Una publicación de Consumer Action

Póngale seguro

Proteja su privacidad en Internet

Internet les permite a individuos y a familias socializar, hacer compras, realizar operaciones bancarias, trabajar, aprender y entretenerse prácticamente en cualquier lugar y en todo momento usando una computadora o dispositivo móvil. Acogerse a Internet recompensa con enormes beneficios. Y, en su mayor parte, Internet es seguro. Esto se debe a que la mayoría de las empresas le dan gran importancia a la protección de la privacidad y a la seguridad de las cuentas de sus usuarios, otorgándole prioridad al uso de tecnología avanzada para proteger a los consumidores en línea.

Pero la seguridad y privacidad en Internet es una responsabilidad compartida. Para lograr el nivel de privacidad deseado y el mayor grado de seguridad, los usuarios de computadoras y dispositivos móviles deben hacerse cargo de su propia protección ejerciendo sentido común y aprovechando las herramientas de seguridad disponibles, como las que ofrecen las grandes empresas de tecnología como Google y Microsoft. Para disfrutar de una vida digital sana y salva se debe adoptar un papel activo.

Asegure sus cuentas

La tecnología evoluciona de manera constante y nuevas formas de impedir que algún extraño acceda a sus cuentas y datos personales aparecen muy seguido. Desde la banca en línea hasta las redes sociales, los sitios web que procesan información personal delicada ofrecen herramientas para mantener sus datos a salvo de las miradas indiscretas. Para proteger los datos personales, una contraseña fuerte es importante; pero aún mejor es la autenticación con dos factores.

Contraseña: La contraseña es la primera línea de defensa y el método que más se utiliza para resguardar una cuenta. A continuación se detallan los pasos necesarios para proteger sus cuentas con una contraseña eficaz.

- La contraseña debe tener por lo menos ocho caracteres y una combinación de letras, números y símbolos al azar. Visite Google (*bit.ly/1MoNVfk*), Microsoft (*bit.ly/1JnLHbp*) o ConnectSafely (*bit.ly/1Kyu2i2*) para aprender más sobre la creación de contraseñas robustas. Una herramienta en línea como PasswordsGenerator.net también le puede ayudar a crear contraseñas.

- Mantenga sus contraseñas en secreto. En lugar de anotarlas, utilice una herramienta que las almacena a todas y así sólo necesitará recordar una. En PCMag.com (*bit.ly/10tbirr*) y Lifehacker (*bit.ly/1QXEc1b*) encontrará información sobre gestores de contraseñas.

- Utilice una contraseña distinta para cada cuenta. Cámbielas cuando sea necesario, por ejemplo, si alguien pudo haber encontrado su contraseña o si se hubiera producido alguna filtración de datos (la exposición o el robo de una gran cantidad de datos de usuarios).

- Elija preguntas de seguridad a las que solo usted pueda responder. Tenga cuidado de no elegir preguntas con respuestas que se puedan descubrir fácilmente, como "¿Cuál es el apellido de soltera de su madre?" o "¿Cómo se llama su mascota?" (Algunas cuentas usan preguntas de seguridad para verificar su identidad si se le olvida su contraseña o si intenta acceder a la cuenta desde una computadora o dispositivo desconocido).

- Cierre la sesión cuando termine y, si comparte algún dispositivo con otras personas, no permita que el navegador guarde la información de inicio de sesión. (Pulse el botón "Ahora no" ("Not now"), "Nunca para este sitio" ("Never for this site") u opción similar cuando se le pregunte si le permite al navegador guardar su contraseña; o, en el menu de "Configuración" o "Preferencias" ("Settings" o "Preferences") del navegador marque/desmarque las casillas correspondientes en las pestañas de "Seguridad", "Contraseñas", "Sincronización" o "Autocompletado".)

- Requiera una contraseña de inicio de sesión para poner en marcha la computadora o para "despertarla". Así agregará otra capa de protección contra cualquiera que intente acceder a sus cuentas en su computadora. Aprenda cómo hacerlo en una Apple (Mac) (*apple.co/1V9p5Yt*) y en un PC (*abt.cm/1Wiy72s*). (Requiera también una contraseña, PIN (número de identificación personal) o huella dactilar para sus dispositivos móviles).

Autenticación de dos factores (2FA): Se refiere a protección mucho más fuerte que una contraseña sola. Requiere dos tipos de información para acceder a la cuenta (por ejemplo, una contraseña más la confirmación en pantalla de algún retrato o gráfico que usted haya elegido; o una contraseña más el escaneo de una huella digital; o una contraseña más un código de acceso enviado vía mensaje de

texto o correo electrónico). Este proceso puede compararse a tener que deslizar su tarjeta de débito además de ingresar un PIN en el supermercado. Para obtener más información sobre la autenticación de dos factores consulte en Stop.Think.Connect (*bit.ly/1DQlzpY*).

