cybersecurity protection and scam recognition is vital to reduce the threat of identity theft ...

Mar. 16, 2022

The Internal Revenue Service is urging people to stay resolute against ongoing scams and schemes by properly securing computers, tablets and phones. Solid cybersecurity protection and scam recognition is vital to reduce the threat of identity theft inside and outside the tax system.

The IRS works closely with the Security Summit, a partnership with state tax agencies and the private-sector tax industry, to help protect taxpayer information and defend against identity theft. Taxpayers and tax professionals can take steps to

help in this effort by doing things like minimizing cybersecurity footprints and

utility account numbers can be used to help steal a person's money or open new accounts.

- **Use strong passwords.** Use a password phrase or series of words that will be easy for you to remember. Use at least 10 characters; 12 is ideal for most home users. Mix letters, numbers and special characters. Try to be unpredictable – don't use names, birthdates or common words. Don't use the same password for many accounts and avoid sharing them. Keep passwords in a secure place or use password management tools.
- **Set password and encryption protections for wireless networks.** If a home or business Wi-Fi is unsecured, it allows any computer within range to access the wireless network and potentially steal information from connected devices. Whenever it is an option for a password-protected account, users should also opt for a multi-factor authentication process. Multi-factor authentication is critical to protecting your password.
- **Avoid phishing scams.** The easiest way for criminals to steal sensitive data is simply to ask for it. IRS urges people to learn to recognize phishing emails, calls or texts that pose as familiar organizations such as banks, credit card companies or even the IRS. Keep sensitive data safe and:
    - Be aware that an unsolicited email with a request to download an attachment or click on a URL could appear to come from someone that you know like a friend, work colleague or tax professional if their email has been spoofed or compromised.
    - Don't assume internet advertisements, pop-up ads or emails are from reputable companies. If an ad or offer looks too good to be true, take a moment to check out the company behind it.
    - Never download "security" software from a pop-up ad. A pervasive ploy is a pop-up ad that indicates it has detected a virus on the computer. The download most likely will install some type of malware. Reputable security software companies do not advertise in this manner.

- **Use security software.** An anti-virus program should provide protection from

storage. Store discs, drives and any paper copies in secure, locked locations.
- **Know the risk of public Wi-Fi.** Connection to public Wi-Fi is convenient and often free, but it may not be safe. Hackers and cybercriminals can easily steal personal information from these networks. Always use a virtual private network when connecting to public Wi-Fi.
- **Review ID Theft Central.** Designed to improve online access to information on identity theft, it serves taxpayers, tax professionals and businesses.

The IRS doesn't initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information. Generally, the IRS first mails a paper bill to a person who owes taxes. In some special situations, the IRS will call or come to a home or business.

People should be alert to scammers posing as the IRS to steal personal information. There are ways to know if it's really the IRS calling or knocking on someone's door.

Taxpayers can find answers to questions, forms and instructions and easy-to-use tools online at IRS.gov. They can use these resources to get help when it's needed at home, at work or on the go.

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.