Steven M. Vogt, CPA, EA

Don't Be A Victim To IRS Phone And Email Scams

Don't be a Scam Victim

Thieves use taxpayers' natural fear of the IRS and other government entities to ply their scams, including e-mail and phone scams, to steal your money. They also use phishing schemes to trick you into divulging your SSN, date of birth, account numbers, passwords and other personal data that allows them to scam the IRS and others using your name and destroy your credit in the process. They are clever and are always coming up with new and unique schemes to trick you.

These scams have reached epidemic proportions, and this article will hopefully provide you with the knowledge to identify scams and avoid becoming a victim.

The very first thing you should be aware of is that the IRS never initiates contact in any other way than by U.S. mail. So if you receive an e-mail or a phone call out of the blue with no prior contact, then it is a scam. DO NOT RESPOND to the e-mail or open any links included in the e-mail. If it is a phone call, simply HANG UP.

Additionally, it is important for taxpayers to know that the IRS:

- Never asks for credit card, debit card, or prepaid card information over the telephone.
- Never insists that taxpayers use a specific payment method to pay tax obligations.
- Never requests immediate payment over the telephone.
- Will not take enforcement action immediately following a phone conversation. Taxpayers usually receive prior written notification of IRS enforcement action involving IRS tax liens or levies.

Phone Scams

Potential phone scam victims may be told that they owe money that must be paid immediately to the IRS or, on the flip side, that they are entitled to big refunds. When unsuccessful the first time, sometimes phone scammers call back trying a new strategy. Other characteristics of these scams include:

- Scammers use fake names and IRS badge numbers. They generally use common names and surnames to identify themselves.
- Scammers may be able to recite the last four digits of a victim's Social Security number. Make sure you do not provide the rest of the number or your birth date. That is information ID thieves can use to make your life miserable.
- Scammers alter the IRS toll-free number that shows up on caller ID to make it appear that the IRS is calling.
- Scammers sometimes send bogus IRS e-mails to some victims to support their bogus calls.
- Victims hear background noise of other calls being conducted to mimic a call site. • After threatening victims with jail time or driver's license revocation, scammers hang up, and others soon call back pretending to be from the local police or DMV, and the caller ID supports their claim.

DON'T GET HOODWINKED. This is a scam. If you get a phone call from someone claiming to be from the IRS, DO NOT give the caller any information or money. Instead, you should immediately hang up. Call this office if you are concerned about the validity of the call.

E-Mail Phishing

Always remember, the first contact you will receive from the IRS will be by U.S. mail. If you receive e-mail or a phone call claiming to be from the IRS, consider it a scam.

Do not respond or click through to any embedded links. Instead, help the government combat these scams by forwarding the e-mail to phishing@irs.gov.

Unscrupulous people are out there dreaming up schemes to get your money. They become very active toward the end of the year and during tax season. They create bogus e-mails disguised as authentic e-mails from the IRS, your bank, or your credit card company, none of which ever request information that way. They are trying to trick you into divulging personal and financial information they can use to invade your bank accounts, make charges against your credit card or pretend to be you to file phony tax returns or apply for loans or credit cards. Don't be a victim.

STOP-THINK-DELETE.

Scammers become very active toward the end of the year and during tax season.

What they try to do is trick you into divulging your personal information such as bank account numbers, passwords, credit card numbers, Social Security numbers, etc.

You need to be very careful when responding to e-mails asking you to update such things as your account information, pin number, password, etc. First and foremost, you should be aware that no legitimate company would make such a request by e-mail. If you get such e-mails, they should be deleted and ignored just like spam e-mails.

We have seen bogus e-mails that looked like they were from the IRS, well-known banks, credit card companies and other pseudo-legitimate enterprises. The intent is to trick you and have you click through to a website that also appears legitimate where they have you enter your secure information. Here are some examples:

- E-mails that appeared to be from the IRS indicating you have a refund coming and they need information to process the refund. The IRS never initiates communication via e-mail! Right away, you know it is bogus. If you are concerned, please feel free to call this office.

- E-mails from a bank indicating it is holding a wire transfer and needs your bank routing information and account number. Don't respond; if in doubt, call your bank.

- E-mails saying you have a foreign inheritance and they need your bank info so they can wire the funds. The funds that will get wired are yours going the other way. Remember, if it is too good to be true, it generally is not true. We could go on and on with examples. The key here is for you to be highly suspicious of any e-mail requesting personal or financial information.

Whats In Your Wallet?

What is in your wallet or purse can make a big difference if it is stolen. Besides the credit cards and whatever cash or valuables you might be carrying, you also need to be concerned about your identity being stolen, which is a far more serious problem. Thieves can use your identity to set up phony bank accounts, take out loans, file bogus tax returns and otherwise invade your finances, and all an identity thief needs to be able to do these things is your name, Social Security number, and birth date.

Think about it: your driver's license has two of the three keys to your identity. And if you also carry your Social Security card, bingo! An identity thief then has all the information he needs.

