THE VOICE OF PENNSYLVANIA COUNTIES SINCE 1886

Scam Warning: Fraudsters Using New Tactics to Steal Personal Data During COVID-19 Pandemic

Harrisburg, PA — Pennsylvanians should take steps to protect themselves from phishing scams that are targeting people who are expecting a stimulus payment from the federal government following the outbreak of COVID-19, the Department of Revenue and Department of Banking and Securities announced today.

“As we all work together to help prevent the spread of COVID-19, this unprecedented situation has created new opportunities for criminals to target Pennsylvanians, including those who are vulnerable or struggling,” Revenue Secretary Dan Hassell said. “We want to remind everyone that they should not provide their direct deposit or other banking information to anyone who contacts them on the phone, through email or text messages, or on social media.”

The stimulus payments, otherwise known as economic impact payments, are being distributed by the federal government as part of the federal economic stimulus legislation that was signed into law in response to the COVID-19 pandemic. According to the IRS, in most cases the payments will be directly deposited into the bank accounts that taxpayers previously listed on their federal tax returns.

However, the IRS has reported seeing a surge of scam artists perpetrating phishing schemes where they pose as government officials to trick people into turning over their banking information. Doing so may allow a criminal to steal your identity, file a fraudulent tax return in your name or use your personal data for other illicit purposes.

“If you have received an unsolicited email or phone call asking for your personal or financial information, the safest response is to delete the email or hang up the phone,” advised Acting Secretary of Banking and Securities Richard Vague. “Consumers must remain vigilant about protecting their finances, especially if they are being pressured to act quickly.”

How to Recognize the Scam

According to the IRS, some of the electronic messages associated with these phishing scams say, “In order to receive your stimulus check via direct deposit, you will need to confirm your banking information.” These messages are targeting not only individual citizens, but also tax professionals.

Pennsylvanians are encouraged to remember several warning signs from the IRS, which says scammers may:

- Emphasize the words “Stimulus Check” or “Stimulus Payment.” The official term is economic impact payment.
- Ask the taxpayer to sign over their economic impact payment check to them.
- Ask by phone, email, text or social media for verification of personal and/or banking information saying that the information is needed to receive or speed up their economic impact payment.
- Suggest that they can get a tax refund or economic impact payment faster by working on the taxpayer’s behalf. This scam could be conducted by social media or even in person.
- Mail the taxpayer a bogus check, perhaps in an odd amount, then tell the taxpayer to call a number or verify information online in order to cash it.

Tips to Avoid Scams

- **Look for imposters**: Many times, criminals will pose as a government entity or an official business. If you are targeted by a scam artist through the mail, phone or email, do not provide personal information or money until you are sure you are speaking to a legitimate representative.
- **Approach unusual attachments and links with caution:** Links to a website or attachments to an email could be infected with malware that download malicious software. Spyware can track the recipient’s keystrokes to obtain passwords, Social Security numbers, credit card numbers or other sensitive information.
- **Conduct research online**: Using information included in a potentially fraudulent notice or communication, such as email address domain name, company name, address or telephone number, conduct a search online to see if a scam has been reported by other people or government agencies.