nes bancarias o de pagos. Desconecte y cierre la aplicación o la ventana del navegador cuando haya terminado la sesión o cuando se aleje de la pantalla. Si está usando una computadora compartida o pública, borre su historial del navegador haciendo clic en el menú "Tools" (útiles) de la mayoría de los navegadores y seleccione "Delete Browsing History" (borrar historial del navegador) o "Clear Private Data" (borrar datos privados).

No envíe por correo electrónico datos delicados. No envíe información personal como números de tarjetas de crédito, claves, su fecha de nacimiento o número de Seguro Social por correo electrónico. Lo más recomendable es conectarse directamente a su cuenta en el sitio web de la compañía; así, con la mayoría de las compañías que tratan con información delicada, podrá enviar correo electrónico al departamento de servicio al cliente y recibir respuestas de forma segura.

Revise la seguridad del sitio web. Verifique que "https://" (y no solo http://) figura en la barra de direcciones del navegador. Todos los sitios comerciales y financieros legítimos usan esta codificación SSL (Secure Sockets Layer) para que la banca o los pagos en línea sean seguros.

Asegure con llave su red inalámbrica. Dejándola abierta permite que cualquiera dentro del alcance de su señal wifi pueda conectarse y posiblemente capturar los datos que envía y recibe en un sitio sin codificación. Para asegurar su red inalámbrica proteja su enrutador con una clave.

Evite las compras o operaciones bancarias en "hotspots" públicos. Si tiene que usar wifi público verifique que está en un sitio seguro (https://), inhabilite su capacidad para compartir expedientes y use una red privada virtual o VPN (siglas de virtual private network) tal como Private WiFi (www.privatewifi.com) para proteger su identidad en línea.

Use una billetera digital. Su banco o procesador de pago podría ofrecer un servicio de billetera digital que le permite hacer compras en línea sin tener que ingresar sus números de tarjeta de crédito u otra información de pago. La compra se le carga a su cuenta de billetera digital segura, la cual se ha registrado previamente y permanece fuera de su red.

Haga tratos comerciales sólo con personas y compañías en las que confía. Verifique la reputación (historial de quejas e índice de satisfacción de clientes) de todo comercio que no conozca antes de ingresar información personal o acerca de pagos. Se puede obtener mucha información con una simple búsqueda en línea del nombre de la compañía.

Investigue sus "apps". No descargue alguna *app* desconocida hasta haber leído las críticas de usuarios y haberse asegurardo que el diseñador es legítimo. Lea la política sobre privacidad del diseñador, que podrá encontrar en "Settings" o en "About This App". TRUSte certifica las prácticas de privacidad de los diseñadores de *apps* móviles y también de los propietarios del sitio web; por lo tanto, busque el logo de TRUSTe. De ser necesario, reinicie la configuración de privacidad de la *app* hasta un nivel que le resulte seguro. Tenga presente que para ser efectivas algunas aplicaciones deben poder localizarlo.

Esté atento a las comunicaciones fraudulentas. Si duda de la autenticidad de un mensaje de correo electrónico o de texto, o de una llamada telefónica, no responda. Comuníquese con la compañía directamente para aclarar cualquier duda. Los comercios legítimos nunca se comunican con usted para solicitar su número de Seguro Social, nombre de usuario, clave ni ninguna otra información delicada. Si cae en un fraude *phishing* por correo electrónico y reconoce su error, cambie inmediatamente la clave de su cuenta y avísele a la institución donde estableció cuenta. Aproveche los filtros contra *spam* y *phishing* que ofrece su servicio de correo electrónico. Siempre ingrese la dirección web del sitio que desea visitar en lugar de hacer clic en un mensaje de correo electrónico que lo podría dirigir a un sitio falso.

Protéjase contra programas maliciosos ("malware"). Use programas antivirus y antiespías y asegúrese de actualizarlos regularmente para evitar programas maliciosos que pueden robarle información cuando está en línea. Active el cortafuegos o "firewall" incluido con su computadora para crear una barrera virtual entre usted y Internet.

Borre los viejos mensajes de texto referentes a operaciones bancarias y otras operaciones. Mensajes de texto viejos que contienen información sobre el saldo de sus cuentas u otra información privada deben borrarse de su teléfono y de dispositivos sincronizados al teléfono.

Proteja su dispositivo. Como los teléfonos inteligentes y PDA pueden almacenar una gran cantidad de información delicada y pueden perderse o ser robados fácilmente, es lógico hacer un esfuerzo por protegerlos. Use una clave para asegurar el teléfono cuando no esté en uso. Y fije el teléfono para que se active el seguro después de una cierta cantidad de minutos sin ser utilizado.

Borre el disco duro. Antes de vender, donar o deshacerse de una computadora o dispositivo móvil debe borrarle el disco duro. Esto implica más que sólo borrar los expedientes. En el menú "Help" o en el sitio web del fabricante puede buscar instrucciones, o comuníquese con su compañía de servicio inalámbrico para asistencia con un teléfono o PDA. ReCellular (www.recellular.com/recycling/data_eraser/default.asp) ofrece instrucciones para borrar muchos modelos de teléfono. Si le proporcionaron el teléfono o la computadora en su trabajo, comuníquese con la persona en el trabajo encargada de asuntos técnicos. Tenga presente que su empleador tiene el derecho de obtener acceso a la información almacenada en dispositivos que son propiedad de la empresa.

Asistencia e información

Federal Trade Commission www.ftc.gov

FTC educa al público sobre cómo protegerse en el mercado y acepta quejas sobre comercios que infringen los derechos y la privacidad del consumidor.

Consumer Action

www.consumer-action.org
Línea directa de consejo y remisiones:
hotline@consumer-action.org o 415-777-9635
Se hablan chino, inglés y español

Consumer Action creó la serie Sus dólares digitales con fondos proporcionados por Visa Inc.

VISA consumer action
Education and advocacy since 1971

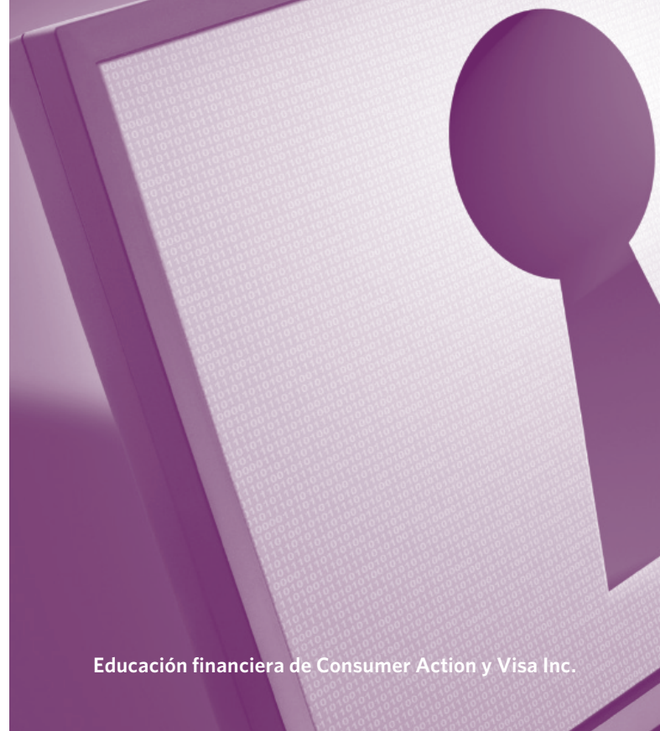
Visite el programa de educación financiera de Visa, Su Dinero: Destrezas Prácticas para toda la Vida en ***www.vidaydinero.com***

Encuentre consejos y conocimientos prácticos en inglés y español para proteger la información de sus cuentas, evitar los fraudes de tarjetas de pago y resolver el uso no autorizado de tarjetas en: ***www.visasecuritysense.com***

Sus dólares digitales

Seguridad y privacidad en las operaciones en línea y móviles

Proteja su identidad e información en operaciones bancarias y pagos digitales



Educación financiera de Consumer Action y Visa Inc.

A medida que más tareas diarias se hacen por computadora o dispositivo móvil, incluso compras, operaciones bancarias y actividades del trabajo y sociales, las oportunidades de revelar información personal aumentan.

