FEDERAL DEPOSIT INSURANCE CORPORATION

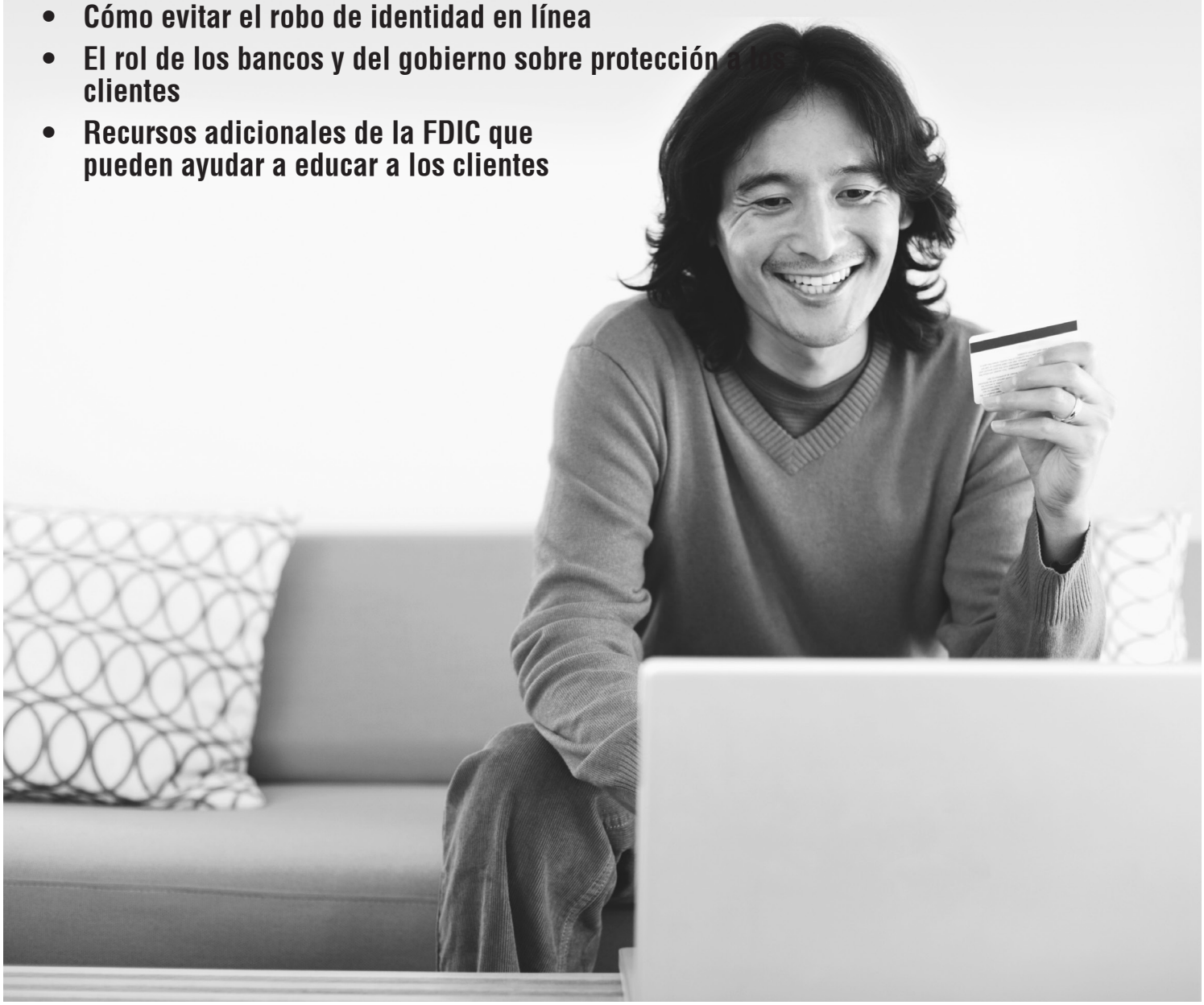
FDIC Consumer News

EDICIÓN ESPECIAL — Invierno de 2016

Guía sobre ciberseguridad para clientes de bancos

Qué pueden hacer los clientes ...
y qué *están haciendo* los bancos y los reguladores ...
para ayudar a evitar robos y fraudes en línea

- **Precauciones de seguridad para servicios bancarios o compras por el Internet**
- **Cómo evitar el robo de identidad en línea**
- **El rol de los bancos y del gobierno sobre protección a los clientes**
- **Recursos adicionales de la FDIC que pueden ayudar a educar a los clientes**



Proteja su "hogar cibernético " con una base sólida

Pasos simples para proteger sus computadoras y aparatos móviles para servicios bancarios y compras por Internet

Su hogar tiene cerrojos en las puertas y las ventanas para proteger a su familia y evitar que los ladrones roben dinero, aparatos electrónicos, joyas y demás pertenencias físicas. Sin embargo, ¿cuenta con medidas de disuasión para evitar la pérdida o el robo de activos electrónicos, incluida información de cuentas bancarias y demás información que conste en sus computadoras personales, en su hogar y al realizar compras y operaciones bancarias de forma remota por Internet?

"Piense en todos los puntos de acceso hacia y desde su computadora, por ejemplo, conexiones de Internet, cuentas de correo electrónico y redes inalámbricas", dijo Michael Bernardo, gerente de la Sección de Fraudes Cibernéticos y Delitos Financieros de la FDIC. "Siempre se deben proteger. De lo contrario, es similar a dejar la puerta de entrada abierta de par en par mientras uno esté fuera para que cualquier persona pueda entrar y llevarse lo que desee".

Tenga en cuenta las siguientes estrategias.

Para servicios bancarios mediante computadoras o aparatos móviles

Tome precauciones adicionales al iniciar sesión en cuentas bancarias y demás cuentas financieras. Entre estas medidas se incluyen usar identificaciones y contraseñas de usuario "complejas" eligiendo combinaciones de minúsculas y mayúsculas, números y símbolos que sean difíciles de adivinar por los piratas informáticos. No use su fecha de nacimiento, dirección ni otras palabras o números que los estafadores pudieran descubrir o adivinar con facilidad. Tampoco use la misma contraseña para diferentes cuentas porque si un delincuente obtiene la contraseña puede iniciar sesión en las otras cuentas. Mantenga en secreto sus identificaciones y contraseñas, y cámbielas con regularidad. Asegúrese de cerrar sesión de cuentas financieras cuando finalice las transacciones o se aleje de la computadora.

Considere usar una computadora aparte exclusivamente para compras y servicios bancarios en línea. Cada vez más personas compran computadoras básicas y las usan únicamente para servicios bancarios en línea y no para navegar por Internet, enviar mensajes de correo electrónico, relaciones sociales electrónicas, jugar juegos ni otras actividades que resulten más susceptibles a software malintencionado (conocido generalmente como "malware") y que puedan obtener acceso a computadoras y robar información. Como alternativa, puede usar una computadoras antigua con este fin limitado, pero desinstale cualquier software que ya no necesite y analice toda la computadora para corroborar la existencia de software malintencionado antes de proseguir.

Tome precauciones si proporciona información financiera sobre cuentas a terceros por Internet. Por ejemplo, algunas personas usan servicios de "agregación de cuentas" que, desde un único sitio web, pueden ofrecer una manera conveniente de pagar facturas, supervisar saldos de cuentas de depósito e inversión, e incluso llevar un registro de las millas de viajero frecuente. Si bien estos sitios web pueden resultar beneficiosos, también pueden suponer posibles problemas vinculados con la seguridad de la información de la cuenta que compartió con ellos. Si desea usar sus servicios, investigue a fondo a la empresa que se encuentra detrás del sitio web, lo cual incluye asegurarse de que esté tratando con una entidad legítima y no un sitio fraudulento. También consulte qué protecciones ofrece el sitio web si este experimenta una filtración de información o pérdida de datos.

Revise periódicamente sus cuentas bancarias para detectar signos de fraude. Si realiza operaciones bancarias en línea, controle las cuentas de depósito y las líneas de crédito en intervalos regulares para detectar e informar errores o transacciones fraudulentas, como lo haría al revisar un resumen impreso. Los servicios bancarios en línea facilitan y aceleran la supervisión de las cuentas. Esto es importante porque mientras más pronto pueda detectar un problema con una transacción, más sencillo resultará resolverlo.

Las leyes federales en general limitan su responsabilidad del uso no autorizado de sus tarjetas de débito, crédito y prepagas, en especial si informa el problema a la institución financiera en los plazos especificados, que varían según las circunstancias (consulte la página 8 para conocer más detalles). Un buen principio rector consiste en revisar sus cuentas en línea una o dos veces por semana. Además, muchos bancos facilitan el seguimiento de las cuentas por parte de los clientes mediante la oferta de alertas por correo electrónico o mensajes de texto cuando los saldos descienden por debajo de un determinado nivel o bien cuando se produce una transacción que supere un monto específico.

