



Guía de seguridad en línea para la familia



Por Marian Merritt

Prólogo de Lauren Nelson
Miss América 2007



Prólogo de Lauren Nelson, Miss América 2007

Uno de mis objetivos como Miss América 2007 es aumentar la concientización por la protección de nuestros niños en Internet. El tema de la seguridad en Internet se volvió importante para mí a los 13 años de edad, cuando mis amigas y yo fuimos interceptadas en una sala de chat en Internet por una persona, que más tarde descubrimos que era un depredador en línea. Cometimos el error de proporcionarle información personal, incluidos nuestros nombres, dónde estábamos y nuestra edad. Una semana después recibimos fotografías obscenas en el correo. De inmediato, se lo dijimos a nuestros padres. Tuvimos suerte de que la situación terminara sin incidentes. Aprendimos una lección muy valiosa sobre cómo protegernos en Internet.

Espero que los niños aprendan estas lecciones antes de que se encuentren ellos mismos en una situación peligrosa, como mis amigas y yo. Internet es una herramienta excelente para enterarse de las novedades, realizar búsquedas y comunicarse con otros, pero también tiene su lado oscuro: creadores de spam, estafadores y depredadores en línea. Si enseñamos a los niños de forma temprana cuáles son los peligros de Internet y cómo evitarlos, podemos ayudar a que Internet sea un lugar seguro para ellos.



La organización Miss América se asoció con Symantec para generar conciencia sobre los peligros de Internet y educar a los padres sobre cómo pueden mantener a sus hijos protegidos en Internet. Buscábamos un socio que fuera líder en tecnología de la seguridad, que llegara a las personas y en el que confiaran millones de consumidores, para promover mi proyecto personal de mantener a los niños protegidos en Internet.

Symantec se destaca como empresa y ha demostrado su compromiso con la juventud de América a través de numerosas iniciativas de seguridad para niños y “Digital Family”. En mis viajes por el país este año, podré compartir mi mensaje y su filosofía para educar y generar conciencia acerca de este serio tema.

Mi objetivo es ayudar a los padres a orientar a sus hijos en el uso de Internet. También deseamos asegurar que los niños disfruten de un entorno seguro en línea donde puedan explorar, divertirse y crecer para llegar a ser “ciberciudadanos”. Al colaborar con Symantec, podemos ayudar a hacer de Internet un lugar mejor donde los niños se comuniquen, se sociabilicen y se conecten.

Lauren Nelson



Introducción

Mi marido y yo somos padres de tres niños maravillosos que utilizan activamente los equipos de la familia. Mis hijos ponen a prueba constantemente mis conocimientos y lo que creía acerca de la tecnología y cómo ésta se adapta a sus vidas. Conozco los placeres y los peligros de Internet. Sin embargo, a medida que navegan solos por la Web (para buscar sitios de juegos nuevos, descargar música y comunicarse con amigos por correo electrónico y mensajería instantánea), me doy cuenta de que todo consiste en conocer y mantenerse al día de sus actividades.

Todos tratamos de manejar la independencia cada vez mayor de nuestros niños y de hacer todo lo posible para defenderlos y defender nuestros equipos contra muchos de los graves peligros de Internet. En esta guía, trataremos las principales preocupaciones acerca de Internet. Si desea saber más sobre el tema, le recomendaré publicaciones y sitios web que lo mantendrán informado a medida que las condiciones cambien día tras día. Quiero felicitarlo por su interés en este tema y por su deseo de aprender más. Nada me frustra más que los padres que se desentienden del tema y dicen: “¡Mis hijos saben más que yo de esto!”. Usted puede aprender lo suficiente para ayudar y saber cuándo es necesaria la asistencia de profesionales de la seguridad y del software para recuperar el control de estos asuntos.

Por eso, si su preocupación se centra en que los niños en edad escolar aprendan cómo utilizar motores de búsqueda, o en manejar la creciente dependencia de su hijo adolescente en un sitio de redes sociales, nosotros investigaremos estos temas y le brindaremos consejos y pautas fáciles de entender para abordarlos. ¡Siga adelante!

Marian Merritt

Contenido

A través de los años

<i>Niños en edad escolar (de 5 a 7 años)</i>	7
<i>Preadolescentes (de 8 a 12 años)</i>	8
<i>Adolescentes (de 13 a 17 años)</i>	10
<i>Después de la escuela y más tarde</i>	11

Sigan las normas

<i>Padres</i>	2
<i>Hijos</i>	12

Pautas básicas

<i>Navegación segura</i>	13
<i>Proteja su contraseña</i>	13
<i>Asegure su red inalámbrica</i>	14
<i>Software de control para padres</i>	15
<i>Favoritos en línea</i>	16

Riesgos

<i>Depredadores en Internet</i>	16
<i>Plagio y engaños</i>	17
<i>Acoso y acecho cibernético</i>	17
<i>Uso compartido de archivos y descargas de música y videos</i> ..	18
<i>Información privada y robo de identidad</i>	19
<i>Sitios de redes sociales</i>	20
<i>Sitios de pornografía, apuestas, racismo, anorexia y odio</i> ..	21
<i>Privacidad en línea de los adolescentes</i>	21
<i>Correo electrónico y mensajería instantánea</i>	22
<i>Blogs</i>	24
<i>Virus, gusanos y software espía</i>	24
<i>Tomar los bots en serio</i>	25
<i>Fotografías digitales</i>	26

Contenido (continuación)

<i>Compras en línea</i>	27
<i>Pago de facturas en línea</i>	28
<i>Transacciones bancarias en línea</i>	29
<i>Juegos en línea y signos de adicción</i>	29
Por último	30
Principales consejos para proteger a su familia en Internet	30
Sitios de recursos importantes	31
Marian Merritt	31

A través de los años

Niños en edad escolar (de 5 a 7 años)

En la actualidad, ésta es la edad en la que muchos niños se introducen en Internet. Ahora que más y más escuelas cuentan con laboratorios de informática, equipos o Mac en el aula, es posible que un niño utilice un equipo por primera vez en la escuela. Otros tendrán su primera experiencia con un equipo en el hogar, donde aprenderán de sus padres o hermanos mayores. De acuerdo con la resolución del Senado de los Estados Unidos que nombra el mes de junio como el mes de la seguridad en Internet, 35 millones de niños estadounidenses, desde el jardín de infantes hasta los 12 años, tienen acceso a Internet, y el 80 por ciento se conecta al menos 1 hora a la semana.

