March 2006

Treasury Inspector General for Tax Administration
Office of Investigations

Computer Security Bulletin

Phishing Scams

Taxpayers Beware of Widespread Phishing Schemes Involving the IRS

Electronic fraud relating to the Internal Revenue Service (IRS) has been escalating in number and sophistication since December 2005. ***Phishing***, as it is called, is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The current phishing scheme attempts to convince the users that they are receiving an email from the Internal Revenue Service (IRS).

This scam sends emails with an official IRS seal to potential victims, telling them how to get their refund status or a tax refund credited to their credit card by providing the needed information. Unsuspecting recipients are asked to provide personal information, such as their social security, credit card and bank PIN.

What is a Phishing Scam

Identity theft has always been around. By gaining access to someone else's personal data and impersonating them, a criminal may pursue a crime in near anonymity. Today, electronic identity theft has never been easier. The e-mail directs the user either to directly submit personal information or visit a Web site where they are asked to update this personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

The purpose of phishing is clear – to defraud financial institutions and their customers out of significant sums of money. Once personal account information is obtained, the identity theft begins and can result in drained savings accounts, new credit accounts being opened, countless online purchases, stock trades and other types of e-commerce transactions in the victim's name.

If you receive a suspicious e-mail that claims to come from the IRS, you can relay that e-mail to a new IRS mailbox, **phishing@irs.gov**.
Contact the IRS on the web here.

What to do if you become a victim of an IRS related Phishing scam

The Treasury Inspector General for Tax Administration (TIGTA) investigates groups or individuals who impersonate the IRS.

If your identification has been stolen, you have paid money or provided personal identification to someone who falsely purported to work for or represent the IRS

Report the incident to TIGTA

Toll free: 1-800-366-4484
or on the web:
www.treas.gov/tigta/contact_report.shtml

Contact your credit card company and tell them your Account may have been compromised.

Call your bank and tell them that your account may have been compromised and how this occurred.

Change your password on any Internet accounts.