ENJOY SAFER TECHNOLOGY®

TAXING TIMES: TIPS FOR PREVENTING FRAUD

Taxing times: Tips for preventing fraud

By ESET staff

Tax season is crime season, and you need to be prepared.

It's the time of year when scammers and cybercrooks try to cash in on tax refunds or impersonate the IRS to demand money. And small office/home office proprietors are especially vulnerable, because small businesses are popular targets for cybercriminals.

Almost three-fourths of all security breaches target small businesses,[1] which are known for having fewer resources for preventing attacks.

Worse, among small and medium sized businesses that suffer a breach, a staggering 60% go out of business within six months.[2]

Since your reputation, finances and business depend on staying ahead of the criminals, ESET offers these timely security tips.

Two common tax-related crimes include tax refund fraud and phone scams.

1 U.S. Small and Medium-Sized Business 2014-2018 forecast, IDC
2 Experian, 2013

Tax refund fraud

Also known as tax-related identity theft, occurs when someone uses your stolen Social Security number to file a tax return claiming a fraudulent refund.

It's one of the fastest growing crimes in the U.S. Losses are expected to hit a whopping $21 billion in 2016, up from just $6.5 billion two years ago, according to the Internal Revenue Service.

Why? Because tax identity fraud is an easy and relatively risk-free way to turn law breaking into money making. Consider the case of Rashia Wilson of Tampa Bay, Florida, the self-proclaimed "Queen of IRS Tax Fraud." She raked in more than $3 million filing bogus returns, then bragged about her crimes on her Facebook page, with her real name and photos of her holding huge wads of cash.

Thanks to such lapses in judgment, Wilson is now serving a 21-year prison sentence, but she also serves as living proof that ripping off the IRS is way too easy.

Generally, an identity thief will use your SSN to file a false return early in the year. You may be unaware you are a victim until you try to file your taxes and learn one already has been filed using your SSN. If someone has filed a fraudulent return, your return will be rejected if you're filing electronically. If you filed by mail, you'll get a letter from the IRS telling you a return has already been filed.

You could potentially find the IRS asking you to return money it paid out in your name to a scam artist, and it might take you a long time to resolve the issues—we're talking months, not days.

You could also find yourself turned down for a loan because of discrepancies between your tax record and those that the IRS has (because the IRS was tricked into accepting a return that is not yours).

What to do:

If you discover another tax return has been filed with your Social Security number, use IRS Form 14039, Identity Theft Affidavit, to alert the IRS.

Another form of tax fraud uses phone calls.

The Treasury Inspector General for Tax Administration (TIGTA) reports an ongoing phone fraud scam perpetrated by individuals misrepresenting themselves as Internal Revenue Service (IRS) employees.

TIGTA has received reports of roughly 736,000 contacts since October 2013 and has become aware of approximately 4,550 victims who have collectively paid over $23 million as a result of the scam, in which criminals make unsolicited calls to taxpayers fraudulently claiming to be IRS officials and demanding that they send cash via prepaid debit cards.

The IRS only contacts people by mail—not by phone or email—about unpaid taxes or other issues. The IRS would never ask for payment using a

prepaid debit card or wire transfer, nor would the IRS ask for a credit card number over the phone. Be sure to share this info with your employees, and let them know the IRS does not use unsolicited email, text messages, phone calls or any social media to discuss personal or business tax issues.

What to do:

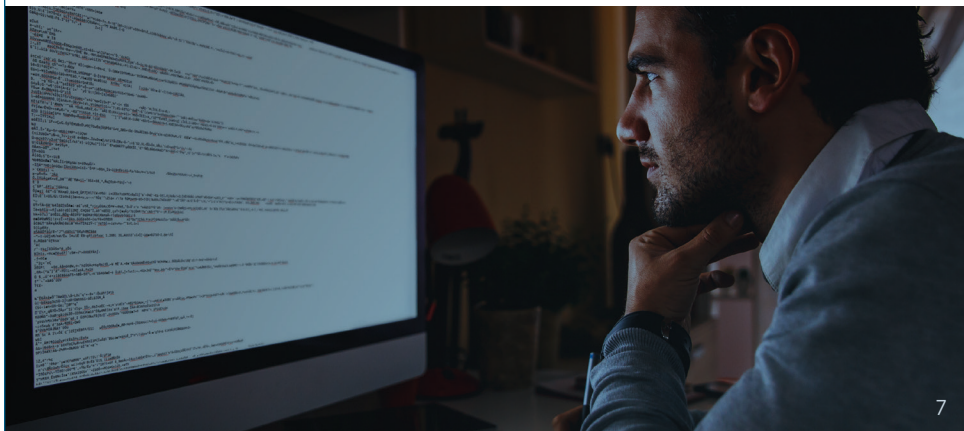
If you get a call from someone claiming to be with the IRS asking for a payment, here's how to respond:

- If you owe Federal taxes, or think you might owe taxes, hang up and call the IRS at 800-829-1040. IRS workers can help you with your payment questions.
- If you do not owe taxes, hang up and fill out the "IRS Impersonation scam" form on TIGTA's website, www.treasury.gov/tigta, or call TIGTA at 800-366-4484.

Why is tax identity fraud so common?

Cybersecurity experts say it's made possible by a number of factors:

- The IRS does not cross-check W2 forms and taxpayer details closely for accuracy.
- In 2015, a major data breach of the IRS exposed prior-year return information for about 100,000 U.S. households.
- Additional high-profile data breaches in industries ranging from healthcare to federal agencies have exposed millions of Social Security numbers and other stolen personal data that can be used for identity theft.
- Fraud is further facilitated by the options to file electronically and get refunds on pre-paid cash cards.
- While efforts are underway to close loopholes, the IRS still faces pressure to process returns and refunds rapidly and electronically, while failing to fund key areas of IRS operations.



Preventing tax fraud

By using these tips from the IRS, and protecting your data and networks with a comprehensive Internet security program, you can take a proactive stance against tax fraud.

- Order your IRS transcript at www.irs.gov to see what the IRS has on record for you in terms of tax payments and refunds.
- File your returns early to limit the opportunity for fraud in the current filing period.
- Monitor your bank accounts. Try to review account transactions once a week and immediately alert your bank when you see something that you didn't authorize.
- Ask your bank to put an ACH debit block on your account. This prevents crooks from taking money with this type of transfer, however, it could prevent you from executing legitimate online or over-the-phone electronic payments.
- Guard your bank account info and social security numbers at all times. These are the ingredients for tax identity fraud and you don't want to make it easy for the bad guys. To keep this info protected, give personal information over encrypted websites only. If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for "https" at the beginning of the web address (the "s" is for secure).
- When you're banking or buying online, use an Internet security program such as ESET Smart Security or ESET Multi-Device Security that includes Banking and Payment Protection. This feature automatically opens a new, secured browser when you're making financial transactions online.
- If you store sensitive tax and financial records on your computer, use a file encryption program such as DESlock+ Data Encryption to add an additional layer of security should your computer be compromised.
- Make sure your online security solution includes a personal firewall, which protects your data from being accessed when you're using public Wi-Fi; and anti-phishing, which prevents identity theft by blocking fake websites attempting to get your information.
- Protect mobile devices that contain banking and other information by adding two-factor authentication, such as ESET Secure Authentication, that adds an extra layer of security in case of loss or theft.
- You can easily protect all your Windows, Mac and Android devices with ESET Multi-Device Security.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY®