada, es muy sencillo conseguir una dirección de correo aparentemente inocente, entablar conversación con un menor y ganarse su confianza hasta obtener datos de su vida privada muy relevantes. Por tanto, la segunda regla de oro es no fiarse de cualquiera que nos esté hablando a través de MSN: incluso aunque aparentemente sea un amigo, a ese amigo pueden suplantarle la identidad (por ejemplo, mediante el robo de la contraseña de acceso a MSN, como se ha comentado anteriormente). De hecho, hay gusanos que inician conversaciones automáticas con los contactos MSN de su víctima con el objetivo de propagarse; es muy importante no aceptar ficheros enviados por MSN y que puedan resultar sospechosos, aunque aparentemente sean legítimos: si nuestro amigo, sin mediar palabra, nos trata de enviar un archivo, o inicia una conversación en inglés cuando habitualmente hablamos en castellano, debemos sospechar.

Otra regla muy importante a la hora de utilizar mensajería instantánea, al igual que cuando utilizamos redes sociales o correo electrónico, es no facilitar nunca datos de carácter personal que puedan comprometer nuestra seguridad (teléfono móvil, dirección, instituto, horarios...). Por supuesto, tampoco se debe facilitar ningún tipo de clave a cualquiera que nos la pida, ya que esta contraseña proporciona el acceso directo a nuestros contactos -y probablemente a nuestro correo electrónico-.

Cualquier sistema de mensajería actual (por supuesto, también MSN) permite no sólo intercambiar conversaciones o ficheros, sino también utilizar la webcam del usuario para entablar videoconferencias; esto constituye un riesgo añadido a la utilización habitual de la mensajería instantánea, ya que no sólo estamos transmitiendo texto, sino vídeo y audio; debemos concienciar al menor para que no active jamás la webcam con un contacto desconocido, ya que es habitual la utilización de estos sistemas por parte de pederastas que, haciéndose pasar por menores, tratan de ganarse la confianza de un tercero y obtener así imágenes de éste. Es conveniente que el ordenador se encuentre en una zona común de la casa para evitar acciones o actividades comprometidas por parte del menor.

Muchas cámaras web actuales pueden ser activadas por control remoto, tal y como veremos en el capítulo dedicado a la seguridad de los sistemas, lo que implica que el menor puede ser grabado incluso no estando conectado a MSN, si alguien ha comprometido la seguridad de su equipo. Adicionalmente, siempre que se inicia una videoconferencia, estamos proporcionando a un tercero la posibilidad de grabar o capturar las imágenes transmitidas, con las implicaciones que el mal uso de estas imágenes puede acarrear: las imágenes pasan a estar fuera de nuestro control, y a partir de ese momento pueden ser publicadas en webs, foros, o distribuidas de cualquier otra forma por Internet.

Para acabar este capítulo, es necesario hacer especial hincapié en el riesgo de chantaje y extorsión a menores que puede implicar el mal uso de la mensajería instantánea. Debemos recomendar, que el adulto esté siempre alerta y dispuesto a tratar estos problemas con el menor, advirtiéndole de los peligros que corre y transmitiéndole confianza para que le cuente cualquier incidencia de este tipo, y por supuesto prestándole todo su apoyo para resolverla. Y obviamente, el adulto debe saber que muchos de éstos comportamientos pueden ser constitutivos de delito y puede ser necesario formular la correspondiente denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado.

6. SEGURIDAD EN P2P

El P2P es sin duda el protocolo de intercambio de ficheros más ampliamente utilizado hoy en día, tanto por menores como por adultos; todos los riesgos generales de utilización de este tipo de mecanismos, comentados en diferentes capítulos del presente curso, en el caso de los menores estos riesgos se agravan, ya que entran en juego, una vez más, factores como la inocencia, las ganas de hacer amigos o el afán de protagonismo.

Para comenzar, es necesario hacer hincapié en la falta de confianza de cualquier archivo descargado desde una red P2P; lo que a primera vista es un vídeo inocente, puede resultar no sólo un contenido inapropiado para un menor (pornografía, violencia...), sino que puede convertirse en el medio de transporte de cualquier tipo de malware: virus, gusanos, troyanos... Es necesario insistir, una vez más, en la necesidad de utilizar sistemas antivirus correctamente actualizados y, en este caso concreto, de validar por parte de un adulto los contenidos que el menor descarga de redes P2P.

