MARCH 01, 2018

LEARN HOW NOT TO BE A VICTIM OF CYBERCRIME THIS TAX SEASON

The IRS reports that from January through November last year, it blocked $8 billion in fraudulent tax returns, including when someone uses your ID to claim your tax refund. That doesn't even include other crimes.

As if it wasn't enough to stress-out about filing and paying our taxes on time, now we have to worry that if doing so hasn't exposed us to cybercriminals trying to steal our money. Those criminals are counting on you being stressed-out and confused by all the tax forms comin g in the mail and the flood of information the IRS requests from you. This also explains why so much emphasis has been placed on ramping-up internet security efforts to protect the millions of tax-payers filing their taxes on-line. According to the IRS, cybercriminals use several methods to steal your information and why people continue falling prey to their schemes to get your Social Security numbers, financial account information and passwords.

CRIMINAL SCHEMES TO WATCH FOR:

1. Phone extortion- If you've been receiving alarming phone calls that are supposedly from the IRS, with scary prerecorded messages about them taking legal action against you, those are very likely cybercriminals. Since 2013, about 900,000 of these phone calls have made by criminals claiming to be from the IRS. The IRS will NEVER call you. If necessary, they'll use US post office to contact you.

2. Phishing- Cybercriminals may use a technique called phishing (an email disguised to look like it's a legitimate company with official looking logos and letterheads). An email may appear to be from the IRS, but it's from a cybercriminal. This email takes you to websites where they'll collect your personal information, and may infect your device with malware. "When in doubt, call the IRS," experts advise.

3. False filings- Cybercriminals will use your information to file your tax return, and take your refund. If you get a rejection letter from the IRS when you file your taxes, saying you've already filed your return, immediately call the IRS.

PROTECT YOURSELF FROM CRIMINALS

It's always important to be cautious when it comes to giving people your Social Security number, or any identifying information by phone or email. But, during tax season, you need to be extra vigilant.

It's estimated that almost 25% of the scams tracked by the Better Business Bureau last year involved taxes. Here are three ways you can protect yourself, your ID, and your finances this tax season.

1. Verify, then trust - If you are contacted by anyone claiming to be with the IRS, call them back to ensure that the phone call or email came from them. If you really owe money to the IRS, it is almost certain that the communication will come by postal mail in order to include a payment form, so any other method of contact should set off alarm bells.

2. ID and credit monitoring - As we often suggest to you, it's important to have strong Internet security software protecting your devices, and strong passwords to keep cybercriminals out. Beyond that, think about signing up with a company that "proactively monitors your credit and ID," using either a company that specializes in this, your credit card, or your bank. Click here to learn what monitoring service we recommend for keeping your tax return safe (sponsor).

3. Don't share your identity with anyone "Unless you can confirm that you are really chatting with an agent of the government for legitimate purposes, there is no need to hand over it over." The best way to make sure you're talking with a legitimate IRS agent is to be the one making the call. Learn more about spotting and dealing with a scam IRS call.