

# Alerta de la FTC para Consumidores

Comisión Federal de Comercio ■ Buró de Protección del Consumidor ■ División de Educación del Consumidor y los Negocios

## Quiebras, Fusiones y Adquisiciones de Bancos: El Plato del Día de los “Pescadores de Información”

### Bank Failures, Mergers and Takeovers: A “Phish-erman’s Special”

Si los recientes cambios del mercado financiero lo tienen confundido, usted no está solo. Es posible que la institución financiera con la cual operó la semana pasada hoy tenga un nombre nuevo, y mañana sus cheques y sus resúmenes de cuenta podrían llegar con un diseño o aspecto diferente. Puede que un nuevo prestador haya adquirido su hipoteca, y usted podría estar enviando sus pagos por correo a un nuevo administrador hipotecario. También es probable que hayan cambiado los procedimientos para hacer trámites bancarios en línea. De acuerdo a la Comisión Federal de Comercio (*Federal Trade Commission*, FTC), la agencia nacional de protección del consumidor, la agitación del mercado financiero puede estimular la avidez de los estafadores para salir a la “pesca” de su información personal.

Los pescadores de información o “*phishers*” (que se pronuncia “*fishers*”) pueden enviar mensajes de correo electrónico que requieren su atención y que aparentan provenir de la institución financiera que adquirió recientemente su entidad bancaria, de ahorro y préstamo o hipotecaria. La intención de estos estafadores es recolectar o capturar su información personal, como por ejemplo los números de su tarjeta de crédito, información de su cuenta bancaria, número de Seguro Social, contraseñas u otra información delicada. En el texto de sus mensajes pueden indicarle que “actualice”, “valide” o “confirme” la información de su cuenta. Por ejemplo, puede recibir mensajes parecidos a los siguientes:

*“Recientemente, hemos comprado el Banco ABC. Debido a asuntos concernientes a la seguridad e integridad de nuestros nuevos clientes que operan en línea, hemos emitido este mensaje de advertencia... Por favor, haga clic sobre el enlace electrónico para renovar la información de su cuenta”.*

*“Recientemente, hemos adquirido la hipoteca de su vivienda y estamos en proceso de validar la información de su cuenta. Por favor, haga clic aquí para actualizar y verificar la información”.*

*“Durante la adquisición de la entidad Savings & Loan XYZ, hemos sufrido un incidente de seguridad del sistema informatizado de datos. Sospechamos que se ha efectuado una transacción no autorizada en su cuenta. Para garantizar la seguridad de su cuenta, por favor haga clic en el siguiente enlace electrónico para confirmar su identidad”.*

Los mensajes de este tipo lo dirigen a un sitio Web que aparenta ser el verdadero sitio de su nueva institución financiera o del nuevo prestador. Pero no lo es. Es un sitio Web falso cuyo propósito es persuadirlo engañosamente con el objetivo de que usted divulgue su información personal para que los operadores puedan robarle su identidad y endeudarse o cometer otros delitos usando su nombre.

---

Para ayudarlo a no caer en las redes de una estafa de pesca de la información, la FTC le ofrece las siguientes recomendaciones:

- No responda ningún e-mail ni mensaje *pop-up* que le solicite información personal o financiera, y no haga clic sobre los enlaces incluidos en este tipo de mensaje — aunque aparente provenir de su banco. Tampoco use la función cortar y pegar para copiar el enlace electrónico en la barra de su navegador de Internet. Los “*phishers*” pueden crear enlaces que aparentemente lo llevan a un sitio Web, pero en realidad lo redirigen a otro.
- Algunos estafadores llaman usando un mensaje grabado, o envían un e-mail que simulan provenir de una institución pidiéndole que llame a un número de teléfono para actualizar los datos de su cuenta. Como usan la tecnología de telefonía en Internet o VoIP, el código de área registrado no corresponde al lugar desde el cual realmente lo están llamando. Para comunicarse con la institución con la que opera, llame al número que figura en el resumen de cuenta.
- Use un programa antivirus y *anti-spyware* y también un *firewall*, y actualícelos con regularidad.
- No envíe información financiera ni personal por e-mail. El e-mail no es un sistema seguro para mandar datos delicados.
- Revise los resúmenes de sus cuentas financieras tan pronto como los reciba para controlar si hay algún cargo no autorizado.
- Tenga cuidado al abrir o descargar archivos adjuntados a los mensajes electrónicos recibidos, sea quien sea el remitente. Estos archivos pueden contener virus u otros programas que pueden disminuir el nivel de seguridad de su computadora.
- Reenvíe los mensajes de correo electrónico “*phishing*” a [spam@uce.gov](mailto:spam@uce.gov) — y a la institución o compañía invocada falsamente en el e-mail. También puede reportar este tipo de mensajes a [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org). La organización llamada *Anti-Phishing Working Group*, es un consorcio de Proveedores de Servicio de Internet, vendedores de sistemas de seguridad, instituciones financieras y agencias encargadas de velar por el cumplimiento de la ley que usan estas denuncias para combatir el *phishing*.
- Si lo estafaron, visite el sitio Web de la FTC sobre Robo de Identidad [ftc.gov/robodeidentidad](http://ftc.gov/robodeidentidad) donde podrá informarse sobre los próximos pasos a seguir.

Para consultar más recomendaciones del gobierno federal y de la industria tecnológica que lo ayudarán a mantenerse alerta contra el fraude perpetrado en Internet y a proteger su computadora y salvaguardar su información personal, visite [www.AlertaenLinea.gov](http://www.AlertaenLinea.gov).

La FTC trabaja en favor del consumidor para la prevención de prácticas comerciales fraudulentas, engañosas y desleales y para proveer información para ayudar a los consumidores a identificar, detener y evitar dichas prácticas. Para presentar una queja o para obtener información gratuita sobre temas de interés del consumidor visite [ftc.gov/consumidor](http://ftc.gov/consumidor) o llame sin cargo al 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. La FTC ingresa las quejas presentadas por los consumidores a una base de datos segura y herramienta investigativa llamada Red Centinela del Consumidor (*Consumer Sentinel*) que es utilizada por cientos de agencias de cumplimiento de las leyes civiles y penales en los Estados Unidos y del extranjero.

FEDERAL TRADE COMMISSION	<a href="http://ftc.gov">ftc.gov</a>
1-877-FTC-HELP	FOR THE CONSUMER