Por lo general, a los niños pequeños les atraen mucho los juegos simples y los sitios educativos, pero rápidamente aprenderán de sus compañeros acerca de sitios nuevos. Algunos sitios web, como Neopets, Webkinz y Club Penguin, son para niños a partir de los 7 u 8 años de edad. A ellos nos referimos como sitios de redes sociales de nivel inicial, ya que muchos tienen chat y otras funciones de comunicación. Los padres de niños pequeños deberían desactivar estas funciones desde el principio. A los niños de esta edad les resulta difícil entender el “peligro de los desconocidos” asociado con alguien que contacta con ellos a través de la interfaz amigable de su juego favorito o de un sitio social. Más adelante, usted podrá enseñarles que existe la posibilidad de conversar con personas que conocen, como tíos, primos o amigos (pero asegúrese de reiterarles que siempre deben consultarle antes de hablar con alguna persona en línea).

Lo ideal sería que cuando los niños alcancen esa edad, usted ya estará al tanto de sus actividades en línea de la misma manera que lo está de sus tareas escolares. Por ejemplo, deberá asegurarse de tener a la vista el equipo que utiliza el niño. El software de control para padres lo ayuda a limitar los sitios a los que su hijo tiene acceso, aun cuando usted no está con él. Los controles también restringen todo

tipo de información que no desea que su hijo comparta, ya sea su nombre, edad, número de teléfono o cualquier otra información privada. Debe encender todas las funciones de filtrado y seguridad del motor de búsqueda de su equipo (como la función de búsqueda segura de Google) para evitar que sus hijos puedan acceder a un sitio de adultos o inapropiado). Asegúrese de mostrar a su hijo cómo cerrar la ventana de un navegador y hágale saber que SIEMPRE CONVIENE cerrar un sitio si ocurre algo sorprendente o molesto. Dígales que nunca conversen, escriban mensajes o compartan información con personas de estos sitios, salvo si usted está con ellos.

Recomendaciones clave:

- *Limite los sitios web aprobados y las horas que dedican a Internet.*
- *Defina configuraciones de alta seguridad con navegadores, pertenencia a sitios y sitios de redes sociales.*
- *Instale y mantenga software de seguridad en Internet y controles para padres.*
- *Utilice controles para padres para limitar los sitios web que pueda visitar su hijo.*
- *Supervise el uso que su hijo le da al equipo y siéntese con él/ella cuando esté conectado a Internet.*
- *Háblele acerca de proteger la información privada (nombre, número de teléfono, etc.) y de no compartir nunca las contraseñas con los amigos.*

Preadolescentes (de 8 a 12 años)

Los preadolescentes son mucho más sociales y aventureros en el uso de los equipos. Hablan con sus compañeros de escuela y aprenden acerca los sitios más nuevos y “más de moda”. Podrían registrarse en su primera cuenta de correo electrónico y mensajería instantánea. Pregúntele a su hijo sobre esas cuentas y cuáles son sus contraseñas para poder supervisar sus actividades y saber con quiénes se comunica. Es posible que los niños de esta edad también comiencen a consultar sitios de redes sociales, como MySpace, Facebook y Friendster, que son populares entre adolescentes y

adultos. La mayoría de ellos no creará una página hasta que sean un poco más grandes, pero conversarán con amigos, hermanos mayores y otros familiares que tengan sus páginas y perfiles, y por lo tanto, visitarán dichas páginas y se suscribirán a ellas.

A los preadolescentes también les interesa mucho la música, e Internet les resulta una forma sencilla de escuchar, descubrir y descargar canciones nuevas, además de reunirse con otros que comparten sus mismos intereses musicales. También podrían seguir las últimas novedades acerca de un grupo favorito o una celebridad visitando su blog o su sitio web y consultando diferentes sitios para obtener los últimos chismes y descargar fotografías. Los sitios de videos por Internet, como YouTube! son muy populares. Muchos de los videos contienen lenguaje fuerte o material violento, por eso es necesario supervisar atentamente las visitas de los preadolescentes. Los preadolescentes más creativos aprenden la forma de tomar sus propias fotografías digitales, editar videos y compartir sus creaciones con amigos y familiares. Con su ayuda, o con la ayuda de un amigo con más experiencia, también comienzan a publicar sus creaciones en Internet.

Recomendaciones clave:

- *Consulte con frecuencia el historial de Internet de su equipo para ver los sitios que han visitado sus hijos y supervise sus cuentas de correo electrónico y mensajería instantánea para ver con quiénes se comunican.*
- *Establezca normas sobre la comunicación por Internet, la descarga ilegal y el acoso cibernético.*
- *Sus hijos deben saber que nunca deben hacer clic en un vínculo de un correo electrónico o de un mensaje instantáneo, ya que es la forma más común de recibir virus o de revelar información privada a los delincuentes.*
- *Conversen acerca de los riesgos y problemas que implica publicar y compartir información privada, videos y fotografías.*

- *Esté atento ante los signos de conductas obsesivas o adictivas en Internet (vea la sección Juegos en línea y Signos de adicción).*
- *Coloque los equipos en áreas comunes de la casa.*
- *Promueva la comunicación abierta y motive a sus hijos a que le cuenten si hay algo en Internet que los hace sentir incómodos.*

Adolescentes (de 13 a 17 años)

Los adolescentes están adquiriendo una independencia aún mayor, y esto se refleja en sus actividades en línea. Esa independencia conlleva responsabilidades, entre ellas, tener cuidado en su mundo en línea. En estas edades, los adolescentes por lo general ya participan en mundos en línea como MySpace, Friendster, Facebook y otros, o se han suscrito a ellos. Los adolescentes se cuentan entre sí los detalles de sus vidas mediante nombres, blogs, perfiles y otros elementos de Internet que visitan diariamente. En toda la Web, pueden quedar los rastros digitales de sus pensamientos. Muchas veces, no saben (o se olvidan) que todo lo que publican en la Web queda allí para que todos lo vean, y probablemente permanecerá allí indefinidamente. Con sólo hacer una simple búsqueda en Google, el director de admisiones de una universidad o una empresa (por cinco, diez o incluso veinte años desde el presente) podrá acceder a todas las fotografías, opiniones y pensamientos de su hijo adolescente, ya que estarán allí, al alcance de todos, de por vida. ¡Por eso es muy importante tener precaución!

