CONSUMER ALERT

BILL SCHUETTE
ATTORNEY GENERAL

The Attorney General provides Consumer Alerts to inform the public of unfair, misleading, or deceptive business practices, and to provide information and guidance on other issues of concern. Consumer alerts are not legal advice, legal authority, or a binding legal opinion from the Department of Attorney General.

IRS SCAMS & TAX-RELATED ID THEFT

IRS Will Never Ask for Taxpayers' Personal Information by Phone or in E-mails

Anybody contacting you claiming to be from the IRS and asking you for personal identifying information is a crook. Every year the IRS issues warnings about rebate or other scams being perpetrated by con artists claiming to work for the agency. The goal of these crooks is to commit identity theft, take control of personal computers, or simply duping people out of cash. IRS scams enable con artists to get bank account information, Social Security numbers, or credit and debit card details that are then used to commit identity theft.

IRS E-MAIL SCAMS

E-mail continues to be the method of choice for IRS scams. Common e-mail tricks used by these crooks include using:

- the official IRS logo,
- whole sections of text from the IRS's website,
- a fake "from" address (reported Michigan variations include irs@getrefundnow.com, support@irs.gov, service@irs.jg.gov, tax-refunds@irs.gov and other variations on the irs.gov theme),
- forms with numbers similar to those the IRS already uses, often with a jumble of numbers and letters.

Don’t fall for any e-mail scams! The IRS never initiates e-mails to taxpayers!

Refund E-mail. Several variations of this bogus e-mail exist, all falsely claiming to come from the IRS and informing the recipient to click on a link to access a refund claim form that requires personal identifying information. The crooks try to make this look legitimate by using a specific refund sum that sounds convincing (reported Michigan variations include $134.80 and $184.80). A recent new twist is aimed at tax-exempt organizations and includes the name and a fake signature of an actual IRS employee.

The "Where's My Refund?" variation of this bogus e-mail offers track your refund and asks for your last name, Social Security Number, and credit card information.

Audit E-mail. This bogus e-mail informs the recipient that his or her tax return will be audited. As if the threat of an audit was not enough to get someone's attention, the e-mail may include a greeting in the body addressed to the specific recipient by name.

Tax Law Changes E-mail. Directed at accountants and businesses, this bogus e-mail invites the recipient to download information on tax law changes. Clicking on the link downloads malware. Malware is short for malicious software and describes software designed to infiltrate or damage a computer system without the owner's informed consent. Malware can take over the victim's computer hard drive, giving someone remote access to the computer, or it could look for or record passwords or other information and send that valuable personal identifying information to the crook.

Cash Reward for Completing Online Customer Satisfaction Survey. This e-mail purports to pay taxpayers for completing an online survey that, of course, includes questions asking for personal identifying information.

IRS PHONE SCAMS

Back Taxes or Penalty Phone Call. High pressure calls threaten legal action that can only be avoided by immediate payment. Payment must be made by difficult-to-trace Green Dot or similar money transfer methods. Victims provide the card numbers and PINs to the caller, and the caller quickly wipes the cards clean of cash.

Rebate Phone Call. Aimed at seniors, the caller identifies himself as an IRS employee and tells the targeted victim that he is eligible for a sizable rebate for filing taxes early. The fake IRS employee states that he needs the target's bank account information for direct deposit of the rebate. Providing your bank account details gives criminals access to your funds.

Paper Check Phone Call. In this telephone scam, a fake IRS employee indicates the IRS sent a check that has not been cashed and the IRS needs to verify the individual's

bank account number. The only way the IRS collects your bank account details is if you choose to put them in your tax return.

WHAT TO DO IF YOU GET AN E-MAIL OR PHONE CALL PURPORTING TO COME FROM THE IRS

If you know the e-mail or call purports to be from the IRS, don't open the e-mail or answer the phone. You may forward e-mails to phishing@irs.gov, the address established by the IRS to receive, track, and shut down these scams. Detailed instructions for how to send the e-mails are in the IRS's publication "Protect Yourself from Suspicious E-Mails or Phishing Schemes."
You may not receive an individual response to your e-mail because of the volume of reports the IRS receives each day.

You may also report misuse of the IRS name, logo, forms, or other IRS property to the Treasury Inspector General for Tax Administration toll-free at 1-800-366-4484.

Also remember that the only genuine IRS website is www.irs.gov. You should never get to this site using a link embedded into an e-mail - instead enter the address in your browser. A website embedded into an e-mail can easily take you to a fake site.

BEWARE OF ADVANCE REFUND LOANS

An advance refund loan is a loan based on money you are expecting to get as a tax refund. These loans can be legitimate but lenders charge huge rates of interest and fees. Sending your return in on time will sometimes get your money is just a few weeks, without a hefty price.

TAX-RELATED IDENTITY THEFT

Tax-related identity theft occurs when someone uses your stolen Social Security number to file a tax return claiming a fraudulent refund. The IRS is often the first to inform a victim that identity theft has occurred. Victims should immediately contact the IRS Identity Protection Specialized Unit at 800-908-4490. Report the fraud and ask for ID Theft Affidavit Form 1439 (form is also available online through Publication 5027 Identity Theft Information for Taxpayers).

Complete the form and continue to pay your taxes and file your tax return, even if you must do so by paper.

One of the most effective ways to protect yourself from this type of identity theft is to file your tax return as soon as possible. Additional identity theft prevention measures are

outlined in the Attorney General's Identity Theft Information for Michigan Consumers consumer alert,

ADDITIONAL INFORMATION

Consumers may contact the Attorney General's Consumer Protection Division at:

Consumer Protection Division
P.O. Box 30213
Lansing, MI 48909
517-373-1140
Fax: 517-241-3771
Toll free: 877-765-8388
http://www.mi.gov/ag (online complaint form)