Income Tax-Related Identity Theft Scams Down But Not Out: How to Protect Yourself

Author : David Gurliacci

Categories : Public Safety

Tagged as : Crime Prevention, Crime Prevention 2017, Darien Identity Theft, Darien Identity Theft 2017, Darien IRS Phone Scam, Darien IRS Phone Scam 2016, Identity Theft 2017, IRS Identity Theft, IRS Identity Theft 2017, IRS Scam, IRS Scam 2017, Tax Fraud

Date : March 19, 2017

The good news is that ID theft scams are less prevalent than they were in previous years. The bad news is that there's plenty still around.

Both the Internal Revenue Service and Better Business Bureau have (overlapping) advice about protecting yourself from scammers who want your personal information for identity theft and tax fraud.

"Everyone should guard their personal information by protecting their computers and using extreme caution when viewing emails or getting surprise phone calls," IRS Commissioner John Koskinen said.

> "We also encourage people to share this information with their friends and family," he said. "We all know someone who is challenged by technology, and some easy, common-sense steps could help protect these people from identity theft."

The IRS is handling cases related to identity theft and income tax returns faster than it was years ago, but it can still take four months for an ID theft victim to get a case resolved, according to a March 15 report in Accounting Today:

> "Several years ago, it took an average of 300 days to close a case, but more recently the IRS has been meeting its goal of closing a case in an average of 120 days or less. The case inventory for identity theft victims has also declined from about 95,000 at the end of fiscal year 2015 to 28,900 last month."

Here's what the IRS and BBB suggest you should do:

Tips from the Connecticut Better Business Bureau

The CT BBB on March 13 announced*:*

Connecticut Better Business Bureau says hard work by law enforcement and the Internal Revenue Service is bearing fruit, resulting in a substantial drop in tax return fraud last year.

The IRS says identity theft income tax return fraud plummeted in 2016, with a 46 percent drop in the number of victims, to 376,000. In addition, the agency says it also stopped one million fraudulent refunds from being issued last year with savings of almost $6.6 billion.

"It took considerable work to make a significant dent in the number of tax fraud victims, but clearly the efforts are paying off in a big way, and that is very good news for consumers," according to Connecticut better Business spokesman Howard Schwartz. "After years of fear on the part of taxpayers, especially those who need their refund to survive, this is very positive news,"

The most recent cases in Darien:

- Darien Residents Report Attempted IRS Tax Scams with Stolen Identities (March 19)

Income Tax Return Fraud begins identity theft. Scammers gather people's personal information from a variety of sources. That information is subsequently used to file a tax return in your name and claim your refund. Victims usually discover what has happened after they file a legitimate return and are told it already has been processed and the refund sent out.

If you have yet to file your income tax return, Connecticut Better Business Bureau has some tips to help you find and evaluate a tax preparation service or professional:

- **Verify qualifications** - Check the preparer's credentials. Attorneys, CPAs and enrolled agents can represent taxpayers before the IRS in all matters, including audits, collection and appeals. Other tax return preparers may only represent taxpayers for audits of returns they actually prepared.
- **Ask about additional service fees –** This includes what happens if your return is more complex than anticipated, so ask about what that would cost.
- **Carefully review the completed tax return –** Make sure it is signed both by you and the preparer and that they put their Preparer Tax Identification Number PTIN on the return as well.
- **Get contact information –** In case of any sort of problem with your return, you want to be able to reach the preparer not just for the next month or two but for three, four or six months down the road.
- **Don't wait too long –** Get your tax return done as soon as possible, and sign up to get your refund deposited directly to your bank account.

Tax professionals have differing levels of skills, education and expertise. If your return is simple, national income tax preparation franchise preparers do a great job. If your income tax return is complex, you might want to consider using an account or tax specialist.

You can save money by preparing your tax return online with IRS eFile or software, or have a trusted friend or relative prepare your return. The caveat, is that if there is a problem you will probably feel a lot more comfortable if an enrolled agent, tax lawyer or certified public accountant does your return, inasmuch as they can represent you in tax court if necessary.

You can check out or find a tax preparation professional at BBB.org/.

Security Tips from the IRS

A March 9 announcement *from the IRS (we've highlighted some tips):*

The IRS urges taxpayers to be safe online and reminds them to take steps to help protect personal information and guard against identity theft. This is true all year long, but particularly at tax time, when taxpayers may anticipate hearing about a tax refund or the status of their return.

"The IRS works year-round to protect taxpayers against scams and identity theft," said John Koskinen, IRS Commissioner. "But we can't do this alone. Taxpayers can do their part by taking certain precautions to stay ahead of these would-be con artists."