Recomendaciones clave:

- *Refuerce las normas de comportamientos adecuados en línea (lenguaje, información privada e imagen, ética cibernética, descarga ilegal, límites en las horas de uso de los equipos y evitar los sitios para adultos).*
- *Esté al tanto de la vida en línea de su hijo adolescente (sitios de redes sociales, fotografías, información privada, actividades de clubes y deportivas), ya sea en su sitio, en el sitio de un amigo o en las páginas web de sus escuelas.*

- *Revise los sitios que visita; no tenga miedo de discutir y tal vez de tener que restringirle sitios que encuentra ofensivos o preocupantes.*
- *Recuerde que su hijo adolescente accede a Internet desde el hogar, la escuela, la casa de un amigo, la biblioteca, el teléfono celular o incluso desde un sistema de juegos; por eso, converse con él acerca de sus actividades en todos esos casos.*
- *Pídales que no descarguen archivos (ya sea música, juegos, protectores de pantallas, ringtones) ni que realicen transacciones financieras sin su autorización.*
- *Enséñeles que nunca deben compartir las contraseñas y que deben ser precavidos al escribir información privada cuando estén en un equipo compartido o público, o en uno que piensen que podría no ser seguro.*
- *Enséñeles que nunca deben hacer clic en un vínculo de un correo electrónico o de un mensaje instantáneo, ya que es la forma más común de recibir virus o de revelar información privada o útil a los delincuentes.*
- *Coloque los equipos en áreas comunes de la casa y no en el dormitorio del adolescente.*
- *Promueva la comunicación abierta y motive a su hijo adolescente a que le cuente si hay algo en Internet que lo hace sentir incómodo. Recuerde que son adolescentes, pero aún siguen siendo niños.*
- *Recuérdale a su hijo adolescente que asuma la responsabilidad de mantener el software de seguridad en Internet actualizado, tanto para la protección de él como para la suya.*

Después de la escuela y más tarde

A medida que su hijo adolescente crece y abandona el hogar, ya sea para ir a la facultad o al trabajo, necesitará entender otras responsabilidades de los adultos que debe asumir para moverse en el mundo en línea. Dichas responsabilidades incluyen proteger la privacidad, especialmente el número de la seguridad social y la

información financiera, impedir el robo de identidad y evitar los riesgos relacionados con el historial crediticio, que es particularmente importante para un adulto joven. Si su hijo adolescente utiliza un equipo portátil en la universidad o en su nuevo trabajo, asegúrese de que comprende los riesgos adicionales que implican el uso de las conexiones inalámbricas y de que adquiera el software de seguridad necesario, además de una solución de copia de respaldo confiable. Es posible que se sientan tentados de obviar estas cuestiones, por eso es bueno insistir en la vigilancia cuando se trata de la seguridad de su equipo portátil.

Sigan las normas

Padres

- **Manténganse actualizados** con la tecnología. No tienen que ser expertos, pero comprender, aunque sea un poco, la tecnología contribuye notablemente a mantener a su familia protegida en Internet. Reciban capacitación técnica básica y conozcan los productos nuevos ni bien estén disponibles. Visiten www.norton.com/familyresource para estar actualizados.
- **Mantengan una comunicación** fluida con sus hijos acerca de todo lo que experimentan en Internet. Aprendan su dialecto y pregúntenles cuando no entiendan algo. Trabajen para mantener sus líneas de comunicación abiertas.
- **Consulten siempre** las actividades en Internet de sus hijos. Sepan lo que visitan en línea. Háganles saber que les seguirán consultando porque los quieren y desean que entiendan que Internet es un foro público y nunca es verdaderamente privado.

Niños (cortesía de *iKeepSafe.org*)

- **Manténganse seguros:** mantengan protegida su información personal... ¡toda! Nunca les den su nombre verdadero, dirección, número de teléfono, nombre de la escuela o fotografía a nadie por Internet.

- **Manténganse alejados:** los extraños que aparecen en Internet son peligrosos... MANTÉNGANSE ALEJADOS. No importa lo que les digan, NUNCA se encuentren con ninguno de ellos en persona. No hay forma de saber quiénes son en realidad. No hablen con ellos en línea, y nunca les digan dónde viven.
- **Manténganse comunicativos:** cuéntenles a sus padres o a un adulto de confianza todo lo que ven por Internet. Cuando algo los haga sentir incómodos, hablen siempre con ellos. Recuerden que no todo lo que ven o escuchan en Internet es “verdad” o incluso “normal”.

Pautas básicas

Navegación segura

Asegúrese de que el navegador esté configurado para que brinde las funciones de protección y seguridad integradas. Por ejemplo, Microsoft® Internet Explorer (el navegador más popular) ofrece configuraciones de seguridad y privacidad. Se encuentran en “Herramientas” y luego en “Opciones de Internet”.

Los motores de búsqueda populares, como Google, también ofrecen algunas funciones de seguridad. Por ejemplo, SafeSearch de Google, que se encuentra en “Preferencias”, en la página de inicio de Google, le permite restringir la aparición de sitios y contenido explícitos (de sexo) en los resultados de búsqueda de su familia. Obviamente, cualquier usuario con cierto conocimiento podrá eliminar fácilmente la configuración, pero resulta útil con los usuarios más jóvenes de la Web.

Proteja su contraseña

Evite usar contraseñas fáciles de adivinar, como palabras del diccionario, nombres o fechas que su hijo o un hacker puedan descubrir. Le presentamos un buen método para administrar las contraseñas. Seleccione una contraseña maestra que pueda recordar y adapte para cada sitio web. El primer paso consiste en elegir una contraseña maestra

apropiada que tenga más de seis caracteres y una combinación de letras y números (en lugar de palabras verdaderas). En este caso, usaremos la frase “mifflin8”. Luego, agréguele la primera y la última letra del sitio web (por ejemplo, de Amazon.com: “Amifflin8n”). Esto me ayuda a recordar todas esas contraseñas diversas e incluso a que sean lo suficientemente complejas como para que a un hacker le resulte difícil adivinarlas. Esta secuencia tiene sentido para mí, pero no para los demás. También es útil tener contraseñas distintas para las diferentes cuentas. Si la contraseña de una cuenta está en peligro, las restantes seguirán estando seguras.

¡Las contraseñas se están multiplicando rápidamente! Cada vez son más complicadas. Es difícil mantenerlas actualizadas y recordarlas cuando se necesitan. Entonces, ¿cómo las administra? Existen algunas aplicaciones informáticas que administran contraseñas, y ahora algunos navegadores incluyen la capacidad de almacenarlas. Es muy inseguro llevar un registro de todas las contraseñas en una lista guardada en un equipo, en notas escritas en papel junto al equipo, etc. Nota para los padres: asegúrense de tener las contraseñas de sus hijos para el correo electrónico, la mensajería instantánea e incluso los sitios de redes sociales. Es útil para poder saber con quiénes se comunica su hijo y, ante cualquier problema, será importante que usted tenga acceso.

