



Un asunto de conveniencia

Digamos que usted disfruta visitando al cajero del banco del vecindario y no ve ninguna razón de molestarse con el Internet. ¿Pero qué si usted necesita viajar por negocios o está fuera de servicio a partir de un accidente automovilístico o se enferma durante un largo período? ¿Qué tal la madre ocupada que extravía su chequera o está sin estampillas y los pagos de las facturas necesitan irse hoy en el correo? ¿No sería más fácil acceder a la banca en línea y hacerse cargo de sus necesidades bancarias desde la conveniencia de su cocina, estudio u oficina?

Eso es lo atractivo acerca de la banca en línea, la facilidad y comodidad de todo. Además, cuando se trata de pagar facturas en línea, usted puede programar cuando deben ser realizados los pagos, de modo que ahorre dinero en cargos por pagos tardíos u otros cargos, además se puede ahorrar de \$8 a \$12 o más al mes en estampillas y sus papilas gustativas evitarán la desagradable degustación de esos sobres.

Otra gran ventaja sobre la banca en línea es que usted puede acceder a la información que no está fácilmente disponible en su sucursal. Puede comprobar, ver e imprimir la actividad de la cuenta por cualquier rango de tiempo que usted especifique, no más espera del estado de cuenta mensual. La banca en línea también le permite transferir fondos, re-ordenar cheques y pagar las facturas, siempre que lo desee.

Empezar es fácil. Acceda a la página Web de su banco o cooperativa de crédito y empiece desde allí. Registrarse generalmente implica proporcionar información básica como su dirección y número de cuenta bancaria, la firma de un acuerdo de privacidad y de un acuerdo para pagar todos los costos asociados con la cuenta. Normalmente, si usted tiene suficiente dinero en su cuenta, no hay cargos. En caso contrario, puede que tenga que pagar una cuota mensual por el servicio de banca en línea de pago de facturas. Esto varía de banco en banco.

Los beneficios y riesgos de la banca en línea

Una de las ventajas más significativas y convenientes puestas a disposición del público con la llegada del Internet, es la banca en línea. Prácticamente cada organización de cooperativa de crédito y banca a través de los Estados Unidos, ahora ofrecen tales servicios, lo que significa que usted puede comprobar los saldos de su cuenta, transferir dinero de su cuenta de cheques a su cuenta de ahorros y viceversa, hacer los pagos del vehículo e hipoteca y pagar sus facturas—siempre y cuando usted tenga acceso a una computadora e Internet.

Lamentablemente, con la conveniencia de la banca en línea vienen ciertos riesgos cibernéticos, lo que significa que es importante educarse sobre como ocurre el acceso no autorizado a su información financiera y los pasos que usted puede tomar para protegerse. Este volumen de *Dólares & Sentido* provee información útil para consumidores bancarios en línea, diseñada para ayudarlo a obtener y retener el control del bienestar cambiando el histórico refrán: “Un centavo ahorrado es un centavo ganado” a “Un centavo ahorrado es un centavo guardado”. ■

Comience con el pago de facturas en línea

Si usted está considerando la posibilidad de hacer el salto a la banca en línea, el mejor lugar para comenzar es con el pago de facturas en línea. Con él, usted puede pagar prácticamente a cualquier

(Continúa en la página 2)

Un asunto de conveniencia *(Continúa de la página 1)*

persona o empresa en Estados Unidos. Factura de electricidad, factura de la compañía de cable o al dentista. Usted incluso puede utilizar el pago de facturas para enviar dinero a amigos y familiares. La mayoría de los bancos y las cooperativas de crédito tienen procedimientos similares para la creación de pagos de facturas en línea:

1. Establezca sus beneficiarios. Su tarjeta de abono bancario o préstamos ya son típicamente establecidos como beneficiarios para usted, cuando se inscribe. Para establecer a sus otros beneficiarios, usted necesitará su factura para encontrar la dirección de la compañía y su número de cuenta.

2. Programe sus pagos. Indique la cantidad que quiere pagar y cuando quiere que el dinero sea tomado de su cuenta corriente. El sistema le hará saber cuánto tiempo tiene para cada beneficiario—esto generalmente es de tres a cinco días hábiles antes de que usted desee que el

dinero esté allí.

