Guía para padres de protección infantil en Internet

INTRODUCCION

Los niños son el activo más grande que tenemos, nuestro futuro. Para eso, no obstante, es necesario guiarlos en el desarrollo de la vida. Esa responsabilidad, en el mundo de hoy, representa un verdadero desafío para los padres. Con equipos informáticos cada vez más modernos y un lenguaje que evoluciona rápidamente, los padres de hoy sufren la presión de tener una doble tarea: **educarse para poder educar.** Esta guía le brinda la posibilidad de conocer cuáles aspectos deberá tomar en cuenta para poder asegurarles a sus hijos una experiencia sana y segura en Internet; y en todo lo que el ciberespacio ofrece.

¿QUIÉN DEBE HABLARLES?

Usted.

En el transcurso de su infancia, el niño irá conociendo personas que van a tener un rol muy importante en su vida, como por ejemplo: familiares, amigos, docentes. Sin embargo, ninguna de esas personas va reemplazar la figura de los padres, que son el mayor referente para sus hijos.

¿CUÁNDO DEBE HABLARLES?

Ahora.

A medida que el niño crece se van presentando diferentes problemáticas. La educación debe estar presente desde el comienzo, ya que eso ayudará a facilitar la comprensión de los hechos. A partir del momento en que se empiece a manifestar interés por la computadora y la web, entonces es posible llevar lo aprendido sobre seguridad en general, a la seguridad en Internet. El medio cambia, no obstante, las amenazas siguen siendo las mismas.

LOS PADRES EDUCAN A LOS NIÑOS Y APRENDEN DE ELLOS

Los padres suelen sentir que los niños "saben más de informática" que ellos mismos. Mientras los menores de edad, en la actualidad, suelen ser nativos digitales que nacieron junto a una computadora; los padres han incorporado este hábito ya en la adultez.

No obstante, esto no significa que los niños deban llevar el control de los equipos informáticos del hogar. La costumbre en el uso de Internet, no es lo mismo que el conocimiento profundo de las implicancias de las tareas realizadas, y en este sector están los niños.

No es necesario que los padres sepan más que los hijos sobre qué está disponible en la web. Sin embargo, el adulto debe mantener el control, y al momento de encontrar cuestiones desconocidas, ese es el momento de sentarse junto a ellos e informarse al respecto, generar un ambiente de colaboración familiar y, fundamentalmente, ser paciente.

¿Qué hacer y a qué edad?

A continuación, compartimos un conjunto básico de reglas que fortalecen las actividades de los niños en línea, de acuerdo la edad.

Hasta los 10 años:

A *"Acompáñelos en sus primeras experiencias en la web"*

Asegúrese de estar presente en sus primeros pasos. Los primeros contactos del niño con Internet son una buena oportunidad para sentarse con ellos y guiarlos durante esa nueva aventura.

B *"Defina condiciones para el uso de Internet"*

En primera instancia, se deben establecer las reglas para la utilización de Internet en el hogar. Supervisar la cantidad de horas y fijar horarios permitidos, son buenas prácticas para esta medida.

C *"Sea un buen ejemplo"*

Los niños normalmente toman el reflejo de los padres en su comportamiento, sea en línea o no. Si los demás miembros de la familia mantienen una conducta positiva, ésta se transmitirá inmediatamente al niño.

De 11 a 14 años:

A *"Utilice herramientas de Control Parental"*

Aproveche la tecnología existente y utilícela a su favor. Las herramientas de control parental permiten bloquear sitios que contengan material potencialmente ofensivo. En algunos casos se puede impedir el acceso a determinada categoría de páginas.

B *"Enseñe a no compartir información que pueda identificarlos"*

Es importante aclarar a los niños que en el mundo virtual, no todas las personas son amigos y que algunos podrían hacerles daño. Por lo tanto, es clave no compartir información como: dirección, teléfonos, instituciones a las que asisten, etc. A su vez, el niño debería estar debidamente autorizado por sus padres, antes de compartir fotos familiares en Internet.

C *"Mantenga abierto el diálogo"*

Fomente una comunicación con sus hijos acerca de lo que ven en Internet. Procure ubicar el equipo en un lugar común de la casa donde pueda estar bajo su supervisión y no en su dormitorio.

De 15 a 18 años:

A *"Nadie debe conocer sus contraseñas"*

Las contraseñas son como las llaves de la casa. No deben existir copias en manos de extraños. Nunca se debe dar una contraseña, ya sea por Internet o personalmente, dado que ésta **nunca debería ser solicitada** por ningún proveedor de Internet, servicio de correo electrónico o cualquier otra organización.