Active la autenticación de dos factores siempre que esté disponible. Aunque no todos los sitios la ofrecen, muchos sí, entre otros, Google, Apple, Facebook, Twitter y PayPal. Esta lista muestra muchos sitios que ofrecen, y que no ofrecen, 2FA: *bit.ly/1JpGz6w*. (Si los sitios que utiliza no ofrecen la autenticación de dos factores, puede solicitar que comiencen a ofrecerla.) Cada sitio tiene sus propias instrucciones para habilitar 2FA. Primero busque en "Configuración" o "Settings", y si no lo encuentra, póngase en contacto con el equipo de soporte del sitio web.

Operaciones seguras en línea y móviles

Las compras y la banca en línea pueden ahorrarle tiempo y dinero. Estas son dos buenas razones para gastar y administrar su dinero de manera digital. Además todas sus cuentas estarán seguras si toma algunas precauciones simples y eficaces, tal como lo haría con su billetera. Tenga por seguro que existen varias herramientas de seguridad fuertes.

Cifrado: Esta es una tecnología que codifica (encripta) la información electrónica que se envía por el ciberespacio, por lo que es mucho más difícil para los piratas informáticos rastrear sus actividades y robarle los datos.

Para determinar si un sitio web utiliza cifrado para proteger su información al ser enviada entre usted y el sitio web, busque la "s", que significa "seguro", en la dirección del sitio (dirección URL) (busque https:// en lugar de solo http://). A veces, cuando visita un sitio seguro verá un candado, o la barra de direcciones se pondrá verde. Verifique que haya una o más de estas garantías antes de hacer una compra, acceder a sus cuentas financieras o realizar cualquier tipo de operación.

Tenga en cuenta que algunos mensajes estándar de correo electrónico y texto no están cifrados, así que no envíe nunca sus números de cuenta, o de Seguro Social o alguna otra información delicada de esta manera.

Si usted cuenta con una conexión wifi en casa, entonces también tiene un "enrutador" o "router" inalámbrico. Para evitar que alguien que esté cerca obtenga acceso a la información que envía por Internet a través de su red inalámbrica, debe asegurarse de que la función de cifrado del enrutador esté activada (a menudo viene apagada). Asimismo, debe crear una contraseña sólida para su red inalámbrica (al menos 14 caracteres al azar). De esta manera el enrutador impedirá que intrusos dentro del alcance de la señal accedan a su conexión wifi. Para obtener detalles sobre cómo proteger su red inalámbrica visite OnGuardOnline.gov (*1.usa.gov/1G2Eiya*).

Porque no siempre se puede estar seguro de que una red externa esté cifrada, lo mejor es utilizar la red de su proveedor de servicio móvil en lugar de una red wifi pública para hacer compras u operaciones bancarias cuando está lejos de casa. Si utiliza una computadora o dispositivo compartidos, debe cerrar siempre la sesión de banco o de compras al terminar para que nadie pueda acceder a su cuenta después que se retire. Para obtener más información acerca del uso seguro de wifi público, consulte con la Federal Trade Comisión (FTC) (*1.usa.gov/1L62Nlr*).

Cortafuegos: La mayoría de sistemas operativos vienen con un cortafuegos ("firewall") incorporado; una barrera entre el mundo exterior y su equipo. Los cortafuegos incorporados no siempre vienen activados. Compruebe la configuración de seguridad de la computadora (a menudo se encuentra bajo "Preferencias" o "Preferences") para asegurarse de que el cortafuegos esté activo. Si no encuentra los controles, haga una búsqueda en línea de la palabra "firewall" junto con el nombre de su sistema operativo para obtener instrucciones.

Seguridad de los dispositivos móviles

Con un "smartphone" (teléfono inteligente) o una computadora "tablet" (tableta) puede llevarse las capacidades de Internet a todas partes. Su portabilidad y la tecnología que los activa ofrecen grandes ventajas para los usuarios, pero los dispositivos móviles presentan desafíos únicos de privacidad y seguridad. Esto no significa que no los debe usar como prefiera, sino que si toma algunas medidas adicionales o diferentes, puede proteger su privacidad y sus datos.