3. Su pago es enviado. El dinero es descontado de su cuenta y enviado al beneficiario como usted indicó. Si usted lo elige, también puede recibir un correo electrónico que confirma que el pago ha sido enviado.

Puede también utilizar el pago de facturas en línea para no perder de vista su historial de pago, así que puede mirar atrás, tanto hasta un año completo para supervisar cuánto y cuándo pagó a cada uno de sus beneficiarios.

Lo que es necesario investigar

Si decide comenzar la banca en línea, a continuación le proporcionamos cuatro sugerencias de cosas que sería bueno investigar:

- **Cuotas bajas**—Todos los bancos le permiten comprobar la actividad de su cuenta en línea de forma gratuita. Si hay un cargo por los servicios de

pagos de facturas, averigüe cuánto es y si usted puede ahorrarse ese dinero al ir con otro banco o cooperativa de crédito diferente.

- **Atención al cliente**—En caso de que usted encuentre un problema, asegúrese de que es fácil localizar a una persona real en el banco o centro de asistencia del banco. Algunos bancos tienen representantes de servicio al cliente las 24 horas del día y los 7 días de la semana (24/7) en espera de llamadas, otros prometen responder a mensajes de correo electrónico dentro de 24 horas.
- **Política de privacidad**—La clave para saber cómo su banco utilizará su información personal es leer su política de privacidad. La mayor parte de tales políticas declaran que la institución financiera no venderá su información a terceros, pero si la pasarán a sus “compañías afiladas”—por lo general vendedores de seguro e inversiones. Idealmente, usted quiere una política que permita rechazar el compartir su información a cualquier compañía, afiliada o no. ■

Nunca envíe su información personal dentro de un correo electrónico.

La mayoría de las personas hoy en día, no pueden vivir sin sus cuentas personales de correo electrónico; ellos hacen conexiones con amigos y familiares y es más fácil que los viajes a la oficina de correos y las llamadas telefónicas interrumpidas de las últimas décadas. Lamentablemente, la mayoría de los emisores de Spam y Phishing también saben esto y toman ventaja total de los medios. Esto ya no es como la estafa de la princesa africana exiliada, que solicitaba enviar ayuda esperando hasta que los mil millones de dólares retenidos de sus padres fueran liberados de un banco, lo cual solía envolver a las personas. Estos tipos de correos electrónicos falsos son fáciles de reconocer y en un rápido clic en el icono de eliminar, removerá fácilmente este molesto correo electrónico de su bandeja de entrada. Hoy día los emisores anónimos de spam están enviando correos electrónicos disfrazados como si fueran de su banco local o de compañías de servicios públicos. Muchos de estos correos electrónicos son difíciles de distinguir de los verdaderos. Ellos se hacen cada vez más convincentes y más difíciles de detectarse.

El problema más común en los correos electrónicos, es que con frecuencia vienen de emisores de spam que se hacen pasar por alguna de las siguientes compañías:

Ebay, PayPal, IRS, Chase Bank, Citibank, Bank of America, Capital One y son casi iguales como cualquier otro banco local o institución financiera o cualquier compañía que emite tarjetas de crédito como Sears u otras.

Muchos de estos correos electrónicos aparecerán en su bandeja de entrada como alarmas de actividad o advertencias de que su cuenta en línea se ha visto comprometida o puesta en riesgo.

Es importante evaluar individualmente cada uno de estos mensajes de correo electrónico. En primer lugar pregúntese, “Yo tengo una cuenta con esta institución?” El ochenta por ciento de las veces, ni siquiera tiene un motivo para asociarse con esa organización. Después, nunca haga clic en los enlaces presentados en estos correos electrónicos.

Consejos para la seguridad de la banca en línea

Como se explicó por US-CERT (www.us-cert.gov) cuando se trata de servicios bancarios en línea, no hay manera de garantizar absolutamente su seguridad. Sin embargo, las buenas prácticas existen para poder reducir los riesgos planteados a sus cuentas en línea. Considere estas útiles sugerencias para aumentar las posibilidades de que las mejores prácticas están siendo seguidas y aplicadas:

Revise la información de su banco en línea acerca de sus políticas y prácticas de privacidad. Por ley, los bancos están obligados a enviarle anualmente una copia de sus políticas y prácticas de privacidad; también puede solicitar una copia de esta información. Los sitios Web bancarios también deben tener esta información. Cuando usted lea esto, ponga particular atención a cualquier mención de los métodos utilizados para cifrar transacciones y autenticar información de usuario. También, verifique para ver si el banco requiere información adicional de seguridad antes de autorizar un pago a un negocio o individuo que nunca ha recibido un pago antes.

