Common Sense opina sobre la seguridad en línea

¿Cuál es el problema?

Al igual que sucede en la vida real, es importante que los adolescentes sepan a quién pueden confiarle información por Internet. Es muy común proporcionar información como el nombre, la edad y la dirección en formularios y perfiles en línea, pero los adolescentes pueden ser monitoreados por compañías o ser víctimas de fraudes que los expongan al riesgo de robo de identidad. Pueden hacerles creer que están completando un formulario para un concurso ficticio. Pueden hacer clic en un adjunto que instale programas espías (*spyware*) en sus computadoras, o pueden hacer clic en publicidades e ingresar su dirección de correo electrónico, que el anunciante puede luego vender a otras compañías.

La seguridad digital se refiere a las medidas que tomamos para protegernos y para proteger nuestra información y nuestros dispositivos digitales de amenazas externas. Estos problemas nos afectan a todos: adolescentes, familias, e incluso las comunidades en línea en su conjunto. Los problemas relacionados con la seguridad en línea se pueden clasificar en tres categorías:

Estafas y robo de identidad. Los delincuentes pueden engañar a los adolescentes para sacarles información privada. Esa información la utilizan luego para realizar un robo de identidad, el cual puede arruinar el futuro financiero de un adolescente al impedirle hacer compras y obtener préstamos. Los delincuentes eligen jóvenes y niños pues tienen antecedentes financieros más limpios que los adultos. Los riesgos incluyen:

- *Phishing:* es la práctica de enviar correos electrónicos falsos, mensajes de texto o enlaces a sitios web ficticios para engañar a las personas y sacarles información personal y financiera.
- *Clickjacking:* es la práctica de engañar a los usuarios para que hagan clic en una página web aparentemente inofensiva, en general, en el sitio de una red social, con el fin de robar información o estafar a otros.

Virus y *spyware*. Muchos adolescentes descargan y comparten música, películas o juegos. No obstante, los adolescentes solo deben descargar contenido de sitios seguros y evitar hacer clic en enlaces o adjuntos que los puedan poner en riesgo. Los virus y *spyware* pueden ser bloqueados con herramientas de seguridad. Los riesgos incluyen:

- *Virus informático:* es un programa que se reproduce y propaga de una computadora a otra a través de Internet, CD, DVD o memoria USB. El virus se adjunta a un programa de modo que cada vez que se ejecuta, el virus lo hace también, provocando problemas en la computadora.
- *Spyware:* es un programa que recopila información en secreto acerca del usuario de una computadora sin que éste se dé cuenta.

Compañías que monitorean a los usuarios. Una de las estrategias que más rápido está proliferando en el mundo de los negocios consiste en monitorear la información, el comportamiento e incluso la ubicación de los usuarios de Internet. Las compañías hacen esto para poder luego personalizar las experiencias de los visitantes y vender la información de estos a anunciantes. La desventaja es que la mayoría de los adolescentes no sabe que su actividad en línea está siendo monitoreada. La ley no obliga a las compañías a compartir cómo monitorean los comportamientos de los consumidores, información que habitualmente está oculta en la letra pequeña de las políticas de privacidad. La ventaja es que a los adolescentes les puede gustar tener sitios web personalizados según sus intereses. Los riesgos incluyen:

- *Cookies:* archivos de datos que se almacenan en las computadoras cuando los usuarios visitan determinados sitios, que las compañías pueden usar para identificar a clientes recurrentes y personalizar las experiencias de los visitantes.
- *Publicidades dirigidas:* anuncios que se personalizan según la información que las compañías recopilan sobre los usuarios de Internet.

¿Por qué es un tema importante?

Los adolescentes deben comprender que cuando están navegando por Internet, las compañías están observando y monitoreando sus actividades y que puede haber estafadores intentando engañarlos para robarles información. Si los adolescentes no entienden los riesgos relacionados a la seguridad digital, sus dispositivos pueden resultar dañados, pueden ser víctimas de estafas, o pueden incrementar el riesgo de robo de identidad. Ellos mismos son quienes deben protegerse para no ser víctimas de estos delitos.

Qué pueden hacer las familias

¿Cuáles son las ventajas y desventajas de que las compañías monitoreen la información, las actividades y la ubicación de los usuarios de Internet?

Al descargar contenido de Internet, ¿cómo te aseguras de que proviene de un sitio seguro?

¿Alguna vez te encontraste en un problema de suplantación de identidad (phishing)?

Common Sense dice

Crear contraseñas seguras. Una contraseña segura es una herramienta de protección de cuentas muy eficaz. Los adolescentes nunca deben compartir sus contraseñas con amigos y deben actualizarlas a menudo. www.strongpasswordgenerator.com es un sitio excepcional para crear contraseñas seguras.

Pensar dos veces antes de descargar. El contenido que los adolescentes descargan de sitios no seguros puede infectar una computadora con *spyware* y virus. Insista a sus hijos que descarguen información únicamente de sitios seguros.

Tener cuidado al descargar información. Los adolescentes deben tener cuidado al compartir información, por ejemplo, su nombre completo, dirección y números de cuenta. Los mensajes donde se les pide que compartan información privada son señales de alerta de fraude. Ante una sospecha de fraude, los adolescentes no deben responder al mensaje o hacer clic en los enlaces que contiene. Fomente a sus hijos a denunciar casos de *phishing* al proveedor del servicio.

Entender de qué se trata el *phishing* y el *clickjacking*. Es una excelente manera de saber qué hacer para no dejarse engañar. Para ver ejemplos de estas prácticas, visite www.consumerfraudreporting.org.

Instalar las últimas actualizaciones de seguridad. Su computadora puede ser protegida de un virus, *spyware* y otros problemas de seguridad usando herramientas de seguridad actualizadas.

Limitar la recopilación de datos. Ayude a sus hijos a mantener su propia información bajo control, mediante las siguientes acciones: 1. deshabilitar las "cookies" de modo que las compañías no puedan monitorear sus actividades por Internet; 2. no hacer clic en todas las publicidades que aparecen; y 3. leer la política de privacidad del sitio web antes de revelar cualquier tipo de información.

Fuentes

Common Sense Media "Protecting Our Kids' Privacy in a Digital World." Diciembre de 2010. <http://www.commonsensemedia.org/privacy.>

Stecklow, S. "On the Web, Children Face Intensive Tracking." *The Wall Street Journal*. 17 de septiembre de 2010.