Cómo asegurar sus dispositivos: Debido a su portabilidad, se corre un riesgo mayor de perder o de que le roben un dispositivo móvil que, por ejemplo, de que pierda o le roben una computadora de escritorio. Además de mantenerse atento y cuidar su dispositivo, puede también aprovechar las herramientas tecnológicas diseñadas específicamente para mantener al dispositivo móvil y a sus datos seguros.

Para empezar, asegure su dispositivo con una contraseña o PIN (o huella digital, dependiendo de la versión). Configúrelo para que quede bloqueado después de varios minutos de inactividad. Asimismo, inscríbase en un programa de localización/bloqueo/borrado remoto como Find My iPhone (Apple) o Android Device Manager. Esto le permitirá encontrar su dispositivo si lo extravía, o bloquearlo o borrarle los datos a distancia si lo pierde o se lo roban.

No se olvide de borrar los datos de su dispositivo antes de venderlo, donarlo o desecharlo para que nadie pueda acceder a su información personal. CTIA-The Wireless Association ofrece consejos y enlaces a instrucciones para borrar la información de dispositivos móviles, según el tipo que tenga (*bit.ly/1jeEDZN*).

Para obtener más información sobre cómo proteger su teléfono cuando navega por Internet, visite AARP (*bit.ly/1FfksoF*).

Aplicaciones móviles: Las aplicaciones móviles o "apps" son programas de "software" diseñados específicamente para dispositivos móviles. Gran parte de la funcionalidad de un smartphone o una tablet proviene de las aplicaciones que se descargan. Estas le permiten vigilar su condición física, compartir una "selfie" (autofoto), notificarle a sus amigos dónde va a cenar, supervisar sus inversiones, jugar Words With Friends y mucho, mucho más. Debe asegurarse que aplicaciones tan potentes funcionen a su favor y no en su contra.

- Investigue sus aplicaciones. Sólo descargue las que provienen de fuentes de confianza. Lea los

comentarios de otros usuarios y esté seguro de la legitimidad del desarrollador de la aplicación antes de descargarla.

◆ Configure sus aplicaciones según la privacidad que desee. Muchas dependen de poder recuperar y compartir información personal de los usuarios, tal como los contactos, calendarios y hasta la ubicación. Para controlar lo que una aplicación recoge y comparte, compruebe la configuración de la aplicación misma (a diferencia de la configuración del dispositivo). Si la aplicación quiere recoger más datos personales de los que usted desea proporcionar, no la descargue. Revise la política de privacidad de la aplicación, si la tiene. Si no, considere elegir una diferente.

◆ Evite aplicaciones que anuncian su ubicación a otras personas, o desactive esa función si tiene la opción. Si comparte su ubicación física con desconocidos podría correr el riesgo de que entren a robar a su casa o de poner en peligro su seguridad y privacidad. (Algunas aplicaciones, como las que proporcionan mapas y direcciones, utilizan su ubicación para ofrecer un servicio pero no la divulgan).

◆ Instale las actualizaciones de software cuando estén disponibles para asegurarse de que siempre tenga la versión de la aplicación más reciente.

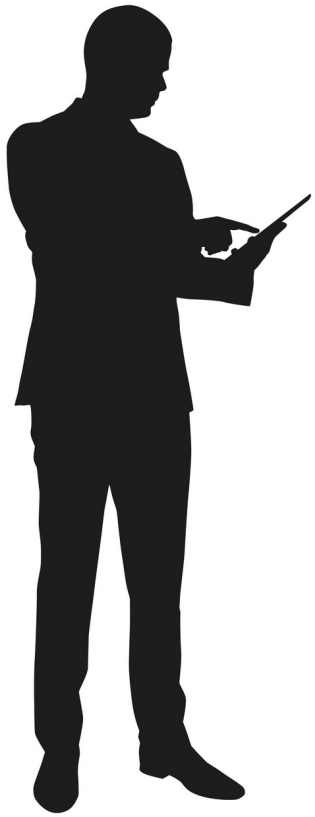
◆ Lea las notificaciones de cambios en las condiciones de uso o de cambios en la política de privacidad para que pueda desinstalar la aplicación si es que van a recoger o compartir más datos de los que a usted le parezca. Dependiendo de la aplicación y la importancia de los cambios, usted podría recibir una notificación directa (por lo general, por correo electrónico o dentro de la misma aplicación, a lo que se le llama "push notification"). En otros casos, de la única forma que se enterará de un cambio será volviendo a revisar las condiciones de uso o la política de privacidad en la aplicación o en su página web.

