IRS Warns of Phishing Scams Related to COVID-19 Stimulus Payments

The coronavirus pandemic is leading to an increase in cybersecurity attacks and scams.

Faith Ryan

Thu, 04/02/2020 - 15:24

Photo credit: designer491/iStock

The Internal Revenue Service is warning the public about emails and other potential cybersecurity attacks related to the coronavirus pandemic after seeing a surge in phishing scams looking to take advantage of taxpayers.

Observed activity include emails or calls asking individuals to verify banking information to speed up their economic impact payment or sign over their direct payment, which is expected April 17, according to the IRS. Criminals are also sending fake checks to individuals by mail enclosed with correct or incorrect recipient information, and asking recipients to call or verify their information via a scam website or phone number for payment approval.

"We urge people to take extra care during this period. The IRS isn't going to call you asking to verify or provide your financial information so you can get an economic impact payment or your refund faster," IRS Commissioner Chuck Rettig said in a press release. "That also applies to surprise emails that appear to be coming from the IRS. Remember, don't open them or click on attachments or links. Go to IRS.gov for the most up-to-date information."

With the CARES Act signed into law last Friday calling for sending up to $1,200 in stimulus payments per qualifying individual, no additional actions would be needed on the individuals' parts, according to IRS. Using 2019 or 2018 tax return information, the IRS will provide individuals with immediate, automatic payments via direct deposit. Those without direct deposit information on file will receive a check by mail or can apply for it through the IRS' secure portal that is expected to launch in mid-April.

“Seniors should be especially careful during this period,” the IRS noted, emphasizing that those who receive social security benefits and do not typically file tax returns will not be asked to provide additional information and receive automatic payments.

The World Health Organization has also warned about malicious phishing emails from senders posing as doctors and those disguised as the organization about COVID-19. Emails may include attachments that look legitimate, but deploy malware onto an individual’s device once opened or hyperlinks that direct individuals to web pages asking for sensitive information.

Other federal agencies, such as the Cybersecurity and Infrastructure Security Agency and the Department of Health and Human Services, have emphasized the need for public vigilance regarding cybersecurity during this uncertain time.

Moreover, the IRS has advised the public to stay alert to all phishing attempts from those claiming to be the agency or any of its affiliated organizations aiming to gather personal information, which includes those from social media and texting.

(Those who receive suspected phishing and online scams from the IRS or affiliated organizations can forward them to phishing@irs.gov.)

View printer friendly version
Federal Cybersecurity
cyberattacks
IRS
coronavirus
Health Human Services
Cybersecurity and Infrastructure Security Agency
Standard