Tome control

Personalice la configuración de privacidad en las redes sociales

Las plataformas de medios sociales crean una comunidad en línea que ofrece todo tipo de recompensas: nuevos amigos, entretenimiento, un foro de aprendizaje y mucho más. Pero, asimismo, la actividad en internet aumenta los riesgos concretos que corre su privacidad. Esta publicación plantea las posibles consecuencias de compartir demasiado en las redes sociales, explica cómo lograr el nivel deseado de privacidad en las plataformas de medios sociales más populares y proporciona consejos útiles, herramientas, y recursos sobre privacidad.

La importancia de la privacidad

El internet, las redes sociales y otras opciones digitales de interacción nos permiten comunicarnos con amigos (y desconocidos) en todo el mundo. Si bien puede ser una poderosa herramienta para crear comunidad, la mayoría de personas consideran que es aconsejable e inteligente poner límites sobre qué se revela sobre ellos y a quién.

Por ejemplo, puede ser arriesgado compartir:

- Su horario o planes de viaje
- La fecha de nacimiento o el apellido de soltera de su madre
- Los nombres de sus hijos y a qué escuelas asisten
- Su estado civil o financiero
- Una foto de usted cuando anda "de parranda"

Si elije un público de familiares y amigos, esta información no corre peligro. Pero cuando se comparte con extraños o un público indeseado, puede exponerle al acoso o a la atención indeseada, causarle daño a su imagen personal, tener repercusiones profesionales, exponerle al acecho, robo de identidad y otras consecuencias.

Afortunadamente, las plataformas de redes sociales

han evolucionado para permitir que el usuario elija la cantidad de privacidad que desea y pueda ajustar los controles de la plataforma para que se adapten a sus necesidades.

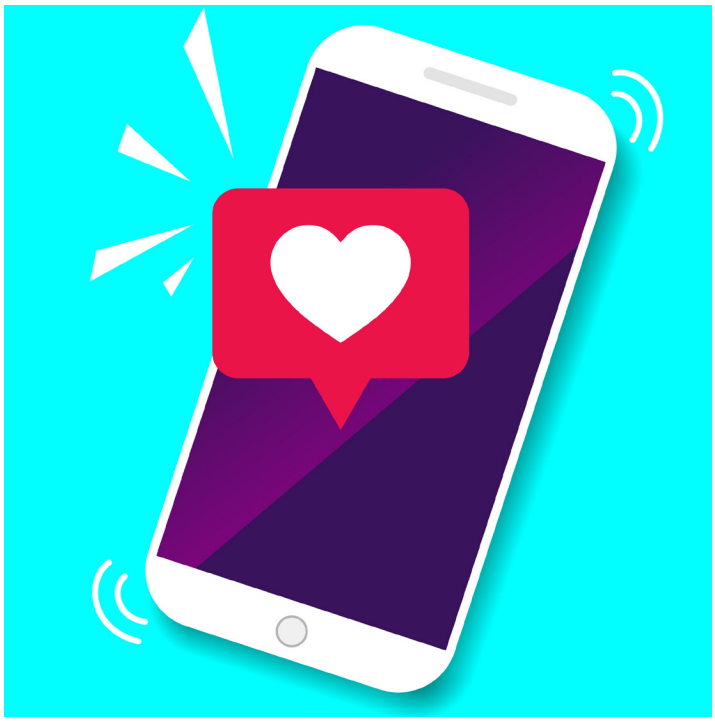
Niveles de control

Los controles de privacidad que puede ajustar y sus opciones de personalización varían según la plataforma. Por ejemplo, una podría permitirle ser más específico en la selección de su público que otra. Es importante comprender, *antes* de empezar a usar una plataforma de redes sociales, lo que puede y *no puede* controlar. Si no puede alcanzar un nivel de privacidad con el que se sienta cómodo, debe elegir otra plataforma que se adapte mejor a sus necesidades.