Seguridad en las redes sociales

Para muchos, los medios sociales forman parte de la vida cotidiana. El intercambio de información puede ser algo positivo si comparte sólo lo que usted quiere y con el público que usted elige. Para evitar las posibles consecuencias de compartir demasiado, piénselo dos veces antes de publicar, tuitear o de cualquier otra forma revelar información personal. También utilice las herramientas disponibles para controlar lo que ven los demás.

Mantenga su privacidad: No todos los que utilizan los medios sociales actúan en beneficio de usted. Es importante tomar decisiones inteligentes sobre lo que comparte y con quién para prevenir que sus datos personales sean usados de alguna manera que no fue su intención.

Comience por modificar la configuración de privacidad de la red social al nivel que considere cómodo; desde no compartir con nadie hasta compartir sólo con su círculo de amigos, o compartir con el público en general. Primero, inicie la sesión de su cuenta. Luego, busque la pestaña o el encabezado "Privacy" ("Privacidad"), "Privacy Controls" ("Controles de privacidad"), "Privacy Settings" ("Configuración de privacidad"), "Account Settings" ("Configuración de cuenta"), o "Preferences" ("Preferencias"). Si no lo encuentra, utilice la función "Help" ("Ayuda") del sitio, o envíe un mensaje por correo electrónico al equipo de soporte del sitio web.



No comparta información personal; por ejemplo, su nombre completo, dirección, número de teléfono, nombre de soltera de su madre o su año de nacimiento, ya que podrían utilizarse para fines de identificación (y fraude de identidad). Y no comparta su ubicación actual ni sus planes de viaje, ya que podrían ponerlo en peligro a usted o a su propiedad.

Es buena política no aceptar invitaciones o peticiones de "amistad" de personas que no conoce.

Obtenga más información sobre la privacidad en las redes sociales en la publicación **Privacy and Control for Social Media Users** de Consumer Action (*bit.ly/1xPC8PO*).

Protección de su reputación en Internet: Todo lo que comparte: fotos, videos, actividades y opiniones, revela información acerca de usted. La buena administración y protección de su reputación digital puede ayudarlo a evitar una situación vergonzosa y a evitar las posibles consecuencias de dar un mal paso en los medios sociales. A continuación se presentan algunas recomendaciones para protegerse de los efectos colaterales de las redes sociales.

◆ Tenga en cuenta lo que un empleador, reclutador, funcionario de admisiones de la universidad, prestamista, propietario, cliente, agencia gubernamental, asegurador o alguna otra persona que toma decisiones, podría pensar acerca de lo que usted está compartiendo. Recuerde que mucha gente que no lo conoce personalmente puede recurrir a las redes sociales para saber algo sobre usted.

◆ Tenga presente que un "amigo" puede volver a publicar o tuitear, o de alguna manera revelar lo que usted pensó haber compartido sólo con su audiencia seleccionada. Y si publica algo en el perfil público de otra persona, no tendrá control sobre quién lo ve.

◆ Dé marcha atrás si fuera necesario. Algunas redes sociales le permiten borrar publicaciones anteriores, retirar fotos, cambiar quién puede ver sus publicaciones, etc. Esto permite que lo que compartió en el pasado ya no puedan verlo nuevas personas. (Por supuesto, no puede hacer nada acerca de quienes ya vieron lo que compartió.)

◆ Busque su nombre en "Google" para ver lo que aparece. Si encuentra fotos, videos o mensajes poco favorecedores que lo incluyan a usted, pídale a quienes los publicaron que los retiren.

◆ Asegúrese de que sus cuentas estén seguras para que no puedan ser pirateadas y usadas en su contra.

Para obtener más información sobre cómo administrar su reputación en línea, visite Google Safety Center (*bit.ly/1FunANi*).

Internet apto para familias

Internet ofrece una amplia variedad de contenido de alta calidad no sólo para adultos, sino también para niños de toda edad. Existen ciertas

protecciones, y también puede tomar algunas precauciones, para asegurarse que su familia pueda disfrutar de lo mejor que ofrece Internet y a la vez evitar cualquier cosa desagradable.

Cómo bloquear contenido inapropiado: Hay mucho contenido excelente en Internet que se ajusta a la edad del niño. También hay algún contenido inapropiado. Muchas empresas que facilitan la transmisión del contenido, desde los proveedores de servicio de banda ancha hasta las empresas de medios de comunicación social, permiten que los padres limiten desde la cantidad de tiempo que pasan los hijos en línea hasta los sitios que pueden visitar, los videos que pueden ver y los foros y salas de chat que pueden visitar.

Para obtener más información sobre los controles parentales visite Family Online Safety Institute (*bit.ly/1L63Emf*) y Google Safety Center (*bit.ly/1G2F7XP*).