B *"Informar los acosos inmediatamente"*

El ciberacoso (cyberbullying en inglés) es la manifestación de los acosos personales a través de Internet. Sus efectos, de igual manera que los acosos fuera de la web, dañan al niño psicológicamente de forma recurrente y repetitiva. Por eso, se debe orientar a que el niño informe a sus padres inmediatamente, en caso de ocurrencia de este tipo de agravios.

C *"Las transacciones financieras en línea son para los adultos"*

Comprar en Internet no debe representar un problema, siempre y cuando, esta actividad se realice de forma prudente. El envío de información personal financiera debe ser realizado bajo la supervisión de los padres hasta que los hijos comprendan las medidas a llevar a cabo.

EDUCAR SOBRE LA SEGURIDAD EN LÍNEA ¿EN EL HOGAR O EN LA ESCUELA?

Los padres deberían estar permanentemente informados si las escuelas desarrollan algún plan de capacitación para los niños en materia de seguridad en Internet. En lo posible, participar y apoyar este tipo de actividades escolares, ya que los docentes pueden tener un rol elevado en la vida de los niños y pueden aprovechar ese "modelo" que representan para transmitir sugerencias acerca del comportamiento en la red. Los padres, no obstante, siguen siendo el mayor referente de los niños. La educación debe provenir, en primera instancia, del hogar, y posteriormente, darle continuidad en la escuela.

¿QUÉ ES EL CONTROL PARENTAL?

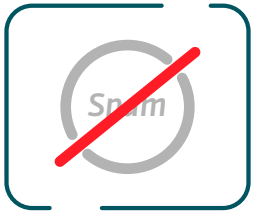
Son programas informáticos específicos, para poder administrar el contenido que se puede ver en Internet. De esta forma se configuran roles de usuarios en donde es posible bloquear ciertos contenidos o incluso la cantidad de horas de utilización del equipo informático. Soluciones de seguridad antivirus y configuraciones en los navegadores, entre otros; también brindan a los padres una manera de poder controlar lo que los niños pueden ver en Internet.

¿QUÉ SON LAS REDES SOCIALES?

Una red social es una estructura social que relaciona personas. Pertenecer a una red social en Internet es parte fundamental de las premisas de comunicación modernas. En estas redes coexisten muchos individuos con el fin de interactuar con los demás integrantes. Así como es una herramienta muy positiva de comunicación, su uso, no obstante, debe ser acompañando y monitoreado.

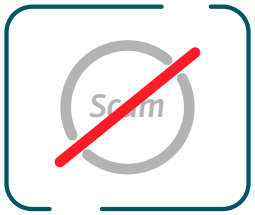
Malware

Es el acrónimo en inglés de software malicioso (malicious software). El objetivo de este tipo de aplicaciones es dañar la computadora. En la mayoría de los casos, la infección ocurre por "errores" realizados por los usuarios, al ser engañados por el atacante. Existen muchas herramientas (antivirus, antispyware) y buenas prácticas, que reducen el riesgo de infección, ante todas las variantes de códigos maliciosos: virus, gusanos, troyanos, spyware, etc. La diferencia entre estas variantes radica en la forma en que se distribuyen: algunas veces se aprovechan de sistemas vulnerables y otras de usuarios no precavidos.



Spam

El spam es el famoso "correo basura". Son aquellos mensajes que no fueron solicitados por el usuario y que llegan a la bandeja de entrada. Normalmente, este tipo de correos contienen propagandas – muchas veces engañosas – que incitan al usuario a ingresar a páginas, con ofertas "milagrosas", cuyo contenido es potencialmente dañino para el usuario.



Scam

Los scam son engaños o estafas, que se llevan a cabo a través de Internet. Se realizan de diversas formas como, por ejemplo, a través de correos no solicitados (spam), así como también a través de técnicas de Ingeniería Social. Estas últimas, intentan convencer al usuario de la prestación de un servicio cuando en realidad sólo quieren acceder a información confidencial. Un ejemplo son los mensajes falsos solicitando nuestra contraseña y clave de redes sociales a través de Internet.

Ciberacoso

Es una conducta hostil que puede ser practicada hacia los niños. La víctima de este tipo de acosos, es sometida a amenazas y humillaciones de parte de sus pares en la web, cuyas intenciones son atormentar a la persona y llevarla a un quiebre emocional. Estas prácticas pueden ser realizadas a través de Internet, así como también, teléfonos celulares y videoconsolas. También denominado en inglés, cyberbullying, no siempre son realizadas por adultos, sino también son frecuentes entre adolescentes.

