



COVID-19 SCAMS

Scammers are constructing schemes related to COVID-19 (coronavirus) to commit fraud.

The United States Department of Justice recommends that Americans take the following precautionary measures to protect themselves from known and emerging scams related to COVID-19:

- **Independently verify** the identity of any company, charity, or individual that contacts you regarding COVID-19.
- **Check the websites and email addresses** offering information, products, or services related to COVID-19.
- **Be wary of unsolicited emails** offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes.
- **Do not click on links or open email attachments** from unknown or unverified sources.
- **Make sure the anti-malware and anti-virus software** on your computer is operating and up to date.
- **Ignore offers for a COVID-19 vaccine, cure, or treatment.**
- **Check online reviews** of any company offering COVID-19 products or supplies.
- **Research any charities or crowdfunding sites** soliciting donations in connection with COVID-19 before giving any donation.
- **Be wary of any business, charity, or individual requesting payments** or donations in cash, by wire transfer, gift card, or through the mail.
- **Be cautious of “investment opportunities”** tied to COVID-19, especially those based on claims that a small company’s products or services can help stop the virus.

If you suspect that you are a victim of a scam or attempted fraud involving COVID-19, contact the National Center for Disaster Fraud Hotline at 866-720-5721 or via email at disaster@leo.gov, or report it to the FBI at tips.fbi.gov. If it is a cyber-scram, submit your complaint through ic3.gov/default.aspx.