Especialmente en el caso de los menores, una precaución básica en la utilización de redes P2P consiste en no compartir jamás material propio (fotografías, vídeos, documentos...) a través de estos mecanismos. Si colgamos una foto, un trabajo del instituto, o un vídeo personal en eMule, es muy difícil garantizar que sólo quien nosotros queramos podrá descargarlo. Lo más probable es que este material acabe en manos de terceros, que como siempre podrán hacer con él lo que estimen oportuno. En este sentido, es necesario configurar correctamente cualquier programa P2P, para garantizar que no estamos compartiendo archivos que realmente no queremos compartir: un sencillo error de configuración puede llevarnos a dejar accesible a Internet todo nuestro disco duro, con lo que esto puede implicar para nuestra privacidad, reputación, etc.

7. SEGURIDAD EN REDES SOCIALES

Facebook y Tuenti son hoy en día las dos redes sociales más utilizadas por los menores de todo el mundo. A través de ellas, los usuarios intercambian fotos, comentarios, datos personales, tendencias, aficiones, y todo tipo de características, creando (o tratando de crear) una identidad digital lo más similar posible a su identidad real.

Como en tantos otros ejemplos, el principal problema de la utilización por parte de menores de estas redes sociales es la pérdida de privacidad. Es necesario, una vez más, hacer hincapié en la necesidad de no proporcionar jamás datos que puedan comprometer la seguridad del menor: teléfonos de contacto, direcciones, etc. Cualquier dato publicado en una red social, al igual que los publicados en una página web, es susceptible de saltar al dominio público y, a partir de ese momento, será imposible de controlar (los mecanismos de seguridad de las redes sociales para evitar ésto suelen ser ineficientes). Debemos tener presente que la información que publicamos en una red social permanecerá en algún sitio de la red, de una u otra forma, por un tiempo indefinido.

Al igual que sucedía en los sistemas de mensajería instantánea, debemos tener en cuenta que no todo el mundo que te agrega en Facebook o Tuenti, tiene por qué ser un amigo real; por tanto, es necesario tener especial cuidado en qué conexiones aceptamos o dejamos de aceptar en estas redes sociales -o en cualquier otra-, ya que estos contactos, en caso de ser aceptados, pueden tener acceso a información que no queremos que vean.

El uso responsable de las redes sociales -como de cualquier otro elemento, en Internet o en el mundo real- es otro de los aspectos a destacar a la hora de hablar de menores en la red; al igual que las imágenes o los vídeos, cuando se publica una opinión o un comentario en una red social, es necesario pensar dos veces lo que se va a escribir antes de hacerlo. Ese comentario u opinión potencialmente puede ser leído por miles de personas, y el autor puede perder el control de quién accede al mismo y de qué forma lo hace (algo similar a lo que sucedía cuando hablábamos de blogs). Por supuesto, no podemos utilizar comentarios que atenten contra los demás (xenofobia, racismo, insultos...), y debemos siempre preservar la privacidad de terceros (de nuevo, no facilitar datos privados, no colgar fotografías de otras personas...). Un mal uso de Internet en este sentido puede llegar a considerarse delito (ver la parte de legislación de los foros del CSIRT-CV), por lo que los menores -y por supuesto los adultos- deben ser cuidadosos con lo que cuelgan en una red social.

Para finalizar los aspectos dedicados a redes sociales, es necesario hacer hincapié, una vez, en el apoyo que los adultos debemos prestar al menor en caso de problemas en la red (chantajes, amenazas...), mostrándole nuestra confianza y apoyándole en lo que sea necesario (de nuevo, inicialmente, en una denuncia de cualquier hecho que pueda llegar a considerarse delictivo).

Toda aplicación de redes sociales debe tener un apartado de configuración que permita limitar la visibilidad de la información que ofrecemos, de forma que ésta solo sea accesible por amigos e incluso limitar lo que los buscadores pueden recabar de nuestra información.

