dame" u otra similar para almacenar claves o información de pago en sitios web o en *apps*. Cambie su clave de forma regular e inmediatamente si piensa que pudo haber sido comprometida.

Desconéctese de la sesión y cierre la ventana de su navegador o cierre la *app* cuando haya terminado. Cuando no los esté usando, apague los dispositivos Bluetooth que se conectan a su teléfono. También asegure su teléfono con una clave cuando no lo esté usando.

No envíe información sensible por correo electrónico o mensaje instantáneo (IM) ya que no se codifican automáticamente. Guarde el número de contacto o código corto de su banco en la libreta de direcciones de su teléfono para ver el nombre cuando reciba un correo o mensaje de texto legítimo. Y no responda cuando le pidan su clave u otra información privada por texto, correo electrónico o de cualquier otra forma, aun cuando le digan que ya tienen una relación comercial con usted.

Evite los sitios web falsos, o sea copias de sitios legítimos diseñados para incitarlo a revelar su clave y otra información sensible. Marque como "favorito" el sitio legítimo de su banco. (Así evitará la posibilidad de equivocarse al escribir la dirección web, o URL.) No use una conexión que le envíen por correo electrónico o texto para llegar al sitio.

Descargue aplicaciones únicamente de sitios de confianza. Si la fuente es desconocida, haga una búsqueda en línea de críticas y opiniones de usuarios para informarse si otras personas han tenido problemas con la aplicación. La aplicación Lookout Mobile Security (www.mylookout.com/about) es una aplicación gratuita para teléfonos Blackberry y Android que revisa las aplicaciones buscando programas maliciosos, programas espías y virus.) Antes de usar una aplicación nueva revise su política sobre operaciones disputadas o no autorizadas.

Use la red de su compañía de servicio inalámbrico en lugar de wifi público (sin clave) para realizar compras u operaciones bancarias. Verifique que en la barra de direcciones de su navegador aparezca "https" en lugar de sólo "http", lo que indica que el sitio es seguro y está codificado.

Confirme antes de hacer un pago o una compra que le darán un recibo. Guarde su recibo hasta que reciba y esté satisfecho con su compra.

Vigile la actividad en sus cuentas regularmente; hasta semanal o diariamente. De esta manera podrá detectar el fraude en sus principios. Además, en la mayoría de los casos, debe reportar actividad no autorizada en su cuenta dentro de un cierto plazo (por ejemplo 60 días a partir de la fecha en que se registró la operación) para que lo proteja la garantía de "cero responsabilidad". Su compañía de servicio inalámbrico y otros procesadores de pagos mantienen políticas para disputar cargos no autorizados en su cuenta, pero no todas las compañías ofrecen garantía de cero responsabilidad. Por lo general, la protección contra responsabilidad por actividad no autorizada es más fuerte y le dará menos problemas cuando use una tarjeta de crédito o débito que tenga una política de cero responsabilidad.

Sepa en cuánto tiempo se procesan sus operaciones para que pueda solicitar sus pagos y hacer sus depósitos y demás actividad puntualmente.

Comuníquese con su proveedor de servicio inalámbrico inmediatamente para suspender su servicio si pierde el teléfono. Luego conéctese a sus cuentas financieras en una computadora y desactive los servicios bancarios por texto y cambie sus claves. (Llame al banco si necesita ayuda.)

Muchas de las prácticas de seguridad para la banca móvil son las mismas que se recomiendan para la banca por Internet. *(Aprenda más en "La banca en línea segura", el folleto acompañante de la serie "Sus dólares digitales" en www.consumer-action.org).*

Aunque no es un problema de seguridad, tenga presente que la actividad bancaria móvil puede resultar en cuentas de servicio móvil más altas. De ser así, considere hacer operaciones bancarias en línea en la computadora de su casa o pregunte sobre otros planes de servicio móvil que se ajusten más a su uso.

Asistencia

Puede comunicarse directamente con el departamento de servicio al cliente de su institución financiera para pedir ayuda, sea usted un cliente que actualmente utiliza el servicio de banca móvil o un cliente que apenas comienza. Asimismo comuníquese con el vendedor o comerciante de la *app* sobre cualquier pregunta o problema sobre pagos móviles.

Si no está satisfecho con una compra, trate primero de resolver el problema directamente con el vendedor. Si no puede llegar a un acuerdo y desea disputar un pago, comuníquese con la compañía de tarjeta de crédito o institución financiera que emitió la tarjeta que usó para la compra.