Las áreas típicas sobre las que tendrá cierto control en la mayoría de las plataformas incluyen:

- Detalles del perfil (quién puede ver su información personal, tal como dónde vive, el estado de su relación sentimental, o su información de contacto)
- Público general (quién puede ver su contenido)
- Público de algún contenido en particular (quién puede ver un tweet, foto, historia, video, etc. en particular)
- Etiquetado de fotos (si se identifica con su nombre en una foto y dónde aparece la imagen)
- Información de ubicación (si su ubicación se anuncia en el momento de la publicación)
- Estado de actividad (si otros pueden ver la última vez que utilizó la plataforma)

Además de estos ajustes de privacidad más comunes, las plataformas de medios sociales ofrecen muchas otras opciones, incluso algunas que pueden ser exclusivas de una plataforma en particular. La única manera de saber cuáles son todas sus opciones de privacidad es visitando la sección de *Privacidad* o *Ayuda* del sitio web o de la aplicación. (También puede obtener consejos de usuarios y autores de temas tecnológicos haciendo una búsqueda en línea de "[nombre de la plataforma]" más "opciones de privacidad" o "configuración de privacidad" o palabras clave similares.) (En inglés buscaría "[nombre de la plataforma]" más "privacy options" o "privacy settings" o palabras similares.)

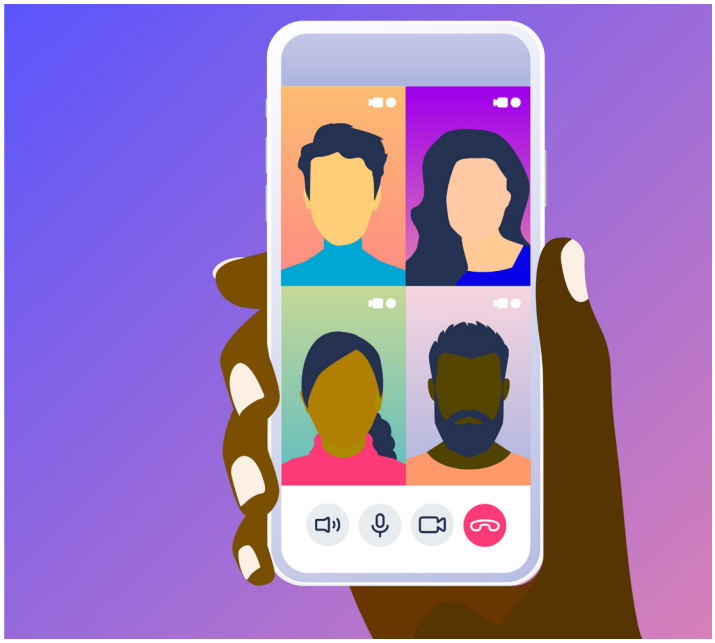


También hay aspectos de la privacidad que no podrá controlar en todas las plataformas, o tal vez en ninguna. Por ejemplo, podría ser inalterable o parcialmente controlada la forma en que la propia plataforma recopila (o comparte) datos. Si para usted eso es inaceptable, su única opción es no usar la plataforma.

Personalice su privacidad

Todas las cuentas de redes sociales comienzan con una configuración de privacidad predeterminada cuando se abre la cuenta. Antes de su primera publicación (tweet, etc.), debe ajustar el nivel de privacidad para que coincida con sus preferencias. Para ello, inicie sesión en su cuenta y busque la sección *Configuración* (o, en algunos casos, *Privacidad* o *Configuración y privacidad*) (a menudo se encuentra bajo el icono de su perfil o bajo el icono de "equipo" o "herramientas", o utilice las funciones *Ayuda* o *Soporte* para encontrar y comprender las características y herramientas de esa red).

A continuación, se presenta información básica (y algunos consejos) para personalizar la configuración de privacidad de algunas de las plataformas de redes sociales más populares. (También puede hacer una búsqueda en línea con el nombre de la red social más las palabras "configuración de privacidad" ["privacy settings"] o "consejos de privacidad" ["privacy tips"] para encontrar orientación adicional.)



