That Email or Text From the IRS: It's a Scam!

"Thousands of people have lost millions of dollars and their personal information to tax scams," according to the IRS. The scams may come in through email, text messages, telephone calls or regular mail. Criminals regularly target both individuals and businesses and often prey on the elderly.

Important: The IRS will never contact you by email, text or social media channels about a tax bill or refund. Most IRS contacts are first made through regular mail. So if you get a text message saying it's the IRS and asking for your Social Security number, it's someone trying to steal your identity and rob you. Remember that the IRS *already* has your Social Security number.

"Scammers are coming up with new ways all the time to try to steal information from taxpayers," said IRS Commissioner Danny Werfel. "People should be wary and avoid sharing sensitive personal data over the phone, email or social media to avoid getting caught up in these scams."

Here are some of the crimes the IRS has identified in recent months:

Email messages and texts that infect recipients' computers and phones. In this scam, a phony email claims to come from the IRS. The subject line of the email often states that the message is a notice of underreported income or a refund. There may be an attachment or a link to a bogus web page with your "tax statement." When you open the attachment or click on the link, a Trojan horse virus is downloaded to your computer.

The trojan horse is an example of malicious code (also known as malware) that can take over your computer hard drive, giving someone remote access to the computer. It may also look for passwords and other information. The scammer will then use whatever information is gathered to commit identity theft, gain access to bank accounts and more.

Phishing and spear phishing messages. Emails or text messages that are designed to get users to provide personal information are called phishing. Spear phishing is a tailored phishing attempt sent to a specific organization or business department.

For example, one spear phishing scam targets employees who work in payroll departments. These employees might get an email that looks like it comes from an official source, such as the company CEO, requesting W-2 forms for all employees. The

payroll employees might erroneously reply with these documents, which then provides criminals with personal information about the staff that can be used to commit fraud.

The IRS recommends using a two-person review process if you receive a request for W-2s. In addition, employers should require any requests for payroll to be submitted through an official process, like the employer's human resources portal.

Scams keep evolving

These are only a few examples of the types of tax scams circulating. Be on guard for any suspicious messages. Don't open attachments or click on links. Contact us if you get an email about a tax return we prepared. You can also report suspicious emails that claim to come from the IRS at phishing@irs.gov. Those who believe they may already be victims of identity theft should find out what do by going to the Federal Trade Commission's website, OnGuardOnLine.gov.