

Redes sociales

Los sitios de redes sociales son un lugar para que los usuarios de internet se reúnan. Por ejemplo, Facebook, Twitter e Instagram son servicios que la gente puede usar para conectarse con otros para compartir información como fotos, videos y mensajes personales.

A medida que la popularidad de estos sitios sociales crece, también lo hacen los riesgos de usarlos. Estos sitios fomentan y permiten a personas el intercambio de información acerca sí mismos, compartir fotos y videos, y usar blogs y mensajería privada para comunicarse con amigos, otras personas con intereses mutuos, y a veces incluso con el mundo en general. Los Hackers, spammers, escritores de virus, ladrones de identidad y otros criminales siguen el tráfico. Debido a que usted debe divulgar cierto nivel de información personal para utilizar al máximo y beneficiarse de estos sitios sociales, existe el riesgo de robo de identidad para personas que los utilizan.

Consejos para protegerse

- **Elija cuidadosamente su red social.** Evalúe el sitio que planea usar y asegúrese de

entender la política de privacidad. Averigüe si el sitio controla el contenido que las personas publican. Usted proporcionará información personal a este sitio web, así que use el mismo criterio que usaría para seleccionar un sitio de internet donde proveería su tarjeta de crédito.

- **Conozca lo que ha publicado sobre usted.** Sea inteligente y consciente de lo que publica. No anuncie cuando saldrá de la ciudad. Proteja su reputación. Asuma que todo lo que publica en una red social es permanente. Piense dos veces antes de publicar imágenes que no desearía que sus padres o futuros empleadores vean. Una investigación reciente encontró que el 70% de reclutadores de trabajo rechazaron candidatos basados en información que encontraron en línea. Tenga cuidado con la cantidad de información personal que proporciona en sitios de redes sociales. Cuanta más información usted publique, más fácil será para un hacker u otra persona usar esa información para robar su identidad, acceder a sus datos o cometer otros crímenes tales como acecho. Evite publicar

información como su fecha de nacimiento, ciudad natal y año de graduación. Si el sitio lo permite, componga sus propias preguntas de contraseña y no las extraiga de material que cualquier persona pueda encontrar con una búsqueda rápida.

- **Conozca y maneje sus amigos.** Las redes sociales pueden ser usadas para una variedad de propósitos. Parte de la diversión es crear una gran piscina de amigos de muchos aspectos de su vida. Eso no significa que todos los amigos sean iguales. Utilice herramientas para administrar la información que comparte con amigos en diferentes grupos. Si está intentando crear una persona pública como blogger o experto, cree un perfil abierto o una página de "fans" que fomente una amplia participación y limite la información personal. Utilice su perfil personal para mantener a sus verdaderos amigos (los que conoce y son de confianza) más sincronizados con su vida diaria.
- **Sea honesto si esta incómodo.** Si un amigo publica algo sobre usted que le hace sentir incomodo o cree

que es inapropiado, hágase saber. Del mismo modo, mantenga la mente abierta, si un amigo se acerca a usted porque algo que ha publicado hace que él o ella se sienta incómodo(a). Las personas tienen diferentes tolerancias para cuanta información el resto del mundo conoce acerca de ellos, respete estas diferencias.

- **Mantenga una maquina limpia.** Tener el software de seguridad, el navegador y el sistema operativo más reciente son las mejores defensas contra virus, malware y otras amenazas en línea.
- **Haga las contraseñas largas y fuertes.** Combine mayúsculas y minúsculas con números y símbolos para crear una contraseña más segura. Recuerde usar contraseñas diferentes para los bancos en línea y sitios de redes sociales para frustrar a los cibercriminales.
- **Tenga cuidado cuando haga clic en los enlaces que recibe en mensajes de sus amigos en su sitio web social.** Trate los enlaces en mensajes de correo electrónico de estos sitios como lo haría en los mensajes de correo electrónico. Si parece sospechoso incluso si conoce la fuente, es mejor eliminarlo o si es apropiado, marcarlo como correo basura.
- **No confié en que un mensaje es realmente de quien dice ser.** Los Hackers pueden entrar en cuentas y enviar mensajes que parecen

ser de sus amigos, pero en realidad no lo son. Si sospecha que un mensaje es fraudulento, use un método alternativo para ponerse en contacto con sus amigos para averiguar. Esto incluye invitaciones para unirse a nuevas redes sociales.