Facebook (*https://www.facebook.com*): Facebook permite que los usuarios se conecten y compartan con familiares, amigos y comunidades a través de su sitio web y aplicación móvil. El público puede ver cierta información en su perfil; su nombre, foto de perfil y portada, género, y nombre de usuario. Tiene la opción de personalizar otras configuraciones, por ejemplo, qué público puede ver sus publicaciones, quién puede ver y publicar en su "biografía", quién puede enviarle "solicitudes de amistad", qué información se puede recopilar sobre usted, si los motores de búsqueda pueden encontrar su perfil, y mucho más. También puede controlar su exposición a ciertos individuos en particular al eliminarlos de su lista de amigos, dejarlos de seguir o bloquearlos. La *Comprobación de privacidad* de Facebook le ayuda a revisar algunos ajustes de privacidad importantes (en el sitio web, haga clic en "?" en la esquina superior derecha de la pantalla y seleccione *Comprobación de privacidad* en el menú. Desde ese mismo menú, puede entrar a *Accesos directos a la privacidad* (*https://www.facebook.com/privacy/*), que es una lista más larga de opciones de privacidad y seguridad. Para acceder a *Comprobación de privacidad* en la aplicación, seleccione el menú en la esquina inferior derecha de la pantalla, abra *Configuración y Privacidad*, luego *Configuración*, y haga clic en *Revisar algunos ajustes importantes*. *Accesos directos a la privacidad* se encuentra directamente bajo *Configuración* y *Privacidad*.

CONSEJO: Muchas aplicaciones y sitios web le permiten iniciar sesión con su nombre de usuario y contraseña de Facebook. Verifique a qué información la aplicación está solicitando acceso y limite las categorías que no quiera compartir. Si ya usó Facebook para iniciar sesión en alguna aplicación o servicio de terceros, puede controlar los datos que está compartiendo con esa aplicación o sitio web en la sección *Aplicaciones y sitios web* de *Configuración* en Facebook.

Instagram (*https://www.instagram.com*): Instagram es una aplicación (propiedad de Facebook) para compartir fotos y videos que permite que los usuarios compartan imágenes y videos cortos con sus seguidores, quienes, a su vez, pueden comentar sobre las imágenes. De forma predeterminada, cualquiera puede ver sus fotos de perfil e "historias" (fotos o videos que desaparecen después de 24 horas), pero usted tiene la opción de calificarlos como privados para que solo sus seguidores aprobados puedan ver lo que publica. También puede eliminar seguidores, ocultar su estado de actividad, bloquear comentarios en una publicación, impedir que se vuelva a compartir su historia en forma de mensaje, activar o desactivar el uso compartido de sus publicaciones de Instagram en otras redes sociales (Facebook, Twitter, Tumblr, etc.), y mucho más. (Aun así, independientemente de su configuración de privacidad, cualquier usuario podrá leer su biografía, y enviarle una foto o video directamente.) La mayoría de la configuración de privacidad de Instagram se accede a través de la aplicación móvil; haga clic en el icono de perfil en la esquina inferior derecha de la pantalla, luego haga clic en el icono de menú (tres líneas horizontales) en la esquina superior derecha, seleccione *Configuración* en la parte superior de la lista, y desde allí se puede acceder a *Privacidad, Seguridad* y otras opciones. Cada vez que haga clic para publicar fotos o videos en Instagram, tendrá la oportunidad de ver ajustes adicionales. Obtenga más información en el *Servicio de ayuda* de Instagram (*https://help.instagram.com/196883487377501*) y en el *Centro de privacidad y seguridad* (*https://help.instagram.com/285881641526716*).

CONSEJO: Cualquiera puede etiquetarlo en fotos y videos en Instagram, excepto las personas que bloqueó. Dado que no todas las fotos las querrá compartir, puede elegir aprobar las imágenes manualmente antes de que aparezcan en su perfil (en la aplicación, en *Configuración*, haga clic en *Privacidad*, luego *Etiquetas* y active *Aprobar etiquetas manualmente*).