Asegure su red inalámbrica

Las redes inalámbricas domésticas presentan otros problemas de seguridad, y usted deberá hacer un gran esfuerzo para garantizar la protección de los equipos contra intrusos desconocidos que podrían utilizar su ancho de banda o, aun peor, usar su sistema como host para enviar spam y otros ataques. Además, con un equipo portátil y una red inalámbrica sus hijos pueden acceder a Internet desde

toda la casa y burlar todos sus esfuerzos por supervisar sus actividades.

Si en su casa tiene conexión inalámbrica (o “wifi”), asegúrese de hacer todo lo posible para que esté protegida: redefine la contraseña del router de modo que cumpla con las pautas de contraseña apropiadas y no sea fácil de adivinar; active el cifrado de contraseñas para impedir que un extraño detecte su red desde Internet; restrinja el acceso que su sistema comparte en la red y asegúrese de mantener actualizado el software de seguridad en Internet. Algunos padres optan por desconectar el router y llevarlo a su dormitorio por la noche (lo que considere mejor está bien).

Software de control para padres

El software de control para padres le permite elegir los sitios a los que sus hijos pueden acceder en Internet y asegurarse de que no vean temas inadecuados.

Los controles para padres varían según la aplicación que ofrece esta función. Por lo general, existen varios niveles para personalizar el programa según el niño al que se desea proteger. Por ejemplo, para un niño de cinco años, proporcionaría una "lista blanca" con los sitios web preseleccionados aprobados por los padres mediante la que le permitiría al niño visitar dichos sitios. También podría configurar cuentas que requieran el inicio de sesión de los padres para que el niño pueda navegar por la Web o límites de horarios para que sus hijos no pasen demasiadas horas navegando en lugar de hacer sus tareas.

Puede permitir que los niños más grandes o los adolescentes obtengan más acceso y flexibilidad. Puede restringir el acceso a la Web mediante categorías de los sitios en la biblioteca del programa, para evitar quedar expuesto a material racista, pornográfico u objetable.

No obstante, recuerde que ningún software brinda protección absoluta. Los padres deben utilizar una combinación de software, educación, supervisión y comunicación para proteger a sus hijos,

independientemente de la edad que éstos tengan. La Web es un recurso ilimitado y no permite restricciones totales. Los padres deben hablar con sus hijos para asegurarse de que sus creencias, principios y valores se mantengan cuando están en línea.

Favoritos en línea

Los sitios de redes sociales como MySpace, Friendster, Facebook y Xanga son muy populares entre los adolescentes. YouTube también es popular, pero es una preocupación para los padres, ya que no se puede filtrar el lenguaje o el contenido para adultos. Consulte al administrador del laboratorio informático de la escuela de su hijo para saber cuáles son los más usados. Pregunte a sus hijos adolescentes si tienen cuentas (pero siempre intente comprobarlo usted mismo).

Los niños más pequeños visitan sitios de entretenimiento, como Stardoll, Webkinz y Club Penguin, y se suscriben a ellos. Estos sitios proporcionan juegos y actividades, incluso chat. De alguna forma, son como una “ventana a las redes sociales”. Los sitios educativos como Starfall.com y funbrain.com enseñan habilidades de lectura y matemáticas. Pregunte a sus hijos, ya sean adolescentes, preadolescentes o niños, cuáles son los sitios más populares para ellos y sus amigos. Pregúnteles a cuáles se suscribieron y pídeles que se los muestren. Rápidamente sabrá si los aprueba o no. Mantenga la conversación en un tono “impersonal”, para que no se sientan interrogados.

Riesgos

Depredadores en Internet

Si bien estadísticamente es poco probable que a su hijo se le acerque un depredador sexual por Internet, hubo casos graves con resultados trágicos y preocupantes para cualquier padre. Según estudios realizados por el Centro Nacional para Menores Desaparecidos y Explotados (NCMEC, por sus siglas en inglés), uno de cada siete niños recibe solicitudes sexuales en línea, pero algunos de esos contactos provienen de amigos, más que de extraños.

Asegúrese de que sus hijos sepan que nunca deben intercambiar correo electrónico, conversaciones o mensajes de texto con extraños y que NUNCA ESTÁ BIEN encontrarse con un extraño personalmente. Asegúrese de que entienden que alguien que ven o que conocen por Internet sigue siendo un EXTRAÑO, no importa con qué frecuencia conversen en línea. Algo más preocupante son los niños que hablan sobre sexo con extraños por Internet (está demostrado que esto generalmente lleva a aun más encuentros físicos). Si un extraño se le acerca a su hijo cuando está conectado para hablarle sobre sexo, visite www.missingkids.com e informe el incidente. No es aceptable hablar sobre sexo con un extraño, y cualquier niño que reciba una pregunta de un extraño sobre temas sexuales deberá notificárselo de inmediato a sus padres o a un adulto de confianza.

Plagio y engaños

Es muy fácil encontrar en línea guías de tareas para todos los libros de texto escolares conocidos, y muchos sitios web ofrecen ensayos y tesis. El engaño nunca ha sido tan fácil ni tentador ni ha estado tan disponible para sus hijos. Recuerde a sus hijos que es muy importante usar Internet sólo para realizar búsquedas. También, explíqueles por qué el contenido generado por los usuarios, como el que se encuentra en Wikipedia, no siempre es tan confiable como las fuentes de información más tradicionales, como las enciclopedias, pero sirven como un muy buen punto de partida para una investigación.

Acoso y acecho cibernético

La tecnología brinda a sus hijos más formas de conectarse, sociabilizarse y comunicarse que nunca. Por desgracia, algunos niños envían fotografías y mensajes de texto por correo electrónico, mensajería instantánea y teléfonos celulares para avergonzar o acosar a otros niños. También, es posible editar los mensajes digitales de los niños para cambiarles el significado y luego reenviarlos a otros niños para avergonzarlos, intimidarlos o insultarlos. Según el

National Crime Prevention Council de los EE.UU., en febrero de 2007, el 43 por ciento de los niños había sido víctima de acoso cibernético. Asegúrese de que sus hijos sepan que deben proteger hasta el mensaje de texto más informal y tener cuidado con lo que escriben. Nunca deben acosar a nadie, y si son ellos víctimas de algún tipo de acoso cibernético, siempre se lo deben contar. Guarde una copia del mensaje de acoso. Para ello, presione la tecla “Imprimir pantalla” de su teclado y copie el mensaje en su procesador de texto.

