

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).