LinkedIn (*https://www.linkedin.com/*): LinkedIn es una plataforma para profesionales en la que pueden

compartir sus historiales de empleo, currículums y carteras; interconectar con otros profesionales; construir sus "marcas"; y, si se desea, buscar nuevos puestos de trabajo. Se le da control sobre una serie de configuraciones de cuenta y privacidad, incluyendo lo que comparte sobre usted y con quién (perfil, dirección de correo electrónico, conexiones, etc.), quién puede ver cuándo inició sesión, quién puede seguirle y cómo la plataforma en sí utiliza sus datos. Si no quiere que todos sepan qué empresas está siguiendo, a quién está recomendando o los cambios que realiza en su perfil, asegúrese de desactivar la configuración de *Transmisiones de actividad*. Si no quiere que los que están fuera de su red se suscriban a sus actualizaciones de actividad (sin agregarle como conexión), vaya a la configuración *Elegir quién puede seguir tus actualizaciones* y limite el público de sus conexiones. Obtenga más información en la página de la plataforma *Gestionar tu configuración de cuenta y de privacidad: Resumen* (*https://www.linkedin.com/help/linkedin/answer/66*). Vea y cambie las configuraciones de su cuenta y de privacidad en *https://www.linkedin.com/psettings/*.

CONSEJO: Si no quiere que se sepa que ha visto el perfil de alguien, active el modo privado de visualización de perfiles. Esta configuración se encuentra en la sección *Privacidad* de *Configuración*, en *Opciones de visualización de perfiles*.

Pinterest (*https://www.pinterest.com/*): Al igual que Instagram, Pinterest es una plataforma orientada a lo visual; permite a los usuarios publicar por medio de un "pin" imágenes y videos de interés (a menudo dentro de un tema elegido) en sus "tableros", navegar por lo que otros han publicado y compartir sus propios tableros con el contenido que han seleccionado. En comparación con otras plataformas de redes sociales, la configuración de privacidad de Pinterest es bastante sencilla. Tiene la opción de ocultar su perfil de los motores de búsqueda. También, mediante el uso de tableros "secretos" que sólo pueden ver usted y personas que invita, puede impedir que otras personas vean sus "pines". Se puede acceder a estas y otras opciones haciendo clic en el icono de su perfil y seleccionando *Configuración*. Obtenga más información sobre la configuración de privacidad en la sección *Ayuda* de Pinterest: *https://help.pinterest.com/en/article/edit-account-privacy*.

CONSEJO: Pinterest y los terceros con los que se asocia utilizan información sobre sus visitas a otros sitios y sobre las aplicaciones que usa para personalizar los anuncios que usted ve en línea. Si prefiere anuncios al azar (en lugar de sentirse vigilado), puede fijar en "No" la pestaña *Usar información de nuestros socios publicitarios* en *Configuración*.

Snapchat (*https://www.snapchat.com/*): Snapchat es una aplicación de mensajería utilizada para compartir fotos, videos, texto y dibujos que desaparecen en pocos segundos o, en el caso de "historias", en 24 horas. Dada la corta vida útil de los "snaps", los usuarios pueden sentir una falsa sensación de seguridad (en otras palabras, sienten que la privacidad no es un problema ya que nada será visible durante mucho tiempo). Aun así, los usuarios deben seguir los pasos para personalizar algunos ajustes de privacidad. De forma predeterminada, solo los usuarios que haya añadido como amigos pueden enviarle "snaps" o ver su "historia". Sin embargo, debe desactivar la función *Añadido fácil* si no quiere aparecer en las listas de "sugeridos" de los amigos de sus amigos. Si figura en las listas de amigos de usuarios desconocidos, puede bloquearlos en su perfil en la sección *Amigos añadidos* > *Me añadieron*. Su ubicación en "Mapa de Snaps" solo se actualiza cuando tiene abierto Snapchat, pero es posible que no quiera compartirla. Sus opciones incluyen el *Modo fantasma* (nadie podrá ver su ubicación), *Seleccionar amigos* (elija individuos específicos) y *Mis amigos* (todos los amigos que agregó) (*https://support.snapchat.com/es/news/ghost-mode-timer*). Obtenga más información sobre las opciones de privacidad de su cuenta en la página *Ayuda de Snapchat* (*https://support.snapchat.com/es/article/privacy-settings2*).