Mensaje para los lectores

La Federal Deposit Insurance Corporation ha publicado ***FDIC Consumer News*** trimestral desde 1993 para ayudar a las personas a proteger su dinero, incluidas sugerencias en prácticamente todos los temas sobre cómo evitar el robo y el fraude financiero. Mucho ha cambiado en el transcurso de los años, en especial el aumento de la dependencia de los consumidores en las computadoras e Internet (el mundo "cibernético") en todos los aspectos desde las compras y las comunicaciones hasta los servicios bancarios y el pago de facturas. Si bien los beneficios de servicios cibernéticos más rápidos y convenientes para los clientes bancarios resultan claros, es posible que los riesgos que suponen estos servicios, así como las estrategias para evitar y recuperarse de delitos relacionados con actividades cibernéticas, no sean tan bien conocidos por el consumidor promedio y el propietario de pequeñas empresas.

Es por ello que la FDIC ha producido esta edición especial de nuestro boletín: una guía para servicios bancarios en línea seguros, donde constan precauciones que se deben tomar en el hogar y al realizar actividades bancarias de manera remota (mediante computadoras portátiles, smartphones y demás aparatos móviles). Incluimos sugerencias e información para padres y custodios legal que desean proteger a sus hijos del robo de identidad y del fraude en línea, y para las pequeñas empresas que necesitan proteger sus sistemas de computación y sus datos. También conocerá qué hacen los bancos y los reguladores bancarios para proteger su dinero.

Importante: Estos y otros temas de ***FDIC Consumer News*** se pueden leer o imprimir en www.fdic.gov/consumernews. Vuelva a consultar el sitio web para obtener versiones de este número para lectores electrónicos y reproductores de audio portátiles (MP3). Se encuentran disponibles copias individuales de esta edición especial y los artículos a los que se hace referencia si se solicitan al Centro de Información Pública de la FDIC (a la línea gratuita 1-877-275-3342 o a publicinfo@fdic.gov). Nuestra publicación puede imprimirse nuevamente en su totalidad o en parte sin permiso alguno.

Sugerencias básicas sobre seguridad

Mantenga actualizado el software. Los fabricantes de software permanentemente actualizan sus productos para solucionar vulnerabilidades o deficiencias de seguridad cuando las encuentran. "Todo el software se debe revisar y actualizar según la recomendación general del fabricante o cuando se encuentran fallas", explicó Kathryn Weatherby, especialista en exámenes de fraudes de la FDIC. "Este consejo se aplica a todo desde el sistema operativo hasta el software de procesamiento de texto, los navegadores de Internet, el software de hojas de cálculo e incluso las aplicaciones de fotografía cibernético . Una vulnerabilidad en un programa de software, independientemente de qué tan insignificante pudiera parecer, puede ser aprovechada por un pirata informático y ser empleada como ruta de ingreso a toda la computadora".

Algunos fabricantes de software pueden publicar "revisiones" que debe instalar para actualizar un programa. Otros simplemente pueden brindarle una versión totalmente nueva del software. "Antes de instalar cualquier software que reciba, asegúrese de que sea legítimo, especialmente si se le envía por correo electrónico", afirmó Benardo. "Corrobore el sitio web del fabricante del software o comuníquese directamente con la empresa para verificar la validez de la actualización. Cómo es conocido los delincuentes imitan a los proveedores de software que proporcionan actualizaciones de seguridad cuando, en realidad, distribuyen malware. Una vez que confirme que la actualización es legítima, instálela tan pronto le resulte posible para corregir cualquier falla de seguridad que pudiera existir".

Instale software antivirus que evite, detecte y elimine programas malintencionados. Los malhechores y los piratas informáticos siempre desarrollan nuevo malware para obtener acceso a las computadoras y robar información, por ejemplo, contraseñas de cuentas o números de tarjetas de crédito y débito. Es posible que estos programas también puedan destruir datos de unidades de disco duro infectadas de la computadora.

El malware puede introducirse en la computadora de muchas formas, tal vez como archivo adjunto de un correo electrónico, un archivo descargado de un sitio web infectado o bien de un disco o un aparato de memoria contaminado. Defiéndase instalando software antivirus que periódicamente se ejecute en segundo plano en la computadora para buscar y eliminar malware. También asegúrese de configurar el software para que se actualice automáticamente de modo que pueda protegerlo del malware más reciente. Para obtener más información sobre malware, consulte la página 5.

Use un programa cortafuegos para evitar el acceso no autorizado a su computadoras. Un cortafuegos es una combinación de hardware y software que establece una barrera entre la computadora personal y una red externa, por ejemplo, Internet, y luego, supervisa y controla el tráfico de red entrante y saliente. En términos simples, un cortafuegos actúa como un guardián que ayuda a repeler a los piratas informáticos, el malware y demás intrusos que intenten acceder a su computadora desde el Internet.

Emplee únicamente productos de seguridad procedentes de empresas reconocidas. Algunos cortafuegos y

software antivirus se pueden comprar, mientras que otros son gratuitos. De cualquier modo, resulta una buena idea analizar estos productos leyendo resumenes en publicaciones informáticas y de consumidores. Busque productos que tengan clasificaciones elevadas respecto a la detección de problemas y la oferta de asistencia técnica si se infecta la computadora. Otras maneras de seleccionar los productos de protección adecuados para la computadora consisten en consultar al fabricante de la computadora o del sistema operativo, o bien pregúntele a una persona reconocida como experta en informática.

Aproveche las funciones de seguridad de Internet. Cuando realice operaciones bancarias en línea, compre por Internet o complete una solicitud por la cual se pida información personal confidencial, por ejemplo, números de cuentas bancarias, de tarjeta de crédito y de tarjeta de débito, asegúrese de estar operando con empresas reconocidas. También puede confiar en mayor grado en un sitio web que cifre (codifique) la información cuando sale de su computadora o ingresa en ella. Busque un símbolo de candado en la página y la dirección web que comienza con "https://." La "s" significa "seguro".

Además, las versiones actuales de los navegadores de Internet y los motores de búsqueda más populares a menudo indicarán si visita un sitio web sospechoso o una página que no se pueda verificar que es de confianza. Resulta más adecuado no permanecer en páginas con estos tipos de advertencias. Revise las instrucciones para el usuario del navegador de Internet y explore las pestañas "herramientas" y "ayuda" para obtener más información sobre la configuración de seguridad y las alertas que se ofrecen.

Tenga cuidado dónde y cómo se conecta a Internet. Una computadora pública, como la de un cibercafé o del salón de negocios de un hotel, pueden no tener un software de seguridad actualizado y podría estar infectada con malware. De manera similar, si usa una computadora portátil (por ejemplo, una laptop o un aparato móvil) para sus servicios bancarios en línea o para realizar compras, evite conectarla a una red inalámbrica (Wi-Fi) en un "punto de acceso" público como una cafetería, un hotel o un aeropuerto. La red Wi-Fi de áreas públicas puede ser usada por delincuentes para interceptar las señales de su aparato y como punto de obtención de información personal.

En definitiva, especialmente en lo relativo a cuestiones confidenciales tales como servicios bancarios en línea y actividades en las que interviene información personal, tenga en cuenta únicamente obtener acceso a Internet mediante su propia computadora a través de una conexión segura y de confianza, y conectar las computadoras portátiles y los aparatos móviles solamente a redes confiables.

Para obtener más sugerencias sobre la seguridad de computadoras e Internet para clientes de bancos, mire la presentación multimedia de la FDIC "No sea víctima en Internet: cómo protegerse contra ladrones de Internet y estafas electrónicas" en www.fdic.gov/consumers/ consumer/guard. También visite https://www.alertaenlinea.gov/ para obtener información del gobierno federal sobre cómo permanecer protegido en Internet. Este sitio incluye videos de la Comisión Federal de Comercio (FTC, por sus siglas en inglés) sobre qué se debe hacer si piratean su cuenta de correo electrónico o un malware ataca su computadora.

Adopción de servicios móviles: cómo estar más seguro al usar un smartphone o una tableta

No importa hacia dónde mire, las personas usan smartphones y tabletas como computadoras manuales y portátiles. "Lamentablemente, los ciberdelincuentes también están interesados en utilizar u obtener acceso a estos aparatos para robar información o cometer otros delitos", afirmó Michael Benardo, gerente de la Sección de Fraudes Cibernéticos y Delitos Financieros de la FDIC. "Eso hace que resulte esencial para los usuarios de aparatos móviles tomar medidas para protegerlos, al igual que lo harían con una computadora de escritorio".

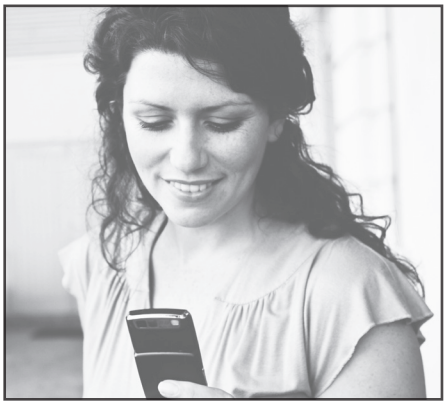
Estos son algunos de los pasos básicos que puede implementar para proteger sus aparatos móviles.

