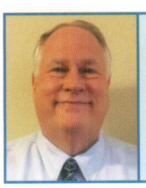

Common IRS and Tax Scams

By Charles Smith and Cathleen Henniges

Have you or any of your clients received a threatening phone call from someone claiming to be with the IRS or a law enforcement agency regarding a supposed tax matter? You are not alone. Scam calls and emails are on the rise. The Arizona Department of Revenue (ADOR), IRS, Arizona Superior Court of Pima County, United States District Court of Arizona, and the Better Business Bureau (BBB) all caution individuals to be on the lookout for IRS and tax-related scams affecting citizens nationwide.

One of the more frequent ways scammers attempt to con individuals out of their financial and personal information is through threatening phone calls. Arizona residents report receiving phone calls from so-called IRS agents claiming that they owe taxes. These "agents" state that the individuals must make payment using a specific prepaid debit card or wire transfer in order to avoid immediate arrest.

Another IRS scam is the Electronic Federal Tax Payment System (EFTPS) scam, in which callers claiming to be IRS agents state they have sent two letters via certified-mail regarding payment, both of which have been returned as undeliverable. The caller then threatens arrest if immediate payment is not made using a prepaid debit card supposedly linked to the EFTPS site, when in fact, it is linked directly to the scammer's account.

Perhaps one of the more unique IRS scams to affect Arizonans is the Refund Return Scam, also known as the Fake Tax Refund Scam. Beginning in 2018, scammers began filing fraudulent tax returns using information stolen during an Equifax data breach. After the tax return is filed, the fraudulent refund is deposited into the individual's bank account, followed by a phone call demanding the money be returned by someone claiming to work for the IRS, law enforcement, or third-party collection agency. The IRS reports that one of the scammers claims to be "Sue Wang" with "Debt and Credit Consulting Services" acting on behalf of the IRS to collect the erroneous payment. As with the other scam techniques, the perpetrators threaten the individual with criminal charges if the money is not returned. If you receive a refund you were not expecting, report it to the IRS and/or ADOR.

With technology being so prevalent, more scammers are relying on email communications to con victims out of their personal information. In some cases, emails are sent by false IRS agents advising that there is a problem with the refund, or that the refund can be viewed or received by clicking on a link within the email. In other instances, the emails appear to come from a common tax website such as TurboTax, and make the same claims regarding a problem with a return or that the account needs to be "recovered." These phishing emails allow scammers to obtain personal and confidential information from unsuspecting victims, ultimately gaining access to Social Security Numbers, bank account numbers, credit or debit card information, and more.

One email scam going around currently purports to be an automated email from the IRS regarding taxes that are due "right away." Aside from the typical tell-tale signs of a scammer, such as incorrect capitalization and poor grammar, the email at a glance looks like it could be legit. The IRS's logo is used at the top, with a footer using the IRS's actual address and a security logo. The scammers copy the style of typical email notices, using fake communication names and numbers. The paragraph explaining the amount due used a fake form number (1040B), which is additionally confusing as IRS Form 1040 does have a Schedule B. The scammers additionally made an effort to make the email appear as if it is coming from the Internal Revenue Service. However, upon closer examination, you can view the actual email address, which uses a random domain name.

According to the IRS and BBB websites, the IRS will always initially notify taxpayers of any problem through regular mail and does not contact taxpayers via phone, email or in-person except in very limited circumstances and after the taxpayer has already been made aware of the situation through multiple written communications.

If you or one of your clients become the victim of an IRS or tax-related scam, the incident can be reported to:

- The Treasury Inspector General for Tax Administration using the IRS Impersonation Scam Reporting web page https://www.treasury.gov/tigta/contact_report_scam.shtml or by calling 800-366-4484,
- The Federal Trade Commission using the FTC Complaint Assistant tool on www.ftc.gov,
- The BBB's Scam Tracker at https://www.bbb.org/scamtracker/tucson.

Make sure to remind your clients, particularly elderly clients, to be aware of these various scams and to avoid falling victim to any of them. Visit https://www.irs.gov/, https://www.bbb.org/en/us, https://azdor.gov/, or https://www.sc.pima.gov/ for more information and tips on how to protect yourself and your clients from these and other scams.