CONSEJO: Aunque Snapchat da la ilusión de impermanencia, un destinatario puede tomar una captura de pantalla de su Snap y convertirlo en permanente y compartible. La aplicación le notificará si alguien toma una captura. Saberlo podrá ayudarle a decidir qué envíarle a ese destinatario en el futuro. Si bien estas notificaciones son útiles, tenga en cuenta que se pueden encontrar instrucciones en línea que explican cómo tomar una captura de pantalla sin provocar que la aplicación envíe una notificación.

Tumblr (*https://www.tumblr.com/*): Tumblr es una plataforma de blogs que le permite publicar imágenes, GIF, videos, música, texto, enlaces y más. La plataforma permite una cantidad limitada de controles de privacidad, como ocultar el estado de

su actividad, evitar que lo puedan encontrar con su dirección de correo electrónico, ocultar su blog de los resultados de los motores de búsqueda y poner restricciones sobre qué aplicaciones de terceros, de haberlas, pueden acceder a sus datos de Tumblr. Visite el *Centro de ayuda* de Tumblr para obtener información sobre las configuraciones que puede ajustar y cómo hacerlo *https://tumblr.zendesk.com/hc/es*.

CONSEJO: Su blog principal, que configura al abrir la cuenta de Tumblr, es público y no está, por defecto, protegido con contraseña. Para lograr mayor privacidad, puede configurar blogs secundarios protegidos por contraseña de forma que sólo tengan acceso aquellos que conocen la contraseña o usuarios que usted añadió como miembros.

Twitter (*https://twitter.com/*): Twitter permite que los usuarios se comuniquen con mensajes cortos (280 caracteres) llamados tweets que pueden llevar enlaces, fotos y videos. Por defecto, su cuenta de Twitter es pública, como tal, todos pueden ver sus tweets e información. Tiene la opción de hacer que su cuenta sea privada, o sea que solo los usuarios aprobados por usted puedan suscribirse y ver sus tweets; tweets que anteriormente eran públicos se ocultarán de quienes no sean sus seguidores aprobados; sus tweets ya no aparecerán en las búsquedas de Google ni podrán ser reenviados; y las respuestas directas que envíe no serán vistas, a menos que las envíe a sus seguidores aprobados. Ese y otros cambios los puede hacer en la sección *Privacidad y seguridad* (*https://twitter.com/settings/safety*) al ajustar la configuración de su cuenta. Desde ahí mismo, para mantener privada su ubicación (lo que es aconsejable), elimine la marca (o no marque) la casilla *Añadir mi ubicación a mis Tweets*. También puede tomar ciertas decisiones sobre tweets individuales que envía y recibe. Visite la página *Cómo controlar tu experiencia en Twitter* (*https://help.twitter.com/es/safety-and-security/control-your-twitter-experience*) para obtener una guía clara de lo que puede y no puede controlar en la plataforma.

CONSEJO: Si le molestan ciertas palabras o frases, puede "silenciar" (filtrar) tweets que las contengan agregándolas a su lista. Busque *Palabras silenciadas* en *Configuración y privacidad*. También puede "bloquear" o "silenciar" cuentas completas, una diferencia clave es que cuando bloquea a alguien, se les notifica, mientras que silenciar es más sutil (sin notificación).

