National Tax Security Awareness Week: Recognize Phishing Email Scams

IRS Tax Tip 2017-83
November 28, 2017

The IRS reminds people to be on the lookout for new, sophisticated email phishing scams. These scams not only endanger someone's personal information, but they can also affect a taxpayer's refund in 2018.

This tip is part of National Tax Security Awareness Week. The IRS is partnering with state tax agencies, the tax industry and groups across the country to remind people about the importance of data protection.

Phishing attacks use email or malicious websites to get personal information from the user. In many cases, the criminal fools someone into believing the phishing email is from someone they trust. The emails often have the look and feel of authentic communications. These targeted messages can trick even the most cautious person into doing something that may compromise data.

People should be vigilant and skeptical. Even if the email is from a known source, people should use caution because cybercrooks are very good at mimicking trusted businesses, friends and family.

Here are six examples of email phishing scams:

- Emails requesting personal information. The thief might ask for bank account numbers, passwords, credit cards and Social Security numbers. This is the most common way thieves steal data.

- An email urgently warning the recipient to update online financial accounts at a hyperlink provided in the email. The link goes to a fake site.

- A message with an email address spoofing a familiar address to look like trusted businesses, friends and family. The fake address has a slight change in text, such as name@example.com vs narne@example.com. Merely changing the "m" to an "r" and "n" can trick people.

- Emails saying the recipient has a tax refund waiting at the IRS or that the IRS needs information about insurance policies. The IRS doesn't initiate spontaneous contact with taxpayers by email to request personal or financial information.

- The message has hyperlinks that take someone to a fake site. In one example, the email says: "Following recent calculations, we notice that you are eligible to receive a tax refund. In order to start the refund procedure, please visit this link and follow the steps required." The link goes to a fake site. The IRS doesn't send emails asking for refund verification.

- The message includes a PDF attachment that may download malware or viruses. Never open an attachment from a suspicious email address.

More Information:

Taxes. Security. Together
Protect Your Clients; Protect Yourself
Don't Take the Bait