Evite aplicaciones que puedan contener malware. Compre o descargue en tiendas de aplicaciones conocidas, tales como aquellas establecidas por el fabricante de su teléfono o el proveedor de servicios celulares. Consulte el sitio web de su institución financiera para confirmar dónde descargar la aplicación oficial para servicios bancarios en línea.

Mantenga actualizadas las aplicaciones y el sistema operativo de su aparato. Considere optar por actualizaciones automáticas porque hacerlo garantizará que tenga las revisiones más recientes de toda falta de seguridad que descubra el fabricante. "Los ciberdelincuentes intentan aprovecharse de las fallas conocidas, por lo que mantener actualizado el software ayudará a reducir su vulnerabilidad en caso de actividades ilegales", afirmó Robert Brown, especialista sénior en Defensoría del Pueblo de la FDIC.

Considere usar un software de seguridad móvil y aplicaciones que protejan su aparato. Por ejemplo, el software antimalware para smartphones y tabletas puede adquirirse a través de un proveedor reconocido.

Utilice una contraseña u otra medida de seguridad para restringir el acceso en caso de que pierda o roben su aparato. Active la función de "tiempo fuera" o "bloqueo automático" que protege su aparato móvil cuando no se lo utilice durante una cierta cantidad de minutos. Configure esa función de seguridad para que se inicie después de un período relativamente breve de inactividad. Hacerlo reduce la probabilidad de que un ladrón pueda usar su teléfono o su tableta.



Realice copias de seguridad de los datos de su smartphone o tableta. Esto resulta adecuado en caso de que su aparato se extravíe, sea robado o simplemente un día deje de funcionar. De forma sencilla, se pueden realizar copias de seguridad de los datos en una computadora o un servicio de respaldo, que puede ofrecer el operador móvil.

Debe contar con la posibilidad de eliminar datos de forma remota desde su aparato si este se extravía o es robado. La "eliminación remota" protege los datos de las miradas curiosas. Si se ha realizado una copia de seguridad del aparato, la información puede restaurarse en un aparato de reemplazo

continúa en la página 9

Qué están haciendo los bancos y los reguladores bancarios para proteger a los clientes de las amenazas cibernéticas

En el mundo en que vivimos actualmente, las instituciones financieras deben tener conocimiento de las amenazas ciberneticas actuales y tomar las precauciones que correspondan para proteger el dinero y la información personal de sus clientes. "Los bancos son objetivos tentadores para los ladrones cibernéticos que desean cometer fraude financiero", dijo Jeff Kopchik, analista sénior de políticas de la FDIC. "Pero lo que los clientes deben recordar es que los bancos y los reguladores trabajan en conjunto para evitar estos delitos".

Los bancos cuentan con empleados o utilizan empresas externas que trabajan para prevenir los fraudes cibernéticos. Además, las instituciones financieras deben mejorar permanentemente sus programas de seguridad de la información para que puedan responder con eficacia a las amenazas cibernéticas más recientes.

La FDIC y demás reguladores también trabajan con instituciones financieras para ayudar a proteger el dinero y la información de los clientes. Desde 2001, las regulaciones y la ley federal han exigido que las instituciones financieras cuenten con programas para garantizar la seguridad y la confidencialidad de la información de los clientes. Los examinadores bancarios federales y estatales también realizan con regularidad exámenes in situ de instituciones aseguradas por la FDIC y sus empresas externas con la finalidad de corroborar que cumplan con estas y otras regulaciones.

Los reguladores bancarios trabajan con instituciones para compartir perspectivas generales del panorama de las amenazas cibernéticas y analizar pasos que pueden tomar para estar preparados. Por ejemplo, en 2015 la FDIC produjo un video educativo sobre ciberseguridad para ayudar a la junta directiva y oficiales de los bancos a protegerse de las posibles amenazas. Ese mismo año, los reguladores presentaron una "herramienta de evaluación de ciberseguridad" voluntaria para ayudar a las instituciones a identificar los riesgos y evaluar su preparación.

"Los bancos pueden emplear cualquier herramienta de evaluación de riesgos que elijan. Examinadores de la FDIC están disponibles para analizar los resultados con la gerencia de los bancos y ayudarles a enfocarse áreas que necesiten mejorar", afirmó Mark Moylan, subdirector de riesgos operativos de la FDIC. "Consideramos que esta comunicación es una parte importante de nuestra estrategia para ayudar a garantizar la seguridad de la información financiera de los clientes".

La FDIC también recomienda que las instituciones se sumen a organizaciones de la industria que brinden información oportuna y confiable diseñadas para ayudarlas a proteger sistemas esenciales de las amenazas cibernéticas.

"Los ciberdelincuentes buscan constantemente formas novedosas de cometer fraude financiero contra un banco y sus clientes", manifestó Kopchik. "Es por eso que la FDIC dedica una cantidad considerable de recursos al cumplimiento por parte de las instituciones financieras de las leyes federales de seguridad de la información y alerta a las gerencias de los bancos respecto a las amenazas cibernéticas más recientes, así como también de las contramedidas más eficaces. Constituye parte de la misión de la FDIC mantener la estabilidad y la confianza pública en el sistema financiero del país". 🏛

Protéjase del malware: ¡Piense antes de hacer clic!

El software malintencionado (o "malware", como es su forma abreviada) constituye una clase amplia de software desarrollado con una intención maliciosa. "Es posible que haya escuchado que se hace referencia al malware como 'error informático' o 'virus" porque la mayoría de este está diseñada para propagarse como una enfermedad contagiosa e infectar a otras computadoras con los que entre en contacto", afirmó Michael Benardo, gerente de la Sección de Fraudes Cibernéticos y Delitos Financieros de la FDIC. "Y si no protege su computadora, puede infectarse con malware que robe su información financiera personal, lo espíe capturando las pulsaciones del teclado o incluso destruya datos".

Los organismos de aplicación de la ley y los expertos en seguridad han observado un aumento de un determinado tipo de malware conocido como "ransomware", que restringe el acceso de una persona a una computadora o un smartphone (literalmente secuestra el aparato) hasta que se pague un rescate. Si bien hasta la fecha las víctimas han sido más empresas que consumidores, muchos usuarios de computadoras domésticas han sido objeto de ransomware. Para obtener más información, consulte una alerta emitida por el Departamento de Seguridad Nacional de los Estados Unidos en www.us-cert.gov/ncas/ alerts/TA13-309A.

La forma más común en que se propaga el malware es cuando una persona hace clic en un archivo adjunto a un mensaje de correo electrónico, que puede ser desde un documento hasta un archivo de fotografía, video o audio. Es posible que los delincuentes también intenten hacer que descargue malware incluyendo un enlace en el texto de un correo electrónico o en una publicación en una red social que lo dirija a otro lugar, a menudo a un archivo o una página web infectada en Internet. El enlace podría ser parte de una historia que suene muy provocativa, por ejemplo, que tenga un titular que rece: "¡Cómo hacerse rico!" o "Tiene que ver esto".

El malware también puede propagarse por una red de computadoras enlazadas, descargarse de un sitio web infectado o transmitirse en un aparato de almacenamiento portátil contaminado, por ejemplo, un aparato de memoria o una unidad flash.

A continuación se incluyen recordatorios, además de sugerencias adicionales, sobre cómo mantener el malware alejado de su computadora en general.

No abra de inmediato archivos adjuntos de correos electrónicos ni haga clic en los enlaces de mensajes de correo electrónico no solicitados o con aspecto sospechoso. ¡Piense antes de hacer clic! Los ciberdelincuentes son buenos para elaborar mensajes de correo electrónico falsos que parezcan legítimos pero puedan instalar malware. Puede ignorar las solicitudes no deseadas de abrir archivos adjuntos o archivos individuales, o bien verificar de manera independiente que la supuesta fuente efectivamente le envió el mensaje de correo electrónico (haciendo uso de una dirección de correo electrónico o un número de teléfono publicado). "Incluso si el archivo adjunto procede de una persona que usted conozca, analice si verdaderamente necesita abrirlo, en especial si el mensaje de correo electrónico tiene un aspecto sospechoso", agregó Benardo.

Instale un buen software antivirus que se ejecute periódicamente para buscar y eliminar malware. Asegúrese de configurar el software para que se actualice automáticamente y realice análisis en busca del malware más reciente.

Sea diligente en cuanto al uso de filtros de spam (correo no deseado) que proporcione su proveedor de correo electrónico. Estos servicios ayudan a bloquear los correos electrónicos masivos que podrían contener malware y evitar que lleguen a su bandeja de entrada.

