Phishing, phone scams and identity theft top the list of items normally reported. However, following hurricanes and other disasters, the IRS urged taxpayers to be on the lookout for schemes stemming from these recent events.

Oct. 13, 2017

The Internal Revenue Service is warning taxpayers about tax and information-stealing scams that continue to be reported around the country. Phishing, phone scams and identity theft top the list of items normally reported. However, following hurricanes and other disasters, the IRS urged taxpayers to be on the lookout for schemes stemming from these recent events.

“These scams evolve over time and adjust to reflect events in the news, but they all

solicitations for donations may involve contact by telephone, social media, e-mail or in person.

Below are some of the more typical scams the IRS has seen:

Email Phishing Scams

The IRS has recently seen email schemes that target tax professionals, payroll professionals and human resources personnel in addition to individual taxpayers.

In email phishing attempts, criminals pose as a person or organization that taxpayers trust and recognize. They may hack an email account and send mass emails under another person’s name. They may pose as a bank, credit card company, tax software provider or government agency. If a person clicks on the link in these emails, it takes them to fake websites created by fraudsters to appear legitimate but contain phony login pages. These criminals hope victims will take the bait and provide money, passwords, Social Security numbers and other information that can lead to identity theft.

Scam emails and websites also can infect computers with malware without the user knowing it. The malware can give the criminal access to the device, enabling them to access sensitive files or track keyboard strokes, exposing logins and other sensitive information.

If a taxpayer receives an unsolicited email that appears to be from either the IRS or a program closely linked to the IRS, such as the Electronic Federal Tax Payment System (EFTPS), report it by sending it to phishing@irs.gov. Learn more by going to the Report Phishing and Online Scams page.

The IRS generally does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic

communication, such as text messages and social media channels. The IRS has

accounts are being assigned to one of four private-sector collection agencies. Because of this, taxpayers should be on the lookout for scammers posing as private collection firms. The IRS-authorized firms will only be calling about a tax debt the person has had – and has been aware of – for years. Taxpayers also would have been previously contacted by the IRS about their tax debt.

How to Know It's Really the IRS Calling or Knocking on Your Door

The IRS initiates most contacts through regular mail delivered by the United States Postal Service.

However, there are special circumstances in which the IRS will call or come to a home or business, such as when a taxpayer has an overdue tax bill, to secure a delinquent tax return or delinquent employment tax payment, or to tour a business as part of an audit or during criminal investigations.

Even then, taxpayers will usually first receive several letters (called "notices") from the IRS in the mail. For more information, visit "How to know it's really the IRS calling or knocking on your door" on IRS.gov.

Tax Refund Fraud — Identity Theft

Tax-related identity theft occurs when someone uses a stolen Social Security number or Individual Taxpayer Identification Number (ITIN) to file a tax return claiming a fraudulent refund.

In 2015, the IRS joined forces with representatives of the software industry, tax preparation firms, payroll and tax financial product processors and state tax administrators to combat identity-theft refund fraud and protect the nation's taxpayers. This group — the Security Summit — has held a series of public awareness campaigns directed at taxpayers called "Taxes.Security.Together." For tax

professionals, the "Protect Your Clients; Protect Yourself" and "Don't Take the Bait"

the security software is always turned on and can automatically update. Encrypt sensitive files such as tax records stored on computers and devices. Use strong passwords.

- Learn to recognize phishing emails, threatening phone calls and texts from thieves posing as legitimate organizations, such as a bank, credit card company and government agencies. Do not click on links or download attachments from unknown or suspicious emails.
- Protect personal data. Don't routinely carry Social Security cards, and make sure tax records are secure. Treat personal information like cash; don't leave it lying around.

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.