Una publicación de Consumer Action

Lo que no 'Me gusta'

Cómo proteger su privacidad en las redes sociales

YouTube, Instagram, Facebook, Twitter y otros son medios de comunicación social que la mayoría de los consumidores "conectados" reconocen instantáneamente. De hecho, el uso de redes sociales es uno de los pasatiempos favoritos de adolescentes y adultos por igual.

El intercambio puede ser divertido y gratificante, pero usted podría sufrir consecuencias si no tiene cuidado sobre lo que revela y a quién. Afortunadamente, el usuario de medios sociales puede limitar lo que comparte y puede proteger su información personal de muchas formas. Si ejerce precaución y es proactivo, podrá disfrutar de los medios de comunicación social a la vez de tener tanta privacidad como desee.

La importancia de la privacidad

La gente comparte todo tipo de cosas en las redes sociales. Algunas, como un video de su mascota haciendo algo curioso, podría compartirlas con todo el mundo sin consecuencias negativas. Otras, como anunciar que ganó la lotería, pueden ser riesgosas. El primer paso para protegerse es ser capaz de reconocer la diferencia. Pruebe si sabe reconocer los riesgos en estos mensajes compartidos abiertamente en los medios sociales:

Sarah vive en San Francisco. Escribió en Twitter, desde Hawái, que la está pasando de maravillas en su semana de vacaciones. (Cuando regresó, Sarah se llevó la sorpresa de que alguien había entrado a robar en su apartamento).

Joe, que tiene esperanzas de ser ascendido de puesto, publicó una queja sobre su empleo: "¡La compañía donde trabajo trata a sus empleados como esclavos!" (El jefe de Joe vio su publicación en la página de Facebook de un compañero de trabajo. No se vislumbran posibilidades de ascenso en el futuro de Joe).

A Ricardo le encanta recibir felicitaciones por su cumpleaños, así que publicó el mes y la fecha de su gran día en su perfil público junto con el año que terminó la escuela preparatoria o "high school" ("graduado en el 82"). (Ricardo se convirtió en víctima de robo de identidad. Alguien pudo calcular su fecha de nacimiento completa y, junto con su nombre completo y otra información obtenida en sus publicaciones, la utilizó para ingresar a una de sus cuentas).

Janice, tiene 17 años y cursa el último año de "high school" y acaba de mandar solicitudes de ingreso a las universidades. Por Instagram publicó una foto de sí misma bebiendo cerveza en la fiesta de un amigo. (La universidad preferida de Janice investiga las actividades de los postulantes en los medios sociales y rechaza a quienes participan en comportamiento criticable; por ejemplo, un menor de edad que consuma bebidas alcohólicas.)

No hay nada malo en compartir fotos y videos, estar en contacto con amigos y familia o promover ideas o proyectos. Pero primero es necesario considerar cómo podría utilizarse cualquier información que revela; en especial cuando la pueda ver alguien a quien no tuvo intención revelarla.

Elija su público

Cuando abre una cuenta en una red social, por lo general tiene la opción de cambiar la configuración predeterminada del programa para que coincida con el público que usted prefiere. En algunos casos, también puede modificarla en cada elemento individual que publica o comparte. Antes de empezar a compartir, conozca las opciones de privacidad de la red social en particular y modifíquelas según sea necesario.

Mientras que estos ajustes pueden ser muy eficaces, no deben darle un sentido falso de confianza. Con sólo limitar su público no se puede evitar que otros puedan ver lo que comparte. Por ejemplo, usted no tiene control sobre quién ve los mensajes que agrega a los perfiles de otros, y no puede evitar que otros copien y distribuyan algo que usted ha compartido con ellos. También es posible encontrar sus imágenes, perfiles de cuenta y contenido con simplemente ingresar su nombre en un buscador de Internet.

Por esta razón, siempre es mejor tener cuidado. Antes de compartir algo, piense en todos los que posiblemente puedan verlo; jefe, cliente, compañero de trabajo, profesor, agencia gubernamental, propietario de la vivienda que alquila, compañía de seguros, abuelos, ya sea en la actualidad o en el futuro.