No visite sitios web poco confiables y no crea en todo lo que lee. Los delincuentes pueden crear sitios web falsos y ventanas emergentes con mensajes atractivos que tienen como fin captar su atención y hacer que descargue malware. "Cualquier persona puede publicar información en línea, por lo que antes de aceptar una declaración como un hecho o tomar una medida, verifique que la fuente sea confiable", advierte Amber Holmes, especialista en información de delitos financieros de la FDIC. "Y por favor, no haga clic en un enlace para obtener más información. Si algo parece muy bueno para ser verdad muy probablemente sea fraudulento o dañino".

Tenga cuidado si alguien (incluso si se trata de un amigo o un familiar con buenas intenciones) le entrega un disco o un aparato de memoria para que lo inserte en su computadora. Puede contener malware oculto. "No acceda a un disco ni a un aparato de memoria sin primero analizarlo con su software de seguridad", afirmó Holmes. "Si todavía no está seguro, no se arriesgue".

Para obtener más información sobre cómo protegerse contra el malware, visite https://www.alertaenlinea.gov/articulos/s0011-software-malicioso

Tenga cuidado de las estafas de phishing: no muerda el anzuelo

A los ladrones de identidad les gusta el "phishing" (palabra que se pronuncia "fishing") por Internet y apropiarse de la información financiera personal de los consumidores mediante correos electrónicos y sitios web falsos para engañar a las personas de modo que brinden sus números de Seguro Social, cuentas bancarias y demás detalles valiosos.

Habitualmente, los mensajes de correo electrónico más comunes de phishing simulan proceder de un banco, una tienda minorista o un organismo gubernamental para atraerlo y hacer que divulgue su información financiera personal, y con frecuencia, emplean una variedad de engaños para que el mensaje de correo electrónico tenga un aspecto legítimo. Cabe la posibilidad de que incluyan un gráfico copiado del sitio web de un banco o un enlace que parezcan dirigirse al sitio web de un banco, pero que en realidad conduce a un sitio falso.

También tenga cuidado del "pharming". En esta versión del robo de identidad en línea, un pirata informático secuestra el tráfico de Internet de modo que cuando usted escribe la dirección de un sitio web legítimo, es conducido a un sitio falso. Si introduce información personal en el sitio ficticio, esta es recolectada y usada para cometer fraude o se la vende a otros ladrones de identidad. A continuación se incluyen algunas sugerencias para evitar ser víctima de una estafa por phishing o pharming.

Sospeche si alguien se comunica con usted de manera imprevista por Internet y le solicita información personal. No importa qué tan legítimo pueda parecer el mensaje de correo electrónico o el sitio web. Abra únicamente correos electrónicos que parezcan proceder de personas u organizaciones que usted conozca e incluso en ese caso, tenga cuidado si tienen un aspecto cuestionable.

Por ejemplo, los estafadores pueden acceder a la cuenta de correo electrónico de una persona y enviar mensajes falsos a amigos y parientes, tal vez manifestando que el verdadero titular de la cuenta está varado en el exterior y podría necesitar la información de su tarjeta de crédito para regresar a casa.

Desconfíe especialmente de los mensajes de correo electrónico o los sitios web que tengan errores de ortografía y otros errores obvios. "Debido a que algunas solicitudes provienen de personas que principalmente hablan otro idioma,

continúa en la página siguiente

Uso de sitios de relaciones sociales: tenga cuidado con lo que comparte

Muchas personas usan sitios de redes sociales (por ejemplo, Facebook, LinkedIn, Twitter, Google+ e Instagram) para permanecer en contacto con familiares y amigos, conocer nuevas personas e interactuar con empresas, como su banco. No obstante, los ladrones de identidad pueden usar los sitios de redes sociales con la esperanza de obtener suficiente información sobre las personas a fin de poder descubrir contraseñas, acceder a cuentas financieras o cometer robo de identidad.

Los ladrones de identidad crean perfiles falsos en redes sociales fingiendo ser instituciones financieras y demás empresas y luego, atraen a los visitantes incautos para que proporcionen sus números de Seguro Social, números de cuentas bancarias y demás información personal valiosa. Los ladrones de identidad también han creado perfiles fraudulentos y luego, enviado comunicaciones elaboradas para persuadir a "amigos" a que envíen dinero o divulguen información personal. "Pueden manifestar que trabajan en la misma organización, que han asistido a la misma escuela o que comparten intereses y pasatiempos similares", afirmó Susan Boenau, gerente de la Sección de Asuntos de Consumidores de la FDIC. "Saben que comunicar una sensación falsa de confianza puede ser sencillo en una red social".

"Entre los datos que son valiosos para alguien que busca robar su identidad se incluyen, por ejemplo, el nombre de soltera de la madre, la fecha o lugar de nacimiento, la mascota de la escuela secundaria o el nombre de la propia mascota", explicó Amber Holmes, especialista en información de delitos financieros de la FDIC. "Los artistas del fraude usan los sitios de relaciones sociales para recopilar este tipo de información porque pueden ayudarlos a descubrir las contraseñas de cuentas en línea o las respuestas de 'preguntas de seguridad' que los bancos y demás empresas usan con frecuencia para realizar un segundo nivel de autenticación además de una contraseña. Alguien que tenga su contraseña y pueda responder satisfactoriamente a las preguntas de seguridad puede ser capaz de acceder a sus cuentas, transferir dinero o incluso reestablecer contraseñas y usar una opción que ellos conozcan y usted no".

¿Qué medidas de seguridad puede tomar con su cuenta de red social?

Compruebe la configuración de seguridad de los sitios de redes sociales. Asegúrese de que bloqueen a las personas que usted no desea que vean su página. Si tiene dudas sobre la configuración de seguridad, evite incluir información como su cumpleaños o el año en que se graduó de la universidad. Sin embargo, los expertos dicen que está bien proporcionar ese tipo de información en las páginas de redes sociales.

Tome precauciones al comunicarse con el banco. Si quiere comunicarse con su banco por una red social, tenga en cuenta que sus publicaciones podrían volverse públicas, aunque puede protegerlas hasta cierto punto con la configuración de la cuenta. No debe incluir ninguna información personal, confidencial ni de la cuenta en sus publicaciones. "Además, las redes sociales de buena reputación no le pedirán sus números de seguro social, tarjeta de crédito o tarjeta de débito o sus contraseñas de la cuenta bancaria", dijo el abogado de la FDIC, Richard Schwartz.

Antes de publicar información como fotografías y comentarios, debe buscar un enlace que rece "privacidad" o "políticas" para enterarse sobre qué puede ser compartido por el banco o la red social de este con otras partes, incluidas empresas que quieran enviarle mensajes de correo electrónico de marketing. Lea lo que dicen las políticas sobre si el banco mantendrá segura la información personal, y cómo lo hará. Descubra qué opciones puede tener para limitar la divulgación de su información.

Resulta un buen principio rector evitar publicar información personal en cualquier parte del sitio de red social de un banco. "Los bancos solicitan a menudo esa clase de información para las preguntas de seguridad que se utilizan para controlar el acceso a las cuentas", comentó Schwartz. "Un delincuente puede usar esa información para iniciar una sesión en su cuenta".

Tenga cuidado al otorgar a programas o aplicaciones de terceros, por ejemplo, sitios de juegos o cuestionarios, la posibilidad de usar información de las páginas de sus relaciones sociales. "Algunos de estos terceros pueden emplear la información de la página para ayudarlo a conectarse con otras personas o crear su red, por ejemplo, emparejarlo con extraños que desean jugar el mismo juego", afirmó Boenau. "Pero también podrían vender su información a sitios de marketing y demás sitios, y posiblemente incluso a personas que podrían usarla para cometer fraude".

Realice búsquedas periódicas para corroborar si alguien ha creado una cuenta falsa con su nombre o información personal en un sitio de relaciones sociales. Corroborar en los motores de búsquedas más habituales si figura su nombre y palabras clave o frases (por ejemplo, su dirección y cargo) puede mostrar evidencia de que una persona usa su información de una manera deshonesta.

Para obtener más sugerencias para evitar fraudes en las redes sociales, visite el Centro de Denuncias de Delitos en el Internet en www.ic3.gov/media/2009/091001.aspx.

Estafas de phishing

continuación de la página anterior

a menudo contienen una gramática o una ortografía precarias", afirmó Amber Holmes, especialista en información de delitos financieros de la FDIC.

Recuerde que ninguna institución financiera le enviará un mensaje de correo electrónico y le pedirá que incluya información confidencial como números de cuenta y PIN en su respuesta. De hecho, la mayoría de las instituciones publicita que nunca pedirán información personal del cliente por teléfono ni en un correo electrónico porque ya cuentan con ella.

Debe suponer que una solicitud de información procedente de un banco en el cual usted nunca abrió una cuenta probablemente sea una estafa. No siga el enlace ni introduzca su información personal.

