RECURSOS DE APRENDIZAJE

Cómo mantener protegida a tu familia en el Internet

La seguridad en el Internet para los niños

El Internet es un lugar maravilloso para encontrar información y conectarse con gente y amigos. Sin embargo, presenta riesgos de seguridad y privacidad, especialmente para los menores de edad.

Qué puedes hacer para proteger a tus niños en línea:

- Tan pronto como comiencen a usar el Internet, háblales sobre la seguridad en el Internet. Nunca es demasiado pronto para hacerlo.
- Considera colocar la computadora en un área común de la casa.
- Permanece involucrado en su mundo en línea controlando con quién conversan e intercambian correos electrónicos. Aprende a conocer los sitios web que están visitando.
- Conoce sus nombres de usuario y de pantalla y asegúrate de que sean apropiados.
- Usa buscadores seguros. Para los niños pequeños en particular, usa filtros y software de monitoreo apropiados para su edad.
- Aprende todo lo que puedas sobre computadoras, el Internet y los potenciales riesgos para los niños en línea.

Qué es lo que no deberían hacer tus hijos:

- Dile a tus hijos que nunca compartan sus contraseñas con nadie, incluso sus amigos.
- Enséñales a no llenar formularios sin tu conocimiento, ni abrir correos electrónicos de extraños.
- No permitas que tus hijos participen de salas para charlas privadas.

Redes sociales

Las redes sociales se han hecho muy populares entre adultos y niños por igual. Estos sitios permiten que los usuarios se comuniquen y compartan información. Se puede tener acceso a ellos desde cualquier lugar donde haya una conexión de Internet, incluso a través de *smartphones*.

Lo básico de algunas redes sociales populares:

- **Facebook** es un sitio gratuito de conexión social usado por gente de todo el mundo. Su política requiere que los usuarios tengan 13 años de edad como mínimo, pero muchos niños menores se suscriben simulando ser mayores. De forma predeterminada, los mensajes de los adultos son públicos; los mensajes de los niños pueden ser vistos por amigos de sus amigos.
- **Twitter** es una red de información en tiempo real donde la gente obtiene las noticias más recientes, ideas y opiniones sobre lo que les interesa. No hay límite de edad. De forma predeterminada, los *tweets* son públicos.
- **LinkedIn** es un sitio social que permite que los profesionales se conecten con conexiones de empresas, busquen trabajo y agentes de reclutamiento, se unan a grupos, etc. Los usuarios tienen que tener 18 años de edad como mínimo. Los usuarios tienen un perfil privado y uno público, cuya visibilidad pueden controlar.
- **YouTube** es un sitio gratuito donde se comparten videos y una red social. Todos pueden cargar, ver y compartir videos en YouTube. Si tus hijos desean usar redes sociales, diles cuáles son tus expectativas, cómo tendrían que comportarse, qué es seguro y qué no lo es, cuándo pueden ir al sitio y cuánto tiempo pueden permanecer allí (sí, las redes sociales pueden ser adictivas).

Cómo proteger la privacidad y reputación de tus hijos:

- Revisen juntos las configuraciones de privacidad de Facebook y seleccionen los niveles con los que ambos se sienten cómodos. Haz que tus hijos pidan dar su aprobación antes de que los “marquen” en los mensajes y fotografías de Facebook (una de las configuraciones de privacidad de Facebook). Configuren que los *tweets* estén protegidos (privados) de forma predeterminada.
- Enséñales a nunca publicar información personal tal como direcciones, números de teléfono o dónde están. Lo mismo vale para la información de sus amigos.
- Desalienta el uso de cámaras web. Diles que nunca envíen ninguna imagen o video a un extraño. Bajo ninguna circunstancia tendrían que cargar una foto que contenga desnudez (es ilegal).

- Lo más importante es que les enseñes a usar sentido común en línea: piensa antes de colocar un mensaje o enviar un *tweet*. ¿Desearías que toda la escuela vea ese mensaje, foto o video? Si no le dirías algo a alguien en la cara, no lo digas en un mensaje en línea.

