MENORES EN LA RED

¿Un juego de NIÑOS?

PANDA SECURITY | *One step ahead.*

MENORES EN LA RED
¿Un juego de NIÑOS?

En 2007, el malware (virus, spyware y otros códigos maliciosos) se multiplicó por diez respecto al año anterior. Además, los ciber-delincuentes han encontrado en las nuevas herramientas como la mensajería instantánea (MSN Messenger, Yahoo! Messenger…), los programas de intercambio de archivos (eMule, Kazaa…) o los blogs una nueva forma para infectar a los usuarios o hacerse con sus datos confidenciales.

En otras palabras, los riesgos en Internet van en aumento y los menores, por ser los menos preparados, son también los más desprotegidos.

A continuación exponemos cuáles son las principales amenazas que presenta Internet para los menores, así como la forma en que pueden defenderse de ellas. Gran parte de esa tarea de protección será de los padres, que deben ser capaces de controlar lo que sus hijos hacen en Internet, educándoles en un uso responsable y seguro de las nuevas tecnologías.

Datos significativos: menores e internet

El 49% de los alumnos de Educación Secundaria Obligatoria (ESO) dedica al menos una hora diaria a navegar por Internet, según el avance del *Estudio* del Observatorio Estatal de Convivencia Escolar. Además, el 51,8% de ellos cuenta con poco o nulo control de sus padres a la hora de utilizar Internet.

De hecho, en España, 7 de cada 10 niños y niñas de entre 10 y 14 años *usan Internet*, siendo Cataluña la región donde más menores se conectan a Internet, el 88,5%.

Es decir, Internet es un mundo cotidiano en la vida de los menores. Pasan muchas horas conectados, tanto en el colegio como en casa. Por eso, tanto sus padres como ellos mismos deben conocer qué riesgos les acechan en la Red y cómo combatirlos.

En España, 7 de cada 10 niños y niñas de entre 10 y 14 años usan Internet. Tanto sus padres como ellos mismos deben conocer qué riesgos les acechan en la Red y cómo combatirlos

Principales riesgos

Los niños y jóvenes que navegan por Internet se enfrentan a distintos riesgos. Desde posibles fuentes de infección del ordenador hasta una suplantación de personalidad que puede terminar en un mal encuentro.

A continuación, recogemos una lista de las principales amenazas y la forma en que padres e hijos pueden enfrentarse a ellas.

Las herramientas de mensajería instantánea utilizan email y contraseña como identificadores de usuario. Este sistema dificulta conocer a nuestro interlocutor

La mensajería instantánea y el correo electrónico

La mensajería instantánea (a través de programas como MSN Messenger, Yahoo! Messenger, Google Talk…) se ha convertido en una de las principales herramientas de comunicación entre los jóvenes. Este uso masivo no ha pasado desapercibido a los ciber-delincuentes, que las han convertido en uno de los principales medios en los que actuar.

Uno de los riesgos a los que se enfrentan los niños y jóvenes que emplean estas herramientas es la suplantación de identidad (que alguien se haga pasar por otra persona para engañar a su interlocutor). En estos programas, la identificación de los usuarios se produce a través de una dirección de correo asociada a un password. De esta manera, si alguien accede a la cuenta de uno de nuestros contactos, no habrá nada que indique que con quien estamos hablando no es nuestro interlocutor legítimo. Si tenemos archivos compartidos con ese contacto, el atacante podrá acceder libremente a los mismos. Por eso, es importante no compartir información confidencial (datos personales, dirección física, números de identificación o bancarios, claves, etc.) a través de medios inseguros como la mensajería instantánea.

Otro peligro de la suplantación de identidad – mucho más serio y que ya ha provocado fuertes alarmas sociales- es el de la pederastia. Casos como el de la menor asturiana que fue coaccionada por un pederasta que contactó con ella por Messenger y *otros ocurridos en los últimos meses* han puesto de manifiesto el uso de estos servicios por parte de pedófilos. Éstos, una vez ganada la confianza de los menores, buscan citarse con ellos en persona o conseguir fotos comprometedoras. Para alcanzar esa intimidad, los pederastas se hacen pasar por personas jóvenes, fotógrafos de moda interesados en hacerles un book a los adolescentes y otras argucias similares.