Verifique la validez de un correo electrónico o un cuadro emergente de aspecto sospechoso antes de brindar información personal. Los delincuentes pueden crear correos electrónicos que indiquen que "usted es víctima de fraude" o un cuadro emergente con otro mensaje de carácter urgente para engañar a las personas para que proporcionen información o instalen malware (software malintencionado). Si desea corroborar algo, comuníquese de forma independiente con la supuesta fuente (tal vez un banco o una organización) usando la dirección de correo electrónico o el número de teléfono que sepa que son válidos.

Para obtener más sugerencias, consulte la página de OnGuardOnline del gobierno federal en https://www.alertaenlinea.gov/articulos/s0003-phishing.

Para padres y cuidadores: sugerencias para proteger la información personal de su hijo

Parte de la construcción de una base sólida del futuro financiero de un niño es tomar medidas para minimizar el riesgo de robo de su número de Seguro Social, los detalles de su cuenta bancaria u otra información personal valiosa. A continuación se incluyen sugerencias para ayudar a los padres y los cuidadores a proteger a los jóvenes del fraude financiero y del robo de identidad relacionado con actividades cibernéticas.

Hable con su hijo acerca de prácticas seguras en el Internet. Considere analizar los riesgos de compartir información personal en línea, lo cual incluye la posibilidad de que alguien pueda recoger pequeñas cantidades de información personal para adivinar las respuestas correctas de preguntas de seguridad, reestablecer contraseñas y tomar el control de cuentas financieras.

"Recomiende al joven que sea selectivo con sus 'amistades' en línea, tanto como lo sería en la vida real", afirmó Bobbie Gray, especialista supervisor en asuntos comunitarios de la FDIC. "Analice de qué forma no todo lo que ven en el Internet es verdadero y que algunos delincuentes pueden fingir ser amigos o parientes a fin de obtener información personal o algo peor".

Considere acordar una lista corta de lo que su hijo puede y no puede hacer en el Internet. Para obtener más información, lea nuestros consejos para jóvenes adultos en las **FDIC Consumer News** de otoño de 2012 (www.fdic.gov/consumers/consumer/news/cnfall12/avoidfraud.html).

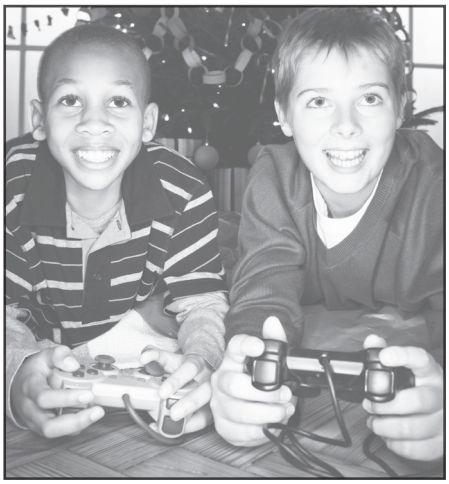
Ayude a su hijo a que aprenda a analizar las publicidades, algunas de las cuales pueden ser fraudulentas. "Explique que las publicidades, incluso en un videoclip en línea, tienen como fin lograr que las personas compren o hagan cosas que habitualmente no harían", manifestó Luke W. Reynolds, jefe de la Sección de Desarrollo de Programas y Extensión de la FDIC. La Comisión Federal de Comercio (FTC, por sus siglas en inglés) cuenta con un juego en línea llamado "Admongo" (www.admongo.gov) para ayudar a los jóvenes de entre 8 y 12 años de edad a pensar críticamente acerca de las publicidades y tomar decisiones más inteligentes como consumidores.

Explique por qué tener dinero en una institución financiera es seguro. Las cuentas corrientes, de ahorro u otras cuentas de depósito que se encuentren en instituciones financieras aseguradas por el gobierno federal ofrecen protecciones vinculadas con el robo y el fraude (consulte la página 8), lo cual las hace un lugar seguro para su dinero. Si su hijo aún no tiene una cuenta de depósito, considere abrirle una. Obtenga información sobre el seguro federal de depósitos si quiebra un banco, lo que incluye cómo verificar que un banco está asegurado por la FDIC, visitando www.fdic.gov/deposit. Y para buscar información adecuada según la edad y actividades para los niños más las guías "Money Smart" de la FDIC que ayuden a los padres y los cuidadores a hablar con sus hijos sobre temas financieros clave, visite un sitio web desarrollado en inglés por la FDIC y la Oficina de Protección Financiera de Consumidores que se encuentra en www.consumerfinance.gov/parents.

Proteja los equipos electrónicos. Asegúrese de que los aparatos de su hijo estén configurados para descargar las actualizaciones más recientes del fabricante, ya que habitualmente incluyen mejoras relacionadas con la seguridad. Casi todos los equipos de videojuegos se conectan con el Internet y pueden vincularse con información tales como números de tarjetas de crédito o débito.

Si una empresa desea recopilar datos sobre su hijo, averigüe por qué. Controlar el acceso a la información de un niño es una de las mejores formas para protegerlo contra el robo de identidad. De conformidad con una ley Federal denominada Ley de Protección de la Privacidad en Línea de los Niños (COPPA, por sus siglas en inglés), los sitios web y los servicios en línea (incluidas las aplicaciones) que están dirigidos a niños menores de 13 años de edad deben notificar directamente a los padres y obtener su aprobación antes de recopilar, usar o divulgar la información personal de un niño. Al notificarle, la empresa debe divulgar de qué forma planea usar la información de su hijo. Es posible que la empresa también pida su aprobación de diferentes opciones para usar la información que desea recabar, por ejemplo, si la puede compartir con otras personas o usarla con fines de marketing. Para obtener más información, comience por la página web de la FTC, denominada "Cómo proteger la privacidad en línea de su hijo" (www.consumer.ftc.gov/ articles/0031-protecting-your-childs-privacy-online).

Esté atento ante posibles signos de que un niño sea víctima de robo de identidad. Los delincuentes pueden robar la identidad de niños para presentar reclamos para recibir beneficios del gobierno o postularse para un préstamo en línea. "Si bien no necesariamente constituye un signo de robo de identidad, el hecho de que su hijo reciba correos o llamadas telefónicas no solicitadas de vendedores puede indicar que de alguna manera se compartió su información



personal. Resulta más adecuado tomarse el tiempo para comprender por qué", puntualizó Reynolds.

Considere consultar a las tres agencias nacionales de informes de crédito más importantes: Equifax, Experian y TransUnion, para corroborar si su hijo menor de edad cuenta con un informe crediticio. Si la respuesta es "sí", revise el informe para determinar si un ladrón ha usado ilegalmente el nombre del niño. Para obtener pautas adicionales, visite la página "Robo de identidad de menores" de la FTC (www.consumer.ftc.gov/articles/0040-child-identity-theft#credit), donde figura información de contacto de las agencias de informes de crédito y sugerencias en caso de que la identidad de un niño haya sido robada, lo cual incluye cómo generar una alerta de fraude en un informe crediticio que pueda minimizar daños en el futuro.

La FTC agrega que en general es una buena idea que los padres realicen esta revisión de los informes crediticios antes de que el niño cumpla los 16 años. Hacerlo permite contar con tiempo para resolver errores u otros problemas antes de que este solicite un préstamo o un empleo.

Para obtener más información y sugerencias sobre cómo proteger a los niños en Internet, visite el sitio web del gobierno federal OnGuardOnline en https://www.alertaenlinea.gov/temas/proteja-a-los-ni%C3%B1os-en-internet. La FDIC también tiene en inglés guías Money Smart que ofrecen ejercicios, actividades e introducciones de conversaciones para padres y cuidadores, con el fin de ayudar a los jóvenes de todas las edades a aprender acerca del dinero (https://catalog.fdic.gov/store/youth).

De qué forma las leyes federales y las prácticas de la industria limitan las pérdidas producto de los ataques cibernéticos

Cuando los delincuentes realizan compras no autorizadas haciendo uso de números de tarjetas de pago robadas u otra información, las leyes federales para consumidores y las prácticas financieras de la industria protegen a las víctimas de pérdidas en determinadas circunstancias. A continuación se incluyen los detalles clave que se deben recordar.

Si ladrones cibernéticos obtienen acceso al número de su tarjeta de crédito: "De conformidad con la ley federal, la responsabilidad de un consumidor normalmente llega un máximo de $50 en el caso de todas las transacciones no autorizadas de cada tarjeta. No obstante, si su número de tarjeta de crédito es robado, pero no la tarjeta, usted no es responsable de ningún uso no autorizado", afirmó Richard Schwartz, abogado en la Sección de Cumplimiento al Consumidor de la FDIC. "Además, normalmente el emisor de la tarjeta de crédito absorbe las pérdidas de las tarjetas de crédito a raíz de las políticas de cero responsabilidad, las cuales impiden que los consumidores tengan que pagar algún monto por un cargo no autorizado. Estas políticas son fijadas por la industria de tarjetas".

