

March 31, 2006



**FRAUD TIP OF THE WEEK**  
**“Phishing” (Fishing) For Your Tax Refund**  
By Detective Paul Henninger

The Internet Fraudsters are currently representing themselves as the “IRS.” They are “Phishing” for your personal information and banking information. This week many of you may have received “Spammed” e-mail from them. They will either ask that you e-mail your response or click on a “link” that will send you to a bogus, counterfeit “IRS” website. Do not “click” on the link or respond in any way. The real “IRS” will never send you an unsolicited e-mail regarding a tax problem or refund. The IRS will never send you an e-mail asking for your personal or banking information, THEY ALREADY HAVE IT.

To date, the U.S. Treasury has identified sites hosting more than two dozen IRS-related “phishing” scams. These scam websites have been located in at least 20 different countries. They will claim to be from the IRS, tell recipients they are due a federal tax refund, and direct them to a counterfeit website that appears to be a genuine IRS site. The convincing interactive site has official looking forms asking for your personal information, banking information, passwords and Personal Identification Numbers (PIN).

If you receive this scam, do not go to the site. Electronically copy the e-mail, with full headers if you know how. Report the crime to the real “IRS.” For this problem, the IRS has established an official complaint website at [phishing@irs.gov](mailto:phishing@irs.gov). That website contains instructions on how to submit the complaint. It also has some good fraud tips. Who knows, your information may lead to the arrest of an international criminal.

Do not report this e-mail scam to your local law enforcement. It is a common scam, and we have already seen it. Of course, if you fell for this scam, it is important that you make file a report with the local law enforcement agency where you reside. File a police report so we can help you minimize your exposure and loss.

Also, make a printed copy of the e-mail. Show it to your co-workers and friends as a warning. Educate them on what you learned from this tip and the IRS website. For those with advanced computer skills, you may want to send a copy to private anti-spamming groups that would love to have a copy of the fraudster’s e-mail. These groups enjoy using their Internet contacts to shut down the scammers’ e-mail addresses and websites.

Since this is tax season, and the frequency of these types of scams increase at this time of year, the Salem Police Department, U.S. Secret Service and Portland Police Bureau are hosting a free 2-hour training class for law enforcement officers, financial fraud investigators, bank managers and lead bank tellers. The topic includes “Current Internet Scams” and “Identification Of Counterfeit U.S. Treasury Checks.” Classes are available on April 11, 12 and 13. Call me for to register at 503-588-6050, ext. 7154.