El acecho cibernético es una extensión peligrosa del acoso cibernético, utilizada por aquellos que acechan en el mundo real o “fuera de línea”. Según el Departamento de Justicia de los Estados Unidos, una de cada doce mujeres estadounidenses será víctima de acecho a lo largo de su vida. Si tienen conciencia del problema, las adolescentes más grandes podrán aprender a defenderse, y sus padres deberán saber cómo ayudarlas. El acechador podrá secuestrar una cuenta de correo electrónico y hacerse pasar por la persona a quien le han secuestrado la cuenta. El atacante podría desfigurar una página de redes sociales o enviar mensajes de odio a los amigos de la víctima, robarle la identidad o intentar destruir el crédito o la reputación de alguien. El acecho cibernético es peligroso y debe denunciarse ante las autoridades, los proveedores de servicios de Internet y los hosts de sitios web. Guarde todas las evidencias de acoso y acecho cibernéticos.

Uso compartido de archivos y descargas de música y videos

Los niños aprenden rápidamente el placer de compartir música con otros niños. Y, por lo general, es en la preadolescencia cuando conocen los sitios para compartir archivos, en especial los gratuitos. Enséñeles a sus hijos los peligros de los sitios y programas para compartir archivos, ya que permiten a los extraños acceder a su equipo. El uso de sitios para compartir archivos podría exponer a su equipo e información a software “bot”, software espía,

registradores de pulsaciones de teclado, virus y otros códigos maliciosos peligrosos. Además, la descarga de música o videos de forma gratuita suele ser ilegal. Muéstreles a sus hijos dónde pueden descargar música y videos de forma legal de sitios como iTunes y Amazon.

Información privada y robo de identidad

Sus hijos no nacen sabiendo lo que significa información “privada”, por eso es necesario que les explique que la información privada es toda información que permite a un extraño acceder a su información personal o financiera. La información privada incluye datos del mundo real, nombre, números de teléfono, dirección, club deportivo, escuela e incluso el nombre del médico. Los delincuentes pueden convertir una pista pequeña en un registro completo de un menor y sus padres. A su vez, intercambian y venden esa información privada para ganar dinero. A ellos les resulta sencillo solicitar un crédito a nombre de su hijo y obtener artículos y dinero del mundo real, mientras arruinan el crédito bancario y el buen nombre de su hijo (o el suyo).

Si sospecha que ha sido víctima de robo de identidad, deberá revisar su informe de crédito para ver si hay pruebas de cuentas o préstamos nuevos. Usted tiene derecho a recibir un informe anual sin cargo de cada uno de los tres servicios de informes de crédito: Equifax, Experian y TransUnion. Se aconseja que cada cuatro meses solicite el pedido a cada una de las firmas para estar seguro de que su identidad y crédito están protegidos. Una vez que obtenga la evidencia del robo de identidad, deberá informarlo ante las autoridades, comenzando por la policía. El informe policial reforzará su caso cuando trabaje con los demás sitios y empresas involucrados. También puede “congelar” su informe de crédito y el de sus hijos. Para más información, visite ftc.gov.

Sitios de redes sociales

Los sitios web de redes sociales están entre los fenómenos de mayor crecimiento en Internet, tanto para niños como para adultos, pero son realmente los adolescentes y los preadolescentes quienes están fomentando ese crecimiento. Entre los más populares se encuentran MySpace, Friendster, Xanga y Facebook. Todos ellos brindan un lugar para que los niños se reúnan en línea con sus amigos y conozcan a otros nuevos. Usados con cuidado, estos sitios aportan a los niños muchas formas de comunicarse y compartir experiencias. De lo contrario, pueden exponer al niño al robo de identidad y a los depredadores.

Enseñe a sus hijos a no publicar información privada ni fotografías inapropiadas o engañosas. Esta información, una vez publicada, se convierte en pública y puede ser almacenada en equipos y en archivos de historial de Internet de otras personas. Y aunque elimine esa información o esas fotografías, es posible que sigan allí, en Internet, y caigan en manos de personas que sacan provecho de ellas.

Los sitios de redes sociales permiten a los niños formar redes de amigos donde pueden comunicarse libremente unos con otros. Asegúrese de que sus hijos no permiten el acceso de desconocidos a sus redes. Deben mantener las páginas en privado, de modo que sólo puedan encontrarse con amigos que ellos inviten. Una vez que los extraños ingresan a la red, los demás integrantes supondrán que son personas de confianza. Si los extraños son depredadores, podrán intentar aprovecharse de su hijo o de los amigos dentro de la red.

Asegúrese de que su hijo define las funciones de comunicación correctamente de modo que es él quien aprueba lo que se publica en su página. Esto incluso limita la posibilidad de que algún amigo pudiera publicar una fotografía que preferiría que nadie viera, ¡o algún comentario privado!

Sitios de pornografía, apuestas, racismo, anorexia y odio

Los rincones más oscuros de Internet incluyen elementos peligrosos e ilegales. Sin los controles para padres o los filtros de los navegadores, resulta casi inevitable que su hijo pueda acceder a contenidos no adecuados. Asegúrese de que sus hijos sepan que deben hablar con usted cuando esto sucede y garanticéles que no se enojará cuando lo hagan.

Algunos niños y adolescentes podrán sentir curiosidad por sitios que incluyan mensajes racistas u ofensivos o que promueven conductas peligrosas, como de anorexia o autolesión. La única forma de descubrirlo es revisando el historial del navegador de su equipo con frecuencia. Incluso una sola visita deberá dar lugar a que hable con su hijo sobre el tema. No suponga que fue simplemente por curiosidad. Explíqueles las normas de la casa sobre esos sitios y pregúnteles sus motivaciones para visitarlos. Cuando hablen, si su hijo muestra problemas, como depresión o autoaversión, no demore en buscar ayuda profesional para niños de parte de un terapeuta u otro especialista capacitado en tratar estos asuntos.

Privacidad en línea de los adolescentes

Enseñe a sus hijos adolescentes cómo utilizar Internet. Ya saben lo suficiente (o deberían) como para darse cuenta de que las personas en línea no siempre son quienes dicen ser. En línea, es fácil mentir sobre la edad, el sexo y la ubicación, por lo que mucha gente lo hace sin malas intenciones. Recuérdeles continuamente a sus hijos adolescentes que no pueden confiar en los extraños con quienes tienen contacto en línea, ni con aquellos con los que tienen contacto en persona. Nunca deben dejar que un extraño se una a sus listas de contactos, a un chat ni a una conversación por medio de un sistema de mensajería instantánea. Tampoco deben aceptar software, tonos de llamada ni protectores de pantalla gratuitos de parte de extraños.

