Alerta de la FTC para Consumidores

Federal Trade Commission ▪ Bureau of Consumer Protection ▪ Office of Consumer & Business Education

Cómo Evitar que lo 'Pesquen' con una Red de Estafa Electrónica

How Not to Get Hooked by a 'Phishing' Scam

"Sospechamos que se ha efectuado una transacción no autorizada en su cuenta. Para asegurar que su cuenta no ha sido comprometida, por favor haga click sobre el enlace que se presenta más abajo para que podamos confirmar su identidad".

"Durante el proceso habitual de verificación de cuentas, no pudimos verificar su información. Para actualizar y verificar su información, por favor presione aquí".

¿Ha recibido un email con un mensaje similar? Pues se trata de una estafa llamada *"phishing"* — e involucra a estafadores que operan en Internet enviando mensajes electrónicos masivos no solicitados *(spam)* o mensajes de aparición automática *(pop-up)* para engañar a los consumidores y lograr que las víctimas inadvertidas revelen su información personal como números de tarjetas de crédito, información de cuentas bancarias, número de Seguro Social, contraseñas y demás información delicada.

De acuerdo a lo que informa la Comisión Federal de Comercio (*Federal Trade Commission*, FTC), la agencia nacional de protección del consumidor, los pescadores de información *(phishers)* envían un email o un mensaje *pop-up* que indica provenir de negocios u organizaciones con los cuales usted mantiene una relación — por ejemplo, su proveedor de servicio de Internet *(ISP)*, banco, servicios de pago en línea y hasta de agencias gubernamentales. El texto del mensaje puede indicarle que "actualice," "valide" o "confirme" la información de su cuenta. Es posible que el texto del mensaje también incluya algún tipo de amenaza sobre las horribles consecuencias que puede sufrir en caso de que no responda. Estos mensajes lo dirigen a un sitio Web que luce similar al de una organización legítima, pero no lo es. Se trata de un sitio Web falso cuyo único propósito es engañarlo para que usted divulgue su información personal y una vez que lo haga, los operadores pueden robarle su identidad y gastar o cometer delitos en su nombre.

La FTC le ofrece las siguientes recomendaciones para evitar ser atrapado por las redes de una de estas estafas de pesca de información:

- **Si recibe un email o mensaje *pop-up* solicitándole información personal o financiera, no responda ni tampoco haga *clic* en el enlace o vínculo del mensaje.** Las compañías que operan legítimamente no solicitan este tipo de información por email. Si está preocupado por la actividad de su cuenta, comuníquese con la compañía mencionada en el email utilizando un número telefónico que le conste como genuino, o bien abra una nueva sesión de navegación en Internet y escriba usted mismo el domicilio Web correcto de la compañía. En ningún caso corte y pegue

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

el enlace que se indica en el mensaje — los pescadores de información pueden aparentar que sus enlaces lo conducen a un sitio, pero en realidad lo llevan a otro diferente.

- **Utilice programas antivirus y *firewall* y manténgalos actualizados.** Algunos de estos mensajes electrónicos que andan a la pesca de información contienen un software que puede dañar su computadora o hacer un seguimiento de sus actividades en Internet sin su conocimiento.

  Los programas antivirus y *firewall* pueden protegerlo evitando que su sistema de correo electrónico acepte inadvertidamente estos tipos de archivos indeseados. El programa antivirus filtra las comunicaciones entrantes en búsqueda de archivos problemáticos o cuestionables. Busque un software antivirus que reconozca los virus actuales y también los más antiguos, que sea efectivo para reparar los daños y que además se actualice automáticamente.

  Un programa *firewall* lo ayuda a mantenerse invisible mientras navega en Internet y bloquea todas las comunicaciones provenientes de fuentes no autorizadas. Si usted tiene una conexión de banda ancha, es particularmente importante tener instalado un programa de tipo *firewall*. Los sistemas operativos (como por ejemplo Windows o Linux) o los navegadores (Internet Explorer o Netscape Navigator) posiblemente le ofrezcan gratuitamente "parches" de seguridad que sirven para tapar los agujeros del sistema que podrían ser explotados por pescadores de información o piratas informáticos.

- **No envíe información personal o financiera a través del correo electrónico.** El email no es un método seguro para transmitir información personal. Si es usted quien inicia una transacción y desea proporcionar información personal o financiera a través del sitio Web de una organización, busque indicadores de seguridad, como por ejemplo el ícono o símbolo del candado *(lock)* en la barra de estado del navegador *(browser status bar)* o un URL (localizador de recursos uniformes) de un sitio Web cuyo domicilio comience con "https:" (la letra "s" es la inicial de seguro). Lamentablemente, no hay indicadores a toda prueba, algunos "pescadores de información" han falsificado íconos de seguridad.

- **Revise los resúmenes de sus cuentas bancarias y tarjetas de crédito tan pronto como los reciba** para verificar si le imputaron cargos no autorizados. Si su resumen de cuenta se demora más de un par de días, llame al banco o compañía de tarjeta de crédito para confirmar su domicilio de facturación y los saldos de sus cuentas.

- **Tenga mucho cuidado al abrir o descargar los documentos o archivos que se adjuntan a los mensajes electrónicos recibidos**, sin tener en cuenta quien sea la persona u organización que los envía. Estos archivos pueden contener virus u otros programas que pueden afectar la seguridad de su computadora.

- **Reenvíe el email recibido a la pesca de información** a spam@uce.gov y a la compañía, banco u organización cuyo nombre fue indebidamente invocado. La mayoría de las organizaciones colocan información en sus sitios Web indicando dónde reportar este tipo de problemas.

- **Si cree que ha sido estafado, presente su queja en línea visitando ftc.gov/espanol** y luego consulte el sitio Web de la FTC sobre Robo de Identidad en ftc.gov/robodeidentidad. Las víctimas de esta práctica de pesca de la información pueden convertirse en víctimas del robo de

identidad. Si bien usted no puede controlar completamente la posibilidad de ser damnificado por el robo de identidad, sí es posible minimizar su riesgo siguiendo algunos pasos. Si un ladrón de identidad está abriendo cuentas a su nombre, muy probablemente estas cuentas aparezcan en su informe crediticio. Usted **tiene la posibilidad** de detectar tempranamente un incidente si solicita periódicamente una copia gratuita de su informe crediticio a las tres compañías principales de informes de crédito. Para consultar en detalle cómo solicitar un informe crediticio anual gratuito, visite en Internet www.annualcreditreport.com.

También puede enterarse de otras formas de evitar estafas de correo electrónico y aprender a lidiar con el correo electrónico masivo engañosos visitando ftc.gov/spam.

La FTC trabaja en favor del consumidor para la prevención de prácticas comerciales fraudulentas, engañosas y desleales y para proveer información de utilidad al consumidor con el objetivo de identificar, detener y evitar dichas prácticas. Para presentar una queja o para obtener información gratuita sobre temas de interés del consumidor visite ftc.gov/espanol o llame sin cargo al 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. La FTC ingresa todas las quejas relacionadas a fraudes de Internet y sistema de telemercadeo, robo de identidad y otras quejas sobre prácticas fraudulentas a una base de datos segura llamada Centinela del Consumidor (Consumer Sentinel) que se encuentra a disposición de cientos de agencias de cumplimiento de las leyes civiles y penales en los Estados Unidos y en el extranjero.