Muchos de ellos simplemente lo llevarán hacia un sitio falsificado esperando conseguir su información personal. Algunos, sin embargo; lo conducen a descargas de virus o a programas espías para su computadora. Evítese dolores de cabeza y no haga caso del correo electrónico. Por último, si está preocupado por el potencial de la advertencia, llame directamente a su banco o visite su sitio Web escribiendo la dirección directamente en el navegador. Muchas instituciones han sido alertadas de correos electrónicos Phishing que utilizan sus nombres y es común que ellos tengan información sobre el sitio Web, le explicarán el correo electrónico falso y las medidas a tomar para evitar problemas. ¡Recuerde; NUNCA envíe su información personal en respuesta a uno de esos correos electrónicos! ■

Antes de establecer cualquier pago de factura en línea, compruebe la política de privacidad de la empresa o servicio a donde usted va a enviar el pago. Usted tiene el derecho de limitar la información que un banco en línea comparte tanto con su organización matriz como



con cualquier otra institución financiera. Tenga en cuenta que algunos bancos en línea pueden tener procedimientos distintos para la tramitación de cada una de estas solicitudes. También puede utilizar un servicio como el Better Business Bureau (Buró de los Mejores Negocios) para ver todo el historial de quejas pendientes de los consumidores sobre violaciones a su privacidad.

Por motivos de seguridad, elija un número de identificación personal (PIN) para el servicio en línea, que sea único y difícil de adivinar. Asegúrese de cambiar su PIN periódicamente. No elija un PIN que contenga información personal como su fecha de nacimiento o número de seguro social, un atacante podría ser capaz de adivinar estos. Independientemente de las circunstancias, nunca dé a alguien acceso a su número de PIN actual.

Instale programas antivirus, cortafuegos (firewall) y anti-espías en su computadora y manténgalos actualizados. La instalación y actualización de estos pro-

gramas protege su computador y su contenido contra el acceso no autorizado. Usted debe activar actualizaciones automáticas para estos programas o si se le solicita, siempre esté de acuerdo para descargar actualizaciones del sistema tan pronto como estén disponibles.

Compruebe periódicamente su saldo de la cuenta en línea por actividades no autorizadas. El tiempo es un factor en su respuesta para las transacciones

electrónicas de fondos no autorizados. Si recibe un documento del saldo de la cuenta, asegúrese de conciliarlo con su saldo en línea.

Utilice una tarjeta de crédito para pagar por bienes y servicios en línea. Las tarjetas de crédito tienen generalmente protección más fuerte contra reclamos de responsabilidad personal que las tarjetas de débito. Algunas tarjetas de crédito limitan la responsabilidad personal para transacciones no autorizadas a \$50. La responsabilidad personal de tarjetas de débito puede ser más alta. Según la Regulación E de la Reserva Federal, si usted reporta un problema de transacción de fondos electrónicos que implica tarjetas de débito a una institución bancaria o financiera en los primeros dos días, usted sólo es responsable por \$50 dólares. Reportando este mismo incidente entre 3 y 60 días aumenta su responsabilidad personal a \$500 dólares. Después de 60 días, no hay ningunas restricciones financieras colocadas en su responsabilidad personal. ■

ARTÍCULOS

Consejos y Trucos

Con la conveniencia vienen algunos riesgos

Ahora que usted ha descubierto los beneficios de la banca en línea, tenga presente que nosotros no vivimos en un mundo ideal. Sin duda, la popularidad de la banca en línea también presenta algunos riesgos y desafíos a su estabilidad económica y a su privacidad personal.

Según lo recomendado por el Equipo de Preparación de Emergencia de Computadoras de los Estados Unidos (US-CERT), (www.us-cert.gov), si se va a utilizar la banca en línea para llevar a cabo transacciones financieras, usted debe estar consciente de los riesgos y tomar precauciones para minimizarlos. US-CERT es una asociación entre el Departamento de Seguridad Nacional de los Estados Unidos y el Sector Público y Privado. Establecida en el año 2003 para proteger la infraestructura de Internet de la nación, US-CERT coordina la defensa y respuesta contra ataques cibernéticos en toda la nación.