Aunque las operaciones digitales están protegidas por muchas medidas que refuerzan su seguridad, el consumidor aun así puede correr riesgos de seguridad en línea y al usar dispositivos móviles. Una conexión wifi abierta, un teléfono inteligente perdido o una clave revelada inadvertidamente representan algunas formas en que su información podría revelarse sin su permiso. Por fortuna, hay muchos consejos y útiles para ayudarlo a hacer operaciones con seguridad en línea y con su móvil desde el lugar en que se encuentre.

¿Por qué es importante la seguridad en línea?

Aunque Internet y la tecnología móvil han mejorado de muchas formas nuestras vidas, también han innovado otras maneras en que la información personal del consumidor puede ser robada, revelada accidentalmente o usada de forma incorrecta. Por ejemplo, un ladrón de identidad puede robarle su información personal desde cualquier parte del mundo atrayéndolo a un sitio web fraudulento donde con engaños lo obligan a revelar su clave. Un teléfono inteligente robado o perdido lleno de claves almacenadas e información sobre cuentas puede significar un peligro mayor que una billetera perdida. Y si un sitio web que ha visitado vende su información a terceros, podría recibir frecuentes (y fastidiosos) mensajes publicitarios por correo electrónico ("spam"), o hasta cargos no autorizados.

Lo bueno es que si tiene cuidado y se mantiene informado puede evitar estos y otros posibles problemas.

Riesgos de operaciones en línea y móviles

Todos corremos el riesgo de que se intercepte alguna correspondencia enviada por correo o que nos escuchen una conversación confidencial. Pero si realiza operaciones bancarias o pagos en línea o con su dispositivo móvil, hay otras formas en que se puede infringir su privacidad.

Si pierde o le roban su computadora o teléfono, quien termine con éstos podría obtener acceso a sus datos personales, números de cuenta e información sobre pagos.

Alguien podría interceptar la información que envía y recibe sobre una red inalámbrica.

Un estafador podría conseguir que usted ingrese su información privada en un sitio web falso o que responda a una solicitud engañosa por correo electrónico ("phishing").

Una brecha en la seguridad de sus datos (el robo o la divulgación no intencional de información almacenada en la base de datos de una institución) podría resultar en que su información y la de otros usuarios termine en manos de un ladrón.

Algún conocido podría obtener acceso a sus cuentas adivinando o descubriendo su clave. O usted mismo podría estar almacenando nombres de usuario y claves en una computadora compartida o un dispositivo móvil sin protección, dándoles la llave a intrusos.

Su computadora o dispositivo móvil podría estar infectado con programas espías o problemáticos capaces de robarle sus datos.

Un comercio que reúne información suya puede venderla o entregarla a una o más personas para fines publicitarios u otros propósitos. Hasta han habido casos en que comercios han compartido información sobre tarjetas de pago, lo que ha resultado en cargos no autorizados.

Qué debe tener presente acerca de proveedores y productos

Una de las mejores formas de proteger sus datos personales es de tratar únicamente con instituciones financieras, comerciantes, diseñadores de "apps" y otros que se esfuerzan por proteger la seguridad y privacidad de sus clientes y visitantes a sitios web. Cuando esté considerando alguna compañía, producto o servicio, procure:

Legitimidad: Un sitio web bien elaborado no indica que una empresa sea legítima o de confianza. Si usted no está familiarizado con la reputación de la empresa, verifique su autenticidad, índice de satisfacción e historial de quejas haciendo una búsqueda en línea. Verifique cualquier información y afirmación (por ejemplo, llame al número indicado).

Codificación: Un candado cerrado o una llave entera (no quebrada) en el marco del navegador y el "http" seguido de una "s" (https://") en la dirección del sitio web indican que el sitio es seguro y que está codificado. (Esto quiere decir que la información se envía en un formato que sólo el destinatario indicado puede leer.) Los logos de empresas como VeriSign y McAfee significan que el sitio web utiliza codificación u otra tecnología de seguridad para proteger sus datos. Haga clic en los logos para obtener mayor información sobre el sitio.

