



## Cómo obtener resultados

Internet ha cambiado la forma en que trabajamos, sociabilizamos y hacemos compras; ahora podemos hacer todo esto sin salir de casa. Pero esto no significa que Internet siempre sea seguro o que siempre sea gratuito. Esta hoja informativa explica sus opciones para obtener servicios de Internet y correo electrónico. También expone los riesgos de usarlo y le ofrece consejos para protegerse y para proteger a su familia, a su información personal, y a los datos de su computadora.

### Servicio de Internet y correo electrónico

- El servicio de Internet puede recibirse por acceso telefónico (*dial-up*) a través de la línea residencial, por cable a través de su compañía de televisión por cable, por DSL a través de las líneas telefónicas, por satélite con una antena parabólica, o mediante servicio inalámbrico (wifi). La transmisión de banda ancha por fibra óptica no está disponible en muchos lugares todavía.
- El servicio pagado más lento es por acceso telefónico (*dial-up*). Los tipos de servicio de Internet más rápidos con frecuencia reciben los nombres de *high-speed* (alta velocidad) o banda ancha.
- El servicio por acceso telefónico puede costar desde \$10 por mes. DSL y cable por lo general entre \$35 y \$65 por mes, dependiendo del proveedor y la velocidad. Los servicios de satélite y fibra óptica, si están disponibles, son más caros. Existen promociones para usuarios nuevos y para clientes que compran el servicio de Internet empaquetado con el servicio de teléfono y/o televisión.
- El servicio de Internet inalámbrico es gratuito en ciertas partes (*hotspots*). En otros lugares (ciertos hoteles, por ejemplo) cobran un recargo. Es posible obtener wifi residencial junto con el modem de cable o el servicio DSL. O, posiblemente pueda comprarlo aparte para usar en todas partes.
- En las zonas urbanas existen más opciones para recibir Internet que en los pueblos pequeños o las zonas rurales. En [www.fcc.gov/cgb/consumerfacts/highspeedinternet.html](http://www.fcc.gov/cgb/consumerfacts/highspeedinternet.html) podrá obtener más información.
- El servicio de correo electrónico es gratuito, ya sea a través de un proveedor de servicio de Internet (ISP, por sus siglas en inglés) o a través de un servicio basado en la Web (Gmail de Google, y Hotmail de Microsoft, por ejemplo).

### Seguridad en Internet

- Ajuste la configuración de su cuenta en redes sociales para mayor privacidad, de forma que sólo comparta información con quienes usted desee y no con el público en general.
- Vigile la actividad de sus hijos por Internet. Deben entender claramente cuál es la información que pueden compartir y cuál no, y que nunca deben encontrarse solos con un “amigo” que hayan conocido en línea. Obtenga más información sobre la seguridad para chicos en línea en <http://kids.getnetwise.org>.
- Reporte las comunicaciones inapropiadas, indeseadas u hostigadoras a las autoridades, incluyendo, por ejemplo, a la policía, a su proveedor de Internet, a autoridades escolares y al FBI ([www.ic3.gov](http://www.ic3.gov)).

### Proteja la privacidad de su información personal

- Proteja la red inalámbrica en su casa con una contraseña segura (como mínimo de 8 caracteres que incluyan letras en mayúsculas y minúsculas, números y símbolos) y habilite las opciones de codificación incorporadas.
- Use el cortafuegos (*firewall*) incorporado en las computadoras nuevas. El contrafuegos actúa como una barrera virtual entre su computadora y Internet por la cual debe pasar toda la información de ingreso y salida.
- No envíe datos confidenciales por correo electrónico o mensaje instantáneo (IM) u otro aparato habilitado para la Web. Tenga cuidado cuando use wifi público.
- Si usa una computadora pública o compartida, nunca almacene su información de ingreso y siempre salga del sistema cuando termine de usarla. De estar disponibles en el navegador, habilite las funciones “en privado” (*in private*) ó “borrar historial de navegación” (*delete browsing history*) para ocultar los sitios que visitó.
- Reduzca los avisos publicitarios en línea revelando la menor información posible sobre sí mismo en los sitios que visita. No haga clic en los avisos que aparecen en ventanas emergentes (*pop-up windows*).
- Lea la política de privacidad de los sitios que visita para saber cómo usarán su información. Busque los logotipos

como TRUSTe o BBBOnline en el sitio que visita.

