Beware of phishing schemes

What is phishing?

Phishing is the act of sending an e-mail to a user falsely claiming to be a legitimate enterprise in an attempt to scam the user into surrendering private information that could be used for identity theft.

According to the Federal Trade Commission, phishers send e-mails or pop-up messages that claim to be from a business or organization, for example, an Internet Service Provider, a bank, an online payment service or even a government agency. The message may ask you to *update, validate* or *confirm* your account information. Some phishing e-mails threaten dire consequences if you don't respond. The messages direct you to a Web site that looks just like a legitimate organization's site — but it's not. It's a bogus site whose sole purpose is to trick you into divulging your personal information so operators can steal your identity and run up bills or commit crimes in your name.

Remember these tips:

- If you get an e-mail or a pop-up message that asks for personal or financial information, do not reply or click on any links in the message. Legitimate companies don't ask for this information via e-mail. If you are concerned about your account, contact the organization in the e-mail by using a telephone number you know or open a new Internet browser session and type in the company's correct Web address yourself. Don't cut and paste the link from the message into your Internet browser — phishers can make links look real, but it actually sends you to a different site.
- Use anti-virus software and a firewall and keep them up-to-date. Some phishing e-mails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files.

Beware of phishing schemes involving the IRS

Although the FTC has reported that the IRS has a low number of identity theft crimes, phishing schemes using the IRS name have been escalating in number and sophistication. The current phishing scheme attempts to convince the users that they are receiving an e-mail from the IRS. The e-mails use an official IRS seal and ask recipients to provide personal information, such as Social Security numbers, credit card numbers and bank PINs. You should only respond in writing or by phone to the phone number listed on an IRS notice.

Remember, the IRS does not initiate communication with taxpayers through e-mail.

What if you believe you've been a victim of a scam?

File a complaint at **www.ftc.gov**, and then visit the FTC's Identity Theft Web site at **www.ftc.gov/idtheft**. Victims of phishing can become victims of identity theft. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early by ordering a free copy of your credit report from any of the three major credit bureaus. See **www.annualcreditreport.com** for details on ordering a free annual credit report.

What if you become aware of an IRS-related phishing scam?

If you receive an unsolicited e-mail communication claiming to be from the IRS, please **forward the original message** to: **phishing@irs.gov**. Find complete instructions at **www.irs.gov**.

How do I report other IRS scams?

You may report misuse of the IRS name, logo, forms or other IRS property to the Treasury Inspector General for Tax Administration at **800.366.4484**.

How do I report tax fraud?

Don't fall victim to tax scams. Remember, that if it sounds too good to be true, it probably is. Report suspected tax fraud activity by sending a completed **Form 3949-A,** *Information Referral*, to Internal Revenue Service, Fresno, CA 93888. You can download the form or call **800.829.3676** to order by mail.

For more information about identity theft prevention and victim assistance, visit www.irs.gov (keyword: identity theft).

IRS Department of the Treasury Internal Revenue Service Pub. 4523 (EN/SP) (Rev. 3-2008) Catalog Number 15145I

Cuidado con estafas de phishing

¿Qué es phishing?

Phishing se le llama a la practica fraudulenta de enviar e-mail a alguna persona haciéndose pasar por algún negocio legitimo en un intento por convencer al usuario a revelar información privada, la cual se usará para robar su identidad.

De acuerdo a la Comisión Federal de Comercio, los *phisers* envían correo electrónico o mensajes de ventanilla instantánea (pop-up) los cuales dicen ser de algún negocio u organización con la cual usted tiene tratos – por ejemplo, de un Proveedor de Servicio de Internet, un banco, servicio de pagos en-línea, o alguna agencia gubernamental. El mensaje puede pedirle que *actualice, verifique*, o *confirme* la información de su cuenta. Algunos correos electrónicos amenazan con graves consecuencias si usted no les responde. Estos mensajes le dirigen a un sitio Web el cual luce similar a los sitios de las organizaciones legítimas. Pero no lo es. Es un sitio falso cuyo único fin es engañarle para que usted revele su información personal y de esa manera los estafadores pueden robar su identidad y hacer gastos o cometer crímenes en nombre suyo.

