



### **Avoiding Fraud and Scams with COVID-19**

#### **How do I avoid fraud and scams?**

The IRS and its Criminal Investigation Division are reporting a wave of new and evolving phishing schemes (scammers who send emails with links to steal personal information that look like they come from legitimate sources) related to COVID-19. Be aware of the tactics fraudsters may deploy, such as:

- Emphasizing the words "Stimulus Check" or "Stimulus Payment." The official term the IRS is using is, "economic impact payment (or "EIP")."
- Asking you to sign over your economic impact payment check to them.
- Asking 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 your economic impact payment.

#### **Are there additional resources available to help me avoid scams?**

Here is a list of additional resources to avoid scams, fraud and identity theft:

If you receive unsolicited emails, text messages or social media attempts to gather information that appears to be from either the IRS or an organization closely linked to the IRS, such as the Electronic Federal Tax Payment System (EFTPS), the IRS is asking that you forward it to [phishing@irs.gov](mailto:phishing@irs.gov).

- Avoid Coronavirus Scams
- FTC Coronavirus (COVID-19) Pandemic: The FTC in Action
- FTC Coronavirus Scam Bingo