8. SEGURIDAD Y SISTEMAS

Los aspectos relevantes para un menor cuando hablamos de la seguridad de los sistemas en Internet son obviamente los mismos que para un adulto, pero con el agravante, no sólo del desconocimiento o del exceso de confianza a los que hemos hecho referencia en varias ocasiones a lo largo del presente capítulo, sino también, con el del uso intensivo que los menores hacen de la red, en la que con frecuencia pasan muchas más horas que los adultos y llegan a convertirse en los expertos tecnológicos de cara a sus padres. De esta forma, los capítulos del presente curso dedicados a malware, seguridad en WiFi, etc. son de total aplicación al menor, y por tanto no vamos a repetir aquí estos aspectos de seguridad en sistemas, tratados con mayor profundidad en otros capítulos de este curso. No obstante, en el presente apartado del capítulo dedicado a los menores, debemos romper una imagen idealista que muchos menores tienen de la seguridad en Internet, en concreto de los hackers (entendidos como piratas informáticos).

La ciberdelincuencia en los últimos años ha evolucionado considerablemente, tanto en complejidad, como en alcance. Los ataques ya no son fruto de la curiosidad y de demostrar la valía de ciertos adolescentes que actuaban desde sus dormitorios. Esa idea ya pertenece al pasado. Se ha pasado a las mafias organizadas de delincuentes, que refinan día a día sus técnicas de ataque, y tienen un claro ánimo de lucro.

En la actualidad, un pirata informático no es más que un delincuente -equivalente a un estafador, un gamberro o incluso un atracador- que suele actuar por dinero y que utiliza todos los recursos y tecnologías presentes en Internet para garantizar su anonimato y cometer todo tipo de fraudes. Pertenecen a mafias organizadas de cibercriminales, cuyas actividades cuestan a las empresas y al propio estado millones de euros al año.

Ojo con los menores que, alentados por películas como “Hackers”, “The Net”, o similares, pueden “jugar” a convertirse en piratas y pueden meterse en problemas penados incluso con cárcel. De la misma manera que ningún padre permitiría a su hijo robar en un centro comercial, ningún padre debe permitir que su hijo se convierta en un delincuente desde su propia habitación.

Pasamos a detallar una serie de buenas prácticas que el menor -y por supuesto el adulto- debe seguir en el uso habitual de su equipo y de Internet.

Son las siguientes:

- Jamás debemos ejecutar programas desconocidos o que provengan de una fuente no fiable (y no todas las páginas web lo son).
- Mantengamos actualizados nuestros sistemas (parches, actualizaciones del sistema operativo, navegador y complementos, ...) y activado nuestro cortafuegos.
- Siempre que conectemos a nuestro correo electrónico debemos asegurarnos que, cuando tecleamos el usuario y la contraseña, el protocolo que utiliza el navegador es HTTPS, no HTTP. De esta forma, nuestros datos viajarán cifrados por la red, lo que evitará que un tercero no autorizado pueda leerlos.
- Ten siempre en ejecución el antivirus (que incluya antispyware, antitroyanos, antiadware...) en tu equipo, y por supuesto mantenlo actualizado para que pueda detectar nuevo malware.
- No utilices ordenadores compartidos (instituto, biblioteca...) para conectar a Internet utilizando tu usuario y contraseña (por ejemplo, para conectar a redes sociales, correo electrónico...). Otras personas pueden haber intervenido el equipo para robarte la información.
- El ordenador debe permanecer en una zona común de la casa para evitar que se haga un mal uso.
- Por supuesto, no compartas tu contraseña con nadie: con frecuencia es lo único que te identifica en la red -como el DNI en el mundo real-, así que mantenla en privado.
- Cada vez que publiques algo en Internet (una foto en Facebook, un comentario en un blog, una modificación de tu página web...) piensa que cualquier persona, desde cualquier parte del mundo, podrá acceder a esta información y utilizarla de muchas maneras, no todas correctas.
- Si detectas cualquier amenaza contra ti o contra cualquier otro menor, notifícalo a los adultos que corresponda en cada caso (padres, tutores, profesores...). Esta recomendación incluye todas las amenazas comentadas aquí, desde la infección por virus hasta el chantaje.
- Recuerda que en Internet puede suceder lo mismo que en el mundo real... por tanto, ten el máximo cuidado cuando conectes, igual que lo tienes cuando cruzas una avenida o sales con los amigos.