YouTube (*https://www.youtube.com/*): YouTube es un servicio de intercambio de videos. Al subir un video, se establece como "Público" de forma predeterminada, lo que significa que cualquiera

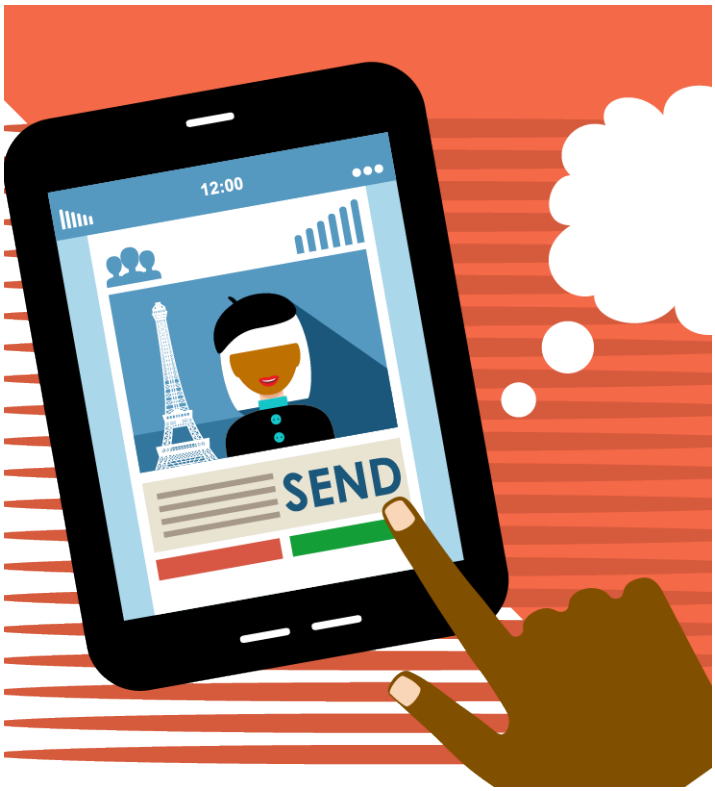
puede verlo. Pero puede cambiarlo a "Privado" o "No listado" durante la carga o más tarde. Un video privado no aparecerá en su canal ni en los resultados de búsqueda, y solo podrán verlo usted y el público que seleccione. Únicamente las personas a las que le da el enlace pueden ver y publicar comentarios sobre un video no listado. Los videos no listados no aparecen en la pestaña *Videos* de la página de su canal ni en los resultados de búsqueda de YouTube (a menos que alguien agregue su video no listado a una lista de reproducción pública). Si alguien publica su información personal o sube un video suyo sin su consentimiento y se niega a eliminarlo, o si ponerse en contacto con ellos para usted es una situación incómoda, puede pedirle a YouTube que elimine el contenido (*https://support.google.com/youtube/answer/2801895*). Visite el *Centro de privacidad y seguridad* de YouTube para obtener más información sobre el uso de YouTube de forma segura (*https://support.google.com/youtube/topic/2803240*).

CONSEJO: Si no quiere que su historial de visualización se comparta en las redes sociales, no haga clic en "Compartir", "Me gusta" o botones similares asociados con un video publicado. Si desea compartir esta información, debe seleccionar el público deseado.

Prácticas recomendadas de privacidad

1. Infórmese bien sobre la pólitica de privacidad. Antes de abrir una cuenta en redes sociales, consulte la política de privacidad de la plataforma y entérese cómo pueden utilizar su información personal o los datos de su dispositivo, y cuánto control tiene usted sobre su privacidad. Es posible que no tenga mucho control sobre la recopilación de datos de la empresa mientras está en el sitio web o en la aplicación, pero podría tener cierto control sobre el uso compartido de datos con terceros, sobre si verá o no anuncios personalizados, y sobre la recopilación de tipos específicos de datos, como su ubicación precisa. Si abre una cuenta, lea todos los anuncios de la empresa para no perderse algún cambio de política. Si no está satisfecho con algún cambio, cancele su cuenta o desinstale la aplicación. (Si es posible, descargue sus datos antes de cerrar la cuenta.)

2. Sea discreto. Cuando cree su perfil, no será necesario que rellene todos los campos. Quien necesite saber su fecha de nacimiento, escuela,



dirección de correo electrónico, número de teléfono y otros datos personales probablemente ya tiene esa información. Del mismo modo, no publique información o fotos (sus planes de vacaciones, su nuevo auto deportivo, el interior de su casa, etc.) que lo vuelvan más atractivo para estafadores y ladrones. Y tenga presente que, si publica algo en el perfil de otra persona, no tiene control sobre quién lo puede ver.

