Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

- **Las tres amenazas principales**
- **Cómo proteger a tus hijos**
- **Recursos**

Cómo proteger a tus hijos en Internet

EDITOR INVITADO

Kevin Johnson es el editor invitado para esta publicación, es Director General de Secure Ideas, maneja el sitio mysecurityscanner.com y es un instructor experimentado del SANS Institute. Puedes consultar más información sobre él en www.secureideas.com

ANTECEDENTES

Todos queremos lo mejor para nuestros hijos, incluso la capacidad de aprovechar la tecnología. Sin embargo, esto implica riesgos de los que ellos no están del todo conscientes o preparados para enfrentar. Es nuestra responsabilidad asegurar que los pequeños entiendan los riesgos y la forma en que pueden protegerse aunque puede resultar difícil, pues nosotros mismos crecimos en un entorno distinto. En este boletín, te explicaremos las tres principales amenazas en Internet para tus hijos y cómo puedes ayudarlos a mantenerse a salvo.

PRIVACIDAD

Para proteger a tus hijos, primero tienes que entender los peligros que enfrentan al estar en línea.

1. **Extraños:** esta es una de las preocupaciones primordiales que los padres tienen cuando quieren proteger a sus hijos en Internet. En este contexto, los desconocidos son individuos (generalmente adultos) que establecen una relación en línea con tus hijos con el fin de tomar ventaja de ellos, estas personas podrían hacerse pasar por niños. Un ejemplo de este tipo de personas son los agresores sexuales.

2. **Amigos:** son personas que tus hijos conocen, regularmente niños de su misma escuela. Los amigos pueden representar un problema serio de acoso en línea. Recuerda que el *bullying* no necesariamente es un enfrentamiento físico. Internet amplifica el problema, ya que permite a los acosadores enviar mensajes a todo el mundo o secuestrar la identidad de quien quieren molestar. Además, los agresores pueden hacer estos ataques de manera anónima, lo que provoca que sean más difíciles de localizar y detener. Finalmente, el anonimato hace que sea más fácil para alguien convertirse en un acosador debido a que existen menos posibilidades de recibir castigo.

3. **Ellos mismos:** en el mundo actual de las redes sociales, los niños pueden ser sus peores enemigos. Cualquier cosa que ellos publiquen es accesible para todo el mundo y, una vez publicado, es difícil o casi imposible

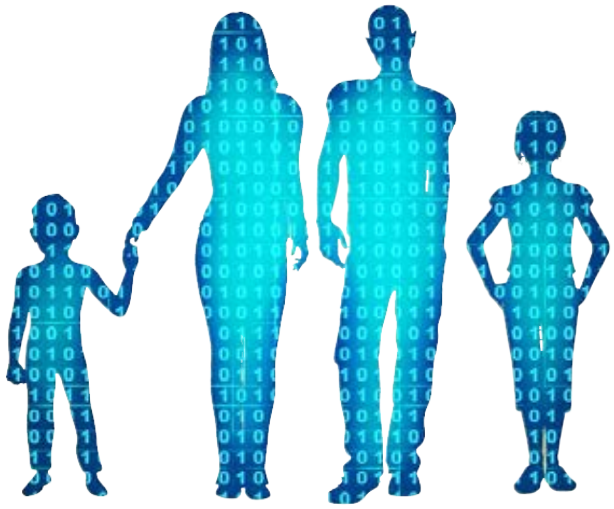
Cómo proteger a tus hijos en Internet

eliminarlo. Los niños no se dan cuenta de cómo esas publicaciones pueden afectar su futuro. Actualmente es en una práctica común para las universidades o empresas revisar las actividades de las personas en sus redes sociales e Internet. Cualquier publicación embarazosa o ilegal hecha por tus hijos puede afectar negativamente su futuro, además, su información personal puede ser utilizada por extraños o amigos con el fin de hacerles daño a ellos o a su familia.

