

From an article on Komando.com

Tax season is here. January 23 marked the first day you could file online, and scammers are already taking advantage.

This time of year also opens the door to identity theft and tax fraud. It's been a major problem for quite a while now.

According to the U.S. Treasury Inspector for Tax Administration, various forms of tax fraud have cost victims more than \$50 million collectively since the year 2013, with the average amount lost being around \$5,200.00.

In 2015, the IRS blocked 1.4 million fraudulent tax returns that would've amounted to \$8.7 billion in stolen tax returns.

Identity theft and tax fraud were so rampant last year that the IRS launched an awareness campaign to "better inform you about the need to protect your personal, tax, and financial data online and at home."

According to the IRS, "People continue to fall prey to clever cybercriminals." These criminals trick you into giving them your Social Security numbers, financial account information and passwords.

Cybercriminals use several methods to steal your information. We'll list three ways that cybercriminals steal your identity. But don't worry, keep reading for three tips to protect yourself this tax season.

## HOW CRIMINALS STEAL YOUR INFORMATION

### 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.** You're not alone in receiving these calls. Since 2013, about 900,000 of these phone calls have been made by criminals claiming to be from the IRS.

"Given the power of the IRS and the complexity of the code, where mistakes can easily be made, concern about this type of communication from the real IRS makes these calls something to take seriously, and not easy to dismiss," noted security experts. "This fear is exactly what criminals hope to exploit."

### 2. Phishing

We often tell you about phishing email scams, where you receive an email from a cybercriminal disguised to look like it's from a legitimate company, with official-looking logos and letterhead.

Cybercriminals use this technique during tax season, too.

You could receive an email that appears to be from the IRS, but it's actually from a scammer. It could contain links that take you to websites where they'll collect your personal information, and may infect your gadget with malware. **"When in doubt, call the IRS,"** experts advised.

### 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 percent of the scams tracked by the Better Business Bureau in 2015 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. Plus, **"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 gadgets, 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.**

### 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 it over."

**The best way to make sure you're talking with a legitimate IRS agent is to be the one making the call.**