Ataques que apuntan hacia las actividades bancarias en línea

Varios tipos de fraude electrónico expresamente apuntan a la banca en línea. Algunos de los más populares para ser tomados en cuenta incluyen:

Ataques de Pesca informática—Utilizan mensajes de correo electrónico falsos de una agencia o persona pretendiendo representar a su banco o institución financiera. El correo electrónico le solicita que proporcione información susceptible (nombre, contraseñas, número de cuentas, etc.) y proporciona enlaces a un sitio Web falsificado. Si usted sigue el enlace y proporciona la información solicitada, los intrusos pueden tener acceso a la información de su cuenta personal y finanzas. En algunos casos, pueden aparecer ventanas emergentes falsas delante de una copia de un sitio Web bancario genuino. La verdadera dirección del sitio Web es visualizada, sin embargo, cualquier información que usted escriba directamente en la ventana emergente irá a usuarios no autorizados.

Programa Malicioso (Malware)—Término para programas elaborados con códigos hostiles/maliciosos. Ahora existen programas de computadora especiales que permiten a intrusos engañarle y hacerlo creer que la seguridad tradicional le protege durante transacciones bancarias en línea. De hecho, es posible que este tipo de programas maliciosos lleven a cabo las siguientes operaciones:

- **Robo de la información de la cuenta**—El Malware puede capturar las pulsaciones de su información de entrada al sistema, además de que también pueden controlar y capturar otros datos que se utilizan para autenticar su identidad (por ejemplo: en especial las imágenes que ha seleccionado o “palabras mágicas” que eligió).
- **Substitución falsa del sitio Web**—El Malware puede generar falsas páginas Web que sustituyen el sitio Web legítimo de su banco. Tal como un ataque MitM o intermediario (“man-in-the-middle attack”) que permite a un atacante interceptar su información de usuario de un sitio. El atacante añade campos adicionales a la copia de la página Web abierta en su navegador.
- **Asalto de la cuenta (Hijacking)**—El Malware puede secuestrar su navegador y transferir fondos sin su conocimiento. Cuando intenta acceder al sitio Web de un banco, el programa lanza una ventana del navegador oculto en el equipo, inicia una sesión en su banco, indica el saldo de su cuenta y clandestinamente transfiere fondos de su cuenta a la cuenta del intruso.

Ataque que interviene las comunicaciones entre el usuario y su proveedor de Internet (Pharming)—Los ataques Pharming implican la instalación de códigos maliciosos en su computadora; sin embargo, ellos pueden ocurrir sin cualquier acción consciente de su parte. En un tipo de ataque pharming, usted abre

un correo electrónico o un archivo adjunto de un correo electrónico, esto instala el código malicioso en su computadora. Más tarde, usted va a un sitio Web falso que se asemeja al de su banco o institución financiera. Cualquier información que usted proporciona durante una visita al sitio falso es puesta a disposición de los usuarios maliciosos.

Todos estos tipos de ataques requieren que usted proporcione información

Todos los tipos de ataque descritos comparten una características en común, con el fin de tener éxito es necesario que proporcione información:

- **En ataques phishing**, usted debe proporcionar información o visitar enlaces.
- **En ataques malware**, usted puede ser engañado en realización a acciones que usted no haría normalmente. Usted tendría que instalar el malware en su ordenador, ya sea ejecutando un programa, como un archivo adjunto de correo electrónico o visitando un sitio Web a través del correo electrónico o un enlace de un mensaje instantáneo.
- **En ataques pharming**, debe abrir un mensaje de correo electrónico o un archivo adjunto de correo electrónico para hacerse vulnerable. Usted entonces visita un sitio Web falso y sin su conocimiento, proporciona la información que compromete su identidad financiera. ■

Family Financial Education Foundation

ACCESS EDUCATION SYSTEMS

724 Front Street, Suite 340

Evanston, WY 82930

contact: (888) 292-4333

www.ffef.org | info@ffef.org



Si usted sabe de alguien que podría beneficiarse con nuestros servicios, hágale llegar esta información.

Esta publicación es propiedad de Family Financial Education Foundation. Todos los derechos reservados. Para más información sobre nuestros servicios o cómo podemos ayudarle con su programa de manejo de deuda, por favor contacte a Family Financial Education Foundation. www.ffef.org