BEWARE OF IRS IMPOSTERS! LEARN HOW TO SPOT A SCAM.

By posing as the IRS, criminals try to trick you into providing sensitive information such as your Social Security number, online passwords or banking details, which they can use to commit identity theft.

Tax Day rolls around each April and, if you're like most people, you pay your taxes on time and are careful to file accurate returns. But what if someone contacts you and claims you owe back taxes – or says there's an issue with your return? While the IRS does reach out to taxpayers when necessary, you may not be dealing with the IRS – but a scammer. Let's look at three common IRS imposter scams, how they work, and how to spot them:

1. **Tax Collection Scam**
   In this scam, a criminal may contact you by phone, claiming you owe taxes and demanding immediate payment. This fake IRS official may threaten to arrest you, take your driver's license, or – if you are an immigrant – even deport you. Through intimidation, they'll try to get you to pay up – often with a prepaid debit card, cashier's check or wire transfer. Don't comply! Hang up the phone immediately. It's important to know that the IRS will never try to intimidate you over the phone or make unusual payment demands.

2. **IRS Verification Scam**
   When you become a target for this scam, you may receive an official-looking email that looks like it comes from the IRS and that asks you to verify your personal information. This is what's called a phishing attack. Criminals want to get your personal information and use it to commit identity theft. If you receive an unexpected email from the IRS, it's NOT the IRS. To protect yourself, don't click on any links or download attachments.

3. **Tax Transcript Email Scam**
   A tax transcript is a summary of your tax return from a given year. You may need a tax transcript to show proof of income to lenders when you apply for a mortgage or an auto loan. In this scam, crooks claiming to be from "IRS Online" send an email with the words "tax transcripts" in the subject line. The email has an attachment named "Tax Account Transcript" or something similar. Don't open the attachment! It contains malware that can infect your computer and possibly steal your personal information.

It's important to know that the IRS will never call, email or text you and ask for your tax information. They also won't send an email with an attachment asking you to update your profile or log in to access your tax transcript. If you get a message like this, delete it. It's a scam!

How You Can Guard Against a Potential IRS Imposter

You can take several steps to avoid getting caught in a scam. Here is what you can do:

- Be aware of an increase in the number of scams during tax season, which starts in January and runs through April.
- Hang up on threatening phone calls.
- Don't pay, especially when you're asked for a hard-to-track payment type like a prepaid debit card or gift card.
- Be wary of any non-mail communications that appear to be from the IRS. If the IRS reaches out, its initial contact is always by letter – not by phone, email or text message.
- Don't always trust your phone's caller ID information, either. To look official, scammers may use a trick known as spoofing to display a fake caller ID.

If you are targeted by an IRS scam, file a complaint with the FTC online at ReportFraud.FTC.gov; if you receive an email, forward it to phishing@irs.gov.