Sin importar cuanto haya limitado su público, nunca comparta lo siguiente:

- Número de Seguro Social
- Apellido de soltera de su mamá, su fecha de nacimiento completa (día, mes y año) u otra información que se utiliza comúnmente para verificar identidad
- Dirección o número de teléfono personal
- Su paradero actual (en tiempo real) o cualquier otra información que podría usarse para rastrearlo
- Cualquier información que revele que no hay nadie en su casa o que usted o sus hijos se encuentran solos en casa

Normas de privacidad

Hay otras maneras importantes, además de limitar su público, para protegerse usted mismo y para proteger su privacidad en línea.

Las siguientes son 16 normas eficaces:

No se sienta obligado a completar todos los campos al crear su perfil, todo es opcional.

No acepte solicitudes o invitaciones de gente que no conoce con la intención de acumular "amigos" o "seguidores". Y no responda a mensajes de desconocidos.

No publique información o fotos, tal como su nuevo coche deportivo, el interior de su casa, etc., ni comparta planes de viaje que podrían atraer a estafadores o ladrones.

No responda a cuestionarios, juegos, ofertas de cupón u otros incentivos que requieran que ingrese información personal. Esto lo expone a mercadeos fastidiosos y también a estafas.

No haga clic en enlaces desconocidos, que podrían estar diseñados para infectar su computadora con un virus o con un programa espía que le robará sus datos.

Personalice la configuración de privacidad

Inicie sesión en su cuenta y busque una sección titulada privacidad, configuración o preferencias ("Privacy", "Settings" o "Preferences") o utilice la función de ayuda ("Help") para encontrar y comprender las características y herramientas de la red. Si incluso así necesita ayuda, utilice el enlace del sitio o la aplicación para ponerse en contacto con el personal de apoyo de la red social, pregunte en el área comunitaria o foro ("Community" o "Forum"), o haga búsqueda de su pregunta en Internet (ejemplo: "¿Cómo utilizo la configuración de privacidad en [nombre de la red social]?").

Desde ahí, puede modificar su configuración para limitar quién puede ver su perfil, ponerse en contacto con usted o ver lo que ha compartido. Si es necesario, aproveche las opciones para cambiar su público en cada elemento individual que comparte, y bloquee o elimine a amigos ("unfriend") para controlar su nivel de exposición. (Tenga en cuenta que incluso si usted tiene la opción de volver atrás y cambiar el público de una publicación existente o eliminarla completamente, puede ser demasiado tarde para mantenerla privada.)

En caso de duda, ¡no comparta!

Sí: Configure la computadora y los dispositivos móviles para que requieran una contraseña o PIN (número de identificación personal) cuando se pongan en marcha o se despierten.

Sí: Invente contraseñas fuertes en sus cuentas (mezcle al menos ocho números, letras y símbolos) y cámbielas con regularidad. No use la misma contraseña para todas sus cuentas, ni el nombre de su mascota o niño si comparte esos detalles en las redes sociales. Cuando se le dé la opción de elegir preguntas de seguridad, elija las que tengan respuestas que probablemente otros no conocerán.

Sí: Asegúrese de cerrar la sesión si utiliza una computadora pública para acceder a sus cuentas. Es buena idea cerrar la sesión incluso en su propia computadora y dispositivos.

No deje que su navegador guarde información de inicio de sesión si se le ofrece esa opción, o, en la sección de configuración o preferencias del navegador, marque o desmarque las casillas correspondientes en las pestañas de seguridad, contraseñas, sincronización o autorrelleno.

Sí: Active y actualice el programa de seguridad (cifrado, barrera de control de acceso o "firewall", programas antivirus y antiespías, etc.).

Sí: Revise la política de privacidad de la empresa antes de abrir una cuenta para saber cómo podrían utilizar su información personal o los datos del dispositivo.

No descargue una aplicación a menos que se trate de una fuente confiable y siempre después de verificar las opiniones de usuarios y de haber leído la política de privacidad.

Sí: Lea todos los avisos que le envíen las redes sociales y aplicaciones para no perderse los cambios de política. Si no está contento con un cambio, cancele su cuenta o desinstale la aplicación.

