TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

March 2020

This monthly publication provided courtesy of Nina Tran, Cyber Security Manager, Tech Hero

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

It's tax season, here are six steps to avoid tax scams

1. File early: Filing as soon as you can is the best way to keep identity thieves from using your data. By getting your 1040 to Uncle Sam first, even if they have your tax information, the IRS won't accept the second return from "you".

2. Beware of IRS Impersonators: If you receive written notice from the IRS about a your taxes, respond promptly. This is the usual way that the tax agency contacts taxpayers when there's an issue with a filing. But again, be careful. Crooks know how the IRS operates and mimic it, even sending fake written correspondence.

Remember, the IRS will not call you with threats of jail or lawsuits. The IRS will not send you an unsolicited email suggesting you have a refund or that you need to update your account. The IRS will not request any sensitive information online. These are all scams, and they are persistent. Don't fall for them. Forward IRS-related scam emails to phishing@irs.gov. Report IRS-impersonation telephone calls at www.tigta.gov. If you have any doubts about the validity of any communication from the IRS, call them at 800-829-1040 or 800-908-4490. I called twice last week, the wait was less than 5 minutes, but as you get closer to April 15th the wait will be longer.

3. Protect your Social Security number: By now we all know this drill, but reminders never hurt. Don't give out your Social Security number unless there's a good reason and you're sure you're sure about the authenticity of the person/office that's seeking it. If your Social Security Number is requested to verify your ID before accessing your accounts, your last 4 digits along with answering correctly several questions that only you know, should be enough. If you need to do this over the phone, obviously be careful not to provide confidential information in public places. Beware of Bluetooth attacks and thefts. Disable Bluetooth when on calls that you must provide confidential information.

4. Research your tax preparer: Make sure your tax preparer is trustworthy before handing over your personal information. A reputable tax pro won't have any problem answering your questions before you hire him or her. Due to the volume of confidential information tax preparers have, they are targets for attacks.. Many small tax preparer companies do not have enough security measures to protect themselves. Choose your tax preparer wisely.

5. Consider getting an Identity Protection PIN (IP PIN): This is a six-digit number, which, in addition to your Social Security number, confirms your identity. Once you get an IP PIN, you must provide it each year when you file your federal tax returns. To obtain an IP PIN, you must be able to verify your identity through a rigorous Secure Access process. Review the Secure Access requirements before you start to learn more about the IP PIN and how to use the Get an IP PIN tool.

At the start of the 2020 filing season, taxpaying residents of these locations will be eligible for the IP PIN program: Arizona, California, Colorado, Connecticut, Delaware, District of Columbia, Georgia, Florida, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, New York, North Carolina, Pennsylvania, Rhode Island, Texas and Washington. Getting an IP PIN this year will allow you to use for next year's tax filling.

6. Don't believe everything you see: Maybe it's just because there are so many more ways to get information nowadays, but sadly it seems like bad people are taking over the world. That means we all need to be more skeptical.

Identity thieves and other scammers are great at mimicking official seals, fonts and other details. Even scam phone callers are getting better, in some cases, at sounding more legit. And spoofing means even Caller ID can be faked.

The key thing to keep in mind is that just because a website, email or phone call seems official, don't automatically assume that it is.

For more useful tips on identity theft or the latest scams, visit the Federal Trade Commission's website https://www.consumer.ftc.gov/