CS CYBER SECURITY & YOU

JANUARY 2020

QUICK TIP

How to avoid being the victim:

- Never send sensitive information in an email.
- Ensure your computer has the latest security updates, anti-virus software is running and receiving automatic updating, and enable a firewall.
- Be wary of sites you visit for tax advice and forms.
- Do not use public Wi-Fi for tax preparation.
- Offers that seem too good to be true usually are.
- The IRS will never call or email you. EVER. Do not answer any of their questions or let them remotely access your computer. Hang up as quickly as possible.
- Use strong passwords and multi-factor authentication whenever possible.

OOPS, I ALREADY TOLD THAT NICE MAN ON THE PHONE EVERYTHING?

If you receive a call or a similar email on your personal account, the IRS encourages you to forward the original suspicious email (with headers or as an attachment) to its *phishing@irs.gov* email account, or to call the IRS at 800-908-4490.

Stay safe from your LASERS IT Department!

LASERS IT
Making Digital Retirement a Reality

REMEMBER THOSE TAX SCAMS LAST YEAR? THEY ARE BACK.

It is tax season again, which means the bad guys will once again try to separate you from your money, your identity, or anything they value. They may offer seemingly legitimate "tax services" that are actually designed to steal your identity and your tax refund. Often times, criminals will lure you in with an offer of larger write-offs or refunds. Such scams might include fake websites and tax forms that look like they belong to the Internal Revenue Service (IRS) in order to trick you into providing your personal information. Due to the rise in data breaches, you should always take steps to minimize your risk of identity theft and other online-related crimes; this is especially important this time of the year. Below are some warning signs to look for and basic precautions you can take to minimize risk and avoid becoming the next victim!

Warning Signs of an Online Tax Scam:

- An email or link requesting personal and/or financial information, such as your name, social security number, bank or credit card account numbers, or any additional security-related information.
- Emails containing various forms of threats or consequences if no response is received, such as additional taxes or blocking access to your funds.
- Emails from the IRS or federal agencies - the IRS will not email you or call you out of the blue.
- Emails containing exciting offers, tax refunds, incorrect spelling, grammar, or odd phrasing throughout.
- Emails discussing "changes to tax laws." These email scams typically include a downloadable document (usually in PDF format) that purports to explain the new tax laws. However, these downloads are almost always populated with malware that, once downloaded, will infect your computer.