March 2016

**CEPP Bulletin**

 **State of Colorado Department of Public Safety Division of Homeland Security**John Hickenlooper, Governor Stan Hilkey, Executive Director **and Emergency Management** Kevin Klein, Director

**IRS Impersonation Scams: Protect Your Money and Your Information**

Tax season has arrived, and with it comes Internal Revenue Service (IRS) impersonation scams intended to steal your money and personal information. Two common scams are the IRS impersonation telephone scam and IRS phishing scam. These can affect people from all walks of life in every state. Although there is a spike in incidents during tax season, these scams can occur any time during the year. Make sure you take the necessary precautions so you do not become a victim.

**Government Impersonation Scams**

Scammers will sometimes pretend to be government officials in order to try and persuade you to send them money.[[1]](#footnote-1) There are a number of methods the imposter may use to get your money, such as stating you won the lottery and your winnings will be collected after you pay a “tax”. These fraudsters may impersonate both federal and state governments. One method that is becoming more and more prevalent is scammers claiming to be the IRS.

**IRS Impersonation Telephone Scam**

The IRS impersonation telephone scam has been called the most pervasive impersonation scam in the history of the IRS.[[2]](#footnote-2) Since 2013, the Treasury Department has received over 900,000 reports of IRS scam calls, or 10,000 to 12,000 calls a week. There have been over 5,000 victims that have paid out more than $26.5 million.[[3]](#footnote-3) According to the IRS and consumer protection groups, 2015 was the worst year for IRS impersonation scams, with a spike in incidents leading up to tax day.[[4]](#footnote-4)

The IRS impersonation telephone scam first targeted seniors. Seniors are more likely to be home, answer the phone, and have the money to pay.[[5]](#footnote-5) The scam then expanded to newly arrived immigrants, and now victims can be anyone.[[6]](#footnote-6) The scam also occurs all throughout the year, not just during tax season.

 The victim will receive a phone call from someone claiming to be an employee of the IRS. The fraudster will sound convincing, using a fake name and IRS badge number, and even altering the caller ID to make it appear as though it really is the IRS calling. He or she will typically know a lot about the victims, such as their name and address. The victim will be told they owe money and need to pay immediately with a pre-loaded debit card or by wire transfer. If the victim refuses, the scammer will often times resort to intimidation, stating failure to comply may result in arrest, deportation, suspension of a driver’s license or business license.[[7]](#footnote-7) These intimidation tactics are just the scammers attempt to bully the victim into doing what they want. If the victim does not answer the phone, scammers will often times leave an urgent call back message. Many times the scam originates outside of the country, which has made it difficult for law enforcement to go after the fraudsters.[[8]](#footnote-8)

**A Case Close to Home**

Colorado is no exception to the IRS impersonation scam. A Colorado Springs woman received a call from impersonators stating a mistake had been made on her 2012 taxes and because it had not been corrected, a warrant had been issued for her arrest. She was told she needed to pay $4,850 immediately or her accounts would be frozen, a lien would be placed on her properties, her driver’s license would be suspended for six months, and to top it off she would go to prison for six years. She was also told if she hung up the phone, IRS field investigators would arrive at her home in 45 minutes.[[9]](#footnote-9) She did not fall victim to the scam, but others have not been so fortunate.

In addition to the IRS impersonation scam, there are fraudsters that claim to represent the Colorado Department of Revenue. These fraudsters use similar tactics as the individuals claiming to be with the IRS. They may identify themselves as the State Tax Investigation Department and state you have a legal case against you for violating banking regulations or for cheating on your taxes. The impersonator tells you to wire them a large sum of money or to pay using a pre-loaded debit card. They will also tell you not to tell anyone or take the matter to court.[[10]](#footnote-10)

**Protect Yourself and Your Information**

The first step to protecting yourself is to know if you owe taxes or not. If you are certain you do not owe or have no reason to believe that you owe, hang up the phone immediately and contact the IRS at **1-800-366-4484** to report the call. You can also visit the IRS Impersonation Scam Reporting website at <https://www.treasury.gov/tigta/contact_report_scam.shtml>. If you know that you owe, or think that you owe, hang up and contact the IRS for help at **1-800-829-1040**.[[11]](#footnote-11)

Always remember the IRS will **NEVER** demand immediate payment or call about taxes owed without having mailed you a bill first. Also, the IRS will **NEVER** demand that you pay money owed without giving you the opportunity to appeal the stated amount, require you to use a specific payment method such as a prepaid debit card or threaten to bring in local police or law enforcement to have you arrested for not paying.[[12]](#footnote-12)

Likewise, the Colorado Department of Revenue does not contact taxpayers over the phone and request credit card numbers through a pre-paid debit card to pay an outstanding tax balance. If a tax payer owes, they will receive written notification through a series of letters mailed to the taxpayers address.[[13]](#footnote-13)

A telephone should be treated like your computer. Stay up to date on the latest scams, and never give out your information unless you are 100% sure who you are talking to![[14]](#footnote-14)

**IRS Phishing Scam**

Another popular method used by IRS impersonators is phishing scams. Fraudsters send an email used to trick victims into revealing personal and financial information that can be used to steal their identity. These include phony emails that lure victims in by telling them they are owed a tax refund. Another email asks individuals to update their IRS e-services portal information and Electronic Filing Identification Numbers (EFINs). Imbedded in the email is a form to enter your information. This allows fraudsters to capture the information as it is being typed. There may also be a link that takes the victim to a fake website that mirrors the IRS website. Once again, fraudsters are then able to capture the information as it is entered into the phony page.

