



The growing anxiety from the COVID-19 pandemic is fueling Disaster Fraud. Fraudsters are using the coronavirus as an opportunity to scam consumers and financial institutions. Pay attention to these warning signals:

- E-mail and text message phishing scams, disguised as being from the Centers for Disease Control (CDC) and the World Health Organization (WHO), are being circulated throughout the world. The messages contain malicious links that download malware. The malware gives cyber-criminals access to data. These messages often times directly ask for information, such as Social Security Numbers, Tax ID Numbers, etc. **ONLY obtain information directly from the CDC website and reputable sources.**
- Fundraising Scams are being setup by fake charities that solicit donations from consumers. They claim to be involved in fighting the spread of the coronavirus.
- Scammers are targeting consumers and encouraging them to “reserve a COVID-19 vaccination over the phone.” The scammer obtains personal information from the victim, including credit card and Social Security Numbers. They claim to be from the CDC, and they are reserving vaccines for “high risk” individuals. **There are NO vaccine reserve programs.**
- Fraudsters are preying on consumers by offering an “advance” on the proposed stimulus package from the U.S. Government. The criminal(s) contact consumers and claim that, for an upfront fee, they will wire the stimulus amount to the victim within hours or days. The fraudster obtains identifying and financial information from the victim and then disappears.
- The U.S. Food and Drug Administration (FDA) and the U.S. Federal Trade Commission (FTC) have issued joint warning letters to at least seven companies for “selling fraudulent products with claims to prevent, treat, mitigate, diagnose, or cure COVID-19.” They include: The Jim Bakker Show, Herbal Amy, Inc., N-Ergetics, Vital Silver, Quinessence Aromatherapy Ltd, GuruNanda, LLC and Vivify Holistic Clinic.
- Illegal price gouging on safety, cleaning, and treatment products is increasing daily. Be aware and diligent of scammers. Be aware of phishing e-mails and **never click unknown attachments or files.**
- Criminals are targeting remote workers. Be aware of phishing e-mails and **never click unknown attachments or files.**

If you think you are a victim of a scam or attempted fraud involving COVID-19, you can report it without leaving your home.

- Contact the National Center for Disaster Fraud Hotline at 866-720-5721 or via email at [disaster@leo.gov](mailto:disaster@leo.gov) or report it to the FBI at [tips.fbi.gov](https://tips.fbi.gov). And, if it's a cyber scam, submit your complaint through <https://www.ic3.gov/default.aspx>