Recuerde a su hijo adolescente que las direcciones de correo electrónico, los nombres de cuenta de usuario y la mensajería instantánea no deben ser su nombre verdadero, el nombre de su escuela ni una combinación de ambos; tampoco deben ser provocativos ni atractivos para un depredador. Esta información debe ser lo más anónima posible. Además, los adolescentes nunca deben compartir una contraseña, ni siquiera con un amigo.

Asegúrese de que el sitio web de la escuela de su hijo esté protegido mediante contraseña o que solicite un inicio de sesión para acceder a información que no sea pública. Por ejemplo, una escuela recientemente publicó en su sitio web un programa de viaje que incluía la información del vuelo y los nombres de los estudiantes que iban a realizar un viaje con el equipo de deporte. Otros posibles problemas incluyen las listas que se publican en el sitio web y que incluyen los nombres de los integrantes de las clases y las direcciones y los números de teléfono de las casas de los estudiantes.

Correo electrónico y mensajería instantánea

Tanto los niños como los adultos deben tener direcciones de correo electrónico diferentes para distintos propósitos. Por ejemplo, es buena idea tener una dirección para realizar compras en línea, otra para transacciones bancarias en línea y otra para la correspondencia con amigos y familiares. De esta manera, por ejemplo, si recibe un mensaje del banco en su correo electrónico familiar, sabrá que es spam malicioso que debe eliminar. Lo mismo sucede con la mensajería instantánea. Si un niño intercambia mensajes o conversa con más de un grupo, debe mantener nombres de usuario diferentes, ya que los depredadores suelen seguir a los niños desde una sala de chat a otra.

Asegúrese de que las cuentas de correo electrónico de sus hijos tengan activado el nivel más alto de filtrado de spam. Según un estudio de investigación de Symantec, el

80% de los niños denuncian la recepción de spam inapropiado todos los días. Deben usar nombres de cuenta de correo electrónico que no atraigan a los extraños. Por ejemplo, no deben utilizar combinaciones de nombre y apellido. Tampoco deben utilizar nombres de pantalla o direcciones sugestivos, como “sensual” o “salvaje”, aunque esté de “moda” hacerlo. Asegúrese de que usen contraseñas fuertes y que nunca las compartan, ni siquiera con sus amigos. Debe conocer las contraseñas de las cuentas de correo electrónico de sus hijos para poder supervisar la actividad de dichas cuentas con frecuencia. Observe a quién envían mensajes de correo electrónico y de parte de quiénes los reciben. ¿Conoce a todos? Y hágale saber a su hijo que esto lo hace para ayudarlo a estar protegido y no porque no confía en él.

Recomendaciones clave:

- *Enseñe a sus hijos a no hacer clic en los vínculos que están en los correos electrónicos que reciben, ya que pueden llevarlos a sitios web falsos.*
- *Desactive la función de vista previa del correo electrónico. Esto evita que se ejecuten posibles códigos maliciosos en el área del mensaje.*
- *Los niños no deben responder al correo electrónico ni a los mensajes instantáneos de quienes no conocen y que no esperaban recibir.*
- *Nunca acepte un vínculo ni descargue un archivo mediante mensajería instantánea.*
- *No debe hacer público el perfil de la mensajería instantánea ni la página de la red social.*
- *Defina preferencias de mensajería instantánea para mantener a los extraños a raya.*
- *No deben dejar que sitios como Yahoo!® (y otros) muestren cuando están en línea ni su identificación o información privada en las páginas que visitan.*
- *Siempre deben cerrar la sesión cuando no usan la mensajería instantánea o cuando editan su página de redes sociales, para asegurar que su privacidad está protegida.*

Blogs

Un blog es un diario o una agenda en línea. Algunos son temáticos y tratan sobre un tema en particular. A menudo, los adolescentes tienen blogs parecidos a los diarios privados tradicionales (excepto que están abiertos a todos los que acceden a Internet mediante el sitio web del adolescente o en un sitio de redes sociales), lo que sería como publicar su diario en línea para que todo el mundo lo viera. Antes de crear un blog, sus hijos deben estar seguros de su objetivo. Los motores de búsqueda generalmente pueden encontrar la información que usted publicó, lo que significa que sus mejores esfuerzos por proteger su privacidad fracasaron. Si publica fotografías o vínculos en sitios web privados en su blog, también puede reducir el nivel de privacidad.

Además, futuros jefes o responsables de la admisión de los alumnos en instituciones educativas pueden leer su blog, y esta exposición también puede afectar otras áreas de su vida. Por ejemplo, muchas personas que se presentaron a entrevistas laborales fueron rechazadas por la información incluida en sus blogs o en los blogs de amigos y familiares en los que se hablaba de ellas. No deje que su hijo adolescente se convierta en una víctima del blog.

Virus, gusanos y software espía

Los virus informáticos han estado presentes de diversas formas durante más de 25 años. Pero con la popularidad del correo electrónico y del intercambio de archivos por Internet, estas amenazas realmente han despegado. Quienes crean virus y otras formas de códigos maliciosos o software malicioso solían causar estragos en los equipos para mostrar sus habilidades informáticas o presumir frente a otros. Pero en la actualidad, lo que está en juego es mucho más que eso, y muchas de estas personas con malas intenciones son delincuentes cibernéticos motivados por obtener ganancias económicas mediante sus actividades ilegales.

La propagación de programas maliciosos por correo electrónico, mensajería instantánea, páginas de redes sociales infectadas y sitios para compartir archivos, y software espía, registradores de pulsaciones de teclado y bots, puede causarle un problema enorme. El software espía y los registradores de pulsaciones de teclado controlan la actividad normal de su equipo e informan sobre sus datos privados por Internet a los delincuentes.

Ayude a mantener a sus hijos y sus equipos a salvo instalando en los equipos software de seguridad en Internet y asegurándose de que está actualizado con los archivos de protección más recientes. Enseñe a sus hijos que no deben desactivar los analizadores de virus o el firewall, ni siquiera aunque consideren que esto podría acelerar un juego. ¡Es aceptar un desafío que no es seguro!

Tomar los bots en serio...