Control de comunicaciones: Al igual que no todo el contenido en Internet es apropiado para sus hijos, no toda persona en las redes sociales tiene como prioridad el bienestar de ellos. Como padre, usted es el guardián principal de cualquier relación que sus hijos formen en el ciberespacio.

Hable con sus hijos acerca de cómo mantenerse seguros y ser responsables en Internet. Establezca reglas claras acerca de qué sitios pueden visitar y con quién pueden comunicarse. Hágase "amigo" de sus hijos en las redes sociales para poder ver lo que comparten, y también para ver lo que otros comparten con ellos. Acláreles que no deben ir solos a reunirse con alguien que "conocieron" en Internet. Prometa no castigarlos o quitarles el acceso a Internet si le cuentan sobre alguna comunicación inapropiada. Consulte los consejos de OnGuardOnline.gov (*http://bit.ly/2eewlAl*).

Informe a las autoridades apropiadas, entre otros, a los funcionarios escolares, a la policía local o a la CyberTipline (*bit.ly/1NMiQDY* or 800-843-5678) sobre los incidentes de hostigamiento y comportamiento depredador.

Cómo evitar la publicidad no deseada: Muchas compañías en Internet recogen información personal de los usuarios. Algunas empresas utilizan los datos para personalizar y mejorar la experiencia del usuario, tal como para sugerir películas y libros que le podrían gustar, mientras que otras los utilizan para personalizar sus mensajes publicitarios y atraer a personas de intereses similares. Y otros, conocidos como "corredores de datos" ("data brokers"), recopilan datos sobre consumidores para venderlos a empresas de publicidad de terceros y a otras que utilizan los datos con el objetivo de enfocar sus anuncios y ofertas. Las empresas de renombre son transparentes con respecto a la manera en que utilizan su información y le ofrecen opciones sobre lo que desea compartir y lo que prefiere mantener en privado.

Usted puede tomar ciertas medidas para enterarse cómo se utilizará su información y cómo obtener un mayor control sobre sus datos personales.

◆ Lea la "Política de privacidad" ("Privacy Policy") o "Política de uso de datos" ("Data Use Policy") de la empresa para saber cómo y cuándo el sitio recopila, utiliza y comparte su información personal. Si usted no está satisfecho con sus prácticas, busque un sitio diferente que le permita mayor control.

◆ Si tiene niños, dígales que no deben revelar información privada en los sitios web que visitan. La ley Children's Online Privacy Protection Act (COPPA) (para la protección de la privacidad infantil en Internet) requiere que los sitios web obtengan el consentimiento de los padres para recoger o utilizar cualquier información personal de los niños menores de 13 años. Informe a la Federal Trade Commision (FTC) (*www.ftccomplaintassistant.gov* o 877-FTC-HELP) sobre las infracciones de esta ley.

◆ Cuando le parezca prudente, active la función "Navegación privada" ("Private Browsing") en su navegador web, lo que le permitirá navegar sin que el navegador guarde información sobre los sitios y las páginas que ha visitado. También use un bloqueador de "ventanas emergentes" (ventanas "pop up") para evitar la apertura de ventanas de publicidad no deseada. (Tenga en cuenta que esto puede dificultar algunas funciones deseables, tales como que un sitio de venta al por menor pueda recordar lo que está en su "carrito" o "bolsa.")

◆ Considere si existe o no un buen motivo para proporcionar más que la mínima información requerida (a menudo indicada con un asterisco) para inscribirse o usar algún servicio. Comparta la menor cantidad posible de información personal.

◆ Comprenda que en cualquier momento que entrega su información personal a una fuente no investigada, incluso en respuesta a un cuestionario aparentemente inocente o para participar en algún juego, pueden utilizar su información para fines no deseados.

La tecnología constantemente nos da nuevas formas para comunicarnos, trabajar, aprender, crear, compartir y divertirnos. No se lo pierda, pero tenga cuidado. Únase al esfuerzo de equipo para mantenerlos a usted y su familia sanos y salvos en Internet. ■

Acerca de Consumer Action

www.consumer-action.org

Por medio de materiales educativos multilingües, extensión comunitaria y defensa enfocada en asuntos del consumidor, Consumer Action faculta a consumidores que carecen de representación en todo el país para que hagan valer sus derechos de consumidor y prosperen.

Consejo y asistencia para el consumidor: Presente quejas de consumidor a nuestra línea directa de asesoramiento y remisiones: *http://www.consumer-action.org/hotline/complaint_form_es* o 415-777-9635.

Se hablan chino, inglés y español

Esta publicación fue creada en colaboración con Google.