VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Junio 2015

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- Contexto
- Los riesgos
- Educar a los niños

# Educar a los niños en ciberseguridad

## Contexto

El número de formas en que los niños de hoy pueden conectarse e interactuar con otros es asombroso: Los nuevos servicios de medios sociales brotan como hierba mala; hay un crecimiento cada vez mayor de aplicaciones y juegos conectados en línea; demás, muchas escuelas están migrando a servicios como Google Drive y algunos o todos los trabajos requieren presentarse y entregarse en línea. Los niños, literalmente están creciendo "conectados". Si bien esto tiene muchos beneficios, las oportunidades también traen riesgos. En este boletín exploraremos tres áreas de riesgo para los niños y lo que podemos hacer para ayudarles a mantenerse a salvo.

### Editor Invitado

Bob Rudis es un científico de Seguridad de Datos en Verizon, autor del reporte "Data Breach Investigations" de 2015 además de cuidar de cuatro niños maravillosos. Bob ha construido y dirigido programas de concientización de seguridad en muchas compañías dentro del top 100 de la revista Fortune. Puedes seguir a Bob en Twitter como **@hrbrmstr**.

## Los riesgos

1. **Conducta**: Al interactuar en comunidades en línea o mundos virtuales, los niños pueden generar conductas que nunca tendrían en el mundo real. La falta de una presencia física puede crear una poderosa sensación de anonimato, especialmente en niños, quienes a menudo se ven tentados a expresarse en formas que podrían lastimar a otros niños, esto es llamado ciberbullying o griefing. Tus hijos, además, podrían convertirse en víctimas de otros que quisieran lastimarlos deliberadamente.

2. **Contacto**: Los niños están en –casi– constante comunicación con los demás, ya sea a través de mensajes de texto, interactuando con comunidades en línea o jugando en mundos virtuales. La falta de una presencia física a menudo hace que olviden que las personas en el otro extremo pueden no ser quienes dicen, o bien, no tener las mejores intenciones. Los depredadores deambulan las calles digitales y utilizarán cualquier táctica que puedan para construir relaciones con las posibles víctimas, incluso se hacen pasar por niños.

3. **Contenido**: No faltan las formas de capturar y subir vídeos, sonidos, imágenes o mensajes de texto en línea, una tentación para que los niños compartan de sobre manera acerca de sí mismos u otros miembros de su familia sin darse cuenta de que las consecuencias son muy reales. Los niños tampoco son conscientes de los peligros como robo de identidad o infecciones de malware cuando contestan encuestas o se les pide tomar acciones

# Educar a los niños en ciberseguridad

como hacer clic en enlaces. Por último, vivimos en una época en la que no podemos “deshacer” cuando hemos publicado algo. Los niños pueden pensar que los mensajes en Kik, Instagram o Snapchat son fugaces, pero todas esas publicaciones pueden volverse contra ellos o contra los miembros de su familia en el futuro.

*La clave para protegerlos en línea es educarlos sobre los peligros que enfrentan y comunicarse con ellos así como buscar que ellos se comuniquen contigo.*

## Educar a los niños

La primera cosa que puedes hacer para proteger a tus hijos es hablar con ellos. Conocer que es lo que están haciendo en línea, educarlos sobre los riegos actuales y qué pueden hacer para protegerse a sí mismos.

1. **Seguridad en casa**. Incluso con la gran movilidad, el hogar es donde el comportamiento seguro en línea comienza. Entre más jóvenes empieces a conversar con ellos y ellos contigo, mejor. Mantén conversaciones periódicas acerca de temas de seguridad, inclusive llegando a tal punto de mostrarles casos negativos que ocurren actualmente. Si no sabes que están haciendo tus niños, simplemente pregunta. Finge ser el padre despistado y pídeles que te muestren cómo son las últimas tecnologías y cómo las usan. Los niños aman la idea de ser maestros y se abrirán contigo. Por ejemplo, quizá ellos estén en Instagram, pídeles que te muestren cómo funciona Instagram, pídeles que te creen una cuenta y síguelos. No solamente estás ahora aprendiendo y monitoreando que están haciendo tus hijos, estás haciendo que sea más fácil para ellos hablar contigo. Además asegúrate, en la medida de lo posible, de que toda actividad en línea ocurra en áreas centrales de la casa y crea límites de tiempo para su uso. Teniendo las computadoras del hogar en lugares centrales, los niños están mucho menos propensos a involucrarse en comportamientos peligrosos. También considera una estación central de carga para dispositivos móviles, con la regla de que todos los dispositivos móviles estén ahí antes de que los niños vayan a la cama por la noche.

2. **Seguridad con los demás**. Cuando los niños están fuera de casa, están en mayor riesgo. Ayúdales a entender que tus ciberreglas aplican donde sea que estén y comunícales tus restricciones a quienes has confiado su cuidado. Si tienen dispositivos móviles, checa patrones de uso (tiempo y ancho de banda) para ver si hay señales de que están tomando ventaja de la dificultad para mantener las restricciones cuando están fuera de casa. No serás capaz de detener todas las infracciones, pero les vendrán a la mente tus palabras de alerta cada vez que estén a punto de llevar sus dispositivos móviles.

# Educar a los niños en ciberseguridad

3. **La seguridad en números**. No estás solo en esta cibervigilancia, por lo tanto deberías incluir a otros padres, tutores, hermanos, maestros y amigos a mantener un ojo en comportamientos potencialmente dañinos. Trata de que tu comunidad esté al día con los niños y anímalos a tener interacciones positivas con ellos cuando vean que los niños comienzan a ir por un camino peligroso.

Finalmente, cuando los niños comentan errores, tómalos como una experiencia para aprender en lugar de dedicarte a realizar una acción disciplinaria inmediata. Explica "porqué" cada vez y recuérdales que tú solamente estás intentando protegerlos de peligros que ellos no pueden ver. Déjales saber que ellos pueden acercarte a ti cuando experimenten cualquier interacción incómoda en línea, incluso pidiéndoles que tomen una impresión de pantalla para que la compartan contigo. Asegúrate también de que ellos se sientan cómodos de acercarse a ti cuando se den cuenta de que han hecho algo inapropiado. Mantener la comunicación del mundo real abierta y activa es la mejor forma de ayudar a los niños a estar seguros en el mundo digital de hoy.

## Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: http://www.securingthehuman.org

## Versión en español

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

## Recursos

| | |
|---|---|
| Contra el ciberbullyng: | http://yoloborro.com/ |
| Alerta en línea: | https://www.alertaenlinea.gov/temas/proteja-a-los-ni%C3%B1os-en-internet |
| Protección infantil: | http://www.microsoft.com/es-xl/security/family-safety/default.aspx#Generalidades |
| Cómic de seguridad Liga SuperSeg: | http://www.seguridad.unam.mx/usuario-casero/liga-super-seg/ |



Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Abril García y Diego Valverde