Common Sense opina sobre la seguridad en línea

¿Cuál es el problema?

Al igual que en la vida real, es importante que los adolescentes sepan a quién pueden confiarle información por Internet. Completar información, como por ejemplo, el nombre, la edad o la dirección, en formularios y perfiles en línea es algo común, pero los adolescentes pueden ser monitoreados por compañías o pueden caer en trampas que los expongan al riesgo de robo de identidad. Es posible que los engañen y les hagan completar un formulario para un sorteo falso. Es posible que abran un documento adjunto que instale programas espía en sus computadoras. También es posible que hagan clic en publicidades e introduzcan sus direcciones de correo electrónico, que el anunciante puede luego vender a otras compañías.

La seguridad digital se trata de proteger a las personas y a sus datos y dispositivos digitales de eventuales amenazas externas. Estos asuntos nos afectan a todos: adolescentes, familias e incluso a las comunidades en línea en general. Los problemas relacionados con la seguridad en línea se pueden dividir en tres categorías:

Fraudes y robo de identidad. Los delincuentes pueden intentar engañar a los adolescentes con el propósito de que les revelen información privada. Usan esta información para cometer el delito de robo de identidad, que puede arruinar el futuro financiero de los adolescentes y generarles problemas al hacer compras y obtener préstamos. Los delincuentes apuntan a la gente joven y a los niños porque tienen mejores antecedentes financieros que los adultos. Los riesgos incluyen:

- *Phishing (suplantación de identidad):* correos electrónicos, comunicaciones y mensajes de texto falsos o enlaces a sitios web ficticios que los estafadores usan para engañar a la gente y convencerla de revelar su información personal y financiera.
- *Clickjacking:* son trucos que usan los estafadores para que los usuarios hagan clic en una página web aparentemente inofensiva, por lo general, en el sitio de una red social, con el fin de robar información o de propagar el artilugio.

Virus y programas espía. Muchos adolescentes descargan y comparten música, películas o juegos. Sin embargo, los adolescentes sólo deben descargar información de sitios seguros y evitar hacer clic en enlaces y documentos adjuntos que puedan ponerlos en riesgo. Los virus y los programas espía se pueden bloquear con herramientas de seguridad. Los riesgos incluyen:

- *Virus informático:* es un programa que puede replicarse y propagarse de una computadora a otra a través de Internet o de un CD, DVD o unidad USB. El virus se adjunta a un programa de modo tal que cada vez que se ejecuta, también se ejecuta el virus, provocando problemas en la computadora.
- *Programas espía:* son programas que juntan en secreto información sobre el usuario de una computadora, sin que éste lo sepa.

Las compañías monitorean a los usuarios. Una de las estrategias empresariales que más está proliferando consiste en monitorear la información, el comportamiento e incluso la ubicación de los usuarios de Internet. Las compañías que lo hacen pueden personalizar las experiencias de los visitantes y vender esta información a los anunciantes. El aspecto negativo es que la mayoría de los adolescentes no sabe que la actividad que realizan por Internet está siendo monitoreada. La ley obliga a las compañías a revelar cómo monitorean el comportamiento de los consumidores, lo cual muchas veces está estipulado en la letra pequeña de sus políticas de privacidad. El aspecto positivo es que a los adolescentes les puede gustar tener sitios web personalizados según sus intereses. Estas cuestiones incluyen:

- *Cookies:* son archivos de datos que se almacenan en las computadoras cuando los usuarios visitan algunos sitios, que las compañías pueden usar para identificar clientes recurrentes y personalizar la experiencia de los visitantes.

- *Publicidad personalizada:* las publicidades se adaptan a los intereses de los usuarios de Internet, de acuerdo con la información que las compañías recaban sobre ellos.

¿Por qué es un tema importante?

Los adolescentes deben entender que cuando navegan por Internet, las compañías están mirando y monitoreando sus comportamientos y los estafadores pueden estar intentando engañarlos para que revelen información. Si los adolescentes no entienden los riesgos inherentes a la seguridad digital, sus dispositivos pueden dañarse, pueden ser víctimas de estafas o pueden incrementar el riesgo de robo de identidad. Los adolescentes deben protegerse para no caer en estas trampas.

Qué pueden hacer las familias

¿Cuáles son las ventajas y desventajas de que las compañías monitoreen tu información, tus comportamientos y tu ubicación por Internet?

Cuando descargas información de Internet, ¿qué medidas tomas para asegurarte de que proviene de un sitio seguro?

¿Alguna vez te topaste con un caso de phishing?

Common Sense dice

Cree contraseñas seguras. Una contraseña contundente es una herramienta maravillosa para proteger una cuenta. Los adolescentes nunca deben compartir contraseñas con amigos y deben actualizarlas con frecuencia. Un sitio estupendo para crear contraseñas seguras es www.strongpasswordgenerator.com.

Piense dos veces antes de descargar información. El contenido que los adolescentes descargan de fuentes no seguras puede plagar sus computadoras de programas espía y virus. Recomiende a los adolescentes que descarguen información solamente de sitios seguros.

Sea prudente al compartir información. Los adolescentes deben ser precavidos al compartir cierta información, por ejemplo, sus nombres completos, sus direcciones y sus números de cuenta. Los mensajes que piden a los adolescentes que revelen información privada son alertas rojas de eventuales fraudes. Si los adolescentes sospechan que un mensaje es un fraude, no deben responderlo ni hacer clic en los enlaces que contiene. Incítelos a denunciar el phishing al proveedor del servicio de Internet.

Aprenda más acerca del phishing y del clickjacking. Es una buena forma de entender cómo protegerse de estos delitos. Visite www.consumerfraudreporting.org para ver ejemplos.

Instale las últimas actualizaciones de seguridad. Puede proteger su computadora de virus, programas espía y otros problemas de seguridad mediante el uso de las herramientas de seguridad más actualizadas.

Considere restringir la posibilidad de juntar datos. Ayude a los adolescentes a tomar las riendas de su propia información: 1. deshabilitando las "cookies" para que las compañías no puedan monitorear su comportamiento por Internet, 2. limitando la cantidad de clics que hacen sobre las publicidades y 3. evaluando la política de privacidad de un sitio web antes de revelar información en éste.

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.