Cómo proteger la seguridad de tus niños:

- Enséñales a sólo aceptar pedidos de amigos de Facebook y seguidores de Twitter que conozcan personalmente ("No hablen con desconocidos").
- Instrúyelos a jamás aceptar encontrarse cara a cara con alguien que sólo conocen por el Internet.
- Mantén abiertas las líneas de comunicación. Tal vez tus niños no te cuenten todo, pero eso no significa que tú no debas preguntar.

Acoso cibernético

El acoso cibernético es usar el Internet para hostigar o acosar a alguien, por ejemplo, propagando falsos rumores o compartiendo imágenes inapropiadas en el Internet

Cómo prevenir el acoso cibernético:

- Conversa con tus hijos sobre lo que es apropiado decir y hacer en línea. Sean amables en línea.
- De vez en cuando, repasa la información de tus hijos en línea. El ver lo que dicen los demás en las páginas de tus hijos te puede ayudar a detener el acoso cibernético.
- Trata de detectar cambios en la conducta de tus hijos que podrían sugerir acoso cibernético, tal como evitar las computadoras o parecer estresados cuando reciben un correo electrónico o mensaje de texto.

Qué hacer si piensas que tus hijos son víctimas del acoso cibernético:

- Dile a tus hijos que no respondan al acoso cibernético, sino que deben detenerse, bloquear y contar. 1) Dejar de interactuar con el acosador. 2) Bloquear al acosador para que no pueda enviar más mensajes. 3) Contarle a un adulto en el que confían.
- Documenta todo. Guarda los correos electrónicos y demás comunicaciones.
- Busca ayuda. Si sientes que tus hijos corren peligro inminente, denuncia de inmediato el incidente a la policía. También puedes contactar la Línea Directa de Garantía de Seguridad de Comcast llamando al 1-888-565-4329.

Cómo proteger tu identidad

El uso de contraseñas seguras protege tu valiosa información personal y te mantiene protegido.

Qué hacer y qué no hacer con las contraseñas:

- Usa una mezcla de letras, símbolos y números.
- No uses secuencias (123 o abc) o información personal tal como tu fecha de nacimiento.
- No uses palabras fáciles del diccionario.
- No vuelvas a usar contraseñas antiguas.

Instala Constant Guard™, la protección en línea más completa, superior a la que ofrece cualquier proveedor de Internet y agrega tus cuentas de banco y/o compras para ayudar a prevenir que te las roben los piratas informáticos.

"Phishing" por correo electrónico

Esto sucede cuando los estafadores envían correos electrónicos que simulan provenir de compañías existentes con el propósito de engañarte para que les reveles información privada, tal como direcciones o números de cuenta.

Cómo evitar el *Phishing*:

- No respondas a los mensajes que te piden información personal o financiera.
- Revisa el enlace: Si no confías en el sitio web o en quién te lo envía, NO hagas clic en los enlaces en el correo electrónico.

RECURSOS DE APRENDIZAJE

Cómo mantener protegida a tu familia en el Internet

Spyware y virus

Esto sucede cuando un programa de computadora recauda tu información sin tu conocimiento o permiso. El programa espía puede hacer que tu computadora funcione mal (navegación lenta, fallas en los programas, etc.).

Cómo reducir el *Spyware*:

- Instala Constant Guard™ Protection Suite y activa Norton™ Security Suite.
- Ten cuidado cuando visites sitios donde se comparten archivos (Gator, Kazaa, Hotbar y LimeWire).

Spam

Correos electrónicos indeseados. Esto sucede cuando las empresas envían correos electrónicos a mucha gente sin permiso.

Cómo reducir el spam de correos electrónicos:

- Mantén tu Norton Security Suite actualizado.
- Si recibes correos electrónicos sospechosos, bórralos de inmediato, no respondas.

Si necesitas dar una dirección de correo electrónico a alguien en quien no confías, crea una dirección adicional. Saca ventaja de las direcciones de correo electrónico adicionales que te ofrece Comcast con tu servicio.

Para más información, por favor visita InternetBasico.com/aprendizaje o llama al 1-855-SOLO-995 (1-855-765-6995)

comcast