EDUCAR A LOS CIUDADANOS DIGITALES

Todos sabemos que Internet es un mundo fantástico de aprendizaje y entretenimiento para los niños, pero, como en el mundo real, también puede haber peligros. Con algunas precauciones, puede preparar a sus hijos para que se conviertan en ciudadanos digitales honestos que liderarán el futuro. Por otro lado, dar a los niños acceso sin restricciones a Internet puede poner en riesgo a su hijo, a su computadora y a sus datos personales.

Participe de forma positiva

Preste atención a los entornos en línea que utilizan sus hijos. Navegue por la web con ellos. Aprecie la participación de sus hijos en sus comunidades en línea y muestre interés en sus amigos. Cuando encuentren material inapropiado, reaccione de manera constructiva y conviértalo en un momento de enseñanza.

Mantenga la máquina limpia

La ciberseguridad comienza con la protección de todos los ordenadores del hogar con un paquete de seguridad, es decir, software antivirus, antispyware y firewall. Las empresas de software a menudo envían actualizaciones que abordan las últimas amenazas de ciberseguridad, así que configure su software para que se actualice automáticamente para no tener que preocuparse por ello. Mantenga también actualizados su sistema operativo, navegadores web y otro software. Es importante realizar copias de seguridad de los archivos de la computadora de forma periódica, ya sea en la nube, en un disco duro externo o en ambos.

Conozca las características de protección de sitios web, software y aplicaciones

Todos los principales proveedores de servicios de Internet (ISP, por sus siglas en inglés) tienen herramientas para ayudarle a gestionar la experiencia en línea de sus hijos. Estas herramientas le permiten seleccionar sitios web aprobados, monitorear la cantidad de tiempo que los niños pasan en línea y limitar las personas que pueden contactarlos. Es posible que su ISP también tenga otras funciones de seguridad, como bloqueadores de ventanas emergentes. También están disponibles herramientas de terceros para limitar las actividades de los niños en Internet. Recuerde que su computadora de casa no es el único lugar donde pueden conectarse. Es importante que sus hijos comprendan el buen comportamiento en Internet dondequiera que accedan a él.

Revise la configuración de privacidad

Mire las configuraciones de privacidad disponibles en las plataformas de redes sociales, computadoras, teléfonos inteligentes, aplicaciones y otras herramientas digitales que usan sus hijos. Involucre a sus hijos en estas decisiones: decidan juntos qué entornos brindan la cantidad adecuada de protección para cada niño. Enseñe el pensamiento crítico: ayude a sus hijos a identificar sitios web y otros contenidos digitales seguros y creíbles. Enséñeles cómo tener cuidado al hacer clic, descargar, publicar y cargar contenido.

Explique las implicaciones

Explíqueles a sus hijos la naturaleza pública de Internet y sus riesgos y beneficios. Asegúrese de que sepan que cualquier información digital que compartan, como correos electrónicos, fotos o videos, se puede copiar y pegar fácilmente en otro lugar y es casi imposible recuperarla. Recuerde a sus hijos que algunas de estas comunicaciones digitales, como publicaciones o fotografías en las redes sociales, podrían dañar su reputación, sus amistades o sus perspectivas laborales futuras y no deben compartirse.

Ayúdelos a ser buenos ciudadanos digitales

Recuerde a sus hijos que deben ser buenos "amigos digitales" y respetar la información personal de sus amigos y familiares, y no compartir en línea nada sobre otros que pueda resultar vergonzoso o hiriente.

Capacite a sus hijos para que aborden los problemas

Sus hijos pueden enfrentarse a situaciones como acoso cibernético, contacto no deseado o comentarios hirientes en línea. Trabaje con ellos en estrategias para cuando surjan problemas. Estas pueden incluir hablar con un adulto de confianza de inmediato, negarse a tomar represalias, hablar con calma con el acosador, bloquear a la persona o presentar una queja. Acuerden los pasos a seguir si la estrategia falla. Es mejor tener estas estrategias preparadas con antelación, en lugar de reaccionar al acoso cibernético después de que ocurre.

Seguir estos pasos ayuda a

Secure Our World.

Todos podemos ayudarnos unos a otros a mantenernos más seguros en línea, así que comparta estos consejos con un familiar o amigo.

cisa.gov/SecureOurWorld