9. SEGURIDAD Y TELEFONÍA MÓVIL

Aunque los móviles no son actualmente parte activa de Internet, tal y como la conocemos hoy en día, no hay duda alguna de que estos dispositivos son otro de los principales medios de comunicación de los jóvenes, con sus ventajas y riesgos. En este caso, se detallarán las ventajas del móvil tanto para situaciones de emergencia (112) como para mantenerse en contacto con la familia, amigos, etc. De la misma manera, se describirán los problemas y amenazas a los que se enfrentan los usuarios de móviles: robo del dispositivo, robo de información personal, sistemas de suscripción, descargas para móviles, etc. La idea es trasladar que el móvil es, desde cierto punto de vista, casi una tarjeta de débito de la que servicios malintencionados pueden abusar sin el consentimiento del usuario.

Internet y los menores

El teléfono móvil puede ser para los menores, al igual que para los adultos, una ayuda indispensable ante situaciones de riesgo de cualquier índole: desde un accidente de tráfico hasta una pelea callejera, pasando por un atraco o una pérdida de la orientación -por ejemplo, en excursiones-. Podemos decir, sin duda, que en la actualidad un teléfono puede llegar a salvar vidas con una simple llamada: no tenemos más que pensar en el número de emergencias (112) detrás del que se encuentra el Centro de Coordinación de Emergencias de la Generalitat Valenciana, centro que con una simple llamada es capaz de poner en marcha a Fuerzas y Cuerpos de Seguridad del Estado, Protección Civil, servicios sanitarios, bomberos, y un largo etcétera de servicios que pueden ser indispensables para que el menor -o de nuevo, un adulto- salve una situación de riesgo. Desde luego, disponer de un teléfono móvil es a día de hoy una garantía en estas situaciones, pero por supuesto, cualquier elemento tecnológico, desde el punto de vista de la seguridad, tiene su parte positiva y su parte negativa.

Cada vez más frecuentemente, los teléfonos móviles son pequeños ordenadores de bolsillo, pequeños ordenadores que se ven afectados por los mismos problemas que hemos comentado en otros capítulos del presente curso, pero con un agravante: siempre van con el menor. Hoy en día, desde muchos teléfonos es posible conectar con nuestro banco online, navegar por Internet o chatear con nuestros amigos, posiblemente fuera del control de los adultos y desde cualquier parte del mundo (con la sensación de anonimato, o el anonimato real, que esto implica). El teléfono no sólo nos sirve para hablar, sino que es agenda, lista de contactos, navegador... de esta forma, los problemas de phishing, robo de información, delitos... comentados durante este curso, se extrapolan casi directamente a muchos teléfonos móviles de los utilizados a diario por los menores: sólo imaginemos que quien accede al teléfono móvil de un menor con toda probabilidad tendrá acceso no sólo a su lista de contactos, sino a su agenda personal (lugares frecuentados, citas, horarios...), a información confidencial de muchos amigos o conocidos, e incluso a imágenes privadas (teléfonos con cámara digital).

Caso aparte son estos teléfonos con cámara, y que con demasiada frecuencia son utilizados para grabar peleas, vejaciones, abusos... en centros educativos, en centros de ocio, o en la propia vía pública. Aparte del delito cometido en estos casos, en el que de nuevo entra la tecnología -aunque sea colateralmente - las cámaras en los móviles pueden constituir un peligro contra la intimidad de nuestros menores, ya que en caso de robo o pérdida del dispositivo, quien lo encuentre puede tener acceso a imágenes personales, con las implicaciones que esto supone para los menores.

En definitiva, a la hora de hablar de la seguridad de los menores, es imprescindible hablar de la telefonía móvil, y en especial de sus implicaciones en la intimidad del menor; es importante la concienciación en este sentido, y no sólo de los adultos, sino sobre todo de los propios menores: a fin de cuentas, casi ningún padre puede controlar el uso que su hijo hace del teléfono cuando no está con él, y debemos explicar claramente a nuestros hijos las connotaciones que puede suponer el robo o la pérdida del teléfono o un mal uso del mismo. La mejor medida de seguridad es, de nuevo aquí, la concienciación adecuada acerca de los peligros que el uso de las nuevas tecnologías implica.