Para proteger a los menores de este riesgo, lo mejor es enseñarles - como se hace en la vida real- a no tratar con desconocidos y darles la confianza suficiente para, en caso de dudas o temor, hablar abiertamente con sus padres u otro adulto.

La infección del ordenador por la entrada de algún virus u otro código malicioso es otro de los riesgos de la mensajería instantánea. Más del 58,6% de los gusanos (códigos maliciosos capaces de difundirse por sí mismos) detectados en el primer semestre del año por PandaLabs estaban diseñados para propagarse a través de estas herramientas. Alguno de ellos están diseñados para capturar

MENORES EN LA RED
¿Un juego de NIÑOS?

Contra el malware que se distribuye a través de Mensajería, lo mejor es: no ejecutar ningún archivo ni seguir ningún link que nos llegue por este medio

contraseñas bancarias de banca online. El riesgo en caso de infección, por lo tanto, ya no es sólo para los jóvenes, sino que en el caso de utilizar el mismo ordenador que sus padres, un uso inadecuado de estos servicios puede suponer el robo de las claves bancarias – y con ellas, del dinero- de los padres.

Para luchar contra los códigos maliciosos que se distribuyen a través de Mensajería Instantánea, lo mejor es seguir un sencillo consejo: no ejecutar ningún archivo ni seguir ningún link que nos llegue por este medio. Al menos, no antes de preguntar a la persona que supuestamente nos lo envía, si de verdad lo está haciendo.

El correo electrónico es otra de las fuentes de riesgo para lo más pequeños. En este caso, las amenazas son varias:

- En primer lugar, está el spam. En muchas ocasiones, llegan al correo e-mails que anuncian todo tipo de cosas, desde casinos online hasta medicinas. Los niños y niñas, mucho más inocentes que un adulto, pueden creer todo lo que se cuenta en estos e-mails y causarse a sí mismos un grave problema. Así, pueden acceder a casinos online y perder dinero, acabar desarrollando una ludopatía o adquirir medicinas – incluso drogas- de procedencia más que dudosas y que, en caso de estar adulteradas, pueden provocarle un grave problema de salud.

- En segundo lugar, se encuentran las falsas ofertas de trabajo. Este riesgo quizás no afecte a los más pequeños, pero sí es un peligro para los adolescentes. Se trata de correos que ofrecen increíbles ofertas de trabajo. El usuario podrá ganar mucho dinero a cambio de no hacer nada o prácticamente nada. Tan sólo tendrá que facilitar un número de cuenta bancaria donde se le ingresará un dinero que tendrá que desviar a otra cuenta, a cambio de una comisión. Parece tan sencillo que a cualquier adulto con sentido común le haría sospechar. Sin embargo, un joven que quiera dinero fácil puede caer en la tentación. Y eso le supondría estar convirtiéndose en el cómplice de un delito, ya que el objetivo de esos movimientos bancarios es blanquear dinero procedente de actividades delictivas.

- Un tercer riesgo es el de que se introduzca algún virus u otro ejemplar de malware en el ordenador. Los códigos maliciosos que se distribuyen a través de este sistema muchas veces incitan a los usuarios a seguir un vínculo o descargar un archivo (lo que provocará la infección) mediante el uso de un tema sugerente: acceder al trailer de una película, imágenes eróticas de famosos, descargas de juegos, etc. Esto se conoce como ingeniería social. Estos ganchos suelen hacer picar a muchos adultos, lo que puede dar una idea de lo fácil que sería engañar a un menor.

Para proteger a los menores ante estas amenazas, lo mejor es enseñarles a desconfiar de los e-mails que proceden de fuentes desconocidas. Hay que convencerles de que no todo lo que se cuenta en esos mails es verdad y de que no deben ejecutar ningún archivo ni pinchar sobre ningún link que proceda de este tipo de fuentes.

Los riesgos de los programas de intercambios de archivos (emule, kazaa, etc.)

El intercambio de archivos a través de estos programas es otra de las principales fuentes de infección de los ordenadores. Muchos códigos maliciosos –generalmente los denominados gusanos- se copian en las carpetas de esos programas con nombres sugerentes (títulos de películas, de programas, etc.) con el fin de que otros usuarios los descarguen y ejecuten en su ordenador.

