Colegio Yapeyú

INTERNET...
¿CHICOS EN RIESGO?

Introducción

Millones de familias en todo el mundo utilizan Internet a diario para aprender, buscar, comprar, realizar operaciones bancarias, invertir, compartir fotografías, jugar, descargar películas y música, hablar con amigos, conocer gente nueva y participar en muchísimas otras actividades. Aunque el ciberespacio ofrece numerosas ventajas, oportunidades y posibilidades, también constituye un riesgo importante, ya que un gran número de nuevas amenazas aparecen todos los días.

No es de extrañar que los ciber criminales se aprovechen de Internet y de los usuarios que la utilizan.

Tanto usted como los miembros de su familia necesitan estar protegidos cuando están online. Además de instalar un potente software de seguridad de una empresa de confianza para proteger a su familia de los piratas informáticos, ladrones de identidad, estafadores de correo electrónico y pederastas, es necesario seguir algunas reglas básicas de seguridad de Internet y utilizar el sentido común del mundo real.

Estadísticas para tomar conciencia

El 50% de los adolescentes han dado a conocer información personal en Internet.

Los hackers atacan equipos con acceso a Internet cada 39 segundos.

Existen 222.000 virus informáticos conocidos actualmente en la red y el número de amenazas aumenta cada día.

El 30% de los adolescentes fueron víctimas de acoso cibernético una o más veces durante el período escolar.

Del 2007 al 2008, los delitos en Internet aumentaron en un 33%.

El 31% de los niños han estado expuestos a contenido perjudicial.

Aproximadamente 3,2 millones de personas en todo el mundo sufren anualmente estafas masivas de marketing online.

Fuentes consultadas
1 EU Kids Online, Comparing children's online opportunities and risks across Europe (2006–2009)
2 Hackers Attack Every 39 Seconds – James Clark School of Engineering, Universidad de Maryland
3 2008 Internet Crime Report, IC3

Plan de seguridad sugerido

Paso 1

Tener presente la ubicación de la PC. En un hogar con niños, la ubicación de la PC es una de las decisiones más importantes que se deben tomar. Le recomendamos que la coloque una zona familiar con mucho movimiento y que limite el número de horas que los niños pueden utilizarlo.

Paso 2

Trabajar en equipo para establecer límites. Decida exactamente lo que considera correcto o incorrecto respecto a:

- Los tipos de sitios Web que se pueden visitar.
- Los foros y salones de Chat en los que se puede participar.
- Comunidades o redes sociales en las que puede interactuar. Sugerimos aquellas que están supervisadas por adultos o empresas responsables.

Paso 3

Acordar conjuntamente las reglas familiares para el uso de la PC
Se recomienda lo siguiente:

- Nunca se registre con nombres de usuario que revelen su verdadera identidad o que puedan resultar provocativos.
- Nunca revele sus contraseñas.
- Nunca revele su dirección ni número de teléfono.
- Nunca publique información que revele su identidad.
- Nunca publique fotografías inadecuadas o que puedan revelar su identidad (por ejemplo: el nombre de una ciudad o un
- colegio serigrafiado en camisetas).
- Nunca comparta información con desconocidos que conozca en la red.
- Nunca se reúna cara a cara con desconocidos que conozca en Internet.
- Nunca abra archivos adjuntos procedentes de desconocidos.

Paso 4

Firmar un contrato sobre el comportamiento adecuado online
Redacte un contrato o utilice el que se muestra como ejemplo:

Dado que el uso de Internet y de la PC es un privilegio que no quiero perder...navegaré, realizaré búsquedas, trabajaré, jugaré y conversaré de forma segura mientras esté online.
Seguiré todas las reglas que hemos acordado.
No revelaré mi nombre verdadero, número de teléfono, dirección ni contraseñas a “amigos” virtuales.
No concertaré una cita en persona con un usuario que haya conocido a través de la red.
No publicare fotos ni videos que ayuden a identificarme
Si me encuentro en una situación insegura o incómoda, prometo informar (a mi padre, madre, tutor o profesor) para que puedan ayudarme.
Prometo cumplir este compromiso y asumo que existen consecuencias respecto a las decisiones que adopte.