10. HERRAMIENTAS GRATUITAS

A continuación se referencian algunas herramientas gratuitas que permiten a los padres conocer y controlar los contenidos a los que sus hijos acceden en la Red (se puede encontrar un listado más completo en este enlace) :

1. **Asesor de contenidos de Internet Explorer**
   Enlace: http://www.microsoft.com/spain/windows/ie/using/howto/contentadv/config.mspx

   Idioma: Español

   Características:

   - Es una opción en el navegador Internet Explorer.
   - Puede configurarse de tal forma que active diferentes filtros y detecte los contenidos según haya sido etiquetada la página.
   - Da la posibilidad de crear listas de páginas "permitidas" para incluir los sitios que consideras adecuados para tus hijos (listas blancas).
   - Permite agregar "filtros adicionales" más complejos que simplemente las etiquetas en la página.

2. **Parental control bar**
   Enlace: http://www.aboutus.org/ParentalControlBar.org

   Idioma: Inglés

   Características:

   - La instalación se hace de la misma forma que una "barra de herramientas" en los navegadores Internet Explorer, Firefox y Safari en computadoras con sistema operativo Windows 98/ME/2000/XP.
   - Cuando se activa el Child Mode, automáticamente se bloquean las páginas etiquetadas con contenidos no aptos, las que no estén clasificadas (esto es configurable) y las que se agreguen a la lista negra.
   - Permite la creación de listas de páginas blancas para incluir los sitios que consideras adecuados para tus hijos.
   - Permite colocar páginas que estén etiquetadas como aptas dentro de las listas negras si contienen información inadecuada.
   - Da la opción de saber en qué páginas ha entrado tu hijo.

3. **Naomi**
Enlace: http://www.naomifilter.org/spanish.html

Idioma: Varios (incluye español)

Características:

- Se instala como una aplicación independiente en Windows NT/ME/2000/XP
- Si detecta un contenido inadecuado, automáticamente cierra el navegador. La detección se realiza por medio de técnicas inteligentes que van más allá del simple etiquetado..
- No se puede configurar. Para dejar pasar páginas aptas que, por defecto han sido bloqueadas, es preciso desactivar el programa..
- Además de bloquear el navegador, bloquea también programas de tipo chat, compartir archivos, etc.

4. **Leopard**
Enlace: http://www.faq-mac.com/noticias/node/26785

Idioma: Español

Características:

- Permite la configuración de cuentas de usuario específicas para los niños
- Permite la restricción de contenidos de tres formas diferentes: acceso ilimitado, limitación selectiva y aprobación selectiva.
- Control del acceso a mail e iChat (aplicaciones de mensajería instantánea relacionadas con MSN aparecerán como otras aplicaciones.)
- Permite un control del tiempo de uso.
- Da la opción de saber en qué páginas ha entrado su hijo.

11. RESUMEN DE RECOMENDACIONES

Por otro lado, tal y como se ha presentado anteriormente, resulta necesario poner al servicio de los usuarios una serie de recomendaciones para evitar que los menores sean víctimas o accedan a contenidos ilícitos e inapropiados. En esa línea, desde INTECO se ofrece a todos los usuarios las siguientes recomendaciones:

Internet y los menores

- Eduque al menor sobre los posibles peligros que puede encontrar en la Red.
- Acompañe al menor en la navegación cuando sea posible, sin invadir su intimidad.
- Advierta al menor de los problemas de facilitar información personal (nombre, dirección, teléfono, contraseñas, fotografías, etc.) a través de cualquier canal.
- Aconséjele no participar en charlas radicales (provocadoras, racistas, humillantes, extremistas, etc.) ya que pueden hacerle sentir incómodo.
- Infórmele de que no todo lo que sale en Internet tiene que ser cierto, ya que pueden ser llevados a engaño con facilidad.
- Preste atención a sus "ciber-amistades" en la misma media que lo hace con sus amistades en la vida real.
- Pídale que le informe de cualquier conducta o contacto que le resulte incómodo o sospechoso.
- Vigile el tiempo de conexión del menor a Internet para evitar que desatienda otras actividades.
- Utilice herramientas de control parental que le ayudan en el filtrado de los contenidos accesibles por los menores.
- Cree una cuenta de usuario limitado para el acceso del menor al sistema.