**Protect Yourself from Phishing Scams**

The most important thing to remember is the IRS will **NEVER** initiate contact by email or social media in order to request personal or financial information. Another way to recognize this scam is by the web address, which often mentions IRSgov, without a period between IRS and gov. [[15]](#footnote-15)

To protect yourself from phishing scams please consider the following:

1. As with the IRS phone scam, phishers will use scare tactics. Do not get pressured into providing sensitive information.
2. Check a website’s privacy policy to see if it does or does not sell its mailing list. Most spam and dangerous phishing emails you receive come because a site you have signed up for has sold your information to another company.
3. Look for generic looking requests. Fraudulent emails are not personalized while legitimate emails often reference an account you have with them.
4. Never use links to connect to a website unless you are certain they are authentic. Instead, open a new browser window and type the URL directly.[[16]](#footnote-16)

If you receive an email that appears to be from the IRS or an organization closely linked to the IRS, such as the Electronic Federal Tax Payment System, report it by sending it to phishing@irs.gov.

**Conclusion**

The IRS impersonation scam is becoming more common. There is an increase in incidents leading up to tax day, but it can occur anytime of the year and happen to anyone. Do not let yourself be pressured into paying or revealing your sensitive information. If you feel as though you have been a victim of an IRS impersonation scam, please report this information to the IRS using one of the following methods:

|  |  |
| --- | --- |
| Phone | **1-800-366-4484** |
| Website | <https://www.treasury.gov/tigta/contact_report_scam.shtml> |
| Email (for phishing scams) | phishing@irs.gov |

1. Government Imposter Scams. *Federal Trade Commission.* Retrieved from http://www.consumer.ftc.gov
/articles/0048-government-imposter-scams. [↑](#footnote-ref-1)
2. Weisbaum, Herb. (April 15, 2015). ‘Imposter’ Tax Scam Worse Than Ever, Congress Holds Hearing. *NBC News.* Retrieved from http://www.nbcnews.com/business/taxes/tax-impostor-scam-worse-ever-congress-holds-hearing-n341906. [↑](#footnote-ref-2)
3. Van Cleave, Kris. (January 19, 2016). Tax Season Kicks Off With IRS Phone Scam Warning. *CBS News.* Retrieved from http://www.cbsnews.com/news/tax-season-kicks-off-with-irs-phone-scam-warning/. [↑](#footnote-ref-3)
4. Zakkour, Michael. (April 14, 2015). IRS Tax Phone Scam Claims for Victims Than Ever as 2015 Tax Day Arrives. *Forbes*. Retrieved from http://www.forbes.com/sites/michaelzakkour/2015/04/14/i-r-s-tax-phone-
scam-claims-more-victims-than-ever-as-2015-tax-day-arrives/#776bd608178f. [↑](#footnote-ref-4)
5. Weisbaum, Herb. (April 15, 2015). ‘Imposter’ Tax Scam Worse Than Ever, Congress Holds Hearing. *NBC News.* Retrieved from http://www.nbcnews.com/business/taxes/tax-impostor-scam-worse-ever-congress-holds-hearing-n341906. [↑](#footnote-ref-5)
6. January 19, 2016. Public Warned about “Ruthless” Scammers Posing as IRS Agents. Retrieved from http://www.cbsnews.com/news/irs-campaign-tackle-phone-scammers/. [↑](#footnote-ref-6)
7. October 21, 2015. IRS Urges Public to Stay Alert for Scam Phone Calls. *IRS.* Retrieved from https://www.irs.gov/uac/IRS-Urges-Public-to-Stay-Alert-for-Scam-Phone-Calls. [↑](#footnote-ref-7)
8. Weisbaum, Herb. (April 15, 2015). ‘Imposter’ Tax Scam Worse Than Ever, Congress Holds Hearing. *NBC News.* Retrieved from http://www.nbcnews.com/business/taxes/tax-impostor-scam-worse-ever-congress-holds-hearing-n341906. [↑](#footnote-ref-8)
9. Sexton, Betty. (October 6, 2015). New Information on IRS Phone Scam. *KKTV 11 News.* Retrieved from http://www.kktv.com/home/headlines/New-Information-in-IRS-Phone-Scam-330780752.html. [↑](#footnote-ref-9)
10. Scams – Warning to Tax Payers. *Colorado Department of Revenue.* Retrieved from https://www.colorado.gov/pacific/tax/scams-warning-taxpayers. [↑](#footnote-ref-10)
11. October 21, 2015. IRS Urges Public to Stay Alert for Scam Phone Calls. *IRS.* Retrieved from https://www.irs.gov/uac/IRS-Urges-Public-to-Stay-Alert-for-Scam-Phone-Calls. [↑](#footnote-ref-11)
12. Tax Scams/Consumer Alerts. *IRS.* Retrieved from https://www.irs.gov/uac/Tax-Scams-Consumer-Alerts. [↑](#footnote-ref-12)
13. Scams – Warning to Tax Payers. *Colorado Department of Revenue.* Retrieved from https://www.colorado.gov/pacific/tax/scams-warning-taxpayers. [↑](#footnote-ref-13)
14. Zakkour, Michael. (April 14, 2015). IRS Tax Phone Scam Claims for Victims Than Ever as 2015 Tax Day Arrives. *Forbes*. Retrieved from http://www.forbes.com/sites/michaelzakkour/2015/04/14/i-r-s-tax-phone
-scam-claims-more-victims-than-ever-as-2015-tax-day-arrives/#776bd608178f. [↑](#footnote-ref-14)
15. Suspicious Emails and Identity Theft. *IRS.* Retrieved from https://www.irs.gov/uac/Suspicious-e-Mails-and
-Identity-Theft. [↑](#footnote-ref-15)
16. 7 Essential Steps to Beat Phishing Scams: Don’t Get Caught on the Net. *Norton*. Retrieved from http://us.norton.com/7-tips-to-protect-against-phishing/article. [↑](#footnote-ref-16)