3. Piense antes de compartir. ¿Qué repercusiones pueden haber si su publicación, tweet, video, etc. fueran transmitidos al mundo entero? Dado que es posible que algo se comparta con personas ajenas a su público previsto, ya sea a propósito o sin querer, pregúntese "¿Qué pensarán de esto mis padres, mi pareja, maestros, oficial de admisiones universitarias, empleador actual o futuro, compañeros de trabajo, clientes, prestamistas, aseguradoras, arrendadores, fuerzas del orden público, etc.?" "¿Cómo puede usar esta información un criminal, acosador, etc.?" Proteja su "reputación electrónica"; mucha gente que no lo conoce personalmente puede usar las redes sociales como fuente de información para juzgarlo.

4. Aliste a sus amigos. Los amigos verdaderos se preocupan por su reputación y respetan su privacidad. Dígales sus límites de privacidad y pídales que los mantengan. Si alguien publica algo

en su propia cuenta de red social que podría presentar un problema para usted, pídale que lo elimine. De no poder ser, averigüe la política de la red social para eliminar ciertos tipos de imágenes o contenido si se solicita.

5. Con frecuencia más pequeño es más seguro. No acepte solicitudes o invitaciones de personas que no conozca sólo para aumentar su público. En su lugar, depure sus listas y no comparta con "seguidores" y conexiones que no conoce lo suficiente como para confiarles. Cuanto más grande sea su círculo interno, mayor será el riesgo de comprometer su privacidad y seguridad. Tenga presente que cualquiera con quien haya compartido puede volver a compartir o exponer lo que usted compartió. (Además, cierre las cuentas de redes sociales que ya no usa para que no corran el riesgo de ser comprometidas.)

6. Bloquee a los intrusos. Utilice todas las herramientas y prácticas de seguridad disponibles para que nadie pueda entrar a sus cuentas y dispositivos. Establezca contraseñas seguras (una cadena de más de ocho caracteres imposible de adivinar). Utilice una contraseña distinta en cada cuenta de red social (los administradores de contraseñas como LastPass o 1Password pueden ayudarle). Habilite la autenticación de dos factores (el inicio de sesión requiere la entrada de un código enviado a su dispositivo). Bloquee su teléfono de manera que sea necesario ingresar un código de acceso para abrirlo después de unos pocos minutos.

7. Mantenga su ubicación en secreto. No comparta su ubicación en tiempo real con sus conexiones o con el público en las redes sociales. Si bien podría ser relativamente seguro decir que hace poco pasó una semana en Hawaii, decirle a su público que está en el aeropuerto, en camino a unas vacaciones de dos semanas en Maui, podría ponerlo en peligro de robo, acecho, etc. Desactive el seguimiento GPS en aplicaciones para las que los datos de ubicación no son esenciales.

8. Resista la tentación. Esa noticia tentadora podría ser "clickbait" (o un "cíberanzuelo") (un fragmento de contenido diseñado para atraerle a hacer clic en un enlace que lo conduce a contenido molesto, inexacto o malicioso). No haga clic en enlaces desconocidos que podrían estar diseñados para infectar su computadora con un virus o software espía de robo de datos. Los cuestionarios, juegos, ofertas de cupones y otros incentivos tentadores a menudo son sólo formas de conseguir que usted divulgue información personal.

Conozca más

La página de StaySafeOnline.org Manage Your Privacy Settings (*https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/*) proporciona enlaces directos a las instrucciones para personalizar sus preferencias de privacidad en todos los dispositivos más populares, motores de búsqueda, plataformas sociales, etc.

