CS

CYBER SECURITY & YOU

MARCH 2021

PROTECT YOUR IDENTITY & MONEY DURING TAX SEASON

It's tax season in the U.S. You're likely focused on gathering all the necessary paperwork and submitting your return on time. Meanwhile, in the criminal world, fraudsters are busy executing schemes in an attempt to steal your identity and money. In fact, the Internal Revenue Service (IRS) identified $2.3 billion in tax fraud in 2020.

TAKE PREVENTATIVE MEASURES

Use a PIN: The IRS now offers an *identity protection PIN* for all taxpayers who successfully verify their identity with the agency. The PIN helps prevent fraudsters from filing a return with your Social Security number (SSN) because it enables the IRS to confirm your identity when you file electronically or by mail. Only you and the IRS will have access to your PIN.

File early: The IRS only accepts a single return for each SSN. In addition to obtaining an identity protection PIN, submitting your return early can help further limit the possibility that a criminal may use your SSN later to file a false return.

Use secure filing websites: Only trust tax-filing portals with "https:" before the URL. This indicates that data transmitted between you and the site is encrypted.

Take advantage of multi-factor authentication (MFA): When filing your taxes online, you should only use a tax service provider that, requires a username and password, and a one-time security code, to access your account.

Create strong passwords: For any portal that can access your sensitive tax information, choose a lengthy, complex, and unique password.

STOP SCAMMERS IN THEIR TRACKS

Beware of phony emails: Fraudsters create "phishing" emails that appear to be legitimate, but are simply a guise to get you to share personal or financial information. These emails may purport to be from the IRS and threaten you with legal or financial consequences if you fail to comply. Do not respond to such emails, click on any links or open any attachments. Instead, report them to the IRS at *phishing@irs.gov*.

Verify payment instructions: If you owe money to the IRS, take the time to confirm the payment instructions directly with the agency through a verified phone number on the official IRS website or your financial advisor. This is especially important when sending wire transfers.

Help the elderly: Cybercriminals often target senior citizens. Many of the scams involve fraudsters calling the elderly to try to scare or intimidate them into acting on the spot. Make sure your senior family members are aware of such scams, and remind them that it's always acceptable to hang up the phone, check in with a trusted partner and then call back using a verified number.

HOW THE IRS CONTACTS YOU

If you are trying to figure out whether outreach is real or fake, remember that the IRS will **never** initiate contact with you by phone, email, text or social media. The IRS won't call, email or text you with threats of lawsuits or arrests, or request your taxpayer PIN.

However, the IRS will contact you by mail. You can help verify the validity of the correspondence by checking if the letter arrives in a government envelope with the IRS seal, contains a notice number at the top right corner of the letter and provides the correct contact information for the IRS.

RECOGNIZE TAX FRAUD WARNING SIGNS

Cybercriminals are clever and relentless. Even if you follow these protective measures, you might still become a victim. To combat tax fraud, the IRS launched its *Identify Theft Central portal*, which contains helpful information for taxpayers. The IRS advises you to be suspicious about possible tax fraud if you:

- Receive a letter from the IRS about a tax return you didn't file;
- Can't electronically file your return because of a duplicate SSN;
- Get a tax transcript in the mail that you didn't request;
- Receive an IRS notice about an online account being created in your name, or stating that your account has been accessed or disabled, when you didn't take these actions;
- Get an IRS notice declaring you owe more taxes, or that you're the target of collection action, when you didn't file a return for that year;
- Receive an IRS notice reporting that you received wages or other income from an employer you didn't work for.

TAKE ACTION

If you suspect that you're a victim of tax-related identity theft, or know that your SSN has been compromised, the IRS suggests you should:

- Contact them immediately by calling the number on the IRS notice. Or, if you didn't receive a notice, call the IRS Identity Protection Specialized Unit (IPSU) at 1-800-908-4490;
- Complete IRS Form 14039 (Identity Theft Affidavit) if your electronic return is rejected because of a duplicate filing under your SSN;
- Visit *IdentityTheft.gov* for more information;
- Read the *Identity Theft Victim Assistance: How It Works* guide;
- *Request a copy of the fraudulent return* in your name (optional).

Keep in mind: Cybercriminals may also target your state income return. If you notice an issue with your federal return, be sure to contact your state tax department, too. ■

LASERS IT
Making Digital Retirement a Reality