Cinco consejos para que tus hijos naveguen seguros por Internet

Los expertos ofrecen trucos para proteger al usuario en la red y promover el uso responsable

La edad de la primera conexión a la red se ha reducido significativamente y los jóvenes cada vez aprenden antes a navegar por Internet. Este martes, con motivo del Día de Internet Segura 2016, expertos y asociaciones ofrecen algunos consejos para promover el uso responsable y seguro de Internet y las nuevas tecnologías, especialmente entre los niños y adolescentes. El lema de este año Play your part for a better Internet (Pon de tu parte para mejorar Internet) quiere recordar a padres y tutores que ellos también tienen la responsabilidad de proteger la privacidad de los menores.

1. Aprender a usar las redes sociales. La brecha abierta entre los llamados nativos digitales y los adultos no deja de aumentar, por esa razón los padres deben ponerse al día en las redes y aplicaciones que usan sus hijos (Facebook, Twitter, Instagram o Snapchat). Identificar para qué sirve cada una, cuáles son sus configuraciones de privacidad y cuáles deberían ser las reglas de comportamiento básico en ellas son algunas de las tareas que deben hacer los adultos, según la Asociación Profesional Española de Privacidad (APEP). Los expertos de Facebook proponen, además, que sean los hijos quienes enseñen los padres a manejar las redes sociales: "Es una forma de hablar también de temas de seguridad y privacidad", señalan.

2. Interactuar pronto y establecer normas. Igual que hay que sentar lo antes posible las bases para la conversación con los jóvenes sobre otros temas, los expertos también recomiendan hacerlo para hablar sobre el uso de Internet. Resulta más complicado lograrlo si se espera demasiado, así que abogan por que se empiece a hablar con ellos sobre tecnología, incluso antes de que empiecen a usar las redes sociales. Después, los datos sobre ciberseguridad indican que los padres deberían incluso interactuar con sus hijos, haciéndose amigos de ellos en Facebook y siguiéndoles en Twitter o Instagram.

3. Enseñar a asegurar las cuentas en redes sociales. Los expertos de seguridad de Sophos Iberia recomiendan que los perfiles de los menores solo sean visibles para los amigos, no para los amigos de tus amigos y muchísimo menos ser un perfil abierto a todos. Además, recuerdan a los padres que tienen un importante papel aplicando al mundo digital los consejos básicos de precaución: no aceptar invitaciones de desconocidos, no dar la dirección o número de teléfono y tampoco acceder a encontrarse con personas desconocidas con las que se haya contactado online.

4. Cuidar las publicaciones. Este consejo, dirigido en principio a los más jóvenes, se puede aplicar también a los usuarios adultos. Todos los expertos advierten que una vez se publica una información (ya sea un comentario, una nota o un chat de vídeo) se pierde el control sobre ella porque se puede compartir de formas que no se habían previsto. Los especialistas de Facebook recomiendan plantearse algunas preguntas antes de publicar algo: "¿Es así cómo quiero que me vean los demás? ¿Podrían usarlo en mi contra o

para dañar mi reputación? ¿Me molestaría que alguien lo compartiera con otras personas? Si lo comparto, ¿qué sería lo peor que podría pasar? ¿Estaría bien que este contenido se distribuyera por la escuela o lo conociera mi futuro jefe?".

5. Formar a los menores para que aprendan a respetar a los demás. Los menores pueden causar daños a terceros publicando fotografías sin consentimiento, lesionando la reputación o agrediendo con comentarios inadecuados. No solo se trata de salvaguardar su privacidad, sino también de que aprendan a respetar la privacidad y los derechos de los demás.

Las claves de Google:
- Revisar la configuración de seguridad: verificar que los sitios web, las aplicaciones y los dispositivos conectados a tu cuenta son los que utilizas y en los que confías. Si observas algo extraño, cambia la contraseña.

- Contraseña segura: Nada del tipo "contraseña", "123456" o la fecha de tu cumpleaños. Una buena contraseña debe incluir una combinación de letras, números y símbolos. Si tienes más de una cuenta crea una contraseña única para cada una. Por último, mantenla en secreto.

- Número de teléfono de recuperación: Este número sirve para verificar tu contraseña, devolver el acceso a tu cuenta si lo pierdes y avisarte de posibles amenazas (por ejemplo, si un usuario intenta entrar en tu cuenta desde un lugar inusual). No se utiliza el número para nada más.

- Verficación en dos pasos: Con este sistema se necesita algo más que tu contraseña para iniciar sesión. Puede ser un código de seis dígitos que se envía a tu teléfono o, para una mayor protección, una llave de seguridad que insertas en un puerto USB de tu ordenador. Esta capa adicional de seguridad puede evitar la suplantación de identidad (phishing) porque, aunque alguien robe tu contraseña, no podrá acceder a tu cuenta.

Fuente: Beatriz Guillén Madrid 9 FEB 2016 - 16:28 CET CORDON PRESS

Cinco consejos para que tus hijos naveguen seguros por Internet