…….
Firma del niño

Como madre, padre, tutor o profesor, prometo estar a tu disposición cuando necesites ayuda y te ayudaré a resolver los problemas que puedan producirse de la mejor manera posible.

……..
Firma del padre, madre, tutor o profesor

Paso 5

Instalar software

Asegúrese de disponer de un potente software de seguridad que proteja su ordenador de virus, hackers y Spyware.
También debe filtrar el contenido, las imágenes y los sitios Web ofensivos. Este software debe actualizarse con frecuencia, ya que aparecen nuevas amenazas cada día.

Paso 6

Utilizar controles parentales (filtros)

Todos los proveedores de software de seguridad más importantes ofrecen controles parentales.
Asegúrese de activarlos. Si está utilizando un programa de distribución libre o software sin controles parentales, contemple la posibilidad de adquirir software con estos controles.
Invierta tiempo en aprender el funcionamiento de los controles y utilice las opciones que filtren o bloqueen material inadecuado. Ante cualquier duda al respecto consulte al profesor de informática del colegio.

Paso 7

Por supuesto, estas herramientas tienen sus limitaciones. Ningún programa puede reemplazar a unos **padres atentos y responsables** que supervisen el uso que hacen sus hijos de Internet.

Paso 8

Recordar a los miembros de la familia que los usuarios que se conocen a través de la red son desconocidos. Cualquiera que se conecte debe comprender lo siguiente:
No importa la frecuencia con la que converse con sus “amigos” virtuales, ni el tiempo que lleve conversando con ellos ni el grado de familiaridad supuestamente adquirido entre las dos partes. Los usuarios que se conocen en Internet son desconocidos.
Mentir es fácil, lo mismo que fingir la identidad de otra persona mientras se encuentra online.
Especialmente los niños necesitan saber que un “amigo” nuevo puede ser en realidad un hombre de 40 años, y no alguien de su misma edad.
Los sitios web de redes sociales, son el lugar ideal para conocer gente nueva a través de la red. Por lo tanto, los padres deben visitar estos sitios y comprobar el perfil de sus hijos para asegurarse de que no generen conversaciones inapropiadas ni publiquen fotografías inadecuadas. Además, deben supervisar las conversaciones de mensajería instantánea de sus hijos para asegurarse de que no estén siendo perseguidos por un pederasta online.

Paso 9

Mantenerse informado.
Cuanto más sepa acerca del tema, más seguros estarán su familia y su equipo.

Paso 10

Hable con su hijo sobre la seguridad de Internet, hágalo con la PC apagada, de manera que pueda captar toda su atención.

Si son pequeños, comience explicándoles que una PC es una herramienta y que Internet es como una biblioteca electrónica gigante llena de información.

Explicar por qué es importante estar seguro en Internet, ya que puede ser una puerta abierta a información personal importante.

Cuénteles que gente mala puede apoderarse de su equipo y romperlo, por lo que deberían comprar uno nuevo.

Además, explíqueles por qué es importante no compartir información personal con otros usuarios online.

Adviértales de que no deben utilizar sus nombres verdaderos ni contar dónde viven ni a qué colegio van.

Además, asegúrese de que sus hijos no estén siendo víctimas de acoso escolar ni que estén acosando a otros niños online.
Cuando los niños dejan el colegio, no dejan necesariamente atrás a sus compañeros ni sus conflictos. Por medio de las PC, los buscapersonas y los teléfonos celulares, los estudiantes pueden mantenerse en contacto en todo momento y pueden abusar de esta tecnología para molestar, acosar y dañar a otras personas.

Fuentes consultadas

Educar
Ministerio de Educación de la Nación Argentina

Plan de seguridad de Internet para su familia. Empresa McAfee

E-México
Ministerio de Educación de México

Sugerencias para la seguridad infantil
Empresa Microsoft

Esperamos que nuestro humilde aporte ayude a toda nuestra comunidad de padres y alumnos en un mejor y más seguro manejo de las nuevas tecnologías.

La Dirección