El peligro es similar al de la ingeniería social – de hecho, este comportamiento podría considerarse una variante de la misma- : el nombre sugerente puede servir para tentar a los niños y niñas que, sin querer, estarán introduciendo en el ordenador un archivo malicioso.

Por eso, los menores deben saber qué archivos pueden bajarse y cuáles no de estas redes. Además, conviene analizar el archivo con una solución de seguridad antes de ejecutarlo por primera vez. Si cuando lo abrimos aparece un mensaje de error u otro en el que se nos pide la descarga de una licencia o de un codec, debemos comenzar a sospechar, puesto que, casi con total seguridad, ese archivo esconde algún código malicioso.

Muchos códigos maliciosos se copian en las páginas más visitadas con el fin de que los usuarios los descarguen y ejecuten

Redes sociales y blogs

Las llamadas redes sociales (portales como Hi5 o Facebook) que sirven para compartir fotos y vídeos, conocer gente, chatear…, son, junto con los blogs o bitácoras, algunos de los sitios web más visitados por los jóvenes. Un elemento común de estas páginas es la necesidad de crear un perfil personal para acceder a las mismas. En esos perfiles se suelen poner datos como el nombre, la edad, etc.

Conviene recordar a los menores que, generalmente, no es necesario dar esta información, sino que basta con una dirección de correo y un nombre, que puede no ser el verdadero, sino un "nick" o seudónimo. Además, conviene que no faciliten datos como su edad, su dirección y, mucho menos, fotografías suyas.

El blog se ha convertido para muchos menores en el sustituto online del tradicional diario personal. Como en éste, en las bitácoras de la web se da en muchas ocasiones más información de lo aconsejable. Por eso, los jóvenes deben tomar precauciones para no publicar datos que puedan servir para identificar al usuario como un menor, o para conocer su lugar de vivienda, de estudio, etc.

Además, en varias redes sociales como Hi5 se pueden compartir archivos y ficheros con el resto de usuarios. Los menores deben tener especial cuidado con qué comparten y a quién dan permiso para ver esta información. No hay problema en colgar fotos, por ejemplo, siempre y cuando éstas se protejan con una clave que sólo se distribuya entre los amigos y familiares.

Los padres deben conocer estos nuevos servicios, su funcionamiento y sus riesgos. Y también ser capaces de transmitir a sus hijos la forma correcta y segura de utilizarlos.

El uso de smartphones con tecnologías como el bluetooth y una rápida conexión a Internet están volviendo a los móviles más vulnerables a los ataques

Móviles con Internet: nueva fuente de riesgo

Según un estudio de la firma Frost & Sullivan, la creciente sofisticación de los teléfonos móviles llevará a que los ciber-delincuentes los sitúen como uno de sus objetivos prioritarios en los próximos años. El uso de teléfonos con tecnologías como el bluetooth (que permite el intercambio de archivos entre teléfonos sin cables) y una rápida conexión a Internet los están haciendo más vulnerables a los ataques a estos dispositivos.

El teléfono móvil es otro de los grandes complementos de los jóvenes de hoy en día. Los riesgos a los que se enfrentan en este campo no distan mucho de aquéllos que se han comentado para el ámbito del PC.

En primer lugar, los servicios de mensajería instantánea para móviles es algo ya habitual. Los chavales pueden chatear en cualquier sitio y los riesgos son los mismos que ya se han comentado más arriba: robo de identidad, malos encuentros, infección del dispositivo, etc.

El spam para el móvil también es algo que está a la orden del día. Ya desde hace unos años se llevan registrando envíos de SMS que anuncian todo tipo de productos y servicios. Muchos de ellos están relacionados con la pornografía. Es decir, ésta ya no sólo se introduce en el ordenador del niño, sino que sigue a éste allá donde va a través de su teléfono móvil.

Por lo tanto, los padres también deberán controlar el uso que sus hijos hacen de la telefonía móvil. Para ello, es aconsejable, en el caso de los más pequeños, comprarles dispositivos que no cuenten con funciones que puedan ser fuente de riesgo y, en el caso de los más mayores, aconsejarles sobre el uso adecuado de estos dispositivos. Hay que recordarles que no deben contestar a mensajes de procedencia sospechosa, ni citarse con desconocidos.