Características de seguridad adicionales: Un sitio bancario que lo desconecta automáticamente después de un cierto período de inactividad es un ejemplo de una medida adicional de seguridad. Esto evita que alguien obtenga acceso a su cuenta si se retira de la computadora sin concluir la sesión o sin cerrar la ventana del navegador. Otra buena señal es un proceso de inicio de sesión que requiere autenticación "doble", como una foto que usted elija y la descripción de la foto escrita por usted, además del nombre de usuario y la clave.

Política de "cero responsabilidad": Garantiza que no tendrá que pagar por nada que resulte de actividad no autorizada y que el total del dinero retirado de su cuenta le será devuelto.

Política fuerte sobre privacidad: La política sobre privacidad, que explica de qué forma se recopila, se usa y se almacena información personal sobre clientes, debe aparecer claramente publicada en el sitio de la empresa. Lo ideal es que indique que la compañía no compartirá su información con terceros (individuos y organizaciones no afiliados). Si fuera necesario debe poder optar fácilmente por no permitir que se comparta su información. Logos de organizaciones como TRUSTe o BBBOnline indican que la política sobre privacidad es confiable o razonablemente fuerte. (Haga clic en el sello para verificar que sea legítimo; la dirección que aparece debe coincidir con la del sitio web oficial de la compañía certificante.) Salga del sitio si no queda conforme que su privacidad será protegida.

La recolección de información sobre el consumidor no es por lo necesario algo malo. Muchas compañías y comerciantes de buena reputación usan la información que obtienen para mejorar la atención al cliente y su eficiencia, resultando en operaciones en línea y móviles más agradables y productivas. Sin embargo, algunas compañías usan esta información para lanzar campañas de publicidad agresivas, venden los datos a uno o más individuos o no protegen los datos contra piratas informáticos, empleados deshonestos u otros que pueden utilizarla de forma maliciosa. Lo más recomendable es ser precavido al decidir con quién tener tratos comerciales y cuánta información personal revelar.

Consejos para proteger su privacidad

Revele únicamente lo que sea necesario. Cuando se registre para un servicio o una cuenta en línea llene únicamente los casilleros que se requieren para usar el servicio o abrir una cuenta. (Estos por lo general están marcados por un asterisco.) Si se lo permiten, elija las opciones que resulten en tener que compartir menos información personal. Si participa en concursos en línea o completa formularios para recibir muestras gratis o cupones corre el riesgo de que se venda su información o que sea compartida para propósitos de publicidad y promociones.

Aproveche las características de su navegador. Los más nuevos navegadores de Internet incorporan características que, cuando las habilita, pueden ayudarlo a proteger su privacidad. Por ejemplo, algunos le advierten cuando está por navegar hacia un sitio que puede ser fraudulento. Lea la sección "Help" (ayuda) en su navegador para obtener mayor información y actualice el navegador de forma regular para aprovechar totalmente las nuevas características sobre privacidad a medida que estén disponibles.

Administre sus "cookies". *Cookies* son archivos pequeños almacenados en su computadora por los sitios que visita. Rastrean su actividad mientras permanece en el sitio. Esta información se usa con frecuencia para enviar publicidad de acuerdo a sus intereses, pero también para otras cosas, como para recordar los artículos en su carrito de compras y reconocerlo como cliente cuando regresa al sitio. Usted puede fijar el navegador para borrar *cookies* automáticamente cuando salga del sitio, o para que no acepte *cookies*. Sin embargo, considere habilitar o deshabilitar la aceptación de *cookies* según el sitio. Consulte la sección "Help" de su navegador para ver las instrucciones.

Proteja sus claves. Establezca claves fuertes para su computadora, dispositivo móvil, cuentas y *apps* y no se las revele a nadie. Nunca guarde su clave en sitios que conservan su información personal o financiera; incluso sitios de comerciantes que tienen registrada su tarjeta de crédito. Aunque sea un inconveniente considere ingresar su número de tarjeta de crédito cada vez que haga una compra en lugar de permitir que la guarde el comerciante.

Desconecte del sistema. Nunca deje desatendidos la computadora o el dispositivo móvil mientras esté conectado a un sitio o *app* de operacio-