Si su pago fue procesado por un intermediario, como a través de una cuenta de servicio de pago por Internet o a través de su proveedor de servicio móvil, siga las instrucciones de la compañía para registrar una disputa.

Más información

Obtenga más información sobre cómo proteger su seguridad al usar dispositivos móviles y dispositivos capacitados para la Web:

OnGuard Online: ***www.onguardonline.gov***

El gobierno federal de los Estados Unidos y el sector de la tecnología ofrecen información y consejos de seguridad en línea.

Privacy Rights Clearinghouse: ***www.privacyrights.org***

La organización sin fines de lucro Privacy Rights Clearinghouse ofrece una extensa colección de información; desde consejos para proteger su privacidad en línea hasta consejos para hacer compras por Internet sin peligro.

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***

Sus dólares digitales

La banca y los pagos móviles

Efectúe desde dónde se encuentre y con seguridad sus operaciones financieras

Educación financiera de Consumer Action y Visa Inc.

Revisar el saldo, transferir dinero, hacer compras... son sólo algunas de las cosas que se pueden hacer con un teléfono u otro dispositivo móvil.

Poder realizar operaciones bancarias o pagos desde casi cualquier lugar tiene muchos beneficios, pero es importante saber cómo hacerlo sin peligro. Para aprovechar al máximo la tecnología móvil es importante comprender qué tipos de operaciones pueden realizarse desde un dispositivo móvil, cuáles son los posibles riesgos de realizar operaciones bancarias y pagos desde el lugar en que se encuentre, y cómo mantener seguros su información personal, su dinero y su crédito.

¿Qué es la banca móvil?

La banca móvil le permite obtener acceso a sus cuentas financieras y llevar a cabo operaciones bancarias inalámbricas con su dispositivo móvil. La mayoría de las instituciones financieras, incluso bancos, cooperativas de crédito, entidades de préstamo y compañías de inversiones ofrecen servicios de banca móvil. Con mayor frecuencia, las instituciones financieras más pequeñas también ofrecen servicios de banca móvil.

Lo que puede hacer con un dispositivo móvil depende de la tecnología que utiliza el banco, de su plan de servicio móvil y del tipo de teléfono, dispositivo inteligente, computadora *tablet* o asistente digital personal (PDA) que tenga. Debe tener un teléfono inteligente con servicio de datos o acceso a Internet para aprovechar la capacidad de realizar las operaciones bancarias móviles más avanzadas. Antes de que pueda obtener acceso a sus cuentas con su dispositivo móvil, es posible que tenga que completar el proceso de inscripción e inicio en una computadora.

Su banco puede ofrecer tres tipos de servicio de banca móvil:

> Texto o SMS (servicio de mensaje corto, por sus siglas en inglés). La banca móvil por texto le permite obtener información sobre su cuenta (como el saldo) y recibir información y alertas por mensaje de texto. Esto es posible con cualquier teléfono móvil capacitado para mensajes de texto, pero por lo general no se pueden hacer operaciones bancarias.

> Banca en línea desde un dispositivo móvil. Ingresa a su cuenta bancaria usando el navegador web de su dispositivo móvil, tal como si fuera una computadora portátil o de escritorio. Le permite hacer lo mismo que puede hacer a través de la banca en línea. Se requiere un dispositivo capacitado para la Web y un plan de servicios de datos o wifi.

> Aplicaciones bancarias móviles o "apps" son programas especialmente diseñados que se descargan y se instalan en un teléfono inteligente, tableta o PDA. Las aplicaciones por lo general son más rápidas y fáciles de usar y navegar que un sitio web en una pantalla pequeña y le permiten efectuar la gama completa de operaciones. (Ciertas aplicaciones hasta le permiten efectuar depósitos tomando una fotografía del frente y dorso del cheque). Para usar una aplicación de banca móvil, debe tener un dispositivo móvil avanzado con wifi o con un plan de servicio de datos.

¿Qué son los pagos móviles?

Los pagos móviles son pagos que usted efectúa usando un dispositivo móvil en lugar de escribir un cheque, entregar efectivo o utilizar una tarjeta de débito o de crédito.

Existen varios tipos de pagos móviles:

Los pagos por web móvil le permiten hacer compras a la distancia cuando usa su dispositivo móvil para hacer compras con una *app* que ha descargado o con su navegador web. El monto de la compra por lo general se carga a una tarjeta de crédito o débito, a una cuenta previamente registrada de servicio de pago por Internet o a una "billetera digital" (un programa que guarda su información de pago y envío para operaciones por Internet y electrónicas).