- **No permita que los servicios de redes sociales analicen su libreta de direcciones de correo electrónico.** Cuando se una a una nueva red social, puede recibir una oferta para ingresar su dirección de correo electrónico y contraseña para averiguar si sus contactos están en la red. Éste sitio puede usar ésta información para enviar mensajes a todas las personas en su lista de contactos o incluso a todas las personas a las cuales haya enviado un mensaje de correo electrónico con esa dirección de correo electrónico. Los sitios de redes sociales deben indicar que van a hacer esto, pero muchos no lo hacen.
- **Escriba la dirección de su sitio de red social directamente en su navegador o utilice sus marcadores personales.** Si hace clic en un enlace a su sitio de red social a través de un correo electrónico u otro sitio web, es posible que introduzca su nombre y contraseña en un sitio falso donde su información personal pueda ser robada.
- **Tenga cuidado al instalar extras en su sitio.** Muchos sitios de redes sociales le permiten descargar aplicaciones de terceros que le permiten hacer más con su

página social. Los delincuentes usan a veces estas aplicaciones para robar su información personal. Para descargar y usar aplicaciones de terceros de forma segura, tome las mismas precauciones que usted toma con cualquier otro programa o archivo que descargue del internet.

- **Acoso en línea.** El acoso en línea puede tomar muchas formas, desde la difusión de rumores en línea y la publicación de información personal, el envío de mensajes privados sin la aprobación del remitente, hasta enviando mensajes amenazantes. Las palabras que escriba y las imágenes que publique pueden tener consecuencias reales. Estas pueden hacer que el objeto de la intimidación se sienta mal, hacer que el remitente se vea mal, y algunas veces, puede traer castigo de las autoridades. Anime a sus hijos a hablar con usted si se sienten el objetivo de un acosador.
- **Conozca que acción tomar.** si alguien le está acosando o amenazando, remuévalos de su lista de amigos, bloqueealos, y repórtelos al administrador del sitio. Si usted siente que podría estar en peligro, infórmelo a la policía.
- **Búsquese usted mismo en Google.** Infórmese acerca de cuál información acerca de usted se encuentra ahí afuera. Usted puede ponerse en contacto directamente con cada operador del sitio web para averiguar cómo puede solicitar

que su información sea removida.

Consejos para proteger a niños y adolescentes

- **Tome medidas adicionales para proteger a los niños más pequeños.** Mantenga la computadora en un área abierta como la cocina o la sala familiar, para que pueda mantener un ojo en lo que sus hijos están haciendo en línea. Utilice el internet con ellos para ayudarles a desarrollar hábitos seguros de navegación. Considere tomar ventaja de las funciones de control parental en algunos sistemas operativos que le permiten administrar el uso de computadoras de sus hijos, incluyendo que sitios pueden visitar, si pueden descargar elementos, o a qué hora del día ellos pueden estar en línea.
- **Hable, y hable a menudo.** Asegúrese de que sus hijos sepan que información debe ser privada y que información puede ser apropiada para compartir. Cuando dan su información personal, renuncian a controlar quien puede llegar a ellos, ya sea con un mensaje de mercadeo o algo más personal. Por otro parte, compartir información personal puede permitirles participar en ciertas actividades o recibir correos electrónicos sobre promociones y eventos en los que están interesados.
- **Aprenda como funciona su computadora.** Pregunte a algún amigo adulto versado en computadoras que le muestre como ver en donde sus hijos

han estado en línea. Compruebe el historial del navegador y los archivos temporales. Tenga en cuenta que los niños mayores pueden saber cómo borrar estos archivos o evitar que se registren. Si desea más controles, investigue que configuración de privacidad su navegador ofrece o considere software de supervisión que ofrece una gama de controles.

- **Aprenda como sus hijos se conectan en línea.** Los niños pueden ponerse en línea usando su computadora o la de alguna otra persona, así como a través de teléfonos móviles y consolas de juego. Conozca que límites usted puede colocar en el teléfono móvil de su hijo. Algunas compañías tienen planes que limitan descargas, acceso al internet, y textos en teléfonos móviles; otros planes permiten que los niños utilicen esas funciones en ciertas horas del día. También verifique que controles parentales están disponibles en las consolas de juego que sus hijos usan.
- **Vaya a donde sus hijos van en línea.** Regístrese y utilice los sitios de redes sociales que sus hijos visitan. Hágalos saber que usted está ahí, y enséñeles como actuar y socializar en línea. Vaya a sitios de red comunes en línea, regístrese y cree un perfil para usted. Proporcione solo la información necesaria para crear un perfil y nada más. A continuación puede buscar la página de sus hijos.

