

Senior Fraud Alert—March 20, 2008

Don't Fall for IRS-Related Scams

Bankrate.com 

by Leslie McFadden and



If you receive an unsolicited call or e-mail from the Internal Revenue Service, watch out. You're not talking to Uncle Sam.

The IRS recently issued a warning about identity theft schemes using the agency's name.

Since 2006, the Internet Crime Complaint Center has received more than 200 complaints about phishing schemes using the bureau as bait. This year scammers are using new twists on old tricks, including personalized e-mail salutations, live phone calls and the promise of tax rebates, to dupe consumers into divulging sensitive information.

Take care not to fall for the following cons:

1. Rebate phone calls

How it works: The IRS reports that a new scam similar to the refund e-mails that have circulated for years involves phone calls from callers posing as IRS employees. These callers tell potential victims they are eligible to receive a rebate for filing their taxes early. Phony IRS representatives ask for the consumers' bank account information, supposedly for direct deposit. Upon refusal, they will deny the rebate.

IRS spokeswoman Michelle Lamishaw says that scammers like to use current events for their purposes. In this case, fraudsters are using the rebate legislation recently passed by Congress as a lure.

Hang up on anyone calling about tax rebates. Checks will go out starting in May, and consumers will receive letters from the IRS explaining the rebates, not phone calls.

"In any case, the IRS would not call them for bank account numbers or credit card numbers," Lamishaw says. Those who choose to have money direct deposited must include their bank account information on their tax return.

The IRS communicates with taxpayers via the U.S. Postal Service; it does not initiate e-mails or phone calls.

2. Tax refund e-mails

How it works: The refund e-mails -- the more common scam using the IRS's name -- can look legitimate.

"Some have IRS logo images and signature images. Most of them have a footer at the bottom of the mail along the lines of 'Copyright 2008, Internal Revenue Service U.S.A.,'" says Paul Wood, MessageLabs senior analyst.

They may have appropriate subject lines, such as "notification from IRS," and come from e-mail addresses with "IRS" in the domain name.

Wood says refund e-mails usually present a link to claim the refund, which is typically between \$100 and \$400. The link takes people to a refund claim form on a spoofed IRS site. The bogus form will ask people for personal information, such as their Social Security number, credit card number or bank account information.

That data would be a goldmine of information to criminals, who could then sell it on the black market or use it to commit identity theft. Don't get curious if you come across one of these e-mails. Simply clicking on a link can download malware designed to allow remote control of your computer or a hunt for bank account information on your PC. "Just clicking on a link is enough to become a victim of ID theft," says Lamishaw.

Rest assured the IRS won't e-mail taxpayers about their refunds. Those who expect a refund should use the IRS' [Where's My Refund tool](#) to track down funds.

3. Audit e-mails

How it works: This new scam employs a scare tactic, rather than the promise of money. Taxpayers receive an e-mail warning that their federal tax return will be audited. Like its popular cousin, the refund e-mail, the message provides a link to complete a form asking for personal information. These e-mails may greet the potential victim by name. According to Wood of MessageLabs, scammers may use contact information gleaned from social networking sites and contact lists from compromised computers to target their e-mails.

While people may not notice the personalized salutation, they are more likely to notice, and dismiss, a generic greeting.

The IRS does not send out unsolicited e-mails or phone taxpayers.

4. Check verification phone calls

How it works: Someone posing as an IRS employee calls consumers, telling them the IRS mailed them a check that hasn't been cashed. The caller will then ask for the taxpayer's bank account information.

In reality, the IRS will not contact you about a check you never cashed. To see what happened to a refund you're expecting, use the IRS' ["Where's My Refund?" tool](#).

Bottom line: The IRS corresponds with taxpayers through the U.S. Postal Service. Consumers should report unsolicited phone calls and e-mails from the IRS to phishing@irs.gov. Copyrighted, Bankrate.com. All rights reserved.

Tax refund e-mail scams

Do's:

- Do use a firewall and update your Internet security software.
- Do report suspicious phone calls or e-mails from the IRS to phishing@irs.gov. Do visit the IRS's official Web site directly at www.irs.gov if you have a question.

Don'ts:

- Don't click on links or open attachments from unsolicited e-mails from the IRS.
- Don't give out any personal information to anyone calling on behalf of the IRS.
- Don't divulge any personal information in an online form to claim a tax refund.