CPA
Practice Advisor

PRODUCT & SERVICE GUIDE

IRS Warns of Christmas Email Phishing Scams

The most common way for cybercriminals to steal bank account information, passwords, credit cards or Social Security numbers is to simply ask for them. Every day, people fall victim to phishing scams that cost them their time and their money.

Nov. 28, 2017

With the approach of the holidays and the 2018 filing season, the IRS, state tax agencies and the nation's tax industry are urging Americans to be on the lookout for new, sophisticated email phishing scams that could endanger their personal information and next year's tax refund.

The most common way for cybercriminals to steal bank account information, passwords, credit cards or Social Security numbers is to simply ask for them. Every day, people fall victim to phishing scams that cost them their time and their money.

Those emails urgently warning users to update their online financial accounts – they're fake. That email directing users to download a document from a cloud-storage provider? Fake. Those other emails suggesting the recipients have a $64 tax refund waiting at the IRS or that the IRS needs information about insurance policies – also fake. So are many new and evolving variations of these schemes.

The Internal Revenue Service, state tax agencies and the tax community — partners in the Security Summit — are marking "National Tax Security Awareness Week" with a series of reminders to taxpayers and tax professionals. In part two, the topic is avoiding phishing scams.

Phishing attacks use email or malicious websites to solicit personal, tax or financial information by posing as a trustworthy organization. Often, recipients are fooled into believing the phishing communication is from someone they trust. A scam artist may take advantage of knowledge gained from online research and earlier attempts to masquerade as a legitimate source, including presenting the look and feel of authentic communications, such as using an official logo. These targeted messages can trick even the most cautious person into taking action that may compromise sensitive data. The scams may contain emails with hyperlinks that take users to a fake site. Other versions contain PDF attachments that may download malware or viruses.

Some phishing emails will appear to come from a business colleague, friend or relative. These emails might be an email account compromise. Criminals may have compromised your friend's email account and begin using their email contacts to send phishing emails.

Not all phishing attempts are emails – some are phone scams. One of the most common phone scams is the caller pretending to be from the IRS and threatening the taxpayer with a lawsuit or with arrest if payment is not made immediately, usually through a debit card.

Phishing attacks, especially online phishing scams, are popular with criminals because there is no fool-proof technology to defend against them. Users are the main defense. When users see a phishing scam, they should ensure they don't take the bait.

Here are a few steps to take:

- Be vigilant; be skeptical. Never open a link or attachment from an unknown or suspicious source. Even if the email is from a known source, approach with caution. Cybercrooks are adept at mimicking trusted businesses, friends and family. Thieves may have compromised a friend's email address or they may be spoofing the address with a slight change in text, such as name@example.com vs narne@example.com. In the latter, merely changing the "m" to an "r" and "n" can trick people.
- Remember, the IRS doesn't initiate spontaneous contact with taxpayers by email to request personal or financial information. This includes text messages and social media channels. The IRS does not call taxpayers with threats of lawsuits or arrests. No legitimate business or organization will ask for sensitive financial information via email. When in doubt, don't use hyperlinks and go directly to the source's main web page.
- Use security software to protect against malware and viruses. Some security software can help identity suspicious websites that are used by cybercriminals.
- Use strong passwords to protect online accounts. Each account should have a unique password. Use a password manager if necessary. Criminals count on people using the same password repeatedly, giving crooks access to multiple accounts if they steal a password. Experts recommend a password have a minimum of 10 digits, including letters, numbers and special characters. Longer is better.
- Use multi-factor authentication when offered. Some online financial institutions, email providers and social media sites offer multi-factor protection for customers. Two-factor authentication means that in addition to entering your username and password, you must enter a security code generally sent as a text to your mobile phone. Even if a thief manages to steal usernames and passwords, it's unlikely the crook would also have a victim's phone.

The IRS, state tax agencies and the tax industry are working together to fight against tax-related identity theft and to protect taxpayers. Everyone can help. Visit the "Taxes. Security. Together." awareness campaign or review IRS Publication 4524, Security Awareness for Taxpayers

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.