El riesgo de infectarse

Hemos visto en los epígrafes anteriores diversas formas en que los usuarios más jóvenes pueden infectar su ordenador o el de la familia (links que llegan a través de la mensajería instantánea o del correo, descarga de archivos infectados…). Los peligros que supone tener un código malicioso corriendo en el sistema son muchos y variados.

En primer lugar, y como se comentó anteriormente, si los jóvenes comparten el ordenador con sus padres, se corre el riesgo de que una conducta de riesgo del joven acabe infectando el ordenador con programas diseñados para robar las claves bancarias cuando los adultos inicien su sesión.

Pero el malware no es sólo un riesgo para los adultos. También lo es para los propios menores. Por ejemplo, puede ocurrir que se introduzca un adware en su ordenador. Estos códigos maliciosos están diseñados para mostrar anuncios mediante ventanas emergentes, banners, etc. En el caso de los adultos, estos ejemplares de malware pueden ser más molestos que otras cosa (aunque también deben tener cuidado, ya que algunos descargan troyanos en el equipo), pero en el caso de los niños y niñas el riesgo es mayor, puesto que algunos muestran anuncios y dirigen a páginas de claro contenido pornográfico. Así, los menores pueden encontrarse con la pornografía en su propio PC, sin necesidad de navegar para dar con ella.

Si los jóvenes comparten el ordenador con sus padres, se corre el riesgo de que las conductas irresponsables infecten la máquina

MENORES EN LA RED
¿Un juego de NIÑOS?

Consejos para los padres

1 **Habla con tus hijos.** La primera tarea que tienes que emprender para proteger a tus hijos es hablar con ellos. Debes saber qué páginas visitan, con quién conversan, qué les gusta ver, etc. Igual que no los dejarías salir de casa sin saber dónde van y con quién, no debes dejarles acceder a Internet sin antes saber si lo que están haciendo está bien.

2 **Infórmate y aconseja a tus hijos.** Para muchos padres, Internet es aún un mundo desconocido. Otros lo utilizan para buscar información, leer la prensa o descargar música, películas y otros archivos, pero para la gran mayoría los servicios que emplean sus hijos son completamente desconocidos. Por ello, un paso muy importante será informarte sobre las herramientas que ofrece la web a los menores, los peligros de las mismas y la forma de evitarlos. Una vez cumplido esto, podrás aconsejar a tus hijos sobre la forma más segura de disfrutar de aquello que les gusta.

3 **Establece reglas firmes del uso de Internet.** Debes poner normas claras y tajantes que regulen el horario, tiempo de conexión y forma de uso de Internet. Además, debes vigilar su cumplimiento, especialmente en lo que se refiere al horario nocturno. Otro aspecto es el de la situación de los ordenadores en la casa: si utilizáis un solo PC para toda la familia, es mejor que éste esté en un lugar común y no en la habitación de un menor.

4 **Prohíbe a los menores dar información confidencial.** Debes enseñar a tus hijos a no facilitar datos como su nombre, su dirección o sus fotos a través de la Red. Recomiéndales que utilicen pseudónimos o nicks en los foros a los que se conectan y enséñales a crear contraseñas seguras (que mezclen mayúsculas, minúsculas y números) que impidan que los ciber-delincuentes o usuarios malintencionados accedan a sus cuentas de correo, de mensajería o similares.

5 **Enseña a tus hijos a desconfiar de las apariencias.** En Internet las apariencias engañan. Hemos visto cómo los códigos maliciosos se disfrazan de códecs o de trailers de películas, cómo muchos pederastas se hacen pasar por quien no son para entablar amistad con menores o cómo un mensaje que parece venir de un contacto conocido de mensajería instantánea puede estar infectado. Por lo tanto, muchas veces en la Red nada es lo que parece. Por eso, debes enseñar a los menores a ser desconfiados y a no realizar acciones que pongan en riesgo su seguridad y su intimidad.

6 **Instala una solución de seguridad eficaz.** Para proteger de los códigos maliciosos a tus hijos, lo mejor es contar con una solución eficiente y actualizada. Las soluciones para el hogar de Panda ya no sólo eliminan el malware, sino que además bloquean aquellas páginas que puedan infectar el sistema, bloquean el spam e, incluso en el caso de Panda Internet Security, cuentan con un sistema de filtrado (control parental) que te permite decidir qué páginas pueden visitar tus hijos y cuáles no.