Grooming

Se trata de la persuasión de un adulto hacia un niño, con la finalidad de obtener una conexión emocional y generar un ambiente de confianza para que el niño realice actividades sexuales. Muchas veces los adultos se hacen pasar por niños de su edad e intentan entablar una relación para, luego, buscar realizar encuentros personales.

Sexting

Proviene del acrónimo formado entre Sex y Texting. Inicialmente, y como lo indica su nombre, se trataba del envío de mensajes con contenidos eróticos. Posteriormente, dado el avance tecnológico, esta modalidad evolucionó hacia el intercambio de imágenes y videos convirtiéndose en una práctica habitual entre adolescentes y niños.

Robo de información

Toda la información que viaja por la web, sin las medidas de precaución necesarias, corre el riesgo de ser interceptada por un tercero. De igual modo, existen también ataques con esta finalidad. La información buscada, normalmente apunta a los datos personales. Un paso en falso ante este tipo de incidentes, puede exponer al menor de edad a la pérdida de dinero familiar o al robo de identidad.

4 SUGERENCIAS FINALES

1

Utilice herramientas de control parental

Éstas pueden ser aprovechadas tanto en los navegadores, así como también, en los programas de antivirus. Se puede apreciar en la versión 5 de ESET Smart Security. Existen este tipo de herramientas para consolas también, como es el caso de Nintendo Wii y Xbox 360.

No envíe información confidencial por Internet. Su información jamás será solicitada por correo electrónico o por chat. Los bancos no solicitan los datos de su cuenta y mucho menos su PIN. Es importante, a su vez, no ceder esta información a sus hijos.

2

No contestar, ni eliminar mensajes de acoso

En caso de que sus hijos reciban mensajes de acoso por Internet, es necesario instruirlo a no tomar represalias al respecto. Normalmente, el acosador busca este tipo de reacción en los niños para poder seguir fomentando su deseo de hacer daño. Este tipo de situaciones deben ser apaciguadas por los padres, y en caso de repetirse, notificar a las autoridades correspondientes. Para eso, los mensajes recibidos no deben ser eliminados, dado que constitutuyen la evidencia del acto.

3

No todo lo que se ve en línea es verdad

Los hijos deben ser conscientes de que no toda la información que se distribuye en la web proviene de una fuente confiable. Hoy por hoy, en Internet, es muy fácil obtener un espacio para poder publicar opiniones. Por ende, se debe ser muy cuidadoso a la hora de recurrir a esos contenidos.

4

Comunicación abierta

La comunicación que tenga con sus hijos juega un rol clave en su seguridad. Resulta mucho más productivo animarlos a comentar sus miedos e inquietudes que reprimirlos con sanciones. Que se mantenga un buen clima y un diálogo abierto, tanto en Internet como en la vida real, pueden llegar a ser la clave del éxito para lidiar con su bienestar.

5 BUENAS PRÁCTICAS PARA LOS PADRES

1. ***Asigne un usuario al niño:***
   Es la única forma eficiente de controlar sus actividades en Internet. El rol de administrador de un sistema debe ser siempre de un adulto.

2. ***Mantenga actualizado su antivirus y su herramienta de control parental.***

3. ***Monitoree el historial de navegación.***
   Si el mismo es eliminado, es un buen motivo para tener una charla.

4. ***Controle la cámara web, y asegure que la misma está desconectada mientras no se la deba utilizar.***

5. ***Revise las configuraciones de las redes sociales del niño.***
   Un muro de Facebook compartido públicamente, sin limitaciones, puede ser un riesgo para la integridad del joven.

CONCLUSIÓN

Denegar el acceso a las tecnologías, no es una solución posible. Estas son parte del día a día de los niños, y son cada vez más importantes para su crecimiento. Por lo tanto, los padres deben asistir el uso de las mismas y participar en la interacción del niño y las computadoras. Además, vale destacar que muchos de estos riesgos también pueden afectar a los adultos, por lo que muchas de las precauciones aquí descriptas, deberían realizarse siempre y para todas las edades.

La seguridad de los niños es responsabilidad de todos, y seguir los consejos brindados en esta guía ayudará a los adultos a proteger mejor la información, los sistemas, y la propia integridad de los menores de edad.

La seguridad de los niños es responsabilidad de todos, y seguir los consejos brindados en esta guía ayudará a los adultos a proteger mejor la información, los sistemas, y la propia integridad de sus hijos.