Los pagos móviles por texto (SMS, siglas en inglés) le permiten efectuar pagos por mensajes de texto, a lo cual a veces se le llama "compra por SMS". La operación puede sumarse a su cuenta de servicio móvil o cobrarse a una tarjeta de crédito o débito previamente registrada, a una cuenta de servicio de pago por Internet o a una billetera digital. Este tipo de pago móvil por lo general se utiliza para montos pequeños, como el costo de las descargas. (timbres telefónicos y canciones, por ejemplo), cargos de estacionamiento, tarifas de transportación y entradas de cine, aunque también es posible autorizar un pago por texto a un familiar en el extranjero o comprar artículos de valor en ciertos comercios.

Las facturas directas al servicio móvil (menos comunes) le permiten agregar sus compras directamente a su cuenta de servicio inalámbrico en la caja si la opción está disponible.

Los pagos de persona a persona (P2P) por lo general son operaciones pequeñas e informales entre dos personas; por ejemplo, para pagarle a la persona que le hizo alguna reparación en su hogar o para cubrir su parte de la cuenta de una cena. El pago puede hacerse usando una *app* o, menos común, haciendo que se toquen dos teléfonos móviles.

Los pagos móviles en el punto de venta (también llamados "pagos por proximidad") posibilitan las compras en la caja u otro punto de venta simplemente con tocar o mover el dispositivo móvil cerca de un lector electrónico. Esta opción de pago se vuelve más disponible a medida que los fabricantes de teléfonos y comerciantes instalan los microchips y lectores de microchips necesarios.

Lo que debe saber

Las compras con su dispositivo móvil y la banca móvil no son especialmente riesgosas, pero esto no significa que no tienen riesgo alguno. Es importante que cualquier persona que utilice la banca móvil y la tecnología para hacer pagos tenga presente que:

> Es posible perder acceso a su cuentas si está fuera de la zona de cobertura de su servicio inalámbrico o si se le descarga la batería del teléfono. Sus pagos podrían llegar tarde si la falta de servicio inalámbrico le impide solicitar que se hagan los pagos. (Este es un motivo excelente para pagar las cuentas por anticipado cuando sea posible.)

> Es mucho más posible perder un dispositivo móvil que, por ejemplo, una computadora de escritorio. Un teléfono perdido no es solamente un inconveniente si no que puede permitirle a quien lo encuentre acceso a sus datos personales, a la información sobre su cuenta y a su capacidad de compra. (Ver "Consejos de seguridad".)

CONSEJO*: Siempre que envíe información sensible a través de una red inalámbrica sin seguridad podría ponerla en riesgo.*

> Aunque hasta ahora no es un problema serio, la programación maliciosa o "malware" (virus, espías y otros códigos diseñados para robar su información o hacerle daño a su dispositivo o a sus datos) podría afectar más seriamente a los teléfonos en el futuro. La protección antivirus y las barreras de control de acceso ("firewall") aún no están ampliamente disponibles para los dispositivos móviles.

> La banca móvil podría costarle dinero si paga el servicio móvil conforme a la cantidad de uso (por cada mensaje de texto o megabyte de datos), si usa más mensajes de texto o datos que los que incluye su plan de servicio mensual o si usa su servicio cuando está fuera de la red de su compañía ("roaming").

Consejos de seguridad

Las instituciones financieras, emisores de tarjetas, comerciantes grandes, redes de pago, proveedores de servicio inalámbrico, etc. se esfuerzan para que la banca móvil y los pagos móviles sean seguros y no causen problemas. Aun así, hay ciertas medidas que usted mismo puede tomar para proteger su información, sus cuentas y su dispositivo móvil.

Proteja su dispositivo móvil tal como si fuera su cartera ya que puede contener información que podría usarse para hacer compras u obtener acceso a sus cuentas. No le preste su teléfono a alguien que no conoce o en quien no confía. Averigüe si puede borrar el contenido del dispositivo a distancia si lo pierde o si se lo roban. (Existen muchos programas que asisten al dueño a localizar su dispositivo o a borrar sus datos personales a distancia.)

Formule claves fuertes tanto para el dispositivo (para encenderlo o cancelarle el modo de suspensión) y para todas sus *apps* bancarias o de pagos. Las claves deben contar con por lo menos ocho caracteres y usar una combinación de letras mayúsculas y minúsculas, números y símbolos. No dé a conocer a nadie sus claves, números de identificación personal, nombres de usuario o respuestas a las "pistas de clave". No use la función "recuér-