Recuerde estos consejos:

- Si usted recibe un e-mail o mensaje pop-up solicitando su información personal o financiera, no conteste ni seleccione los enlaces del mensaje. Las compañías legítimas no solicitan esta información a través de correo electrónico. Si usted esta preocupado por su cuenta, comuníquese con la organización del e-mail por medio de un número telefónico que usted conozca o inicie una nueva sesión de navegación en el Internet y escriba el domicilio Web de la compañía usted mismo. No corte y pegue el enlace desde el mensaje electrónico a su navegador en el Internet – los phisers pueden hacer que los enlaces parezcan verdaderos, pero en realidad esos enlaces le dirigen a usted a sitios diferentes.
- Utilice programas antivirus y firewall y manténgalos actualizados. Algunos mensajes phising contienen software que puede dañar su computadora o rastrear sus actividades en el Internet sin su conocimiento. El software antivirus y el firewall puede protegerlo evitando que su sistema de correo electrónico acepte inadvertidamente estos tipos de archivos indeseados.

Tenga Cuidado con Estafas de phising que involucran al IRS

Aunque la FTC ha reportado que el IRS sólo ha sufrido un pequeño número de crímenes de robo de identidad, las estafas de phising que utilizan el nombre del IRS han aumentado en cantidad y complejidad. La estafa de phising intenta convencer al usuario que ha recibido un e-mail de parte del IRS. Los e-mails utilizan el logotipo oficial del IRS y solicitan que el usuario provea información personal tal como números de seguro social, números de tarjetas de crédito o información como su contraseña. Usted deberá responder sólo por escrito o por teléfono al número que aparece en la carta que le envió el IRS.

Recuerde, el IRS no inicia comunicación con los contribuyentes a través de e-mail.

¿Qué debe hacer si cree que ha sido victima de una estafa?

Presente una queja al FTC en **www.ftc.gov**, y luego ingrese a la pagina Web y vea el tema sobre el Robo de Identidad en **www.ftc.gov/idtheft** y seleccione el enlace en español. Las victimas de las estafas phising pueden convertirse en víctimas del robo de identidad. Si un ladrón de identidad abre cuentas de crédito en nombre suyo, estas cuentas nuevas podrían aparecer en su informe de crédito. Usted puede detectar estos incidentes a tiempo solicitando una copia gratuita de su informe de crédito de parte de alguna de las tres principales agencias crediticias. Visite la página **www.annualcreditreport.com** para mayores detalles sobre como solicitar un reporte gratuito de crédito anual.

¿Qué si se da cuenta de una estafa de phising relacionada con el IRS?

Si usted recibe un correo electrónico no solicitado el cual dice provenir del IRS, por favor envie el mensaje original a: **phising@irs.gov**. Para obtener instrucciones detalladas visite **www.irs.gov**.

¿Cómo informo al IRS sobre otras estafas?

Usted puede informar sobre el uso indebido del nombre, el logotipo, formularios u otra propiedad del IRS al Inspector General de la Tesorería para la Administración Contributiva al **800.366.4484**.

¿Cómo reporto el fraude contributivo?

¡No sea víctima de las estafas contributivas! Recuerde, que si algo parece demasiado bueno como para ser cierto, probablemente no es cierto. Reporte si sospecha actividad fraudulenta contributiva enviando la **Forma 3949-A**, *Information Referral,* al Internal Revenue Service, Freso, CA 93888. Usted puede descargar la forma o llamar al **800.829.3676** y solicitar el formulario por correo.

Para mayor información sobre como prevenir el robo de identidad y ayuda para las victimas, visite www.irs.gov (palabra clave: Robo de identidad)