Si se usa su tarjeta de débito o el número de la tarjeta para retirar dinero de una cuenta corriente o de ahorro: Para minimizar sus pérdidas, debe comunicarse con su banco tan pronto resulte posible si descubre que su *tarjeta* de débito se ha extraviado o ha sido robada. Su responsabilidad máxima de conformidad con la ley federal es de $50 si notifica al banco en el plazo de dos días hábiles luego de tomar conocimiento de la pérdida o el robo de la tarjeta. Pero si informa al banco luego de transcurridos esos dos primeros días, según la ley podría perder más dinero.

¿Qué sucede si le roban el *número* de su tarjeta de débito (no la tarjeta en sí) en un incidente de piratería en línea? Recuerde verificar la actividad de su cuenta de manera regular. El tiempo resulta esencial porque según la ley federal usted no será responsable de la transacción si la informa en el plazo de 60 días posteriores a que se le envíe el resumen de cuenta donde conste la transacción. Pero si no se informa el cargo durante más de 60 días, podría perderse todo el dinero de la cuenta. Sin embargo, recuerde consultar a su banco acerca de la política de cero responsabilidad de las redes de tarjetas de pago, las cuales pueden protegerlo.

Si posee una tarjeta de débito para una cuenta de negocios que se usa de manera fraudulenta: Las tarjetas de débito emitidas para usos de negocios cuentan con protecciones ante pérdidas diferentes de las tarjetas de débito para consumidores. El Código de Comercio Unificado (UCC, por sus siglas en inglés), que establece muchas normas para los negocios, exige un estándar de "atención ordinaria" por parte del titular de la tarjeta a fin de evitar responsabilidades en caso de pérdidas producto de fraudes en línea. "Esto puede ser un área técnica, por lo que debe consultar a un abogado para asegurarse de que gestiona su cuenta de negocios de conformidad con las normas del UCC", sugirió Schwartz.

Si la cuenta de tarjeta prepaga se usa de forma fraudulenta: En las tarjetas prepagas, hay dinero depositado y estas habitualmente no están relacionadas con una cuenta corriente ni de ahorro. En términos de protecciones legales contra pérdidas como resultado del fraude, las normas varían de acuerdo con el tipo de tarjeta prepaga:

- Las tarjetas prepagas usadas por empleadores para pagar a sus empleados están cubiertas por las mismas leyes que se describen anteriormente para las tarjetas de débito de consumidores.
- Las tarjetas prepagas "recargables" para fines generales, que muestran una marca de red como American Express, Discover, MasterCard o Visa, actualmente no cuentan con protecciones que limiten la responsabilidad de conformidad con la ley federal pero, en la mayoría de los casos, incluyen en sus contratos con los clientes las mismas protecciones que aquellas correspondientes a las tarjetas de débito de consumidores. Sin embargo, en cuanto a la responsabilidad de pérdidas, la Oficina para la Proteccion Financiera del Consumidor (CFPB, por sus siglas en inglés) en noviembre de 2014 propuso una norma que incluyera a las tarjetas prepagas recargables bajo el amparo de la ley federal para tarjetas de débito de consumidores. Visite el sitio web de la CFPB en www. consumerfinance. gov para obtener actualizaciones.
- Las tarjetas prepagas de regalo para compras en tiendas normalmente no están registradas y, por ende, no están sujetas a derechos y protecciones federales de responsabilidad para los consumidores. Además, los emisores de tarjetas prepagas de obsequio generalmente no brindan a los titulares de tarjetas su propia cobertura de responsabilidad ante fraudes. "Si pierde su tarjeta de regalo, probablemente perderá el valor completo de ella", afirmó Schwartz.

Para obtener más información sobre las limitaciones de pérdidas según la ley, realice una búsqueda por temas en los sitios web de la CFPB y la Comision Federal de Comercio (FTC, por sus siglas en inglés) (https://www.ftc.gov/es). También debe tener en cuenta que el seguro de depósitos de la FDIC únicamente cubre los depósitos si un banco entra en quiebra y no en el caso de robos de cuentas bancarias (consulte a continuación). Para obtener información sobre cómo protegerse de la filtración de datos, que puede incluir el robo de la información de una tarjeta de crédito o de débito, consulte edición número de primavera de 2014 en inglés (www.fdic.gov/consumers/consumer/news/cnspr14/databreach.html).

Estimada FDIC: Preguntas sobre el seguro de depósitos y los servicios bancarios en línea

Aparentemente algunas instituciones financieras aseguradas por la FDIC pagan tasas de interés superiores en las cuentas de depósito que se abren en línea. Me gustaría aprovechar estas tasas de interés pero nunca realicé operaciones bancarias por Internet. ¿Puede una cuenta en línea estar asegurada por la FDIC? De ser así, ¿me ayudaría el seguro de la FDIC si se produjera un robo u otro problema con una transacción en línea?

La mayoría de los bancos ofrece cuentas de depósito en sus sucursales así como también en línea, y otros únicamente operan por Internet, es decir, no cuentan con oficinas físicas en las que el público pueda abrir cuentas o realizar otras transacciones de negocios. En respuesta a su primera pregunta, las cuentas de depósito que se abran en línea en cualquier banco asegurado por la FDIC estarán cubiertas por el seguro de la FDIC hasta los límites federales. "La cobertura del seguro de depósitos es la misma para los bancos que únicamente operan en línea que para los bancos de ladrillo y cemento", afirmó Calvin Troup, especialista sénior en asuntos de consumidores de la FDIC.

El aspecto más importante que se debe confirmar antes de trabajar con un banco en línea consiste en garantizar que sea legítimo y que no se encuentre en un sitio web ficticio. Un banco puede tener un nombre que use para sus operaciones tradicionales y otro diferente ("nombre comercial") que emplee para el marketing en línea. Puede comunicarse con el número gratuito de la FDIC y solicitar hablar con un especialista en seguros de depósitos, quien lo ayudará a confirmar si el banco en línea en cuestión está asegurado por la FDIC. La herramienta en línea BankFind (en inglés) de la FDIC que se encuentra en https://research.fdic.gov/bankfind también ofrece información útil, por ejemplo, ubicaciones de las sedes e información financiera, correspondiente a todas las instituciones de depósitos aseguradas por la FDIC.

Continúa en la última página

Ciberseguridad para las pequeñas empresas: formas de mantenerse protegido

En el mundo actual, es importante que los propietarios de las pequeñas empresas vigilen la protección de sus datos y sus sistemas de computación. Entre otros motivos: Las protecciones federales para consumidores generalmente no cubren a las empresas en caso de pérdidas producidas a partir de transferencias electrónicas de fondos no autorizadas. Eso significa, por ejemplo, que su banco puede no ser responsable del reembolso de pérdidas relacionadas con un robo electrónico de su cuenta bancaria, es decir, si se produjo negligencia por parte de su empresa, tales como computadoras no protegidas o ser víctima de estafas comunes. (Para obtener más información sobre las normas que corresponden al robo electrónico, incluidas las pérdidas de una tarjeta de débito de negocios, consulte la página anterior).

A continuación se incluyen sugerencias para ayudar a los propietarios de pequeñas empresas a protegerse y a proteger a sus empresas de pérdidas y otros daños. Varias de estas sugerencias reflejan precauciones básicas que hemos recomendado a los consumidores en otras secciones de esta edición.

Proteja a las computadoras y las redes de Wi-Fi. Instale software antivirus y cortafuegos (programas que bloquean el acceso no deseado) en sus computadoras y manténgalos actualizados. Programe el software de seguridad clave para que se actualice automáticamente, si es posible. Y si para su lugar de trabajo tiene una red de Wi-Fi, cerciórese de que sea segura, lo cual incluye proteger el enrutador mediante una contraseña que usted establezca (no la contraseña predeterminada). El manual de usuario de su aparato puede brindarle instrucciones, que en general también están disponibles en Internet.

Aplique revisiones al software de manera oportuna. Los proveedores de software habitualmente ofrecen "revisiones" o actualizaciones de sus productos para corregir fallas de seguridad y mejorar la funcionalidad. Una buena práctica consiste en descargar e instalar estas actualizaciones de software tan pronto como se encuentren disponibles. Puede resultar más eficaz configurar el software para instalar automáticamente dichas actualizaciones.

Establezca procedimientos y capacitación sobre ciberseguridad para los empleados. Considere reducir riesgos a través de medidas tales como revisiones de antecedentes previas al empleo y políticas claramente delineadas respecto del uso personal de las computadoras. Limite el acceso de los empleados a los sistemas de datos que necesiten para sus trabajos y exija permiso para instalar cualquier software. Además, capacite a los empleados sobre temas de ciberseguridad, por ejemplo, correos electrónicos sospechosos o no deseados que indiquen que se haga clic en un enlace, se abra un archivo adjunto o se proporcione información de cuentas. Al cumplir con lo que parece una simple petición, los empleados pueden estar instalando malware en su red. Puede usar recursos de capacitación tales como un curso en línea de 30 minutos de la Agencia Federal para el Desarrollo de la Pequeña Empresa (SBA, por sus siglas en inglés) en www.sba.gov/ tools/sba-learning-center/training/cybersecurity-small-businesses.