Recuerde, sus hijos pueden haber dado un nombre o código

falso por lo que esta búsqueda podría no encontrar su página. Usted puede buscar utilizando otra información, como el nombre de la escuela de su hijo. Todos los niños que han incluido esta escuela en su perfil serán identificados en esta búsqueda. Si su niño no es identificado en esta lista, usted puede seleccionar amigos de su hijo para ver si su hijo está incluido en sus páginas como amigo. También puede realizar búsquedas mediante el uso de palabras clave y direcciones de correo electrónico. En la mayoría de los servicios de redes sociales, ambos usuarios deben confirmar que son amigos antes de estar vinculados. Algunos sitios tienen una herramienta de "favoritos" que no necesita la aprobación del otro usuario.

- **Genere un nombre de pantalla seguro.** Fomente que sus hijos piensen acerca de la impresión que los nombres de pantallas pueden hacer. Un buen nombre de pantalla no revelará demasiado sobre cuantos años tienen, donde viven o su género. Por razones de privacidad los nombres de pantalla de los niños no deben ser los mismos que sus direcciones de correo electrónico.
- **Haga acuerdos.** Asegúrese de que sus hijos sepan lo que su familia ha decidido que está bien y lo que no está bien para divulgar en línea. Considere anotar la lista de reglas que su familia haya acordado y publicarlas donde todos puedan verlas.

- **Revise la lista de amigos de su hijo.** es posible que desee limitar los “amigos” en línea que su hijo realmente conoce y se lleva bien en la vida real. Las redes sociales usualmente tienen controles de privacidad que permiten al usuario el escoger quien puede ver su perfil o contactarlos, etc.

- **Establezca reglas acerca de reunirse con “amigos” de línea en público.** Establezca claramente que si un niño va a conocer a una persona él o ella sólo ha conocido por el internet, debe ser con su permiso, en un lugar público y que usted o algún otro adulto de confianza debe de estar presente.

- **Comprenda las políticas de privacidad de los sitios.** Los sitios deben especificar sus derechos como padre para revisar y borrar el perfil de su hijo si es menor de 13 años. Los sitios deben también proporcionar software que permite a los padres bloquear el acceso a su sitio. La Ley de Protección de la Privacidad de los Niños en Línea (COPPA por sus siglas en inglés) requiere que los sitios web obtengan el consentimiento de los padres antes de recopilar, usar o revelar información personal de niños menores de 13 años.

Para obtener más información sobre cómo mantenerse seguro en línea, visite los sitios web de las siguientes organizaciones:

- **Staysafeonline.org** es un sitio educativo destinado a ayudar a los consumidores a comprender tanto los aspectos positivos del internet como la

forma de gestionar una variedad de cuestiones de seguridad y problemas de seguridad que existen en línea.

www.staysafeonline.org

- **WiredSafety.com** es un grupo de seguridad y ayuda en internet. WiredSafety.org provee educación, asistencia y conocimiento en cybercrime y abuso, privacidad, seguridad y el uso responsable de tecnología. Es también el grupo matriz de Teenangels.org, adolescentes y preadolescentes entrenados por el FBI que promueven la seguridad en el internet.

www.wiredsafety.com

- **ConnectSafely.org** es un foro para padres, adolescentes, educadores y defensores; designado para dar a los adolescentes y padres una voz en la discusión pública sobre la seguridad de los jóvenes en línea y tiene consejos, así como otros recursos para blogs seguro y redes sociales.

www.connectsafely.org

- **OnGuardOnline.gov**, administrado por la Comisión Federal de Comercio, proporciona consejos prácticos del gobierno y la industria de tecnología para ayudarle a estar en guardia contra el fraude de internet, proteger su computadora y proteger su información personal.

www.onguardonline.gov

Para más información o para presentar una queja visite nuestra página web o comuníquese con el Departamento de Protección al Consumidor.

Departamento de Protección al Consumidor
2811 Agriculture Drive
PO Box 8911
Madison, WI 53708-8911

Correo Electrónico:
DATCPHotline@wi.gov

Sitio de Internet:
Datcp.wi.gov

(800) 422-7128

Fax: (608) 224-4677

TTY: (608) 224-5058