



The IRS Dirty Dozen

Every year, the IRS publishes the "Dirty Dozen" list—the list of the top 12 scams. Guess what kind of scam is rising to the top of the list in our Internet Age?

You guessed it: email scams.

The IRS has discovered 104 fake email scams since last November when it issued its 2006 Dirty Dozen list of tax frauds.

Most of these schemes involve "phishing", which arises from the use of increasingly sophisticated lures to "fish" for users.

The IRS defines phishing as "a technique used to gain personal information for the purposes of identity theft, using fraudulent email messages that appear to come from legitimate businesses.

These messages—and their email addresses—look authentic, but they are always asking you to divulge personal information. And Social Security Numbers are the top prize of all the things they may ask for.

If the Social Security number is the best prize, the best bait is the IRS itself. The pitch involves one of two appeals:

Appealing to Fear: You're being audited!

Appealing to Greed: You're due a big and unexpected refund!

These phishing schemes send out hundreds of thousands of emails built on one of these two appeals. They direct you "the IRS website", which looks and sounds official as can be.

The bogus website looks official, because much of it is copied directly from the IRS site. Ultimately, though, it will prompt you for SSAN, credit card numbers, PINs, and similar personal identifiers.

Here are some examples from the IRS website of recent schemes.

The Refund Phish. The email will come from tax-refunds@irs.gov, admin@irs.gov, or other variations on the irs.gov theme.

You would be directed to a website, which is a clone of the actual site, and even includes an interactive page similar to the real one IRS publishes.

The Treasury Inspector General for Tax Administration has currently identified 12 separate web sites in 18 countries hosting variations on this theme.

The Fake Form. The IRS has an official form named Form W-8BEN (Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding). Banks and other financial institutions use this form for foreign individuals.

The fake version asks for—you guessed it—account numbers, PINs, mother's maiden name, and passport number.

The IRS of course does not ask for any of this information. But the fake form looks very much like the real one.

The Anti-Fraud Phish. This one has lots of grammatical

errors and typos. It comes from the IRS Antifraud Commission (sic). It says that someone has enrolled the taxpayer's credit card in EFTPS (the IRS online payment system), and has tried to pay taxes with it.

The email claims the money was blocked, but may be claimed by going to the site. You can guess the questions that will be asked when you get there.

Protecting Yourself

The Basic Rule: Never, ever respond to an email from IRS.

Never. Ever.

These emails look convincing. The Refund phish uses a small refund amount as bait—only \$63.80.

The Audit phish uses an almost exact copy of the real IRS site. It looks like the real thing.

Don't do it. And don't open any attachments, either.

Here's what you can—and should—do. Send the phish to IRS. Send it to phishing@irs.gov.

More Dirty Dozen

Phishing is the #3 item on the IRS Dirty Dozen. What are the other big ones?

Number One Scam: Zero wages. This is a brand-new scam, and is new to the list. It involves taxpayers attaching a corrected 1099 or W-2 to the tax return, showing zero wages, and claiming the previously reported wages were erroneous.

Number Two Scam: Form 843 Tax abatement. This one is also new. Taxpayers use an official form to request relief from previously assessed taxes.

Number Six Scam: Frivolous argument. This one has been on the list for years and years. The taxpayer maintains the government has no right to collect taxes.

Number Seven Scam: Return Preparer Fraud. Some tax preparers promise higher refunds in exchange for inflated fees.

Even if someone else prepares your return, you are still responsible for its accuracy.

As a paid preparer, I'd like to add one comment to this fraud. I attended a Society of Accountants meeting Monday night, where we reviewed the Code of Ethics.

One of the first items discussed was that Preparer fees must not be based on contingency. In other words, a preparer who charges based on the percentage of a refund is in clear violation.

Someone who proposes this type of fee arrangement can earn a felony indictment for tax fraud for him and for you, too!

1171 Market Street, Suite 206, Fort Mill, SC 29708
Phone 803 802 7676

www.beaconsmallbiz.com

Copyright 2007, Bill Belchee
All Rights Reserved