Escuelas sin seguridad informática hacen más factible el grooming

A pesar de que el Internet brinda herramientas e información que contribuyen a la operación de las escuelas y al desarrollo de su importante labor docente. Su uso puede convertirse en una herramienta de los delincuentes que buscan aprovecharse de los menores de edad.

De acuerdo con el más reciente reporte de la Asociación Mexicana de Internet (AMIPCI), la escuela se ha convertido en el tercer sitio más utilizado para conectarse a Internet, después del hogar y el trabajo. El 36 % de los internautas mexicanos se conectan desde un plantel educativo.

Ahora es común que los niños tengan acceso a dispositivos móviles, como teléfonos celulares y tabletas, para conectarse a la red. En este rubro, el 58 % de los cibernautas en México se conecta a través de uno de estos dispositivos móviles. El mismo reporte de la AMIPCI indica que, en promedio, los niños empiezan a usar Internet a la edad de 6 años. Esto significa que aún se trata de personas que no tienen plena conciencia de los peligros a los que se exponen en la red.

No obstante, criminales están aprovechando este acceso descontrolado a Internet para acercarse y abusar de niños y adolescentes. Es así que el acoso sexual a menores en Internet, también conocido como ciberacoso o grooming ha aumentado en la misma proporción que el libre acceso a la red.

Save The Children en 2013 presentó un estudio donde fueron detectadas más de 12 mil cuentas en redes sociales que difundían contenido relacionado con la explotación sexual infantil. Los

acosadores cibernéticos abordan a los menores a través de las redes sociales para después tener encuentros personales en los que logran sus objetivos.

La situación es preocupante ya que, de acuerdo con una encuesta que realizó la Alianza por la Seguridad en Internet A.C. a estudiantes de nivel básico, el 9.2 % reconoce haber platicado de sexo por internet con personas que no conocen. Para conocer el grado de confianza que pueden desarrollar, se les preguntó a los encuestados: ¿te has encontrado en persona con alguien a quien conociste en Internet? El 33.4 % contesto que sí.

En cuanto a la confianza en las herramientas y funciones de seguridad que tienen las redes sociales y otros servicios online, el 41.1% de los encuestados aceptó que ha alguna vez ha compartido su contraseña (ya sea de tu correo, red social, etc…) con algún amigo o pareja. Finalmente, el 53.2 % de los niños y adolescentes piensa que la información personal de su red social (fotos, nombres, dirección, etc…) está segura si se establece el perfil como “Privado”.

Además de la orientación que puedan obtener en la misma escuela con los maestros, y en la casa con sus padres, las instituciones educativas deben brindar a los alumnos un acceso protegido y controlado a Internet para impedir que a través de su infraestructura los delincuentes puedan acercarse a los menores.

Regulaciones como la Ley de Protección Infantil en Internet (CIPA) en Estados Unidos, solicita a las escuelas proteger a los alumnos contra amenazas que hay en línea, bloquear el acceso a contenido inapropiado y vigilar el uso general que los alumnos dan a Internet. Las escuelas deben implementar y hacer cumplir políticas de uso de redes sociales y enseñar a los alumnos a usar estas redes de forma segura.

Las herramientas de Websense buscan ayudar a las escuelas tanto de nivel básico, como niveles superiores a proteger el acceso de los estudiantes a las redes sociales ya que ofrecen controles en más de 30 categorías (11 solo para Facebook). Permiten también, delegar funciones de administración, priorizar el acceso de red a distintos grupos, así como usar plantillas de políticas y mejores prácticas para establecer controles de seguridad web, filtros y en aplicaciones.

La arquitectura de la solución TRITON APX de Raytheon | Websense unifica los productos de seguridad móvil, web, de datos y de correo electrónico en una sola interfaz administrativa. Todos los productos de filtros web y seguridad online de Raytheon | Websense permiten cumplir con la ley CIPA. Además, es posible agregar otras características para cumplir con mejores prácticas, como seguridad para dispositivos móviles y protección contra amenazas avanzadas y el robo de datos.