El centro de seguridad de redes sociales de FightingIdentityCrimes.com (Social Media Security Center) (*https://www.fightingidentitycrimes.com/social-media-education-center/*) proporciona un resumen completo de la privacidad en las redes sociales (inquietudes, información recopilada, riesgos, etc.) junto con enlaces a instrucciones para ajustar su configuración de privacidad en ocho de las plataformas más populares.

La guía de Electronic Privacy Information Center (EPIC) sobre herramientas prácticas de privacidad (Online Guide to Practical Privacy Tools) (*https://www.epic.org/privacy/tools.html*) le informa sobre todo tipo de herramientas de privacidad en línea para mantener su seguridad, desde software antivirus y de firewall hasta administradores de contraseñas y software de red privada virtual (VPN).

La página de la Federal Trade Commission (FTC) Aplicaciones móviles: Qué son y cómo funcionan (https://www.consumidor.ftc.gov/articulos/s0018-aplicaciones-moviles-que-son-y-como-funcionan) explica lo que debe saber acerca de las aplicaciones, incluida la forma de administrar los problemas de privacidad y seguridad.

Los consejos de ZDNet para usuarios de iOS (https://www.zdnet.com/pictures/new-to-ios-11-change-these-privacy-and-security-settings-right-now/) y Android (https://www.zdnet.com/pictures/android-phone-tablet-privacy-security-settings/) le guían acerca de la configuración de privacidad según su dispositivo. (También puede consultar el sitio web de "Soporte" de su dispositivo, por ejemplo, https://support.apple.com/iphone para el iPhone. Si tiene dificultades, en un motor de búsqueda escriba "¿Cómo cambio la configuración de privacidad en un [nombre de su tipo de dispositivo]?" para obtener información específica sobre el dispositivo.)

La unidad de privacidad y protección del California Department of Justice ofrece una guía sobre cómo leer una política de privacidad ("How to Read a Privacy Policy") (https://www.oag.ca.gov/privacy/facts/online-privacy/privacy-policy). La guía ayuda al consumidor a entender la información que divulgan las empresas sobre cómo utilizan los datos recabados, y lo que sería razonable esperar al respecto. (Aunque la guía es de una agencia de California, la información es útil independientemente de dónde viva.)

Acerca de Consumer Action

www.consumer-action.org

A través de educación y defensa, Consumer Action promueve derechos y políticas sólidas a favor del consumidor que impulsan equidad y prosperidad financiera para los consumidores subrepresentados en todo el país.

Asesoramiento y asistencia al consumidor: Envíe quejas sobre asuntos del consumidor a: https://complaints.consumer-action.org/forms/english-form o al 415-777-9635. (Las quejas en español pueden presentarse a: https://complaints.consumer-action.org/forms/spanish-form/.)

Nuestra línea directa acepta llamadas en chino, inglés y español.

Publicaciones de Consumer Action

Noticias falsas: Cómo reconocer y detener la desinformación (https://www.consumer-action.org/spanish/articles/fake_news_sp) explica cómo los usuarios de internet pueden tener un impacto real en detener las noticias falsas. Aprenda a evaluar la exactitud de lo que lee u oye, evite las "noticias falsas" y absténgase de difundir historias engañosas.

¡Tenga cuidado! El video en línea y su privacidad (https://www.consumer-action.org/spanish/articles/watch_out_online_video_and_your_privacy_sp) explica los problemas de privacidad que presenta la transmisión de video y la tecnología de intercambio de video y lo que puede hacer para protegerse.

Póngale seguro: Proteja su privacidad en internet (https://www.consumer-action.org/spanish/articles/put_a_lock_on_it_protecting_your_online_privacy_sp) ofrece información sobre la seguridad y privacidad en línea en general.

Privacidad a su medida: Personalice la configuración de Facebook (https://www.consumer-action.org/spanish/articles/facebook_privacy_controls_sp) explica cómo los usuarios de Facebook pueden proteger su privacidad, ofrece consejos específicos para ajustar sus preferencias en el sitio web de Facebook y en la aplicación, e incluye enlaces a recursos para obtener más información.

Acerca de esta guía

Consumer Action creó esta guía en asociación con Facebook.