



COVID-19

ESF-17 Cyber Risk Management

The IRS and State's Attorney's Offices are reporting significant potential for criminals to steal COVID-19 economic impact payments as well as personally identifiable information (PII) through various means of deception.¹ Phishing schemes posing as government officials designed to trick people into turning over their banking information can allow a criminal to steal your identity, file a fraudulent tax return in your name or use your personal data for other illicit purposes.

Key Facts:^{1,2}

- The Internal Revenue Service recently released guidance informing the public that most people do not need to take any action in order to receive stimulus payments.
- Government agencies are NOT sending out emails asking for personal information in order to receive funds or other pandemic relief opportunities.
- The IRS will deposit your check into the direct deposit account you previously provided on your tax return or send you a paper check as an alternative route.
- The IRS will NOT CALL and ask you to verify your payment details.

Recommendations:^{1,2}

- Any phone, text or email request for personal identifying information, or any other information as a prerequisite for receiving a stimulus payment should be strongly considered a scam.
- If you receive texts or emails claiming you can get your money faster by sending personal or banking information or clicking on links, DELETE them. Do NOT click on any links in those emails or texts.
- Do NOT give out your bank account, debit account, or PayPal account information - even if someone claims it's necessary to get your check. IT'S A SCAM!
- Scammers may also emphasize the words "stimulus check" or "stimulus payment." The official term is economic impact payment.
- There are no fees to receive payment. The government is not asking citizens to pay anything up front to receive an economic impact payment. If someone contacts you asking for any form of payment in order to receive an economic payment, please contact law enforcement.
- If you receive unexpected emails, text messages, or social media messages with attachments or website links, DELETE them. Do NOT click on, download, or open any of the above, as you may be opening malware on your electronic device that can help criminals steal your information.
- Reports are also circulating about bogus checks being distributed. If you receive a "check" in the mail now, it's a fraud. It will take the Department of Treasury a few weeks to mail the legitimate checks to taxpayers. If you receive a "check" for an odd amount (especially one with cents), a check that requires you to verify the check online or by calling a number, it's a fraud.

¹ <https://www.justice.gov/usao-wdla/pr/united-states-attorney-joseph-and-irs-warn-taxpayers-potential-scams-relation-covid-19>

² <https://www.lisbonnh.org/stimulus-check-scam/>