# Tax Scams

By Greg Beck, MPERS Assistant Executive Director

On March 19th the IRS released its 2018 updated list of the top 12 tax scams. The industry has dubbed the list the "Dirty Dozen." This article will not detail all 12 scams as some of them are perpetrated on the IRS itself, e.g. creating fake charities, falsely reporting deductions, and abusing tax shelters. This article will focus on three of the scams that could impact our members.

*Identity Theft*

Identity theft was number five on the IRS list. Generally the IRS defines identity theft as someone using a stolen social security number (SSN) to file a fraudulent return to claim a refund before the actual owner of the SSN has a chance to file a legitimate return. The IRS suggests that taxpayers (and their tax preparers if they use one) should use security software for their electronic tax return software, steer clear of phishing emails, hang up on threatening phone calls, and avoid clicking on links or opening attachments in emails from unknown sources. Those are all good tips to follow at any time to protect your personal data.

*Phone Scams*

Phone scams was number six on the IRS list. Criminals impersonating the IRS are threatening taxpayers with arrest, deportation, or driver's license revocation if they do not pay a false tax bill to the criminals. Perhaps the criminals should do a little research and realize that the state government, not the federal government issues driver's licenses to people. The criminals will use altered caller identifications to make it look like the call is coming from the IRS or similar agency. The callers will give out fake IRS job titles and badge numbers to sound legitimate and will provide the taxpayer with personal data that is readily found on any internet search in order to persuade the taxpayer that the caller is truly from the IRS. Please do not fall for such scams and simply hang up on them. The IRS has said many times that they do not call taxpayers; they send letters in the mail.

*Phishing Schemes*

The last scam I would like to discuss is number eight on the IRS list of the Dirty Dozen – phishing schemes. All taxpayers and their preparers should continue to be aware of phishing schemes. What is meant by the term "phishing"? Phishing is a play on the word "fishing" which we all know to be an activity where an angler uses bait to hook a fish. The "bait" in a typical phishing scheme is the promise of free money if the "fish" i.e., you, provides his or her own money or personal information to the "angler" or criminal on the other end of the email or phone call. The IRS reports that the criminals have lately started targeting tax and payroll professionals, school officials and human resource professionals.

There have been news reports of criminals trying to hack into tax preparer databases by accessing computers through unprotected wireless internet connections. The criminals simply park outside the tax preparers building and download information. Much like the advice above for phone calls, the advice for phishing scams is to simply delete those emails or hang up on phishing phone calls – or simply do not answer calls from numbers you do not recognize. If someone wishes to speak to you, he or she will leave a message.

What does all of this have to do with your retirement benefits? Primarily we want our members to be as financially secure as they can be in retirement. That is the reason we exist. We do not want our members to fall for these scams, and we hope that articles such as these are helpful to that end. Members may receive a phone call from us on occasion. Members are always welcome to ask to whom they are speaking, end the call and then call us back. The member should then ask for the staff person they were talking to and continue the conversation. Our main number is 800-270-1271. We do not mind if members want to take that extra precaution as it is always better to be safe than sorry. Perhaps that is the moral of this article – be safe rather than sorry.

*****