According to the National Cybersecurity Alliance, tax season is prime time for online scams. Cybercriminals are continuously looking to lift your personal information to cash in on a refund request and/or steal your identity. The problem is rampant: In 2015, the Federal Trade Commission received close to half a million complaints, and nearly half (45%) were tax fraud-related.

Cyber thieves are crafty: they can break into your account or device and literally steal your online life—as well as your tax refund.

DON’T BECOME A VICTIM: WATCH OUT FOR TAX SEASON TRICKS

**Phishing Scams**
- Cybercriminals will try to get you to do something, like click on a link or respond to an email, so they can steal your personal information.
- Watch out for unsolicited emails, texts, social media posts or fake websites that may lure you in & prompt you to share valuable personal & financial information.

**Imposters Claiming to be IRS Agents**
- The IRS will never email or call you demanding immediate payment without having first mailed a bill—nor will they ask for a credit or debit card number via email or phone.

**Tax Preparer Fraud**
- The overwhelming majority of tax preparers provide honest services, but some unscrupulous individuals may target unsuspecting taxpayers and the result can be refund fraud and/or identity theft. The IRS reminds anyone filing a tax return, that the preparer must sign it with their preparer tax identification number.

STAY CYBER SAFE—FOLLOW THESE TAX SEASON TIPS

The National Cyber Security Alliance has some easy-to-use STOP.THINK.CONNECT. Tips that will help protect you against fraudster tricks!

**Keep All Machines Clean**
- Having updated software on all devices that connect to the Internet is critical. This includes security software, web browsers & operating systems for PC & your mobile devices. Having current software is a strong defense against viruses & malware that can steal login credentials or potentially use your computer to generate spam.

**Get Two Steps Ahead**
- Turn on two-step authentication—also known as two-step verification or multi-factor authentication—on accounts. Many popular email services & financial institutions offer this key security step for free, but you must opt in to turn it on.

**Make Better Passwords**
- If your passwords are too short or easy to guess, it’s like giving a cyber thief your banking PIN. Longer passwords & those that combine capital & lowercase letters with numbers & symbols provide better protection.

Click here to read important information about Business Email Compromise  
Click here for more information on Protecting Yourself From Identity Theft Refund Fraud