With Hurricane Harvey Comes Money and Data-Gathering Scams via Social Media, Email, Phone

Criminals often send emails that steer recipients to bogus websites that appear to be affiliated with legitimate charitable causes.

by Times Record / August 30, 2017

Shutterstock

(TNS) -- The Internal Revenue Service has issued warnings for people to avoid two new scams.

One scheme uses impersonators of the IRS and the Federal Bureau of Investigation as part of a ransomware scam to take computer data hostage.

The IRS also issued a warning about possible fake charity scams emerging due to Hurricane Harvey and encouraged taxpayers to seek out recognized charitable groups for their donations.

"While there has been an enormous wave of support across the country for the victims of Hurricane Harvey, people should be aware of criminals who look to take advantage of this generosity by impersonating charities to get money or private information from well-meaning taxpayers," an IRS news release states. "Such fraudulent schemes may involve contact by telephone, social media, email or in-person solicitations."

Criminals often send emails that steer recipients to bogus websites that appear to be affiliated with legitimate charitable causes. These sites frequently mimic the sites of, or use names similar to, legitimate charities, or claim to be affiliated with legitimate charities in order to persuade people to send money or provide personal financial information that can be used to steal identities or financial resources.

More information about tax scams and schemes may be found at IRS.gov using the keywords "scams and schemes." Details on available relief can be found on the disaster relief page on IRS.gov.

The scam that impersonates FBI or IRS personnel uses the emblems of both the IRS and the Federal Bureau of Investigation and tries to entice users to select a "here" link to download a fake FBI questionnaire. Instead, the link downloads a certain type of malware called ransomware that prevents users from accessing data stored on their device unless they pay money to the scammers.

"This is a new twist on an old scheme," IRS Commissioner John Koskinen said in a news release. "People should stay vigilant against email scams that try to impersonate the IRS and other agencies that try to lure you into clicking a link or opening an attachment. People with a tax issue won't get their first contact from the IRS with a threatening email or phone call."

The IRS, state tax agencies and tax industries — working in partnership as the Security Summit — currently are conducting an awareness campaign called Don't Take the Bait that includes warning tax professionals about the various types of phishing scams, including ransomware. Victims should not pay a ransom, the IRS states.

"Paying it further encourages the criminals, and frequently the scammers won't provide the decryption key even after a ransom is paid," the IRS news release adds.

Victims are encouraged to immediately report any ransomware attempt or attack to the FBI at the Internet Crime Complaint Center, www.IC3.gov, and forward any IRS-themed scams to phishing@irs.gov.

The IRS does not use email, text messages or social media to discuss personal tax issues, such as those involving bills or refunds. For more information, visit the "Tax Scams and Consumer Alerts" page on IRS.gov. Additional information about tax scams is available on IRS social media sites, including YouTube videos.

If you are a tax professional and registered e-Services user who disclosed any credential information, contact the e-Services Help Desk to reset your e-Services password. If you disclosed information and taxpayer data was stolen, contact your local stakeholder liaison.