Exija una autenticación compleja. Asegúrese de que los empleados y demás usuarios que se conecten a su red empleen contraseñas e identificaciones de usuario complejas para las computadoras, los aparatos móviles y las cuentas en línea aplicando combinaciones de mayúsculas y minúsculas, números y símbolos que sean difíciles de adivinar y se cambien con habitualidad. Considere exigir más información además de una contraseña para obtener acceso a su red de negocios, así como medidas de seguridad adicionales, tales como exigir llamadas de confirmación a su institución financiera antes de que se autoricen determinadas transferencias electrónicas.

Proteja a las tabletas y los smartphones del negocio. Los aparatos móviles pueden ser el origen de problemas de seguridad, en especial si contienen información confidencial o pueden acceder a la red de su empresa. En cuanto a lo último, exija que los empleados protejan mediante contraseña sus aparatos, cifren sus datos e instalen aplicaciones de seguridad para evitar que los delincuentes obtengan acceso al aparato mientras esté conectado a redes públicas. Además desarrolle y aplique procedimientos de informes en caso de equipos perdidos o robados.

Realice copias de seguridad de sistemas y datos de negocios importantes. Hágalo al menos una vez por semana. Para realizar copias de seguridad de sus datos, recuerde usar las mismas medidas de seguridad (por ejemplo, la encriptación) que aplicaría a los datos originales. Además, en caso de que se infecte su computadora principal, realice copias de seguridad de los datos confidenciales de negocios de forma regular en aparatos de almacenamiento adicionales que no estén conectados.

Aplique las mejores prácticas para procesar los pagos de tarjetas en línea. Procure el asesoramiento de su banco o de un procesador de pagos para seleccionar las herramientas y los servicios contra el fraude de mayor confianza y más validados. Esto puede incluir el uso de una sola computadora o tableta para el procesamiento de pagos.

Manténgase atento a signos tempranos de que algo funciona mal. "Controle con regularidad los saldos de las cuentas bancarias en busca de actividad sospechosa o no autorizada", sugirió Luke W. Reynolds, director de la Sección de Desarrollo de Programas y Extensión de la FDIC.

Se pueden encontrar (en inglés) sugerencias sobre ciberseguridad para pequeñas empresas en un nuevo folleto de la FDIC en fdic.gov/consumers/assistance/protection/brochures/CyberBusiness.pdf. También visite (en inglés) OnGuardOnline (www.onguardonline.gov/features/feature-0007-featured-info-small-business) y el sitio web de la SBA (www.sba.gov/content/top-ten-cybersecurity-tips). 🏛

Adopción de servicios móviles

continuación de la página 4

o el original (si lo recupera). Una variedad de aplicaciones reconocidas puede permitir la eliminación remota.

Para obtener más información sobre cómo usar de manera segura smartphones y tabletas, consulte la sección "Aparatos" de la página web de Seguridad de Computadoras de la Comision Federal de Comercio (FTC, por sus siglas en inglés) en www.consumer.ftc.gov/topics/computer-security. 🏛

Pruebe su conocimiento en ciberseguridad

Responda nuestro cuestionario, que tiene como base la información que consta en esta guía especial

1 **Una buena contraseña para usar al iniciar su sesión en el sitio web de servicios bancarios en líneas es:**

a) 123456789
b) Contraseña
c) 1Banana+1Piña
d) Ninguna de las anteriores

2 **Siempre resulta seguro emplear su computadora portátil u otro aparato móvil para obtener acceso al sitio de servicios bancarios en línea desde una cafetería, un aeropuerto u otro lugar público que fomente el uso de su red de Wi-Fi. ¿Verdadero o Falso?**

a) Verdadero
b) Falso

3 **En caso de que su tableta o smartphone sea robado o se extravíe, ¿cuáles de las siguientes precauciones *NO* constituiría una buena forma de restringir el acceso al aparato y los datos que se encuentren en él?**

a) Usar una contraseña para restringir el acceso.
b) Agregar una función de "bloqueo automático" que proteja al aparato cuando no se use durante una cierta cantidad de minutos.
c) Agregar un sistema de rastreo de GPS para el aparato móvil.
d) Descargar una aplicación que le permita eliminar de manera remota los datos del aparato.

4 **Los padres y custodios legal deben asegurarse de que los aparatos que usen sus hijos cuenten con las actualizaciones de seguridad más recientes del fabricante del software. ¿Cuáles de los siguientes equipos debe tener las actualizaciones de seguridad más recientes?**
(Seleccione todas las opciones que correspondan).

a. Computadoras
b. Tabletas
c. Smartphones
d. Aparatos de videojuegos
e. Todo lo anterior

5 **Usted recibe un correo electrónico donde se le ofrece la participación gratuita a un sorteo por un millón de dólares si hace clic en un enlace que lo conducirá al formulario de registro. Es seguro que usted:**

a) haga clic en el enlace pero no descargue el archivo adjunto (el supuesto formulario de registro).
b) elimine el correo electrónico sin hacer clic en el enlace.
c) realice cualquiera de las opciones anteriores.

6 **Nunca incluya su cumpleaños en páginas de redes sociales. ¿Verdadero o Falso?**

a) Verdadero
b) Falso

7 **El seguro de depósitos de la FDIC no protegerá mis depósitos en caso de que por Internet (u otro medio) un ladrón tome el dinero de mi cuenta. ¿Verdadero o Falso?**

a) Verdadero
b) Falso

8 **Si un ladrón emplea una de sus tarjetas de débito para pequeñas empresas con el fin de llevar a cabo compras fraudulentas en línea, las protecciones con las que cuenta contra la pérdida producto de ataques cibernéticos son las mismas que aquellas de su tarjeta de débito personal. ¿Verdadero o Falso?**

a) Verdadero
b) Falso

Las respuestas se muestran invertidas a la derecha.

1. (c) Los expertos recomiendan que cree contraseñas e identificaciones de usuario "complejas" para sus computadoras, aparatos móviles y cuentas en línea aplicando combinaciones de mayúsculas y minúsculas, números y símbolos que sean difíciles de adivinar. En nuestro ejemplo, "1Banana+1Piña" sería una buena contraseña ya que para usted resultaría sencillo recordarla y para otras personas, difícil de adivinar. También debe cambiar sus contraseñas de manera regular. (Consulte la página 2).

2. (b) Falso. No todas las redes de Wi-Fi públicas están actualizadas con las precauciones antivirus y demás precauciones de seguridad que evitarían que los ladrones cibernéticos roben información que se pudiera usar para cometer delitos. En cuestiones confidenciales tales como servicios bancarios en línea, tenga en cuenta únicamente obtener acceso a Internet mediante su propia computadora a través de una conexión segura y de confianza, y conectar las computadoras portátiles y los aparatos móviles únicamente a redes confiables. (Consulte la página 3).

3. (c) Las contraseñas y las funciones de bloqueo automático y eliminación remota son buenos métodos para evitar que un delincuente acceda a su aparato y sus datos. Es además una buena idea realizar copias de seguridad de sus datos en caso de no recuperar su aparato. Si bien puede agregar un rastreador de GPS a una tableta o un smartphone para poder localizar y recuperar el aparato, esto no evitará que un ladrón acceda a números de cuenta y demás datos de importancia. (Consulte las páginas 2 y 4).

4. (e) Cualquier aparato que se pueda conectar al Internet, incluidos las actualizaciones de seguridad. (Consulte la página 7).

5. (b) Elimine el correo electrónico sin hacer clic en el enlace ni abrir el archivo adjunto, que puede contener "malware" (software malintencionado) que un delincuente puede usar para controlar las pulsaciones de teclas, conocer su información de servicios bancarios en línea y transferir dinero de su cuenta. Tan solo hacer clic en el enlace puede resultar suficiente para descargar malware en su computadora. (Consulte la página 5).

6. (b) Falso. Si bien los ciberdelincuentes pueden usar datos tales como su cumpleaños o el lugar en el que nació para poder descubrir contraseñas de cuentas en línea, los expertos dicen que está bien proporcionar ese tipo de información en las páginas de redes sociales pero únicamente si estableció los parámetros de seguridad para evitar que los desconocidos (especialmente los delincuentes) vean estos detalles. (Consulte la página 6).

7. (a) Verdadero. El seguro de depósito de la FDIC únicamente protegé los depósitos si una institución asegurada por la FDIC entra en quiebra; sin embargo, no cubre los robos de las cuentas. No obstante, otras leyes federales para consumidores y prácticas financieras de la industria pueden proteger a las víctimas de robo de pérdidas, en especial si han prestado atención a la actividad de su cuenta. (Consulte la página 8).

8. (b) Falso. Las tarjetas de débito emitidas para usos de negocios se encuentran amparadas por protecciones ante pérdidas diferentes de las tarjetas de débito para consumidores. Las tarjetas de débito para negocios se encuentran cubiertas por el Código de Comercio Unificado (UCC, por sus siglas en inglés), que establece muchas normas para los negocios. (Consulte la página 8).