You can always cancel stolen credit cards or close compromised bank and charge accounts, but when someone steals your identity and opens accounts you don't know about, you can't take any mitigating action.

So if you carry your Social Security card along with your driver's license, you may wish to rethink that habit for identity safety purposes.

What You Should Never Do

Never provide financial information over the phone, via the Internet or by e-mail unless you are absolutely sure with whom you are dealing. That includes:

- **Social Security Number** – Always resist giving your Social Security number to anyone. The more firms or individuals who have it, the greater the chance it can be stolen.

- **Birth Date** – Your birth date is frequently used as a cross check with your Social Security number. A combination of birth date and Social Security number can open many doors for ID thieves. Is your birth date posted on social media? Maybe it should not be! That goes for your children, as well.

- **Bank Account and Bank Routing Numbers** – This along with your name and address will allow thieves to tap your bank accounts. To counter this threat, many banks now provide automated e-mails alerting you to account withdrawals and deposits.

- **Credit/Debit Card Numbers** – Be especially cautious with these numbers, since they provide thieves with easy access to your accounts.

There are individuals whose sole intent is to steal your identity and sell it to others. Limit your exposure by minimizing the number of charge and credit card accounts you have. The more accounts that have your information, the greater the chances of it being stolen. Don't think all the big firms are safe; there have been several high-profile database breaches in the last year.

Phishing

Phishing (pronounced "fishing") is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

Communications purporting to be from popular social websites, auction sites, banks, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing e-mails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail spoofing or instant messaging, and it often directs users to enter details at a fake website that looks and feels almost identical to a legitimate one.

You can help by forwarding phishing e-mail purportedly from the IRS to phishing@irs.gov.

In the meantime, imagine you try to file your return and it gets rejected as already filed. You attempt to get a copy of the bogus return but can't because you don't have the ID of the other unfortunate taxpayer who was used as the other spouse on the return. All the while, the scammers are enjoying their ill-gotten gains with impunity.

Fake Charities

Another fraud and ID theft scam associated with tax preparation involves charity scams. The fraudsters

pop up whenever there are natural disasters, such as earthquakes or floods, trying to coax generous Americans into making a donation that will go into the scammer's pockets and not to help the victims of the disaster. These same crooks might also steal your identity for other schemes. They use the phone, mail, e-mail, websites and social networking sites to perpetrate their crimes.

When disaster strikes, you can be sure that scam artists will be close behind. It is a natural instinct to want to provide assistance right away, but potential donors should exercise caution and make sure their hard-earned dollars go for the purpose intended, not to line the pockets of scam artists.

The following are some tips to avoid fraudulent fund-raisers:

- Donate to known and trusted charities. Be on the alert for charities that seem to have sprung up overnight in connection with current events.
- Ask if a caller is a paid fund-raiser, who he/she works for and what percentage of the donation goes to the charity and to the fund-raiser. If a clear answer is not provided, consider donating to a different organization.
- Don't give out personal or financial information – including a credit card or bank account number – unless the charity is known and reputable.
- Never send cash. The organization may never receive the donation, and there won't be a record for tax purposes.
- Never wire money to a charity. It's like sending cash.
- If a donation request comes from a group claiming to help a local community agency (such as local police or firefighters), ask the people at the local agency if they have heard of the group and are getting financial support.
- Check out the charity with the Better Business Bureau (BBB), Wise Giving Alliance, Charity Navigator, Charity Watch, or IRS.gov.

Protecting Against Indenty Theft

To understand just how big a problem identity theft has become for the IRS, it currently has more than 3,000 employees working on identity theft cases and has trained more than 35,000 employees who work with taxpayers to recognize identity theft and provide assistance when it occurs.

When ID theft happens, it becomes a huge problem for the taxpayer and the taxpayer's tax preparer. So, the best way to combat ID theft is to protect against it in the first place and avoid becoming one of those unfortunate individuals who have to deal with it. Here are some tips to prevent yourself from becoming a victim:

- Never carry a Social Security card or any documents that include your Social Security number (SSN) or Individual Taxpayer Identification Number (ITIN).
- Don't give anyone your or a family member's SSN or ITIN just because they ask. Give it only when required.
- Protect financial information.
- Check your credit report every 12 months.
- Secure personal information at home.

- Protect personal computers by using firewalls and anti-spam/virus software, regularly installing updated security patches and changing passwords for Internet accounts.

- Portable computers, tablets and smartphones can be stolen or lost. Limit the amount of personal information they contain that can be used for ID theft. Be extra vigilant against theft.

- Don’t give personal information over the phone, through the mail or on the Internet without validating the source.

The advice included in this article is not intended or written by this practitioner to be used, and it cannot be used by a practitioner or taxpayer, for the purpose of avoiding penalties that may be imposed on the practitioner or taxpayer.

Chandler Office • 1807 E. Queen Creek Road, Suite 5 • Chandler , Arizona • 85286 • (480) 732-9898