MENORES EN LA RED
¿Un juego de NIÑOS?

Consejos para los menores

1 **No pinches sobre links.** Cuando estés hablando por un sistema de mensajería instantánea o recibas un correo, no pulses nunca directamente sobre ningún vínculo. Si el mensaje o correo procede de un usuario conocido, teclea la dirección en la barra del navegador. Si procede de fuentes desconocidas, es mejor que lo ignores. Aunque lo teclees en el navegador, podrías terminar en una página maliciosa que trate de introducir malware en tu equipo.

2 **No descargues ni ejecutes archivos de procedencia desconocida.** En muchas ocasiones habrás recibido a través de mensajería instantánea un mensaje de un contacto que te invitaba a descargarte una foto, una canción o un vídeo. En ocasiones, ese archivo no habrá sido enviado por el contacto, sino por un programa malicioso que le ha infectado y que está tratando de extenderse a más usuarios. Por ello, lo mejor que puedes hacer es preguntar a tu contacto si de verdad te ha enviado algo. Si contesta que no, infórmale de que está infectado y que debe poner un mensaje en su nick que se lo haga saber a sus contactos, para que estos no se "contagien" también mientras él elimina el archivo dañino de su ordenador.

3 **No hables con desconocidos.** En los chats o en los sistemas de mensajería instantánea, nunca podemos tener una completa seguridad de quién está al otro lado. Menos aún cuando se trata de comunidades online cuyos miembros no tienen ninguna relación previa entre sí. Por eso, procura no entablar amistad con desconocidos y mucho menos quedar con ellos en la vida real.

4 **No proporciones información confidencial a través de la Red.** No envíes información sensible (datos privados, tu dirección, etc) a través de mail o mensajería instantánea y mucho menos aún la publiques en un blog o en un foro. Además, debes tener cuidado cuando crees tus perfiles para servicios como FaceBook o Hi5. En ellos no deben figurar datos confidenciales como tu dirección o tu edad. Además, es aconsejable que no emplees tu nombre real, sino un seudónimo o "nick".

5 **Sospecha al menor indicio.** Si algún programa que no recuerdas haber instalado comienza a mostrarte falsas infecciones o ventanas emergentes o pop-ups en los que se te invita a comprar algún tipo de antivirus, u otro producto, desconfía. Lo más seguro es que en tu equipo se haya instalado algún tipo de malware.

6 **No ejecutes archivos sospechosos.** Si tu solución de seguridad te señala que un archivo es sospechoso de tener un malware o que, efectivamente, lo tiene, no lo abras. Simplemente, elimínalo del sistema.

7 **Habla con los mayores.** Cuando tengas dudas sobre algún tema, veas algo sospechoso o recibas correos o mensajes ofensivos o peligrosos, habla con un adulto. Él podrá aconsejarte.

Consejos para los profesores

Los profesores también tienen una importante responsabilidad a la hora de educar a los más pequeños en el uso correcto de las nuevas tecnologías, sobre todo hoy en día, cuando los ordenadores van ganando cada vez más espacio en las aulas. Por eso, hay una serie de recomendaciones que deben seguir:

1. **Infórmate.** Estudia previamente los conceptos relacionados con los peligros de la Red. Descubre cuáles son y qué consecuencias tienen y cómo puedes hacerle llegar esa información.

2. **Establece un plan de educación en seguridad informática.** Al tiempo que aprenden a manejar y a relacionarse con la informática, los más pequeños deben tomar conciencia de los peligros que encierra. De esta manera, se les estará inculcando desde pequeños una conducta segura. Para ello, conviene que establezcas un plan a seguir, preparando previamente lo que vas a contar y buscando toda aquella documentación que sea necesaria.

3. **Sé ameno y práctico en tus explicaciones.** Un buen método es utilizar ejemplos prácticos. Una de las mejores formas de que los pequeños y jóvenes tomen conciencia de los peligros es mostrarles los efectos que tienen. Busca noticias de casos reales sobre malos encuentros en la Red, información de pérdidas de datos producidas por el malware, etc.

4. **Enséñales a protegerse.** Entre las clases prácticas incluye algunas sobre la configuración del antivirus, la creación de contraseñas seguras, explicaciones sobre cómo comprar online de manera segura, etc.

PANDA SECURITY