Lista de comprobación para ciberseguridad

Recordatorios sobre 10 cosas simples que los clientes de bancos pueden hacer para proteger a sus computadoras y su dinero de los delincuentes en línea

1. Tenga programas de seguridad para computadoras que se ejecuten y actualicen regularmente y que busquen las amenazas más recientes. Instale software antivirus para protegerse de malware (software malintencionado) que pueda robar información como números de cuenta y contraseñas, y use un cortafuegos para evitar el acceso no autorizado a su computadora.

2. Sea inteligente respecto a dónde y cómo se conecta al Internet para realizar operaciones bancarias u otras comunicaciones en las que intervenga información personal confidencial. Las redes públicas de Wi-Fi y las computadoras en lugares como bibliotecas o salones de negocios de hoteles pueden resultar riesgosas si no poseen software de seguridad actualizado.

3. Conozca las funciones a seguridad estándar del Internet. Por ejemplo, al realizar operaciones bancarias o compras en línea, busque el símbolo de candado en la página (esto significa que es segura) y "https://" al comienzo de la dirección web (lo que indica que el sitio web es auténtico y cifra datos durante la transmisión).

4. Ignore los correos electrónicos no deseados que le piden que abra un archivo adjunto o que haga clic en un enlace si no está seguro de quién lo envió en realidad y por qué. Los ciberdelincuentes son buenos para elaborar mensajes de correo electrónico falsos que parezcan legítimos pero pueden instalar malware. La mejor opción es ignorar las solicitudes no deseadas de abrir archivos adjuntos o archivos individuales, o bien verificar de manera independiente que la supuesta fuente efectivamente le envió el mensaje de correo electrónico poniéndose en contacto a través de una dirección de correo electrónico o un número de teléfono publicado.

5. Sospeche si alguien se comunica con usted de manera imprevista por el Internet y le solicita información personal. Una estrategia segura consiste en ignorar las solicitudes no deseadas de información, independientemente de qué tan legítimas parezcan, en especial si piden información como su número de Seguro Social, números de cuentas bancarias y contraseñas.

6. Emplee el proceso más seguro que tenga a su disposición cuando inicie sesión en cuentas financieras. Cree contraseñas "complejas" que sean difíciles de adivinar, cámbielas con regularidad e intente no usar las mismas contraseñas o PIN (números de identificación personal) para varias cuentas.

7. Sea discreto al usar sitios de relaciones sociales. Los delincuentes rastrillan esos sitios en busca de información como el lugar de nacimiento de una persona, el nombre de soltera de la madre o el nombre de una mascota, en caso de que dichos datos puedan ayudarlos a adivinar o reestablecer contraseñas de cuentas en línea.

8. Tenga cuidado al usar smartphones y tabletas. No deje su aparato móvil sin supervisión y utilice una contraseña en el aparato u otro método para controlar el acceso en caso de que se extravíe o lo roben.

9. Los padres y los cuidadores deben incluir a los niños en su planificación de ciberseguridad. Hable con su hijo acerca de la seguridad en línea, incluidos los riesgos de compartir información personal con personas que no conozcan, y asegúrese de que los aparatos que usen para conectarse al Internet tengan seguridad actualizada.

10. Los propietarios de pequeñas empresas deben contar con políticas y capacitación para sus empleados sobre temas similares a aquellos que se indican en la presente lista de comprobación para clientes, además de otros temas que sean específicos del negocio. Por ejemplo, considere exigir más información además de una contraseña para obtener acceso a su red de negocios, así como medidas de seguridad adicionales, tales como exigir llamadas de confirmación a su institución financiera antes de que se autoricen determinadas transferencias electrónicas.

FDIC
Consumer News

Publicado por la Federal Deposit Insurance Corporation

Martin J. Gruenberg, *presidente*

Barbara Hagenbaugh, *presidente adjunta de Comunicaciones*

David Barr, *asistente del. director*, *Oficina de Comunicaciones (OCOM)*

Jay Rosenstein, *escritor-editor* sénior, *OCOM*

Aileen Wu, *diseñadora gráfica*

FDIC Consumer News es producido trimestralmente por la Oficina de Comunicaciones de la FDIC en cooperación con otras divisiones y oficinas. Se pretende presentar la información de una manera no técnica y no pretende ser una interpretación legal de las regulaciones y políticas gubernamentales o de la FDIC. Debido a los cambios periódicos en los estatutos y reglas de la agencia, siempre verifique el sitio web de la FDIC (www.fdic.gov) para obtener información actualizada. La mención de un producto, servicio o empresa no constituye un aval. Esta publicación puede ser impresa nuevamente en su totalidad o en parte. Por favor, acredite a ***FDIC Consumer News***.

Envíe sus ideas de historias, comentarios y otras sugerencias o preguntas a: Jay Rosenstein, editor, ***FDIC Consumer News,*** 550 17th Street, NW, Washington, DC 20429, correo electrónico jrosenstein@fdic.gov.

Encuentre las ediciones actuales y anteriores en www.fdic.gov/consumernews o solicite copias en papel comunicándose con el Centro de Información Pública de la FDIC. Llame a la línea gratuita 1-877-ASK-FDIC (1-877-275-3342) o envíe un correo electrónico a publicinfo@fdic.gov.

Suscripciones: para recibir una notificación por correo electrónico cada nueva publicación con enlaces a las historias, vaya a www.fdic.gov/about/subscriptions/index.html. Para recibir ***FDIC Consumer News*** en el correo, si cargo, llame o escriba al Centro de Información Pública de la FDIC en la dirección detallada anteriormente.

Para obtener más ayuda o información

Visite www.fdic.gov o bien comuníquese con la FDIC de forma gratuita llamando al 1-877-ASK-FDIC (1-877-275-3342)

Estimada FDIC

continuación de la página 8

En cuanto a la segunda pregunta, por ley, el seguro de depósitos únicamente protege a las cuentas *si la institución bancaria asegurada quiebra*. El seguro de depósitos de la FDIC no protege a las cuentas de fraude ni robos en línea (ni tampoco de ninguna otra situación similar). Sin embargo, otras leyes y prácticas de la industria pueden ofrecer cobertura en caso de robos cibernéticos. Para obtener información, consulte nuestro artículo en la página 8.

"Si tiene preguntas sobre como configurar una cuenta en línea, cerciórese de obtener respuestas antes de realizar depósitos", agregó Troup.

Puede obtener más información sobre la cobertura de seguros de depósitos de la FDIC llamándonos gratuitamente al 1-877-ASK FDIC (1-877-275-3342) o visitando www.fdic.gov/deposit. Las personas sordas o con problemas auditivos deben comunicarse al 1-800-925-4618. 🏛

Para obtener más ayuda o información sobre ciberseguridad

La Federal Deposit Insurance Corporation ofrece sugerencias sobre la seguridad de computadoras e Internet a clientes bancarios, incluidas pequeñas empresas. Visite un nuevo sitio web de la FDIC sobre los aspectos básicos en cuanto al conocimiento de la ciberseguridad en fdic.gov/consumersecurity, que incluye dos folletos nuevos, uno para clientes sobre cómo proteger y mantener sus sistemas de computación, y el otro para los clientes de negocios sobre cómo salvaguardar sus sistemas y datos. También realice búsquedas por temas en ediciones actuales o anteriores de las ***FDIC Consumer News*** trimestrales en www.fdic.gov/consumernews y mire la presentación multimedia "No sea una víctima en Internet: cómo protegerse contra ladrones de Internet y estafas electrónicas" en www.fdic.gov/consumers/consumer/guard.

Otros organismos del gobierno federal también publican información sobre cómo protegerse contra delitos cibernéticos.

• Visite www.OnGuardOnline.gov, el sitio web del gobierno federal para obtener información sobre cómo permanecer seguro en internet, sugerencias generales para los consumidores e información más dirigida a padres, jóvenes y pequeñas empresas.

• Diríjase a la página de seguridad de computadoras para consumidores de la Comision Federal de Comercio (FTC, por sus siglas en inglés) en www.consumer.ftc.gov/topics/computer-security, que ofrece enlaces a videos sobre temas como qué hacer si su correo electrónico es víctima de piratería o si programas de malware atacan su computadora.

• Consulte la página (en inglés) web "Cómo proteger su computadora" de la Oficina Federal de Investigaciones en www.fbi.gov/scams-safety/computer_protect, que incluye enlaces a información más detallada sobre ardides de Internet y cómo protegerse al navegar en línea.

• Consulte el recurso integral del gobierno federal para las víctimas de robo de identidad en www.IdentityTheft.gov, donde se incluyen herramientas en línea para desarrollar un plan de recuperación y generar cartas y formularios completados previamente para enviarlos a oficinas de crédito, la policía y demás entidades que puedan ayudarlo luego de un incidente de robo de identidad. 🏛