- Compre únicamente en comercios en línea de confianza. No permita que los sitios conserven su información sobre tarjetas de crédito para compras futuras. Compre con tarjeta de crédito, no de débito.
- Antes de comprar en un sitio desconocido, investigue su historial de quejas. Luego fíjese si en la barra de direcciones aparece la codificación SSL (debe ser <https://> y no <http://>) y si aparece un candado cerrado o una llave intacta en el marco de la ventana. Haga doble clic en el candado o la llave; si los nombres que figuran en la dirección de Internet no coinciden con el certificado de seguridad, el sitio puede ser falso.
- La solicitud de su número de Seguro Social, nombre de usuario, contraseña, o algún otro dato sensitivo indica que un correo electrónico puede ser *phishing* o sea que busca su información personal para usarla de forma fraudulenta. Si usted duda de la autenticidad de algún correo electrónico, no lo conteste. Envíelo a su proveedor de Internet (ISP) y presente una queja ante la Federal Trade Commission (FTC). Obtenga más información o presente una queja en [www.OnGuardOnline.gov](http://www.OnGuardOnline.gov).
- Si ya respondió a un correo electrónico *phishing*, cambie inmediatamente las contraseñas de sus cuentas y avise a las instituciones donde tiene sus cuentas. Obtenga sus informes de crédito (en [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com)) y asegúrese que no contengan alguna señal de que ha sido víctima de robo de identidad. Usted tiene derecho de recibir tres copias del informe por año.

## Seguridad de los datos en su computadora

- Los virus, gusanos, Trojans, y programas espías pueden utilizarse para robarle, dañarle, o borrarle los datos de su computadora e información personal. Siempre use programas antivirus y antiespías, y actualícelos con regularidad para protegerse contra amenazas nuevas. (Programas también actualizaciones automáticas, de ser posible.)
- Use el filtro contra spam de su servicio de correo electrónico. Borre (sin abrir) el correo electrónico sospechoso que atraviese el filtro.
- Tenga cuidado al abrir los anexos o al descargar contenido gratuito de la Web; los archivos podrían contener un virus, un programa espía, o algún otro código malicioso.
- Los sitios maliciosos están diseñados para hacerse pasar por sitios legítimos, pero intentan robar su información o hacerle daño a su computadora y datos. Nunca haga clic en conexiones o visite páginas que le envíe alguien que no conoce y en quien no confía.
- No envíe cartas de cadena. Investigue todos los correos electrónicos dudosos en sitios antifraudes ([www.snopes.com](http://www.snopes.com) o [www.quatloos.com](http://www.quatloos.com)) antes de enviarlos.
- Haga copias de seguridad de sus archivos con frecuencia para no perder datos. (Obtenga más información en [StaySafe.org](http://StaySafe.org).)
- Use programas especiales para limpiar discos o una utilidad en su sistema operativo para borrar totalmente sus archivos personales antes de deshacerse de su computadora.

## Manejo de disputas

- Evite una disputa conociendo los términos de su contrato de servicio.
- Los precios por banda ancha se basan en parte en las velocidades de descarga. Si usted no está satisfecho, pruebe su conexión en <http://www.broadband.gov>. (Tenga presente que las velocidades reales dependen de muchos factores, entre otros, el procesador de su computadora y el tránsito en la Web.)
- Si le dan la opción, opte por no aceptar un acuerdo de arbitraje; no debe renunciar a su derecho de demandar judicialmente al proveedor de servicio o de unirse a una demanda colectiva.
- Trate de resolver el problema directamente con su proveedor de servicio dentro de los 30 días de haber recibido su cuenta. Anote todas sus comunicaciones. Pague la parte de la factura que no disputa antes de la fecha de vencimiento. Si no está satisfecho con la resolución, puede comunicarse con su Better Business Bureau local ([www.bbb.org](http://www.bbb.org)) y con las agencias de protección del consumidor locales y estatales (<http://consumeraction.gov/state.shtml>). La Federal Communications Commission (FCC) no regula a Internet ni a los proveedores de Internet.

*Consumer Action creó el proyecto Empower U con una subvención de California Consumer Protection Foundation. A través de educación y defensa del consumidor en todo el país, Consumer Action habilita a consumidores de bajos y moderados ingresos y a los que no dominan el inglés a prosperar financieramente. Obtenga más información en [www.consumer-action.org](http://www.consumer-action.org).  
© Consumer Action 2010.*