- **Treat personal information like cash – don't hand it out to just anyone. Social Security numbers, credit card numbers, bank and utility account numbers can be used to steal money or open new accounts.**

Every time a taxpayer receives a request for personal information, they should think about whether the request is truly necessary. Scammers will do everything they can to appear trustworthy and legitimate.

Avoid Phishing Scams

The easiest way for criminals to steal sensitive data is simply to ask for it. Taxpayers should learn to recognize phishing emails, calls or texts that pose as familiar organizations such as banks, credit card companies or even the IRS.

See also:

- Darien Police: How to Avoid Being Victimized by IRS Phone Scams (July 8, 2015)

These ruses generally urge taxpayers to give up sensitive data such as passwords, Social Security numbers and bank account or credit card numbers.

They are called phishing scams because they attempt to lure the receiver into taking the bait. The subject line may suggest the recipient just won a free cruise or that they must immediately update an account. Never open a link or an attachment from a suspicious email. It may contain malware.

Also, don't assume internet advertisements, pop-up ads or emails are from reputable companies. Check out companies to find out if they are legitimate. When online, a little research can save money and reduce security risks. If an ad or offer looks too good to be true, take a moment to check out the company behind it. Type the company or product name into a search engine with terms like "review," "complaint" or "scam."

- **Never download "security" software from a pop-up ad.**

A pervasive ploy is a pop-up ad that indicates it has detected a virus on the computer. It urges users to download a security software package. Don't fall for it. It most likely will install some type of malware. Reputable security software companies do not advertise in this manner.

Protect Personal Data

- **Taxpayers should not carry Social Security cards with them or any documents that may include this number.**

Provide Social Security numbers only when necessary. Occasionally businesses will request it when it is not essential.

Give personal information over encrypted websites only. Shopping or banking online should be done only on sites that use encryption. To determine if a website is encrypted, look for "https" at the beginning of the web address (the "s" stands for secure).

Some websites use encryption only on the sign-in page. If any part of the session isn't encrypted, the entire account and the included financial information could be vulnerable. Look for "https" on every page of the site.

Use Strong Passwords

The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users. Mix letters, numbers and special characters. Try to be unpredictable — don't use names, birthdates or common words. Don't use the same password for many accounts. If the password is stolen, it can be used to take over multiple accounts. Don't share passwords on the phone, in texts or by email.

- **Legitimate companies will not send messages asking for passwords. Receiving such a message probably means it's a scam. Keep passwords in a secure place.**

Set password and encryption protections for wireless networks. If a home or business Wi-Fi is unsecured it also allows any computer within range to access the wireless network and potentially steal information from connected devices.

Use Security Software

Make sure you have security software installed on all of your devices that connect to the internet. Many computers come pre-installed with firewall and anti-virus protections. A good broad-based anti-malware program should provide protection from viruses, Trojans, spyware and adware.

Set security software to update automatically so it can be upgraded as threats emerge. Also, make sure the security software is “on” at all times. If retaining important financial documents, such as prior-year tax returns, consider investing in encryption software to prevent unauthorized access by hackers or identity thieves.

Make sure security software has parental control options to protect children from malicious websites. Educate children about the threats of opening suspicious web pages, emails or documents.

Back Up Files

No system is completely secure. Copy important files, including federal and state tax returns, onto a removable disc or a back-up drive, and store it in a safe place. Save tax returns and records.

Federal and state tax returns are important financial documents that a taxpayer may need for many reasons, ranging from home mortgages to college financial aid applications.

- **Print out a copy and keep it in a safe place. Make an electronic copy in a safe spot as well.**

These steps also can help taxpayers more easily prepare next year's tax return. If storing sensitive tax and financial records on a personal computer, use a file encryption program to add an additional layer of security.

The IRS, state tax agencies and the tax industry recently launched a public awareness campaign called Taxes. Security. Together. It provides additional safety tips for taxpayers. Also, see Publication 4524, Security Awareness for Taxpayers.

_____

See also:

- Darien Residents Report Attempted IRS Tax Scams with Stolen Identities (March 19)
- Darien Police: How to Avoid Being Victimized by IRS Phone Scams (July 8, 2015)
- Elderly Woman Loses $1,000 to Thief in IRS Phone Scam (July 29, 2016)
- IRS Phone Scammers Recently Calling Darien Residents (Nov. 2, 2015)
- Darien Woman Loses $2,400 to Phone Scammer Who Said She Owed IRS (July 13, 2015)