¿Ha oído hablar acerca de que los robots se están apoderando de equipos en todo el mundo? No es motivo de risa. Los “bots” y los “botnets” hoy en día se están convirtiendo en una de las últimas amenazas que surgen del lado oscuro de la tecnología. Los bots (forma abreviada de robots) son formas de software oculto que pueden introducirse sigilosamente en su equipo y hacer que desde allí se envíe spam y phishing a otros equipos. Los bots se han vuelto tan comunes que en el Symantec Security Response Center se estima que el 11 por ciento de los equipos de los Estados Unidos ya están infectados.

Muchos negocios ilegales se aprovechan ahora de estos bots que se propagan rápidamente entre cientos de miles de equipos personales desprevenidos con el único propósito de robarle su información personal y engañarlo quitándole todo el dinero que con tanto esfuerzo ha ganado.

¿Cómo lo hacen?

Un bot es un tipo de software malicioso que se introduce furtivamente en su equipo mediante delincuentes cibernéticos y permite a los atacantes apoderarse del control del equipo afectado. Estos “robots web”, por lo general, forman parte de una red de equipos infectados que se utilizan para llevar a cabo diversas tareas automatizadas, entre ellas, la propagación de virus, software espía, spam y otros códigos maliciosos. Lo peor de todo es que los bots se utilizan para robar su información personal y causar estragos en su crédito bancario, incluido el uso no autorizado de sus tarjetas de crédito y cuentas bancarias. Los bots también pueden mostrar sitios web falsos, simulando ser legítimos, y engañarlo para que transfiera fondos y proporcione sus nombres de usuario y contraseñas para realizar más actividades ilegales.

La mejor defensa contra estos horribles robotitos es instalar un software de seguridad de primera clase (Norton™ AntiBot es una buena opción) y asegurarse de configurarlo de modo que se actualice automáticamente para saber que cuenta con la protección más reciente. Los expertos también aconsejan no hacer nunca clic en los archivos adjuntos ni en los vínculos que se encuentran dentro del correo electrónico, salvo que pueda comprobar su origen; esto es algo que debe enseñar a sus hijos.

Fotografías digitales

Muchos niños tienen teléfonos celulares que incluyen una cámara e incluso algunos poseen su propia cámara digital. Converse con sus hijos acerca de la necesidad de proteger las fotografías en línea contra personas extrañas o incluso contra los mismos compañeros, ya que podrían utilizarlas de manera inapropiada. Usted puede hacer un seguimiento del envío de fotografías digitales desde el teléfono (simplemente debe verificar su extracto en línea o impreso). Asegúrese de que su hijo le muestre las fotografías que tiene en su teléfono para que pueda aconsejarle acerca de todo aquello

que considere peligroso o no apropiado para compartir. Si utiliza sitios para compartir fotografías, como Flickr, asegúrese de no permitir que otros utilicen sus fotografías, en especial, las fotografías de personas.

Recomendaciones clave:

- *No haga públicos los álbumes de fotos privados.*
- *Exija a los visitantes de un sitio para compartir fotografías que utilicen una contraseña.*
- *Realice copias de respaldo con un programa especializado, ya que los errores del equipo, las fallas de energía, los incendios y los desastres naturales pueden eliminar las fotos y otros archivos almacenados en el equipo.*
- *Use sólo los servicios para fotografías en línea que brinden protección de seguridad.*
- *Cuando un servicio de fotografías en línea le brinde la opción de enviar correo electrónico mediante su servicio, proteja la privacidad de sus amigos y envíeles, en cambio, un vínculo al sitio.*

Compras en línea

Internet es un paraíso para las compras, en especial, para los adolescentes con tarjetas de crédito o con cupones de regalo prepagos (o con acceso a los suyos). Sin embargo, hay normas que deben seguir para comprar de forma segura. Comience cualquier sesión de compras en línea asegurándose de que el software de seguridad está activado y actualizado. Compre sólo en sitios conocidos y con buena reputación, ya que usar un sitio web desconocido puede resultar peligroso. Para aumentar el nivel de seguridad, asegúrese de que la página donde introduce datos personales, como dirección o números de tarjetas de crédito, utilice una tecnología de cifrado. Podrá darse cuenta de que usan cifrado por la dirección web, que comenzará con “https.” Otro elemento necesario es el icono de un candado en la parte inferior de la ventana del navegador, que indica que el sitio web que está visitando usa cifrado para proteger sus comunicaciones.

Comprar en sitios de confianza es sólo el primer paso para ser un comprador en línea seguro. No haga clic en los vínculos de los mensajes de correo electrónico para acceder a una tienda o a una oferta preferencial. Debe escribir la dirección de la tienda en la ventana del navegador. Esto evitará que se convierta en víctima de un ataque de phishing, mediante el cual es redirigido a una versión falsa del sitio de su tienda favorita. Los phishers pueden robar contraseñas, datos de inicio de sesión, información almacenada sobre la tarjeta de crédito y cosas peores.

Verifique los resúmenes de las tarjetas de crédito con la mayor frecuencia posible (al menos, una vez por mes). Ésta es la mejor manera de saber quién está utilizando su tarjeta y de detectar problemas antes de que sean difíciles de resolver. La empresa de la tarjeta de crédito ofrece protección para el consumidor y colaborará con usted para administrar los cargos controvertidos o no autorizados.

No utilice tarjetas de débito en línea. Las tarjetas de crédito ofrecen más capas de protección: por ejemplo, permiten cuestionar los cargos inusuales. Con una tarjeta de débito, es posible que alguien retire dinero de su cuenta bancaria y que usted sólo se dé cuenta cuando reciba el resumen mensual, que puede tardar bastante en llegar.

Pago de cuentas en línea

Permanezca actualizado sobre todas las actividades bancarias como lo hace con las tarjetas de crédito. Acceda con regularidad a la cuenta de su hijo adolescente para controlar sus transacciones. Asegúrese de que sus facturas se paguen con puntualidad y precisión.

Proteja su equipo de la misma manera que protege la seguridad general en Internet, para evitar que le roben contraseñas o información bancaria. Y no acceda a sus cuentas desde equipos públicos, quioscos, locutorios o conexiones inalámbricas inseguras.

Transacciones bancarias en línea

Si usted o su hijo realizan transacciones bancarias en línea, deben evitar el uso de un equipo público o compartido o en una red inalámbrica que no tenga funciones de seguridad, como un firewall. Podría arriesgarse a que un hacker capture la información de su cuenta y de inicio de sesión, y robe su dinero. Siempre escriba la dirección web de su banco en el navegador web; nunca haga clic en un vínculo de un correo electrónico.