CÓMO PROTEGER A TUS HIJOS

Ahora que entiendes los riesgos principales, aquí están los pasos que puedes seguir para proteger a tus hijos de ellos:

- **Educación**: Es el paso más importante que se debe considerar. Asegúrate de que tus hijos comprendan estas amenazas, habla con ellos acerca de sus actividades y mantente al corriente de lo que están haciendo. Es recomendable crear un entorno donde tus hijos se sientan cómodos para hacer preguntas o comentar problemas que pueden tener en línea.
- **Computadora asignada:** Tener una computadora solo para niños. Si accidentalmente infectan su computadora, esto ayudará a que tus cuentas de servicios bancarios en línea no se vean afectadas ni comprometidas. Además, podrías mantener las computadoras para niños en áreas abiertas para poder monitorear su actividad. Finalmente, asegúrate de que los pequeños utilicen sus propias cuentas sin permisos de administración en el equipo. Esto te permitirá rastrear y verificar lo que ellos hacen.
- **Dispositivos móviles:** Esto podría significar un reto. Considera definir límites en el tiempo que tus hijos tengan para utilizarlo, para que después tengan que devolvértelos (tal vez sea factible concentrar los cargadores de batería en un solo punto). También hay que considerar quitar los dispositivos móviles a los niños por la noche, así no intentarán estar en línea mientras deberían estar durmiendo.
- **Redes sociales**: Conoce lo que hacen tus hijos en línea creando tu propia cuenta en alguna red social como Facebook, Twitter o Instagram. Agrega a tus hijos como amigos a estas cuentas para que puedas ver lo que ellos publican.
- **Reglas:** Crea un documento que contenga las reglas que tus hijos deben seguir al estar en línea. Preferentemente, las reglas deben incluir cuándo pueden utilizar los dispositivos, por cuánto tiempo, qué juegos o aplicaciones pueden y no pueden tener y la información que tienen y no tienen permitido publicar. Considera compartir la forma en que



La clave para proteger a tus hijos al navegar en Internet es educarlos sobre los riesgos a los que se exponen y definir que lo está permitido y lo que no.

Cómo proteger a tus hijos en Internet

aplicarás esas reglas y las posibles consecuencias por faltar a ellas. Revisa el documento con tus hijos y distribúyelo en sus equipos para que ellos sepan y entiendan tus expectativas.

- **Tecnología:** Finalmente, existen tecnologías que pueden ser usadas para filtrar y monitorear las actividades de los niños en línea. La mayoría de los sistemas operativos contienen controles parentales, además existen herramientas libres y comerciales que se pueden utilizar, un ejemplo es la herramienta OpenDNS. Las tecnologías de seguridad son factibles para los niños pequeños, sin embargo, conforme crecen, estas tecnologías se vuelven menos efectivas. No solo los niños más grandes necesitan un mayor acceso a Internet para la escuela o el trabajo, también comenzarán a utilizar dispositivos que no controlan la seguridad, como en sitios públicos, en casa de un amigo o pariente o en la escuela. Además, algunos dispositivos móviles tienen un software de control parental muy simple, como los iPads o iPhones. Es por esto que la educación y las reglas que tú implementes serán más efectivas que cualquier tecnología.

RECURSOS

Algunos de los enlaces mostrados a continuación se redujeron para mejorar la legibilidad a través del servicio TinyURL. Con el fin de mitigar problemas de seguridad, OUCH! siempre utiliza la característica de vista previa de TinyURL (preview), la cual muestra el enlace destino, solicitando tu permiso antes de abrirlo.

Organización no lucrativa dedicada a proteger a los niños
https://twitter.com/iKeepSafeES

Protección Infantil de Microsoft
http://preview.tinyurl.com/bfmyhmr

OpenDNS:
http://preview.tinyurl.com/d892jqq

Reglas para los niños:
http://preview.tinyurl.com/3s5augb

Términos comunes de seguridad:
http://www.kaspersky.com/sp/threats_faq

Tip de seguridad del día del SANS:
http://preview.tinyurl.com/6s2wrkp

Consejos de seguridad en línea
http://www.seguridad.unam.mx/usuario-casero/consejos/

MÁS INFORMACIÓN

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti.
Visítanos en http://www.securingthehuman.org

VERSIÓN EN ESPAÑOL

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad en Cómputo en México reconocido ante FIRST, es una referencia en seguridad de la información en este país.
Sitio web http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Versión en español a cargo de UNAM-CERT: José Luis Sevilla, Fausto Pérez, Célica Martínez, Andrea Méndez