Controle sus aplicaciones móviles

En general, las aplicaciones móviles o "apps" (programas descargables que mejoran la funcionalidad de su teléfono inteligente o tableta) pueden acceder a la mayoría de la información en su dispositivo, incluso contactos y mensajes. Algunas apps, aunque no todas, le piden permiso para acceder a esta información o a su ubicación.

Para administrar la configuración de las aplicaciones de redes sociales, visite el sitio web de la red social y en la sección de preferencias, ajustes o ayuda ("Preferences", "Settings" o "Help") busque "aplicaciones" o "intercambio de datos" ("Apps" o "Data Sharing") o algo similar. Luego ajuste la configuración al nivel en que se sienta cómodo. Para controlar lo que una aplicación recoge e intercambia fuera de las redes sociales, verifique la configuración de la aplicación misma. Lea la política sobre privacidad y uso de datos de la aplicación y entonces decida si se siente confiado o si debe desinstalar la aplicación y encontrar una distinta.

No permita que las aplicaciones anuncien su ubicación.

Sí: Hable con sus hijos acerca de cómo ser responsable y no ponerse en peligro en línea (incluso les debe advertir sobre el envío de mensajes sexuales, "sexting"). También establezca preferencias de privacidad fuertes en las cuentas de ellos, aproveche los controles para padres y vigile con regularidad las comunicaciones de sus hijos.

Sí: Cumpla con la política de su empleo sobre medios de comunicación social, si la hubiera.

Acerca de Consumer Action

www.consumer-action.org

A través de materiales de educación del consumidor en varios idiomas, extensión a la comunidad y defensa en base a temas importantes, Consumer Action faculta al consumidor infrarrepresentado a nivel nacional para hacer valer sus derechos y prosperar económicamente.

Asistencia y asesoramiento al consumidor:
Presente quejas del consumidor en: *https://complaints.consumer-action.org/forms/spanish-form* o 415-777-9635. Se hablan chino, inglés y español.

Recursos

Visite estos enlaces para aprender más sobre cómo proteger su privacidad y permanecer seguro en línea:

StaySafeOnline.com [*https://www.staysafeonline.org*]

Privacy Rights Clearinghouse (privacidad en redes sociales) [*https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social*]

Google Safety Center (centro de seguridad de Google) [*https://www.google.com/safetycenter/*]

Online Safety Institute (buenas normas para padres en relación a la seguridad digital) [*https://www.fosi.org/good-digital-parenting/*]

OnGuardOnline.gov (protección de niños en línea) [*http://www.onguardonline.gov/topics/protecting-kids-online*]

Common Sense Media (uso responsable de medios sociales para jóvenes) [*http://www.commonsensemedia.org/blog/talking-about-sexting*]

TrustArc (consejos de privacidad) [*https://www.trustarc.com/blog/2011/04/27/5-privacy-tips-for-mobile-app-users/*]

How to read a privacy policy (Cómo leer una política de privacidad) [*http://oag.ca.gov/privacy/facts/online-privacy/privacy-policy*]

CNET (protección de su reputación en línea) [*http://www.cnet.com/how-to/how-to-manage-your-online-reputation-for-free/*]

CTIA-The Wireless Association (seguridad en los dispositivos móviles) [*https://www.ctia.org/consumer-resources/protecting-your-data*]

AARP (protección del teléfono) [*http://www.aarp.org/home-family/personal-technology/info-2014/cyberproof-stolen-phone-kirchheimer.html*]

Federal Trade Commission (FTC) (uso seguro de redes wifi públicas) [*http://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks#Mobile*]

Apple (Mac) [*http://www.apple.com/support/osx/passwords/*] o PC [*http://pcsupport.about.com/od/tipstricks/ht/newxppassword.htm*] (cómo configurar su sistema para requerir una contraseña o PIN para iniciar o despertar)

ConnectSafely (creación de contraseñas robustas) [*http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/*]

PasswordsGenerator.net (para crear contraseñas) [*http://www.passwordsgenerator.net*]

PCMag.com (Los "mejores" administradores de contraseñas gratuitos) [*http://www.pcmag.com/article2/0,2817,2475964,00.asp*]

Acerca de esta guía

Consumer Action creó a esta guía con una subvención de Rose Foundation.

© Consumer Action 2016