

COVID-19 SCAM Update

- 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 aware that scammers often employ addresses that differ only slightly from those belonging to the entities they are impersonating. For example, they might use “cdc.com” or “cdc.org” instead of “cdc.gov.”
- Be wary of unsolicited emails offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes. Legitimate health authorities will not contact the general public this way.
- Do not click on links or open email attachments from unknown or unverified sources. Doing so could download a virus onto your computer or device.
- Make sure your computer’s anti-malware and anti-virus software is operating and up to date.
- Ignore offers for a COVID-19 vaccine, cure, or treatment. Remember, if there is a medical breakthrough, you won’t hear about it for the first time through an email, online ad, or unsolicited sales pitch.
- Check online reviews of any company offering COVID-19 products or supplies. Avoid companies whose customers have complained about not receiving items.
- Research any charities or crowdfunding sites soliciting donations in connection with COVID-19 before giving. Remember, an organization may not be legitimate even if it uses words like “CDC” or “government” in its name or has reputable looking seals or logos on its materials. For online resources on donating wisely, visit the Federal Trade Commission (FTC) website.
- Be wary of any business, charity, or individual requesting payments or donations in cash, by wire transfer, gift card, or through the mail. Don’t send money through any of these channels.
- 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 decide to invest, carefully research the investment beforehand. For information on how to avoid investment fraud, visit the U.S. Securities and Exchange Commission (SEC) website.
- For the most up-to-date information on COVID-19, visit the Centers for Disease Control and Prevention (CDC) and World Health Organization (WHO) websites.

On March 23, U.S. Attorney Scott announced the appointment of a COVID-19 fraud coordinator to lead investigations into known and suspected occurrences of financial fraud related to the nation’s ongoing public health emergency.

If you think you are a victim of a scam or attempted fraud involving COVID-19, you can report it without leaving your home through a number of platforms. Contact the National Center for Disaster Fraud Hotline at 866-720-5721 or via email at disaster@leo.gov. Also report it to the FBI at tips.fbi.gov.

COVID – 19 scams to be aware of –

- **Testing scams:** Scammers selling fake at-home test kits or going door-to-door performing fake tests for money.
- **Treatment scams:** Scammers offering to sell fake cures, vaccines, and advice on unproven treatments for COVID-19.
- **Supply scams:** Scammers are creating fake shops, websites, social media accounts, and email addresses claiming to sell medical supplies currently in high demand, such as surgical masks. When consumers attempt to purchase supplies through these channels, fraudsters pocket the money and never provide the promised supplies. Deal with a reputable company. Remember, if it sounds too good to be true, it probably is; check it out first.
- **Charity scams:** Scammers are soliciting donations for individuals, groups, and areas affected by COVID-19. Only use official organizations.
- **Phishing scams:** Scammers posing as national and global health authorities, including the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC), are sending phishing emails designed to trick recipients into downloading malware or providing personal identifying and financial information.