It's Your Money

Holiday Tax Scams To Look Out For

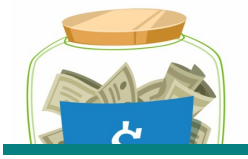
Financial scams are rampant, and you may already have been a victim and gone through steps to remedy the situation. This article attacks the problem from an angle you may not have thought about in your resolution steps. From charitable contribution scams to impersonating delivery services scams, the IRS is warning about scams, not all tax-related, for you to avoid.

- Only donate to known charities, and verify every charity's legitimacy on a site like CharityNavigator.org
- If you shop online only do so on sites that begin with the letters "https:", where the "s" stands for secure
- Don't shop using unsecured public Wi-Fi like hair salons, airports, or restaurants
- Keep your computer and phone security software up to date
- Scammers might pretend to be a business trying to deliver you a package and send you a text or email asking to reschedule the delivery. In reality, they never had access to your package, and are just looking to get you to reveal valuable personal information
- Thieves will send you an email with good news, like a tax refund, or bad news, like an unexpected tax bill. The emails include links to either (1) steal your personal information (bank account, SSN, etc.) or (2) download malware onto your device.

Even if the amount lost due to one of these scams is small, that isn't necessarily the issue. The problem is that someone gains access to your personal data through these scam attacks.

From an IRS perspective this can lead to someone filing a fraudulent tax return in your name. The IRS has sophisticated tools to discover fraud, and your first indication of a problem might be one of three letters from the IRS; Letter 5071C, Letter 4883C, or Letter 5747C.

If you get one these letters first make sure the letter is real. Look for the official IRS logo and letterhead, including the correct address and phone number for the IRS. Dates should be



It's Your Money

Holiday Tax Scams To Look Out For

recent, accurate, and accurately formatted (month spelled out), and they should include official IRS security or file numbers you can refer to for more information. A fake letter won't have this information.

Once satisfied the letter is real, follow the instructions to verify your identity with the IRS.

If, on the other hand, your first indication of a problem is that you can't e-file a tax return because someone already filed using your Social Security Number, you will need to complete Form 14039 online or a paper Form 14039, Identity Theft Affidavit, and submit this to the IRS.

The IRS will send you a letter acknowledging the identity theft, and will help you move through the remaining steps toward resolution. Be aware that this process will not necessarily be speedy; be patient and let the system work.

All confirmed tax-related identity theft victims will be placed into the Identity Protection PIN Program and annually be issued a new, six-digit IP PIN to prevent someone else from filing a return using your identity. This PIN must be used on all future IRS filings.

We've all heard the warnings about identity theft and financial scams. Bottom line: Just be very careful with your identity. If you think you've been a victim, work through the IRS process in addition to the normal steps of contacting your Police department, credit card company, bank, etc. As always, you can contact your Council at (937) 376-5486 to get more information about this important topic.

Link to Form 14039
`irs.gov/dmaf/form/f14039`
Link to Form 14039, Identity Theft Affidavit
`irs.gov/pub/irs-pdf/f14039.pdf`

The Council's Financial Advocate is a volunteer who can help with financial matters. If you are in need of assistance, please contact the Council.