Juegos en línea y signos de adicción

MMORPG: ¿qué es eso? Esto se refiere a los potencialmente adictivos y cada vez más populares “juegos de roles masivos para múltiples jugadores en Internet”. Algunos títulos como World of Warcraft, Lord of the Rings y Everquest son muy populares en la actualidad. Para algunos adolescentes, en especial los varones, son una verdadera distracción de su vida real. Defina con sus hijos normas acerca del tiempo que pueden dedicar a estos sitios, si cuentan o no con dinero para gastar para la membresía o para comprar accesorios de juegos (ya sea en la vida real, como en eBay, o en el juego) y cualquier otra inquietud que pudiera tener.

Según los Computer Addiction Services del McLean Hospital afiliado a la Universidad de Harvard, existen algunos síntomas físicos y psicológicos de adicción:

- *Incapacidad de detener la actividad.*
- *Falta de atención hacia la familia y los amigos.*
- *Mentir a los empleados y a la familia acerca de las actividades que realizan.*
- *Problemas en la escuela o en el trabajo.*
- *Síndrome del túnel carpiano.*
- *Ojos secos.*
- *Desatención de la higiene personal.*
- *Alteración del sueño o cambios en las conductas para dormir.*

Palabras finales

Internet es un recurso maravilloso, con elementos que hacen que parezca una ciudad real. Internet ofrece educación, entretenimiento, noticias del mundo, y mejora nuestras vidas al permitirnos acceder a servicios increíbles como el chat, el correo electrónico, las compras en línea y mucho más. Tener pleno conocimiento y ser consciente de los riesgos y peligros en línea, y usar software de seguridad en Internet actualizado le permiten ayudar a su hijo a navegar por esta asombrosa ciberciudad con mayor independencia. Siga capacitándose y aprenda acerca de las tecnologías y los problemas nuevos en línea. Asegúrese de que su conducta en línea sirva de modelo para sus hijos mediante el empleo de prácticas de Internet seguras. ¡Muchas gracias!

Principales consejos para proteger a su familia en Internet

- Coloque el equipo en una habitación común.
- Establezca normas para usar Internet.
- Comprenda las redes sociales.
- Ayude a sus hijos a mantener su información personal protegida.
- Proteja las contraseñas de sus hijos.
- Consulte con frecuencia el historial de Internet del equipo.
- Dedique tiempo a sus hijos mientras están en línea.
- Enseñe a sus hijos ética cibernética.
- Tenga buenos conocimientos de informática.
- Enseñe a sus hijos a contarles a sus padres, maestros o adultos de confianza si se sienten incómodos por algo que han visto en un equipo.

Sitios de recursos importantes

www.norton.com/familyresource

www.ftc.gov

www.annualcreditreport.com

www.staysafeonline.org

www.ikeepsafe.org

www.webwisekids.org

Marian Merritt

Marian es la defensora de la seguridad en Internet de Symantec Corporation, los creadores del software Norton. Proporciona información sobre los problemas relacionados con la tecnología que afecta a la familia. Marian comunica los problemas técnicos en un idioma fácil de entender para el público. Se reúne regularmente con maestros, padres y niños para garantizar que la empresa “capte” lo que está sucediendo en el mundo de Internet actual y que las familias y las escuelas obtengan la información necesaria para crear usuarios de tecnología inteligentes y seguros.

Anteriormente, Marian ocupó diversos puestos en administración de productos para consumidores en Symantec.

Ella, su marido y sus tres hijos residen en Los Ángeles, California.

Visite el sitio www.norton.com/familyresource:

- Si desea recibir más material educativo y de entrenamiento.
- Si es víctima de un delito por Internet.
- Si desea recibir la información más reciente acerca de las amenazas de Internet en constante evolución.
- Si desea suscribirse a nuestro boletín de seguridad en línea para la familia.
- Si desea leer el blog de Marian.

O bien puede formularle preguntas a Marian escribiéndole a la siguiente dirección:
marian@norton.com

**Ahorre un
25%
Norton 360™**

www.symantecstore.com/360offer

En el carrito de la compra, utilice el código de cupón **norton360**.

La oferta caduca el 31 de marzo de 2008

Oferta disponible sólo en los Estados Unidos y Canadá

SIN GARANTÍA. La información técnica se le entrega TAL COMO ESTÁ y Symantec Corporation no otorga ninguna garantía, ni en cuanto a su exactitud, ni a su uso. Cualquiera que sea el uso que se haga de la documentación o de la información aquí contenida se hace a riesgo del usuario. Es posible que la documentación contenga inexactitudes técnicas o de otro tipo, así como errores tipográficos. Symantec se reserva el derecho a realizar cambios sin previo aviso.

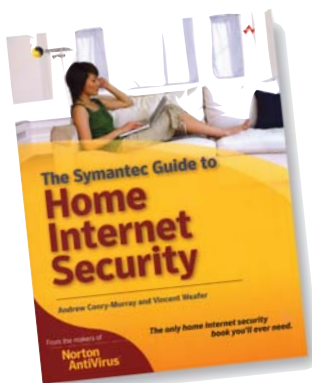
Copyright © 2007 Symantec Corporation. Todos los derechos reservados. Symantec y el logotipo de Norton son marcas comerciales o marcas comerciales registradas en los Estados Unidos y en otros países por Symantec Corporation y sus filiales. Los demás nombres pueden ser marcas comerciales de sus respectivos propietarios. Impreso en EE. UU. 12/07 BR-00247-SL



De los creadores de los productos de seguridad Norton™



“*Own Your Space*” DE LINDA MCCARTHY, es el primer libro serio sobre seguridad que aborda el tema de la seguridad en Internet desde el punto de vista de un adolescente. Este libro cubre amenazas en línea, cuestiones sobre seguridad de MySpace, robo de identidad y mucho más, centrándose en los efectos que estos asuntos causan en los adolescentes y en la forma en que se puede estar protegido en línea.



“*The Symantec Guide to Home Internet Security*” DE ANDREW CONRY-MURRAY Y VINCENT WEAFER. Internet presenta muchos riesgos. Si realiza transacciones bancarias o compras en línea, o incluso si sólo navega por la Web y envía correo electrónico, ya está expuesto a hackers, robos y artistas del engaño. En la actualidad, los delincuentes no necesitan forzar sus candados o romperle una ventana:

pueden atacarlo a usted y atacar a su familia por Internet. ¿Está preparado? Disfrute de una experiencia en línea segura con la sencilla ayuda paso a paso de Symantec, el proveedor de seguridad más confiable del mundo.